FICHA DE CONDICIONES TÉCNICAS ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DEL BIEN (FCT)	**Fecha**	3/11/2026

1. DENOMINACIÓN DEL BIEN O SERVICIO

Contratar la operación global delegada de los servicios TIC del Instituto Colombiano de Bienestar Familiar (ICBF), con el fin de asegurar el soporte integral y la continuidad operativa de los procesos institucionales a cargo del Instituto.

ALCANCE:

La Operación Global Delegada que se pretende contratar comprende la prestación integral de los servicios asociados a la administración, gestión, operación, monitoreo, supervisión, control y soporte de la infraestructura y de los servicios tecnológicos de la Entidad, así como el suministro, instalación, configuración, puesta en funcionamiento, mantenimiento y soporte de los bienes y servicios que resulten necesarios para garantizar la continuidad y adecuada prestación de estos.

La operación deberá estar orientada a garantizar de manera permanente los principios de confidencialidad, integridad y disponibilidad de la información, así como la continuidad, estabilidad, seguridad, desempeño y confiabilidad de los servicios tecnológicos. Para tal efecto, el contratista deberá implementar los mecanismos de monitoreo, gestión, prevención, atención, escalamiento y recuperación que permitan identificar oportunamente eventos que puedan afectar la operación y adoptar las acciones necesarias para mitigar sus impactos.

2. CÓDIGO ESTÁNDAR DE PRODUCTOS Y SERVICIOS DE NACIONES UNIDAS UNSPSC UNv260801 (CCE)

#	CODIGO UNSPSC	DESCRIPCIÓN
1	81161700	Servicios de telecomunicaciones
2	81161600	Servicios de correo electrónico y mensajería
3	81161500	Servicios de administración de acceso
4	81112300	Mantenimiento y soporte de hardware de computador
5	81112200	Mantenimiento y soporte de software
6	81112000	Servicios de datos
7	81111900	Sistemas de recuperación de información
8	81111811	Servicios de soporte técnico o de mesa de ayuda

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

#	CODIGO UNSPSC	DESCRIPCIÓN
9	81111800	Servicios de sistemas y administración de componentes de sistemas
10	81111700	Sistemas de manejo de información MIS
11	81111500	Ingeniería de software o hardware
12	81101700	Ingeniería eléctrica y electrónica
13	72151200	Servicios de construcción y mantenimiento de HVAC calefacción y enfriamiento y aire acondicionado
14	72151600	Servicios de sistemas especializados de comunicación
15	72151500	Servicios de sistemas eléctricos
16	46171600	Equipos de vigilancia y detección
17	44102200	Accesorios para escáneres
18	43233600	Software de equipo eléctricos
19	43233500	Software de intercambio de información
20	43232700	Software de aplicaciones de red
21	43223300	Dispositivos y equipos para instalación de conectividad de redes y Datacom
22	43223100	Componentes y equipo de infraestructura de redes móviles y digitales
23	43222600	Equipo de servicio de red
24	43212200	Sistemas de manejo de almacenamiento de datos de computador
25	43211900	Monitores y pantallas de computador
26	43211700	Dispositivos informáticos de entrada de datos
27	43211600	Accesorios de computador
28	43202100	Accesorios de dispositivos de almacenamiento extraíbles
29	43201800	Dispositivos de almacenamiento
30	43201600	Componentes del chasis
31	43201500	Módulos o interfaces de procesadores de tablero (board) del sistema
32	39121000	Equipamiento para distribución y conversión de alimentación
33	32101600	Circuitos integrados

3. UNIDAD DE MEDIDA

Bienes y Servicios

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

4. DESCRIPCIÓN GENERAL

El ICBF en su operación hace uso de las Tecnologías de Información y las Comunicaciones para el cumplimiento de su objeto misional, el cual consiste en *"(…) Trabajar con calidad y transparencia por el desarrollo y la protección integral de la primera infancia, la niñez, la adolescencia y el bienestar de las familias colombianas (…)"* apoyada en los recursos tecnológicos dispuestos al servicio de la Entidad, para ello se cuenta con la Dirección de Tecnologías de la Información (DTI), la cual es responsable de promover el uso de las tecnologías con el fin de hacer más eficiente el cumplimiento de la misión institucional y la utilización de los recursos tecnológicos, humanos y financieros del ICBF. Esta dirección genera lineamientos y estándares técnicos y asisten a las diferentes dependencias ubicadas a Nivel Nacional (Regionales, Centros Zonales y Dependencias en asuntos de su competencia). Asimismo, la DTI orienta la gestión integral de los servicios de tecnología, definiendo normas y recomendaciones técnicas sobre los sistemas de información, infraestructura y plataformas tecnológicas, realizando el seguimiento y control de calidad de los servicios que soportan dichos sistemas, con el propósito de garantizar un funcionamiento eficiente, confiable y alineado con las necesidades institucionales.

Los servicios tecnológicos corresponden al conjunto de capacidades tecnológicas, procesos, herramientas, infraestructura, aplicaciones y recursos humanos que permiten soportar la operación institucional y satisfacer las necesidades de los usuarios en materia de tecnologías de la información y las comunicaciones. El ICBF mediante Dirección de Tecnologías de la Información ofrece los servicios de centro de cómputo, servidores, Telefonía IP, seguridad informática, almacenamiento, respaldos (backup), Office 365, directorio activo, aplicaciones, bases de datos, herramientas de gestión y monitoreo y administración de licenciamiento, redes de área local (LAN), redes inalámbricas (WLAN), conectividad, parque computacional, mesa de servicio y soporte en sitio, certificados digitales y videoconferencia, los cuales a su vez están conformados por:

- Arquitectura del servicio
- Inventario de bienes del servicio
- CI (Ítems de Configuración del Servicio)
- Configuraciones y parametrizaciones relacionados con los CI
- Personal a cargo del servicio
- Documentación (procedimientos, instructivos, formatos) del servicio o relacionados al mismo.
- Prácticas ITIL relacionados con el servicio
- Aseguramiento del Servicio

Actualmente, la Entidad cuenta con una plataforma tecnológica en operación que garantiza la disponibilidad permanente de los servicios de comunicaciones de datos, voz, videoconferencia, correo electrónico, acceso a Internet, comunicaciones unificadas, Intranet, impresión, acceso a aplicaciones, bases de datos y publicación de información en

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Internet, los cuales soportan de manera transversal la operación institucional en todas sus dependencias y para sus funcionarios.

En consideración a que estos servicios tecnológicos, administrados y ofrecidos por la Dirección de Tecnologías de la Información, son fundamentales para el adecuado desarrollo de los procesos misionales, estratégicos y administrativos del ICBF y teniendo en cuenta que la capacidad de recurso humano disponible en la Entidad no resulta suficiente para asumir de manera directa y permanente la totalidad de las actividades técnicas, operativas y especializadas requeridas para garantizar la adecuada prestación de estos servicios se hace necesario contratar el servicio de operación de la Infraestructura Tecnológica y de la Mesa de Servicios, con el fin de asegurar su continuidad, disponibilidad, calidad y niveles de servicio, de conformidad con los servicios descritos en el numeral 6 del presente documento.

Adicionalmente es indispensable contar con personal especializado para la gestión y soporte de los servicios relacionados en el *Anexo 01 - Personal mínimo requerido*, el ICBF requiere la administración, gestión, operación y monitoreo de sus diferentes plataformas tecnológicas agrupadas de la siguiente manera:

1. **Plataforma Base:** Servidores, Servicio de Gestión y Monitoreo y Respaldo, NOC (Network Operation Center).
2. **Sistemas de Información:** Aplicaciones y Base de Datos híbrida (On-Premise y Cloud).
3. **Redes de Comunicaciones:** Red LAN y Red Inalámbrica (WLAN) servicio a nivel nacional administrado de manera centralizada.
4. **Telefonía IP:** Servidores de Telefonía y periféricos.
5. **Seguridad de TI:** Seguridad Informática y de la Información, Seguridad Perimetral, Protección contra Amenazas, Antivirus, Análisis Forense, Gestión de Vulnerabilidades, SIEM , NOC Network Operations Center y SOC (Security Operación Center) para una integrada de seguridad, NOC Networ operaciones, riesgos y continuidad de TI en la plataforma tecnológica y garantizar la confidencialidad, integridad y disponibilidad de la información, evitando y dando tratamientos a distintas amenazas referentes a la seguridad.
6. **Herramientas de Productividad y Nube:** Directorio Activo, Microsoft Office 365 y Azure.
7. **Centro de Datos y Data Center:** Administración del Centro de Cómputo de la Sede de Dirección General y Data Center Externo.
8. **Mesa de Servicio:** Soporte nivel I y nivel II.
9. **Gestorías**: Lista de las gestorías de acuerdo con los servicios ITIL

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

5. NORMATIVIDAD APLICABLE (específica para el servicio y/o bien)

Sin perjuicio de la aplicación del régimen general de contratación estatal, en especial la Constitución Política, las Leyes 80 de 1993, 1150 de 2007, 1474 de 2011, el Decreto Único Reglamentario 1082 de 2015 y las demás normas que los modifiquen, adicionen o sustituyan, para la prestación del servicio objeto de la presente Ficha resultan aplicables, entre otras, las siguientes disposiciones:

- EIA/TIA 606, estándar para la administración de los sistemas de cableado estructurado.
- EIA/TIA 942, estándar para diseño e instalación de centros de datos.
- Ley 1581, protección de datos personales del Estado Colombiano.
- NTC 2050 Código Eléctrico Colombiano
- NTC 3383
- UL1778
- NTC 3445
- NTC 3654
- Decreto 1496 de 2018
- Decreto Único Reglamentario 1076 de 2015
- Decreto 287 de 2026
- Decretos, resoluciones, leyes, protocolos y demás disposiciones del orden Nacional, Departamental y municipal, emitidas por las autoridades competentes, para la ejecución de obras, transporte de materiales, insumos y personal, e ingreso a infraestructuras del ICBF.
- Las demás normas que modifiquen o complementen las anteriormente citadas.

MARCOS DE REFERENCIA

Ultima versión de los siguientes marcos de referencia:

- ISO/IEC 20000, gestión de servicios de TI.
- ISO/IEC 27001:2022, estándar para Sistemas de Gestión de Seguridad de la Información.
- ISO/IEC 27032 Directrices para la ciberseguridad.
- NIST 800-53 Security and Privacy Controls for Information Systems and Organizations.
- ISO 22301 Gestión de continuidad de negocio.
- ISO 9001, sistemas de gestión de calidad.
- ISO 31000, gestión de riesgos.
- ISO 22310, gestión de la continuidad.
- ITIL, marco de referencia para la gestión de TI.
- COBIT, marco de referencia para el Gobierno de TI.
- PMI, marco de referencia para la gestión de proyectos.
- OSSTMM, (Manual de la Metodología Abierta de Testeo de Seguridad).

- SOC 2
- Modelo de privacidad y seguridad de la información del Estado Colombiano.

6. ESPECIFICACIONES TÉCNICAS MÍNIMAS DE LOS INSUMOS, BIENES, PRODUCTOS, OBRAS O SERVICIOS A ENTREGAR

6.1 INTRODUCCIÓN

El Instituto Colombiano de Bienestar Familiar – ICBF requiere contratar un Servicio de Operación Global mediante el cual el Contratista suministre y preste los servicios definidos en la presente Ficha de Condiciones Técnicas, la cual establece las condiciones esenciales para la adecuada prestación de los servicios sobre la infraestructura tecnológica implementada en la Entidad.

Dicho servicio deberá prestarse en los sitios (sedes) definidos en el *Anexo 07 – Sedes Soporte en Sitio*, y se ejecutará con base en una Línea Base para cada uno de los servicios, conforme a lo detallado en el *Anexo 03 – Línea Base Servicios TI*. Estos anexos podrán ser ajustados durante la ejecución del contrato, de acuerdo con la dinámica de las necesidades tecnológicas e institucionales del ICBF, previo aval del Supervisor del Contrato.

El personal asignado por el Contratista será responsable de la instalación, administración, operación, monitoreo, aseguramiento y soporte integral de la plataforma tecnológica del ICBF, incluyendo tanto la infraestructura propia de la Entidad como aquella que sea arrendada o dispuesta para la prestación de los servicios objeto del contrato, en concordancia con lo establecido en el presente documento y en atención a la evolución y cambios tecnológicos.

Para el cumplimiento de las obligaciones contractuales, el Contratista deberá disponer y mantener la infraestructura operativa necesaria que garantice la adecuada atención y operación de todos los servicios contratados, incluyendo oficinas, recurso humano calificado, recursos tecnológicos, herramientas de soporte y comunicaciones, entre otros elementos requeridos para la correcta prestación del servicio.

La prestación de los servicios a contratar se realizará bajo las buenas prácticas de ITIL en operación de servicios, además de lo mencionado en el numeral 5 - Normatividad Aplicable en los marcos de referencia en su última versión. Esta prestación de servicios que involucre el suministro e instalación de equipos en la infraestructura tecnológica del ICBF debe ser con equipos totalmente nuevos, no remanufacturados, no hayan sido previamente usados, no reparados, libre de defectos e imperfectos, de última generación y/o última tecnología, con el respectivo licenciamiento, software y firmware actualizado según aplique al hardware que se aprovisione. La fecha de fabricación de los equipos que se aprovisionen con el servicio no podrá ser anterior al 02 de enero de 2025 o un (1) año antes del inicio de la etapa de operación, para lo cual se deben presentar los siguientes documentos:

certificación donde se indique la fecha de fabricación, el manifiesto de importación y la factura de compra, así como otros documentos complementarios que determine el ICBF.

Las certificaciones exigidas para el personal deberán ser expedidas por entes certificadores, tales como fabricantes de tecnología, organismos certificadores internacionales o entidades acreditadas, y deberán ser verificables y vigentes, según el rol y las funciones asignadas.

La ejecución del contrato y el cumplimiento de las actividades y obligaciones contractuales se llevarán a cabo en tres (3) diferentes etapas (Transición de entrada, Operación y Transición de salida), las cuales estarán a cargo del Contratista y se describen en el presente documento.

La estrategia para la prestación de los servicios de infraestructura y la calidad del servicio del Contratista deberá contemplar los Acuerdos de Niveles de Servicios (ANS) descritos en el *Anexo 02 - Acuerdos de Niveles de Servicio* para cada uno de los servicios indicados el cumplimiento de los ANS será verificado por el ICBF en la revisión mensual de los informes de gestión presentados para cada uno de los servicios por parte del Contratista. El no cumplimiento de los ANS generará descuentos económicos en el valor mensual del total del servicio de operación global de acuerdo con los niveles de penalidad definidos en dicho Anexo.

6.2 ALCANCE

El alcance del contrato se resume en suministrar, administrar, gestionar, operar y monitorear los servicios TIC y de datos del Instituto Colombiano de Bienestar Familiar – ICBF a nivel nacional, relacionados a continuación, que debe proveer el Contratista, de acuerdo con lo detallado en el presente documento y anexos:

1. **Plataforma Base:** Servidores, Servicio de Gestión y Monitoreo y Respaldo, NOC (Network Operation Center).
2. **Sistemas de Información:** Aplicaciones y Base de Datos híbrida (On-Premise y Cloud).
3. **Redes de Comunicaciones:** Red LAN y Red Inalámbrica (WLAN) servicio a nivel nacional administrado de manera centralizada.
4. **Telefonía IP:** Servidores de Telefonía y periféricos.
5. **Seguridad de TI:** Seguridad Informática y de la Información, Seguridad Perimetral, Protección contra Amenazas, Antivirus, Gestión de Vulnerabilidades, SIEM, SOC, Análisis Forense y Ciberinteligencia (Cyber Threat Intelligence - CTI), orientada a la recolección, análisis, correlación y difusión de inteligencia de amenazas mediante el consumo de fuentes internas y externas, gestión de indicadores de compromiso (IoC), indicadores de ataque (IoA), seguimiento de campañas, actores de amenaza y apoyo a la detección temprana y respuesta ante incidentes de seguridad.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

6. **Herramientas de Productividad y Nube:** Directorio Activo, Microsoft Office 365 y Azure.
7. **Centro de Datos y Data Center:** Administración del Centro de Cómputo de la Sede de Dirección General y Data Center Externo.
8. **Mesa de Servicio:** Soporte nivel I y nivel II.
9. **Gestorías:** Lista de las gestorías de acuerdo con los servicios ITIL

A fin de administrar, gestionar, operar y monitorear los servicios, el Contratista debe contemplar con carácter obligatorio los requerimientos establecidos por parte del ICBF en el presente documento y anexos, debe garantizar los servicios con la calidad ofertada y debe garantizar el suministro de los elementos de hardware, software y recursos que sean detallados en el mismo y/o los que sean necesarios para el desarrollo de sus actividades.

Para cada uno de los servicios TIC incluidos en el presente documento, el ICBF presenta la línea base del servicio de acuerdo con las unidades definidas para cada uno y el contratista deberá actualizar mensualmente la información correspondiente a la línea base para cada servicio con el fin de poder soportar la operación y la administración de los servicios.

El Contratista estará obligado a garantizar la confidencialidad de toda la información que le sea suministrada o a la que tenga acceso en desarrollo del contrato, comprometiéndose a que dicha información no será divulgada, total ni parcialmente, a terceros, ni utilizada para fines distintos a los estrictamente relacionados con la ejecución contractual, en el marco del Acuerdo de Confidencialidad suscrito con el Instituto Colombiano de Bienestar Familiar – ICBF.

El Acuerdo de Confidencialidad deberá ser suscrito y adjuntado de manera previa al inicio de la Etapa de Operación del contrato, y su cumplimiento será exigible durante toda la vigencia contractual y aun después de su terminación, conforme a la normativa aplicable.

De igual manera, el ICBF tendrá la potestad de realizar visitas al (Centro de Operaciones de Seguridad- SOC) y (Centro de Operaciones de Red – NOC) que se requiere para el alcance solicitado en la presente ficha de condiciones técnicas, con el fin de verificar cumplimiento de los requerimientos de servicio.

El contratista debe asignar el personal idóneo para cumplir con el alcance del servicio solicitado, definido en el ***Anexo 01 - Personal mínimo requerido***, en el que se indica la disponibilidad requerida por el ICBF.

MODELO OPERATIVO

El Operador se alineará a los procesos que posee el Instituto Colombiano de Bienestar

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Familiar en su sistema integrado de gestión y que dentro de los más relevantes se deben plasmar en el modelo operativo a ser suministrado por el contratista:

a) Procesos de transición de servicios

1. Proceso de gestión de configuración.
2. Proceso de gestión de cambios.

b) Procesos de la Operación del Servicio:

1. Gestión de Eventos
2. Gestión de Incidencias.
3. Gestión de Solicitudes.
4. Gestión de Problemas.
5. Gestión del Acceso.
6. Gestión de Capacidad
7. Gestión de Disponibilidad.
8. Gestión de Conocimiento.
9. Gestión de Cambios
10 . Gestión de Ciberinteligencia (Analista SOC N3)

c) Funciones de la Fase de Operación del Servicio:

1. Mesa de Servicios TIC
2. Casos escalados desde Nivel 1 y Nivel 2(mesa de servicios TIC)
3. Gestión Técnica.
4. Gestión de Aplicaciones y Bases de Datos.
5. Integración de Servicios TI
5. Gestión de Operaciones de TI.
6. Gestión de Seguridad informática.

El contratista presentará en el Modelo Operativo para cada proceso y función: Objetivo dentro de Operación, diagrama de flujo, listado de actividades diarias, actividades semanales y actividades mensuales con su correspondiente matriz RACI, productos, indicadores de seguimiento y control, listado de actividades de aseguramiento de calidad y riesgos, incluyendo aquellas asociadas a la gestión, integración y disposición de la información y los datos que soportan la operación de los servicios TIC y de los sistemas de información institucionales. La matriz RACI debe indicar, como mínimo, el recurso humano asignado (Rol, Nombre, Identificación, Correo Electrónico, Celular de Contacto). En el mismo modelo operativo el Operador definirá los recursos que estarán en Sitio en las instalaciones del contratista o a Demanda, para lo cual el ICBF dispondrá de puestos de trabajo en la sede Metrópolis y Dirección General del ICBF hasta quince (15) profesionales.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

En estos profesionales se incluyen los de carácter obligatorio o requeridos en la etapa transición de entrada.

El Operador deberá presentar en el Informe de actividades mensuales del contrato soportes de cumplimiento del modelo operativo, de actividades diarias, semanales y mensuales, incluyendo aquellas relacionadas con la gestión y disposición de la información que soporta la operación de los servicios TIC y sistemas de información institucionales. Para los procesos que presentan un nivel de madurez alto tales como gestión de cambios, gestión de problemas, gestión de incidentes, solicitudes, gestión de la configuración, gestión de capacidad y gestión de la disponibilidad, el operador deberá ejercer la administración de estos y presentar de manera semanal y mensual el consolidado de oportunidades de mejora y ajustes al ICBF y a la supervisión. Si dentro de las oportunidades de mejora el operador identifica faltantes en los formatos de registro de información o nuevos formatos que puedan ser incorporados en la Operación, deben presentarse de su parte las posibles opciones conforme a las mejores prácticas de la industria de TI para que sean aprobadas por el ICBF, incluyendo aquellos asociados a la gestión y calidad de la información utilizada en la operación.

6.3 UBICACIÓN GEOGRÁFICA PARA LA PRESTACIÓN DE LOS SERVICIOS

Durante la vigencia del contrato, los servicios se prestarán en la Sede de la Dirección General, Centro de Cómputo, las Sedes Regionales (ubicadas en las ciudades capitales de cada departamento), sedes zonales y el lugar donde esté ubicado el Datacenter Externo y/o principal, de acuerdo con el alcance de los servicios descritos en este documento.

El Contratista deberá garantizar en las instalaciones de la entidad a nivel nacional la presencia física de los agentes de soporte en sitio y cuando la operación lo requiera de los especialistas encargados de los servicios objeto de este contrato, ya sea en las instalaciones de la Sede de la Dirección General o en los Datacenter de la Entidad.

Nota: En caso de que las sedes o sedes anexas se trasladen o cambien sus ubicaciones físicas, el Contratista deberá continuar prestando los servicios de operación TI en las nuevas ubicaciones informadas por el ICBF. Para aquellos lugares diferentes a Bogotá y sus alrededores el servicio podrá ser prestado de forma remota, previa aprobación de la supervisión del contrato.

El contratista deberá garantizar la prestación de servicios y disponer el personal en sitio para soportar la infraestructura tecnológica crítica, según lo requiera la entidad, garantizando continuidad en el servicio.

6.4 HORARIOS DE SOPORTE Y ATENCIÓN

- La disponibilidad del soporte en infraestructura tecnológica crítica debe ser de 7x24x365 sin interrupción, con tiempo de respuesta definida en ***Anexo 02 - Acuerdos de Niveles de Servicio*.**

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- El horario de atención de mesa de servicio será de 7:00 am a 7:00 pm de lunes a viernes, para recibir, registrar y hacer seguimiento sobre todas las solicitudes a nivel nacional, solucionando de igual manera aquellas que le competen de acuerdo con su nivel de atención de manera telefónica, correo electrónico, chat, redes sociales o por acceso remoto y los sábados de 8:00 a.m. a 3:00 p.m. con (2) agentes para la atención de manera remota.
- El horario de los agentes de soporte en sitio será de 8:00 am a 5:00 pm de lunes a viernes y/o de acuerdo con la necesidad de la sede donde se encuentre ubicado para recibir, registrar y hacer seguimiento sobre todas las solicitudes a nivel nacional, solucionando de igual manera aquellas que le competen de acuerdo con su nivel de atención de manera telefónica, correo electrónico, chat, redes sociales o por acceso remoto.
- EL CONTRATISTA deberá manejar Disponibilidad de al menos (2) agentes 7 x 24 recibir, atender y solucionar todas las solicitudes por demanda a nivel nacional, adicional de manera presencial, se debe tener (1) agente con horario de 1:00 p.m. a 9:00 p.m. para brindar soporte de la Sede de la Dirección General.
- Cabe anotar que los horarios de atención descritos anteriormente; están sujetos a cambio por ICBF cuando estos se consideren, previo acuerdo sobre la operación

Nota: Los horarios de atención descritos anteriormente; están sujetos a cambio por el ICBF cuando estos se consideren, llegando a un mutuo acuerdo sobre la operación.

6.5 ENTREGABLES

La relación de entregables por servicio y fases del proyecto se encuentran en el ***Anexo 05 – Entregables*** para los cuales el ICBF establecerá los criterios de aceptación detallados y formatos aplicables al inicio de ejecución del contrato durante la etapa de transición de entrada.

Elaborar, documentar e implementar (previa aprobación del ICBF) planes de trabajo, planes de mejora, mantenimiento, y de proyectos para todos los servicios objeto del presente proceso.

El contratista deberá presentar un PLAN DE PROYECTO GLOBAL de acuerdo con las mejores prácticas del Project Management Institute (PMI), que permita conocer la ejecución de trabajos, actualizar las estrategias, realizar control sobre los entregables, servicios y procesos, así como planes para la implementación. Este debe ser entregado por primera vez a los veinte (20) días contados a partir de la fecha de inicio de ejecución del contrato y de manera mensual la actualización a los planes y estado de avance de estos durante toda la vigencia del contrato. Debe contener como mínimo:

- **Plan de Transición de Entrada:** Corresponde al Plan detallado de actividades requeridas para recibir los servicios y gestorías por parte del proveedor saliente o del

ICBF y realizar las instalaciones y configuraciones necesarias para garantizar la continuidad en la operación de todos los servicios objeto del contrato, este plan debe presentar dentro de los cinco (5) días hábiles contados a partir de la legalización del contrato.

- **Plan de Dirección de proyecto:** Debe corresponder a un consolidado de los hitos de los planes de trabajo, mejora y mantenimiento de cada servicio y gestoría, junto con el cronograma y plan de control de las actividades, tiempos, responsables, ruta crítica y paquetes de trabajo.

- **Plan de identificación y gestión de riesgos del proyecto:** Debe incluir la evaluación de riesgos de la operación, identificación de disparadores de riesgos, sus correspondientes planes de mitigación, remediación y planes de contingencia a los riesgos. Su seguimiento se realizará en la mesa técnica de gestión de riesgos con presentación en el comité operativo y evaluación en el ejecutivo.

- **Plan de calidad del proyecto:** Debe incluir la definición clara, precisa y concertada de los procesos de aseguramiento y control de calidad de los diferentes entregables, así como los criterios de aceptación de cada entregable (Servicio, producto o documento). De igual forma la definición de pruebas, procedimientos de aceptación y proceso de cierre del proyecto. En este plan se definen los criterios mínimos bajo los cuales el supervisor dará por aceptados los resultados del proyecto.

- **Plan de comunicaciones del proyecto:** Debe incluir canales, mecanismos y herramientas de comunicación con los diferentes Stakeholders. (Formatos de reportes, formatos de documentos, matriz de comunicaciones, agenda de reuniones, periodicidad de los informes, reuniones, reportes de avance). Este plan debe ser actualizado y divulgado a todos los Stakeholders.

- **Informe General de estado:** En el ***Anexo 05 Entregables***, se presenta de manera general los entregables mínimos que deben hacer parte del Informe general de estado, así como los reportes de operación mínimos, periódicos y no periódicos, que serán responsabilidad del Contratista**.** El Contratista deberá generar los reportes que requiera el ICBF basados en las herramientas usadas por el Contratista, adecuando la personalización y parametrización de estos de común acuerdo entre el ICBF y el Contratista.

- **Plan de gobierno del proyecto:** Definición de roles y responsabilidades del equipo del proyecto, fechas de entrada y salida de los integrantes del equipo, matriz de escalamientos y matriz de trazabilidad de las novedades presentadas durante la vigencia del contrato. El contratista debe mantener actualizada una matriz de perfiles con los recursos humanos asignados y los enlaces de las evidencias y soportes de la formación, experiencia y certificados específicos solicitados en el ***Anexo 01 - Personal***

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

mínimo requerido, además de los soportes de vinculación de personal, tales como: Acuerdos de confidencialidad, evidencias de capacitación, evidencias de empalme, aprobación de perfiles y gestión de accesos activos TIC. El plan debe incluir los diferentes órganos del proyecto establecidos en el presente documento, incluido el comité de control de cambios del proyecto (este comité es diferente al comité de cambios del servicio u operación definido de acuerdo con ITIL.)

Plan de mejoramiento continuo sobre los servicios: El Contratista deberá establecer e implementar un proceso de mejoramiento continuo para este proyecto. Para ello, deberá elaborar trimestralmente planes de mejoramiento por cada servicio y gestión, realizar seguimiento mensual a las acciones propuestas y verificar su efectividad e impacto.

Dicho plan deberá incluir:

- Las acciones de mejora a implementar.
- Las diferencias o brechas identificadas.
- El estado de avance de las acciones.
- Los obstáculos (stoppers) encontrados y las soluciones aplicadas para resolverlos.

De esta manera, se garantizará el control periódico y la mejora constante de los servicios

Estrategia de Modelo de servicio: El modelo de servicio deberá incluir la estrategia, protocolos y responsables de brindar atención a los incidentes, requerimientos, solicitudes y problemas asociados a la prestación del servicio de manera articulada con el modelo de servicio del ICBF. De igual manera, la estrategia y protocolo de atención de las quejas, reclamos o sugerencias sobre el servicio prestado, así como obtener la percepción de los usuarios, a través de encuestas, estudios, estadísticas o cualquier otro esquema que permita evaluar el nivel de satisfacción sobre el proyecto.

Plan de Transferencia de Conocimiento: El contratista deberá establecer un plan de transferencia de conocimiento hacia los colaboradores de la Dirección de Tecnologías de la Información del ICBF que incluya como mínimo una (1) sesión mensual de transferencia de conocimiento, con material de entrenamiento técnico y evaluación del conocimiento adquirido; con el propósito de potenciar el conocimiento de los colaboradores técnicos del ICBF en la configuración, instalación, administración, aseguramiento y mantenimiento de la plataforma tecnológica del ICBF.

Plan de gestión documental del proyecto: El contratista deberá establecer un plan de gestión documental del proyecto con las actividades administrativas y técnicas necesarias

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

para la planificación, manejo, etiquetado y organización jerárquica de la documentación producida en el marco del contrato, así como las condiciones de custodia y almacenamiento.

Reporte de avance del proyecto: El contratista deberá presentar mensualmente el informe ejecutivo del proyecto conforme a los formatos establecidos por la entidad en la Guía de Gestión de Proyectos e Iniciativas de TI del ICBF y descrito en el Formato Matriz de Seguimiento a Proyectos de la DTI v2 F1.G19.GTI.

Plan de transición de salida: Corresponde al plan de actividades detallado que debe elaborar el contratista para la entrega del conocimiento y estado del proyecto al ICBF o a quien este designe junto con la documentación de informes, procedimientos, instructivos, guías y manuales.

6.6.1 CONSIDERACIONES DEL LICENCIAMIENTO

- Todo hardware y software suministrado por el Contratista debe estar debidamente licenciado, con los certificados expedidos por el fabricante, es de obligación del Contratista presentar los soportes de las renovaciones y/o adquisiciones realizadas durante la ejecución del contrato incluyendo posibles prorrogas, teniendo en cuenta la legislación vigente en materia de derechos de autor.
- El ICBF proveerá el licenciamiento de Software Base para todos los servicios, aplicaciones y máquinas de escritorio y servidores de su plataforma tecnológica y continuará proveyéndolo durante la ejecución del contrato. En caso de que algún licenciamiento dejase se utilizarse por algún motivo, el Contratista deberá estar en la capacidad de utilizar el nuevo licenciamiento que sea provisto por la Entidad.
- El licenciamiento dispuesto por parte del Contratista para la ejecución del contrato debe permitir el acceso a las herramientas cuando el ICBF lo requiera y para los colaboradores que el ICBF solicite.
- El ICBF cuenta con un contrato vigente el cual suministra los servicios de mesa de servicio y soporte en sitio. Dentro de dicho contrato el proveedor dispone el servicio de herramienta de Gestión HelpPeople, a través de la cual se gestionan los tickets de incidentes, requerimientos y controles de cambios y soporta la base de conocimiento y el catálogo de servicio.
- El ICBF entregará al contratista la documentación, manuales, guías, cartillas, formatos y demás elementos que considere pertinentes para la ejecución del contrato y con los que cuente la Entidad.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

6.5.2 MEJORES PRÁCTICAS DE ITIL

El ICBF requiere que el Contratista adopte las mejores prácticas de ITIL V4, para la gestión del servicio y acompañe al Instituto en los procesos de implementación, actualización y sensibilización de las gestiones durante todas las etapas del contrato. Así mismo, deberá elaborar, actualizar, ajustar, adoptar e implementar los procesos de gestión necesarios para la entrega y soporte de los servicios, previa aprobación por parte del ICBF.

El Contratista durante todo el tiempo de ejecución del contrato deberá asignar un (1) responsable Coordinador de Calidad ITIL, así como asignar un (1) responsable que asuma el rol ITIL para cada gestoría cuyo perfil deberá corresponder a lo establecido en el ***Anexo 01 - Personal mínimo requerido.***

Cada gestor a su vez tendrá la responsabilidad de la gestión de su respectivo servicio durante todo su ciclo de vida: desarrollo, implementación, mantenimiento, monitorización y evaluación.

6.6 SERVICIO DE GESTIÓN DEL PROYECTO

El servicio de gestión de proyecto incluye los siguientes profesionales los cuales realizarán las labores de gerencia administrativa, financiera, jurídica y técnica de todo el proyecto de Servicio de Operación Global y la gestión transversal de los servicios en el marco del contrato, aplicando las mejores prácticas del PMI e ITIL:

1. Gerente del proyecto
2. Líder de Integración de Servicios
3. Coordinador de Operaciones
4. Coordinador de Mesa de servicio TI
5. Coordinador de Soporte en Sitio
6. Coordinador de Calidad
7. Gestor de Calidad
8. Gestor de Cambios
9. Gestor de Capacidad
10. Gestor de la Disponibilidad
11. Gestor de Incidentes
12. Gestor de Requerimientos
13. Gestor de Niveles de Servicio
14. Gestor de Riesgos
15. Gestor de Continuidad
16. Gestor de Problemas
17. Gestor de Seguridad de TI
18. Gestor Documental
19. Gestor de inventarios, CMDB y garantías.
20. Administrador de Centro de Cómputo

21. Administrador de Aplicaciones
22. Analista de Aplicaciones
23. Administrador de Portales y Aplicaciones Web
24. Analista de Portales y Aplicaciones Web
25. Administrador de Bases de Datos Oracle, MySQL y MariaDB
26. Administrador de Bases de Datos SQL Server
27. Administrador de Datos: Big Data-Analítica
28. Analista de Bases de Datos SQL Server
29. Administrador SystemCenter y Herramientas de Gestión y monitoreo, Intune y Azure ARC
30. Administrador de la herramienta ITSM y Power BI
31. Administrador Senior Microsoft 365
32. Administrador Microsoft 365-AD
33. Analista Senior Microsoft 365 - AD
34. Administrador de Redes
35. Especialista de Respaldos
36. Oficial de Seguridad de la Información (CISO)
37. Especialista de Seguridad Informática
38. Administrador de Antivirus
39. Líder Operación SOC
40. Operador SOC N1
41. Analista SOC N2
42. Analista SOC N3
43. Especialista Kubernetes Cloud y On-premise
44. Analista y/o Operador NOC
45. Especialista en Observabilidad y AIOps (Administrador de la plataforma NOC-NG)
46. Administrador de Plataforma de Servidores Windows
47. Administrador de Plataforma de Servidores Linux
48. Analista de Servidores
49. Analista de Servidores de Plataforma Telefonía IP
50. Agente Mesa de Servicio
51. Agente de Soporte en Sitio.
52. Gestor de Portafolio y Catálogo de Servicios y Conocimiento
53. Técnico Electricista
54. Especialista en Api Management
55. Especialista en Automation platform
56. Administrador Senior Power Platform

Para el servicio de gestión del proyecto, el futuro contratista deberá discriminar en el acta de inicio los costos mensuales de los recursos humanos anteriormente mencionados.

El Contratista deberá disponer como mínimo del personal exigido en el ***Anexo 01 - Personal mínimo requerido*** *para* la ejecución del contrato y que cumplan con la

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

experiencia y requisitos exigidos en este aparte, de igual manera dar cabal cumplimiento a las obligaciones establecidas en el numeral 7 de la presente ficha de condiciones técnicas.

El contratista debe presentar, dentro de los primeros 3 días hábiles a partir de la firma del acta de inicio del contrato, el organigrama y las hojas de vida del personal mínimo obligatorio, previa a su vinculación, conforme a la ***Anexo 01 - Personal mínimo requerido*"**. Este personal mínimo obligatorio, deberá incluir los soportes y certificaciones de vinculación al contrato, cumpliendo con los requisitos de formación y experiencia mínimo obligatorio y debe soportar la infraestructura tecnológica crítica con:

-1 Líder de servicio de Redes.
-1 Líder de Centro de cómputo.
-1 Líder de Seguridad Informática.
-1 Gerente de Proyectos.
-1 Líder de Integración de Servicios
-1 Coordinador de soporte en sitio.
-1 Coordinador de operaciones.
-1 Coordinador de Calidad

El contratista debe presentar, dentro de los primeros 10 días hábiles contada a partir de la firma del acta de inicio del contrato, el organigrama y las hojas de vida del personal adicional que conformará el equipo de operación TIC. Es necesario que cada perfil se relacione directamente con las funciones a desempeñar. El organigrama deberá estar alineado con el modelo de operación por servicio y los roles establecidos en el ***Anexo 01 - Personal mínimo requerido***". El ICBF revisará las hojas de vida y aprobará al personal si su perfil cumple con las condiciones e idoneidad, previo a su vinculación.

El contratista deberá disponer de todo el personal administrativo y de apoyo necesario para el desarrollo del contrato en general, y del personal técnico en las diferentes áreas de la Operación, garantizando el cumplimiento, sin que el ICBF incurra en costos adicionales.

Los certificados de experiencia que se anexen a las hojas de vida deben ser emitidos por las empresas en los cuales el personal prestó sus servicios profesionales, en caso de auto certificación se debe presentar copia del contrato de trabajo, los que serán revisados junto con las hojas de vida por la supervisión del ICBF, sin embargo se aclara que la totalidad de hojas de vida estarán sujetas a previa aprobación por parte del ICBF o de la supervisión de la entidad, esto acorde a lo contenido en el ***Anexo 01 - Personal mínimo requerido*** para los roles de obligatorio cumplimiento del perfil.

El ICBF, se reserva el derecho de pedir el cambio del personal, cuando advierta que el desarrollo de sus labores no es satisfactorio o cuando sus condiciones académicas y de experiencia no se ajusten a los requerimientos de su labor o que incluya falta de respeto hacia el personal del ICBF y/o los usuarios / ciudadanos. Este derecho, debe ser atendido

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

por el contratista en un término máximo de 20 días hábiles, a partir de la solicitud formal del ICBF.

6.7 GOBERNABILIDAD

La estructura organizacional del ICBF se encuentra detallada en el siguiente enlace: https://www.icbf.gov.co/estructura-organica-icbf

Este organigrama servirá de guía para entender la estructura organizacional y dinámica del ICBF que debe ser tenida en cuenta para el dimensionamiento que se exponga en el presente capítulo y para la efectiva gestión de todos los servicios.

6.7.1 ORGANIZACIÓN DEL PROYECTO

A continuación, se mencionan los “Stakeholders” relacionados para el presente proyecto:

ICBF: Instituto Colombiano de Bienestar Familiar: Es el contratante de servicios de infraestructura, valor agregado y conexo bajo la modalidad de Servicio de Operación Global.

EL CONTRATISTA: Es el responsable de la ejecución del contrato de acuerdo con los documentos que lo soportan. Así mismo, el Contratista debe cumplir con los criterios de ANS establecidos de tal forma que proporcione un excelente servicio para los usuarios del ICBF, debe garantizar la instalación, administración, operación, monitoreo, mantenimiento y soporte de toda la plataforma tecnológica del ICBF, dentro del alcance del contrato, tanto propia como arrendada.

ASEGURAMIENTO DE CALIDAD: Es el responsable de la definición y aplicación de métodos de verificación y control de calidad de los servicios contratados a través de la verificación, realización y control de mediciones y la realización de estudios de apreciación, percepción y valoración del servicio por parte de los usuarios del ICBF.

6.7.2 COMITÉS Y OTROS ÓRGANOS DEL PROYECTO

El ICBF requiere que se conformen comités en los cuales se realiza seguimiento sobre la evolución y resultado del proyecto, entre ellos se encuentran:

- Comité Ejecutivo
- Comité Operativo
- Comité de revisión de los ANS
- Comité de revisión de la Línea Base de cada uno de los servicios
- Mesas de trabajo por líneas de servicio y gestoría ITIL
- Comité de control de cambios del proyecto
- Comité de control de cambios en la operación

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Los integrantes de los comités se definirán en la etapa de transición de entrada.

A las reuniones de trabajo es posible que se inviten a participar a colaboradores del ICBF o del Contratista cuando las condiciones así lo requieran, en estos casos, la participación de dichas personas será convocada a través del Gerente del Proyecto ICBF o por la persona a quien él designe para ello.

Comité Ejecutivo: Mensualmente o de acuerdo con la necesidad del ICBF, se reunirán los representantes gerenciales del ICBF y del contratista, para hacer seguimiento en temas administrativos y financieros; como también para revisar los escalamientos del comité operativo. Estará conformado por el Supervisor del contrato, el Gerente del Proyecto del ICBF y el Gerente del Contratista.

Comité Operativo: Mensualmente y según la necesidad el ICBF o cuando se considere conveniente, se realizará el seguimiento a la prestación del servicio, ajustes a los ANS y Línea Base de servicios, así como las tareas, planes y proyectos acordados entre ambas partes. También será el espacio para tratar aspectos especiales que no se hayan resuelto en las Mesas de trabajo de cada servicio. A este comité asistirá el líder del servicio por parte del ICBF, el coordinador de operaciones, el coordinador de Calidad ITIL y el gerente del proyecto por parte del Contratista, en caso de ser requerido se convocarán otros miembros de cada equipo de trabajo.

Comité de revisión de los ANS: Este comité se realizará de manera trimestral con el propósito de revisar el estado de efectividad de los ANS y establecer directrices de mejora. Este comité estará integrado por los gerentes del proyecto, los gestores de ANS y líderes de servicio del ICBF y del Contratista.

Comité de Revisión de la línea Base de cada uno de los servicios: En este comité se revisa el comportamiento de la Línea Base de los servicios. En todo caso la revisión y actualización de la Línea Base de los servicios se realiza de manera mensual por cada servicio con lo descrito en el presente documento.

Mesas de trabajo por Líneas de servicio y gestoria ITIL: Estas mesas están conformadas por el líder del servicio y gestorías tanto del ICBF como los especialistas de cada servicio y gestoría del Contratista cuyos perfiles están definidos en cada uno de los servicios TIC. Deben estar en continua comunicación con el objeto de mantener el control del funcionamiento de cada servicio, para ello se reunirán mínimo dos (2) veces por mes o de acuerdo con la necesidad del ICBF, con el objeto de validar el informe de gestión mensual presentado por el Contratista, hacer seguimiento a las actividades de los planes de mejora, de trabajo y de mantenimiento, así como satisfacer las necesidades del ICBF referentes a cada uno de los servicios. A las mismas deberán asistir los miembros del equipo de trabajo del Contratista, requeridos según el tema a tratar en cada una de ellas,

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

los coordinadores del equipo de trabajo del Contratista deberán asistir a las mesas de acuerdo con su responsabilidad en cada tema. La citación a dichas mesas será realizada por el líder de servicio del ICBF en el momento requerido. El Gerente de Proyecto del ICBF debe asegurar que las citaciones y realización de las mesas de trabajo se relacionen en los Informes de Gestión entregados mensualmente por el Contratista. De estas reuniones debe surgir un entregable que contenga los acuerdos alcanzados, los avances realizados, las actividades programadas con sus fechas de entrega, responsables y recursos los cuales deberán verse reflejados en el informe de gestión mensual y reportado a los gerentes del ICBF y del Contratista.

Comité de Control de Cambios del proyecto: Este Comité de control de cambios se realiza de acuerdo con lo establecido por el ICBF, el calendario se establece de manera semanal y dando cumplimiento al procedimiento de control de cambios, este tendrá un informe mensual durante la operación del contrato. Está conformado por el Supervisor del Contrato o a quien este delegue, el Gerente de Proyecto por parte del ICBF y del contratista. Resultados de este comité es el acta de aprobación de cambios del proyecto.

Comité de Control de Cambios en la operación: Este Comité debe realizarse de acuerdo con una programación definida previamente mínimo dos (2) veces a la semana para evaluar los cambios proyectados de alto y mediano impacto y cambios de emergencia. Está conformado por la Dirección de tecnologías de la Información, por los profesionales lideres y los gestores de cambio del ICBF y del Contratista. Resultado de este comité es el acta de aprobación de cambios la cual debe ser socializada por el respectivo Gestor de Cambios. Dentro de sus funciones está la de difundir y verificar la adecuada planeación de los cambios a ejecutar, asegurar la firma de las actas de comités de cambios, presentar las solicitudes de cambios postuladas para el comité, exponer al Comité por parte de los Gestores de Cambios de la DIT y Operador TI, la descripción de los RFC, tiempos de ejecución y fecha propuesta de ejecución y la aprobación por parte de los integrantes del Comité de Cambios de los RFC postuladas.

6.7.3 EQUIPO DE TRABAJO DEL ICBF

Es el equipo del ICBF conformado por el Grupo de Verificación y Control, la Gerencia del proyecto, el Grupo de Medición y Seguimiento y los Ingenieros asignados a cada servicio y gestoría, encargados del seguimiento técnico, contractual, financiero, jurídico y administrativo los cuales participan en la ejecución del proyecto y realizarán las siguientes actividades, entre otras:

- Discutir, revisar y aprobar los planes de contingencia propuestos por El Contratista que garanticen la continuidad en los servicios, según las necesidades y prioridades definidas por el ICBF.
- Discutir, revisar y aprobar los planes de mejoramiento, planes de ac

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- ción, planes de proyecto, planes de trabajo y planes de mantenimiento propuestos por el Contratista que garanticen la prestación con calidad de los servicios, según las necesidades y prioridades definidas por el ICBF.
- Verificar el cumplimiento de los aspectos contractuales y otros acuerdos pactados con el Contratista.
- Coordinar y facilitar las actividades por parte del ICBF necesarias para la prestación del servicio por parte del Contratista.
- Informar y divulgar el alcance de los servicios prestados por el Contratista al interior del ICBF.
- Detectar oportunamente las necesidades de las diferentes áreas del ICBF, relacionadas con la prestación de los servicios y realizar propuestas que permitan el cubrimiento a estas necesidades por parte del Contratista.
- Mantener informado al Gerente del proyecto designado por el ICBF los aspectos relacionados con la prestación del servicio y entregar los informes y registros de actividades solicitados.
- Informar oportunamente al Supervisor del contrato, sobre eventos que afecten la correcta ejecución del contrato como son: incumplimientos, anomalías, inconformidades o deficiencias presentadas por el Contratista en la prestación del servicio y obligaciones contractuales.
- Coordinar actividades enfocadas a fortalecer valores tales como confiabilidad e integridad, entre los entes involucrados en el contrato.
- Realizar seguimiento y verificación del servicio prestado por el Contratista y la idoneidad del recurso humano asignado por el contratista a cada servicio o gestoría con el fin de asegurar la calidad de este. Podrán realizarse visitas esporádicas a cualquier sede que este atendida por el Contratista.
- Verificar y aprobar oportunamente informes entregados por el Contratista, actividades que deben realizarse en los tiempos estipulados para el adecuado cumplimiento de las obligaciones del Contratista.
- Verificar el cumplimiento de los ANS y establecer las penalizaciones y excepciones a que haya lugar.
- Verificar la liquidación de los servicios para la facturación que presenta el Contratista. Constancia de esta verificación debe quedar registrada con la firma de los informes mensuales.
- Realizar el seguimiento financiero a la ejecución del contrato.
- Gestionar y tramitar los pagos correspondientes.
- Proyectar comunicados oficiales dirigidos al Contratista.
- Realizar los informes de supervisión del contrato.
- Gestionar incumplimientos asociados al contrato cuando a ello hubiere lugar.

6.8 ETAPAS DEL CONTRATO

La ejecución de este contrato se desarrollará en tres (3) etapas. Las cuales se detallan a continuación:

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012



6.8.1 ETAPA DE TRANSICIÓN DE ENTRADA

Alcance: El operador entrante realiza la recepción de los servicios TIC del proveedor actual y/o del ICBF.

Duración de la etapa: La cual debe ejecutarse desde legalización y formalización del contrato hasta el inicio de la etapa de operación, la cual tendrá una duración de 15 días calendario y debe cumplir con las siguientes actividades:

Descripción de la etapa: En esta etapa el Contratista debe **planear, elaborar y ejecutar el Plan de Transición de Entrada** para recibir los servicios por parte del proveedor saliente o del ICBF. Durante esta etapa se realiza por parte del proveedor entrante la **planeación y diseño** de la recepción de la información de aplicaciones de negocio, sistemas de gestión, estado actual de los servicios, protocolos, credenciales y políticas de operación TIC, asimismo realizará la ejecución de la recepción y establecerá el piloto de la operación en la infraestructura TI. El Plan de Transición de Entrada deberá estar alineado con el plan de transición de salida del operador saliente. Se aclara que durante esta etapa de transición el ICBF contará con dos operadores en paralelo, los cuales desarrollarán las siguientes actividades que no implican traslapo de obligaciones y por ende el concepto de pago por los servicios prestados por cada uno de ellos serán diferentes:

a. Operador Actual (saliente): Encargado de garantizar la operación TIC del ICBF y entregar el servicio al operador entrante.
b. Operador Entrante (nuevo): Encargado de planear y ejecutar la transición recibiendo los servicios para operar tecnológicamente, según modelo operativo.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

A partir de la firma de la suscripción del contrato, la entidad requiere el organigrama y las hojas de vida del personal mínimo obligatorio, previa a su vinculación, conforme a la *Anexo 01 - Personal mínimo requerido*". Este personal mínimo obligatorio, deberá incluir los soportes y certificaciones de vinculación al contrato, cumpliendo con los requisitos de formación y experiencia mínimo obligatorio y debe soportar la infraestructura tecnológica crítica con:

- Un (1) Líder de servicio de Redes.
- Un (1) Líder de Centro de cómputo.
- Un (1) Líder de Seguridad Informática.
- Un (1) Gerente de Proyectos.
- Un (1) Líder de Integración de Servicios
- Un (1) Coordinador de soporte en sitio.
- Un (1) Coordinador de operaciones.
- un (1) Coordinador de Calidad.

Responsabilidades del Operador Entrante: Tiene la responsabilidad de realizar el recibo de los servicios y gestorías TIC, y prepararse para toda la operación de estos una vez se finalice el contrato con el operador saliente.

El operador entrante debe:

- Conocer las instalaciones e infraestructura solicitar inventario de equipos activos de RED (fw, waf, antispam, switches, router, siem y todo equipo implementado en la solución del contrato anterior con su parametrización de ANS.
- Verificar la línea base de software y la respectiva documentación técnica.
- Planear la recepción de los servicios y definir un cronograma detallado para una estabilización en máximo 30 días calendario ..
- Elaborar y ejecutar el Plan de Transición de Entrada.
- Entender y apropiar el Plan de Transición de Salida del proveedor saliente con su respectiva acta de entrega firmadas y aceptadas por cliente.

- Acoplarse a los procedimientos que ya se encuentren aplicados.
- Recibir la documentación técnica asociada a cada línea de servicio, que hace parte del plan de transición de salida del proveedor saliente.

Nota aclaratoria:
- En esta etapa no se penalizan ANS.
- En tanto el servicio se encuentre en etapa de transición de entrada para el operador entrante, no será objeto de pago alguno hasta tanto no se inicie la etapa de operación.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Utilización de Insumos y Guías Documentales de Proyectos Anteriores: El ICBF, de manera meramente potestativa y de acuerdo con su disponibilidad, podrá facilitar al Contratista manuales, guías, cartillas, formatos o caracterizaciones documentales previas provenientes de un proyecto anterior, exclusivamente como material de referencia o apoyo.

El suministro de estos insumos históricos no constituye una obligación de la Entidad, no compromete su responsabilidad legal ni contractual, y su uso por parte del Contratista será estrictamente voluntario, opcional y bajo su propio riesgo. En consecuencia, el Contratista no podrá alegar imposición en el uso de dicha información, ni argumentar que fue constreñido a su aplicación, manteniendo en todo momento su plena autonomía técnica para el diseño y estructuración de sus entregables. El empleo o adaptación de estas guías base de proyectos anteriores en ningún caso exime al Contratista de su responsabilidad por la calidad de los productos, ni podrá alterar, modificar, sustituir o afectar la estructura, codificación, jerarquía o clasificación documental oficial establecida en el Listado Maestro de Documentos (LMD) y las Tablas de Retención Documental (TRD) vigentes en el Instituto

6.8.2 ETAPA DE OPERACIÓN

Alcance: El operador entrante (a partir de ahora Contratista) realizará la operación de los servicios y gestorías TIC descritos en los numerales 6.9 y 7 del presente documento.



Duración de la Etapa: Desde la finalización de la etapa de transición de entrada hasta la terminación del contrato incluidas las prórrogas si a ello hubiere lugar.

En la etapa de Operación, el ICBF realizará pagos mensuales al Contratista por los servicios efectivamente prestados.

Descripción: En esta etapa el Contratista debe iniciar y garantizar la operación de todos los servicios contratados, adicionalmente debe iniciar la medición de ANS y seguimiento de la línea base. El pago mensual por los servicios de Operación Global corresponderá al valor ofertado por cada servicio completamente operativo después de aplicar los respectivos descuentos por ANS que se presentaran en el respectivo mes.

El Contratista tendrá el acompañamiento del operador saliente y/o del ICBF para realizar **el empalme de infraestructura tecnológica crítica** requerido para la migración de servicios, soluciones y ejecución de pruebas necesarias para iniciar la operación de los servicios y realizar las configuraciones necesarias con el objetivo de dar continuidad a la operación de cada uno de los servicios objeto del contrato y asumir la administración y operación de estos.

Empalme de infraestructura tecnológica crítica: El empalme referido anteriormente es crucial para asegurar una transición suave y minimizar cualquier interrupción en la operación, por tanto, se identifican plataformas claves para que el empalme sea efectivo y la operación pueda avanzar sin problemas en la etapa de operación:

- Entregar la plataforma de seguridad perimetral (Firewalll perimetrales) crítica y esencial para la operación de la entidad instalada, configurada y en correcto funcionamiento en, para lo cual el contratista deberá ejecutar instalación y puesta en operación de dicha plataforma en los datacenter interno y externo del ICBF, dentro de los quince días (15) siguientes a la fecha de suscripción del contrato. Es de aclarar que en este empalme los equipos que suministrará el contratista podrán ser equipos de contingencia mientras llegan los equipos nuevos y se cumple con la especificación del numeral 6 de la presente FCT. Se resalta que el tiempo máximo de contingencia será de 45 días contados desde la fecha de inicio de ejecución del contrato.
- Durante la instalación y configuración de la infraestructura crítica e indispensable para garantizar la continuidad de la operación, el Contratista podrá suministrar de manera temporal equipos de seguridad, servidores u otros componentes requeridos, siempre que estos cuenten con características técnicas iguales o superiores a las definidas en los numerales correspondientes a cada servicio, y permitan asegurar la continuidad del servicio tecnológico.El periodo máximo de contingencia será de cuarenta y cinco (45) días calendario. Una vez vencido dicho plazo, el proveedor entrante deberá dar estricto cumplimiento a las especificaciones establecidas en el numeral 6, titulado “Especificaciones Técnicas Mínimas de los Insumos, Bienes, Productos, Obras o Servicios a Entregar”, suministrando, instalando, configurando y poniendo en funcionamiento equipos totalmente nuevos, que cumplan con los

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

requerimientos técnicos mínimos exigidos para la operación de la infraestructura tecnológica del ICBF.

Requerimientos para iniciar la etapa: El Contratista deberá haber recibido los servicios TIC en administración por parte del ICBF con apoyo del operador saliente y se debe aprobar la finalización de la etapa de transición de entrada para iniciar la etapa de operación con los siguientes documentos:

- Documentos de inicio de ejecución del contrato (Copia de Contrato, Pólizas de Garantía y Designación del Supervisor).
- Acta de inicio del contrato.

Actividades:

- Realizar el Acta de inicio de la etapa operación de los Servicios TIC del ICBF.
- Elaborar y presentar los planes de trabajo y mejora y mantenimiento de cada uno de los servicios y gestorías.
- Realizar y presentar la estrategia de administración, gestión y operación de todos los servicios TIC del ICBF.
- Realizar la medición y seguimiento de ANS de todos los servicios TIC.
- Operación, administración, gestión y monitoreo de los servicios TIC con su infraestructura:

  - ✓ **Plataforma Base:** Servidores, Servicio de Gestión y Monitoreo y Respaldo.
  - ✓ **Sistemas de Información:** Aplicaciones y Base de Datos híbrida (On-Premise y Cloud).
  - ✓ **Redes de Comunicaciones:** Red LAN y Red Inalámbrica (WLAN) servicio a nivel nacional administrado de manera centralizada.
  - ✓ **Telefonía IP:** Servidores de Telefonía y periféricos.
  - ✓ **Seguridad de TI:** Seguridad Informática y de la Información, Seguridad Perimetral, Protección contra Amenazas, Antivirus, Análisis Forense, Gestión de Vulnerabilidades, SIEM y SOC (Security Operation Center) para una gestión integrada de seguridad, operaciones, riesgos y continuidad de TI en la plataforma tecnológica y garantizar la confidencialidad, integridad y disponibilidad de la información, evitando y dando tratamientos a distintas amenazas referentes a la seguridad.
  - ✓ **Herramientas de Productividad y Nube:** Directorio Activo, Microsoft Office 365 y Azure.
  - ✓ **Centro de Datos y Data Center:** Administración del Centro de Cómputo de la Sede de Dirección General y Data Center Externo.
- ✓ **Mesa de Servicio:** Soporte nivel I y nivel II.
- ✓ **Gestorías:** Lista de las gestorías de acuerdo con los servicios ITIL

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Realizar la instalación de los servicios a partir de la descripción de cada servicio y de la línea base.
- Apoyar activamente la implementación y configuración de los ANS en la herramienta de gestión de Mesa de Servicios. Recibir los servicios TIC mediante el procedimiento de control de cambios, que se debe ejecutar en conjunto con el Proveedor saliente y/o el ICBF.
- Configurar, medir y ajustar los ANS en la herramienta de Mesa de Servicio.
- Actualizar la Línea Base a la fecha de inicio del contrato.
- Garantizar la continuidad del servicio y tiempos de respuesta.
- Configurar e instalar las herramientas y demás activos a cargo del proveedor conforme a la presente ficha de condiciones técnicas que permitan la operación de los servicios y la información para la medición y monitoreo de los ANS

Excepciones: En esta etapa se realizarán descuentos (no pago) en el caso de no cumplimiento en los ANS por parte del Contratista, en caso de que el posible no cumplimiento sea atribuible al ICBF, se realizaran las correspondientes excepciones una vez el contratista presente las evidencias.

Entrega: Dentro de los últimos 30 días calendarios, previo a concluir la ejecución contractual, apoyar, en forma paralela y sin perjuicio de las demás obligaciones de operación, la entrega de servicios hacia el operador que determine el ICBF.

Responsabilidades del Contratista: Una vez se termine la operación del operador saliente el Contratista tendrá la responsabilidad sobre la operación y la continuidad de los servicios y gestorías TIC del ICBF, velando por la disponibilidad y buen desempeño de estos.

El Contratista debe:

a. Operar los servicios y gestorías TIC
b. Realizar medición a ANS
c. Realizar seguimiento a la línea base

En esta etapa el Contratista inicia la prestación de los servicios y gestorías TIC, con el personal capacitado y requerido para los mismos y con las condiciones técnicas solicitadas en este documento para cada uno de los servicios y gestorías; debe estar preparado para monitorear, administrar y gestionar la infraestructura tecnológica de ICBF.

Los dos (2) primeros meses de operación, **se miden ANS más no se penalizan.** En caso de no cumplir los niveles de servicio, lo anterior con el fin de estabilizar y realizar todos los ajustes sobre las herramientas de gestión y personalizaciones de administración. En los meses siguientes, se miden y penalizan los ANS en caso de no cumplir con los niveles del servicio pactados.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

El Seguimiento de la Línea Base se realizará cada mes, con el fin de monitorear el crecimiento de las cantidades unitarias de cada uno de los servicios TIC.

Esta etapa tiene los siguientes hitos:

- **Finalización implementación y estabilización de los servicios (Hasta 2 meses a partir de la finalización de la etapa de transición de entrada):** En este periodo opera y finaliza instalaciones de los elementos necesarios para brindar el servicio por parte del contratista, además realiza ajustes a los procesos y procedimientos del modelo de gestión.

- **Implementación del SOC (2 meses):** La implementación se realizará desde el inicio del contrato e inicia su operación, medición y gestión a partir de la finalización de la etapa de transición de entrada.

  Nota 1: Teniendo en cuenta el objeto del contrato que se enfoca en la prestación de servicios outsourcing, la entidad establece que no pagará por las fases de implementación y estabilización hasta tanto no esté completamente el servicio operativo, de tal manera, que la entidad pueda confirmar la funcionalidad y estabilidad.

  Nota 2: En caso de que la implementación supere los 2 meses, se acordará entre las partes una extensión de tiempo máximo con la excepción que este tiempo de implementación adicional será descontado en la respectiva facturación, proporcionalmente al porcentaje de implementación funcional y operativo que presente el contratista. En caso, que el contratista disminuya el tiempo establecido en la implementación y estabilización, se establecerá las fechas de inicio de facturación, una vez se haya cumplido con la funcionalidad requerida por el ICBF.

  Nota 3: Si el contratista no cumple con los términos establecidos para la implementación y estabilización del servicio, aun con la extensión de tiempo máximo, referido en la Nota 2, la entidad abordará la situación con la aplicación de penalizaciones según el contrato por el incumplimiento de los plazos o calidad del servicio.

- **Operación de los servicios, medición y penalización de ANS para Implementación del SOC y seguimiento línea base**

  Tras finalizar la implementación, se establece un periodo de estabilización de un (1) mese bajo las siguientes condiciones:

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Mes 1 (Instalación y Afinación): Se iniciará la medición y seguimiento de los ANS para establecer la línea base operativa. Durante este mes no se aplicarán penalizaciones, permitiendo el ajuste de los servicios y procesos.

- Mes 2 (Estabilización con control): Se mantendrá el seguimiento riguroso y se activará la aplicación de penalidades asociadas al incumplimiento de los ANS.

Este esquema asegura que el servicio alcance los estándares de calidad y las expectativas acordadas antes de la operación plena

El Contratista debe cumplir con los tiempos y documentos establecidos por el ICBF para el recibo a satisfacción de los servicios. En caso de no contar con lo mencionado por parte del Contratista por causas imputables al mismo, el ICBF a través de la supervisión del contrato procederá a tramitar el procedimiento para imposición de multas, sanciones y declaratorias de incumplimiento. Lo anterior, en aplicación del artículo 17 de la Ley 1150 de 2007.

6.8.3 ETAPA DE TRANSICIÓN DE SALIDA

Alcance: El Contratista realiza la entrega de los servicios al nuevo operador de Infraestructura de los servicios TIC del ICBF.

Duración de la Etapa: Se ejecutará en paralelo con los dos (2) últimos meses de la etapa de operación.

Descripción: En esta etapa, el Contratista debe planear y ejecutar el Plan de Transición de Salida (en paralelo a la etapa de operación), que debe estar alineado al plan de transición de entrada del Operador Entrante, con todos los servicios, su documentación e instalaciones requeridas. El Contratista realizará el acompañamiento al Operador Entrante y al ICBF para garantizar el empalme, migración de servicios y soluciones, ejecución de pruebas de inicio de operación de los servicios y entrega de documentación, de acuerdo con el plan detallado definido previamente en el Comité exclusivo para tal fin, en donde se detallarán las actividades a fin de entregar cada uno de los servicios, la administración, documentación y operación. El plan debe ser aprobado por el ICBF, en caso de prórrogas al contrato u otras situaciones, el plan de transición de salida podrá modificarse de manera que refleje la realidad del proyecto.

Responsabilidades del Contratista: La responsabilidad sobre la continuidad del servicio será del Contratista, hasta que a través de la gestión de cambios se haga entrega de la administración de la Infraestructura al nuevo operador y dicho cambio sea exitoso.

Requerimientos para iniciar la etapa:

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Entrega de información de los servicios y gestorías administrados.
- Acta de inicio de la etapa de transición de salida.

Actividades: Devolución y Entrega de los Servicios (los dos (2) últimos meses de operación).

- Ejecución del Plan de transición de salida de los servicios TIC.
- Realizar la transición con el nuevo operador.
- Entregar los equipos, información, procedimientos, instalaciones, mejoras y demás elementos a los cuales se encuentra obligado el contratista.
- El contratista debe asegurar el borrado de seguro de toda información propiedad del ICBF que pudiera encontrarse en dispositivos de seguridad, dispositivos de almacenamiento, dispositivos de red, dispositivos de procesamiento, dispositivos de virtualización, clústeres etc. Entregando al ICBF evidencias del procedimiento de borrado seguro ejecutado de todos y cada uno de los dispositivos antes mencionados y que pudieran ser suministrados en préstamo a la entidad como parte de la ejecución servicio plasmado bajo contrato de Operación Global.

Excepciones: Esta etapa no exime al Contratista del no pago de los servicios por el no cumplimiento de los ANS y del desarrollo normal de la operación descrito en la ETAPA DE OPERACIÓN. Los dos meses de la etapa de transición de salida está incluidos en el tiempo de la etapa de operación (es decir son periodos facturables) y el proveedor debe prestar los servicios.

El operador entrante debe entregar su modelo operativo durante esta etapa de transición de entrada.

6.9 SERVICIOS TIC

A continuación, se detalla todos y cada uno de los servicios requeridos para la línea base definida en el ***Anexo 03 - Línea Base de Servicios TI***, infraestructura actual del ICBF, la cual podrá modificarse durante la ejecución del contrato, en consecuencia, el futuro contratista deberá adaptar la prestación de servicios a los cambios que se puedan dar sobre la infraestructura.

Nota: En caso de que las sedes o sedes anexas se trasladen o cambien sus ubicaciones físicas, el Contratista deberá continuar dando cobertura a los servicios de operación global en las nuevas ubicaciones a Nivel Nacional. Para aquellos lugares diferentes a Bogotá y sus alrededores el servicio podrá ser prestado de forma remota.

6.9.1 ADMINISTRACIÓN CENTRO DE CÓMPUTO

6.9.1.1 GENERALIDADES DEL SERVICIO

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

El ICBF cuenta con dos (2) centros de cómputo:

Un (1) centro de cómputo principal (en adelante denominado Data Center Principal) provisto a través de un tercero contratado por medio de los acuerdos marco de Precios. En este centro de datos Externo se encuentran siete (7) rack en donde se disponen los equipos que requieren alta disponibilidad, las aplicaciones y bases de datos, servidores de desarrollo, pruebas y producción.

Adicionalmente el ICBF cuenta con un (1) centro de cómputo secundario (en adelante denominado Centro de Cómputo), ubicado en la Sede de la Dirección General del ICBF (Avenida Carrera 68 No. 64 C – 75 de la ciudad de Bogotá), en este se encuentran algunos equipos de comunicaciones, infraestructura de hyperconvergencia como respaldo de aplicaciones misionales e infraestructura de servidores de desarrollo y pruebas entre otros servicios tecnológicos.

6.9.1.2 ALCANCE

El alcance de este servicio es administrar el Data Center Principal y el Centro de Cómputo de la Sede de la Dirección General, con el fin de alojar el hardware y soportar los aplicativos y bases de datos de producción, desarrollo y pruebas, así como los demás servicios tecnológicos.

El servicio de administración incluye la operación de la infraestructura del Centro de Cómputo, debe contar con soporte, monitoreo y gestión en modalidad 7X24X365; además de gestionar los servicios del Data Center Principal con la flexibilidad, eficiencia, escalabilidad, redundancia y alta disponibilidad requeridos por la Entidad.

Este servicio incluye servicios de operación, administración, gestión, soporte y monitoreo de los elementos mencionados en la línea base de este servicio como UPS, tableros eléctricos regulados y no regulados, sistema detección y extinción de incendios, aires acondicionados, CCTV, entre otros. Adicionalmente incluye actividades de interconexión, gestión, mantenimiento preventivo y correctivo de la infraestructura tecnológica para la prestación del servicio de centro de cómputo de acuerdo con el levantamiento de requerimientos, implementación, pruebas, operación y documentación que garantice el cumplimiento de ANS del servicio.

6.9.1.3 DESCRIPCIÓN DEL SERVICIO

El Centro de Cómputo de la Sede de la Dirección General puede clasificarse como un centro de cómputo básico con características TIER I, que cuenta con control de acceso biométrico, sistema de CCTV independiente con tres (3) cámaras, aires acondicionados de precisión de 5 toneladas, sistema de extinción de incendios con agente FM200, transformador de aislamiento, UPS de 30 KVA exclusiva para el centro de cómputo, piso falso, detectores de

humedad, puerta de salida con barra antipánico, pintura intumescente. Las descripciones de los equipos de estos sistemas se relacionan en la Línea Base de este servicio. Cabe resaltar que actualmente estos equipos no están cubiertos por garantía, sin embargo, se realizan mantenimientos preventivos a los mismos de acuerdo con la periodicidad definida en los requerimientos del servicio.

La temperatura adecuada que se debe mantener para los dispositivos informáticos deberá oscilar entre 18º y 25ºC (64,5º y 77ºF), con una humedad relativa de entre 40 y 55%. Se requiere monitorear las condiciones ambientales del Centro de Cómputo, así como de toda la infraestructura alojada en éste.

El Data Center Principal cumple con los requerimientos de certificación TIER IV, contratado por Acuerdo Marco de Precios de Colombia Compra Eficiente.

6.9.1.4 REQUERIMIENTOS DEL SERVICIO

Las actividades mínimas requeridas en la administración del centro de cómputo de la Sede de la Dirección General son:

- Mantener el Centro de Cómputo de la sede de la Dirección General organizado y libre de obstrucciones.
- Revisión y mantenimiento periódica de tableros eléctricos regulados y no regulados del centro de cómputo.
- Revisión ajuste y mantenimiento de piso técnico de forma semestral, garantizando los pasillos fríos y calientes al interior, mejorando la dispersión del aire y la refrigeración correcta de los equipos.
- Ajuste de cables y circuitos eléctricos, nivelación de cargas eléctricas cuando se requieran.
- Cambios (Instalación) de circuitos eléctricos, acometidas eléctricas, tomas, breaker, dispositivo de protección contra sobretensiones (DPS), fusibles u otros elementos de los tableros eléctricos o acometidas del centro de cómputo y cuarto de UPS cuando se requiera.
- Limpieza de impurezas que se acumulan bajo el piso falso.
- Aseo general del centro de cómputo de la sede de Dirección General, limpieza de rack, piso y paredes.
- Ingreso y conexión de rack nuevos cuando se requiera.
- Inspección, ajuste del sistema de tierras, aterrizaje de racks y equipos del centro de cómputo.
- Conexión de equipos de cómputo o comunicaciones propiedad del ICBF o acompañamiento a proveedores para el ingreso de equipos nuevos cuando se requiera.
- Interconexión (cross conection) de fibras y cables, UPS, incluyendo materiales e instalación.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Implementar un sistema de monitoreo remoto para el centro de cómputo secundario, que permita recopilar, almacenar, consultar y analizar la información asociada a las condiciones ambientales, de seguridad, eléctricas y de operación de la infraestructura tecnológica alojada en el sitio. La solución deberá utilizar sensores inalámbricos de fácil instalación y, cuando no requieran conexión eléctrica directa, contar con baterías de larga duración, con una autonomía mínima de un (1) año.
- El sistema deberá permitir monitorear, entre otros, apertura de puertas y racks con detección de manipulación (Tamper), temperatura, humedad, niveles de ruido, presencia de agua bajo piso falso y parámetros eléctricos tales como voltaje, corriente, potencia, consumo, factor de potencia y THD (Distorsión Armónica Total).
- La información deberá centralizarse en una plataforma web que permita consultar dashboards, gráficas, históricos, eventos y alertas, así como representar gráficamente los ambientes monitoreados. La solución deberá soportar notificaciones mediante correo electrónico y/o aplicaciones de mensajería, integración con dispositivos de diferentes fabricantes, y conectividad mediante APIs, MQTT y Kafka

- Mantenimiento preventivo y/o correctivo de los equipos que se encuentran en el centro de cómputo (transformador de aislamiento, aires acondicionados, sistemas contraincendios, tableros eléctricos) y en el cuarto de UPS (UPS de 30 KVA y de 270 KVA), Proveer los suministros y consumibles requeridos para una correcta operación del Centro de Cómputo de la Sede de la Dirección General, en los equipos: UPS de 30 KVA, UPS de 270 KVA, aires acondicionados, sistema de control de incendios, sistema de control de ambiente y piso técnico, asegurando la prestación del servicio y llevando un registro actualizado de la utilización de los suministros y consumibles. Se debe incluir cambio de baterías cuando sea requerido, así como la respectiva disposición de las baterías de residuo, antes de la etapa de transición de salida. La periodicidad mínima para los mantenimientos preventivos es:

  - UPS: trimestral
  - Aires Acondicionados: trimestral. No obstante, el contrato contempla únicamente aquellas intervenciones puntuales y excepcionales relacionadas con equipos de climatización dedicados o especializados, que soportan de manera directa la operación de los servicios tecnológicos objeto contractual, tales como:

    Aires acondicionados de precisión, unidades dedicadas o sistemas especializados instalados en salas técnicas, cuartos de comunicaciones, data centers, nodos TIC, SOC o NOC, cuando estos equipos:

    Presenten fallas no previsibles durante la ejecución contractual, o Sean críticos para garantizar la disponibilidad, estabilidad y continuidad de la infraestructura tecnológica.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Estos equipos cuentan con características técnicas distintas a los sistemas de aire acondicionado de uso administrativo o general gestionados por la DAD, dado que están diseñados para operar bajo condiciones específicas de control térmico, humedad y continuidad, propias de ambientes tecnológicos críticos.

En caso de requerirse alguna intervención sobre estos sistemas especializados, la misma deberá estar debidamente justificada, contar con concepto técnico del Supervisor del contrato, y limitarse estrictamente al mantenimiento correctivo, ajuste o reposición indispensable para preservar la operación de los servicios tecnológicos contratados, sin sustituir ni solaparse con los contratos de infraestructura física vigentes de la Entidad.

- Sistema de extinción de incendios: semestral
- Transformador de aislamiento: semestral
- Transformador de aislamiento verificación de cargas: semestral
- Limpieza de Impurezas y aseo general: semestral
- Tableros Eléctricos regulados y no regulados: bimensual
- Piso Técnico: 1 Mantenimiento

Sistemas de Apoyo	Actividad	Necesidad del servicio
UPS 30 KVA marca APC	Mantenimientos	1 cada 3 meses
	Monitoreo	Diario
UPS 270 KVA	Mantenimientos	1 cada 6 meses
	Monitoreo	Diario
Aires acondicionados	Mantenimientos	1 cada 3 meses
	Monitoreo	Diario
Sistema de extinción	Mantenimientos	1 cada 6 meses
	Monitoreo	Diario
Transformadores aislamiento	Mantenimientos	1 cada 6 meses
	Monitoreo	Diario
Sistema de control de acceso al centro de cómputo	Mantenimientos	Semanal
	Monitoreo	Diario
Sistema de monitoreo ambiental NetBotz	Mantenimientos	Semanal
	Monitoreo	Diario
Piso Técnico	Mantenimientos	1 cada 6 meses
	Monitoreo	Mensual
Limpieza de Impurezas y aseo general	Mantenimientos	1 cada 6 meses
	Monitoreo	Mensual
Tableros Eléctricos regulados y no regulados	Mantenimientos	1 cada 2 meses
	Monitoreo	Mensual

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Las anteriores actividades de administración se deben ejecutar periódicamente en forma proactiva, esto con el ánimo de anticiparse a posibles daños o fallas que puedan presentarse.
- En caso de presentarse un incidente que requiera el cambio de alguna parte, este debe realizarse dentro de los ocho (8) días hábiles siguientes al reporte de la necesidad. En caso de presentarse algún incidente que requiera realizar cambio de alguna parte sobre los sistemas de apoyo (aires acondicionados, sistema de detección de incendios, sistema eléctrico regulado UPS 30 KVA, UPS 270 KVA, sistemas de control de accesos, circuito cerrado de televisión (CCTV)) el contratista tiene la responsabilidad de garantizar la disponibilidad del servicio bien sea reemplazando partes de un equipo en mal funcionamiento o suministrando como contingencia el equipo afectado con iguales o mejores características.
- Identificación de servidores, equipos de cómputo y comunicaciones, así como su etiquetado con nombre, dirección IP y placa de inventario, etiquetado de patch panel y patch cord en los dos (2) centros de cómputo.
- Manejo (registro, actualización, seguimiento y reporte) de inventario de los todos los equipos de cómputo, comunicaciones y demás equipos que se encuentran dentro del centro de cómputo.
- Elaboración y actualización mensual de diagramas de red, diagramas de interconexión de equipos y diagramas unifilares.
- Administración y gestión de permisos de ingreso de personal (asignación de usuarios) al centro de cómputo de Dirección General.
- Implementación de una bitácora electrónica de registros de acceso (de personal y equipos) del centro de cómputo de la sede de Dirección General.
- Socializar los procedimientos para el ingreso y salida de personas y equipos del centro de cómputo del ICBF, así como los formatos que se utilizarán para este fin.
- El ICBF requiere en cuanto a seguridad física, que:

    - Se implemente como mínimo controles físicos de registro de ingreso de personal autorizado tales: Control de acceso biométrico, bitácora electrónica de registros y cámaras de video (tipo domo con infrarrojo).

Para el centro de cómputo se requiere, el suministro e instalación de ocho (8) cámaras con todo el cableado necesario, de la siguiente forma:

- Una (1) instalada en cada pasillo (para un total de 4 pasillos), una (1) visualizando la puerta de acceso y una (1) visualizando el pasillo de acceso al centro de cómputo, una (1) visualizando el cuarto de UPS y una (1) cámara para exteriores visualizando el acceso al cuarto de baterías de la UPS.

- Las cámaras deben ser IP, como mínimo deben tener las siguientes características:

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Tipo Domo
- Resolución de 5mp
- Con sensor de imagen,
- Iluminación a Color,
- Grabación para el día y la noche,
- Compresión de video H.265, H.264.
- Software del cliente o navegador web
- Protocolos: TCP / IP, UDP, ICMP, http, https, FTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, PPoE, NTP, UPnP, SMTP, SNMP, IGMP, 802.1X, QoS, IPv6
- Grabación con la detección de movimiento para una duración de mínimo 6 meses.
- El mantenimiento de las cámaras de video durante la ejecución del contrato estará a cargo del Contratista.
- Cumplir los procedimientos y normas de seguridad descritas para Centros de Cómputo vigentes. (Norma TIA-942 entre otras)

- El contratista debe contemplar el servicio de mantenimiento y monitoreo para las UPS que hacen parte del centro de cómputo.
- Administrar y monitorear 7X24X365 la operación de la infraestructura del Centro de Cómputo de la Sede de la Dirección General y del Centro de Datos Principal.
- Realizar descubrimiento automático y/o manual de inventario de activos TI de la herramienta de gestión y monitoreo provista por el ICBF.
- Entregar información actualizada de los equipos que administra para la alimentación de la CMDB del ICBF cuando este la requiera, la CMDB será administrada por el Contratista de Mesa de Servicios.
- Gestionar las condiciones ambientales y técnicas necesarias para el funcionamiento adecuado del centro de cómputo de la sede de la Dirección General entregadas por el ICBF, en caso de daño en algún componente este deberá ser arreglado o reemplazado (incluyendo instalación y materiales) en forma inmediata por el Contratista con el fin de normalizar la operación.
- Acompañar al personal técnico que adelante trabajos (cualquier actividad) en el Centro de Cómputo del ICBF durante el desarrollo de su labor, previa comunicación del ICBF al Contratista.
- Mantener actualizada la información de los elementos que componen el Centro de Cómputo de la sede de la Dirección General, los cuales incluyen entre otros:

    - Mapas e inventario de racks y/o equipos al servicio de ICBF alojados en ellos.
    - Mapas distribución sistema contra incendio.
    - Diagramas unifilares de tableros, puesta a tierra y sistemas eléctricos.
    - Inventario de equipos con marca, modelo y referencia, incluyendo:
    - Sistema contra incendio.
    - Aires acondicionados y climatización.
    - Trasformador de aislamiento

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Gestión de alarmas.
- Control de seguridad (seguridad perimetral, sistemas de vigilancia, sistemas de control de accesos).
- Sistema eléctrico regulado UPS 30 KVA y 270 KVA
- Topología del Data Center Principal y Centro de Cómputo

- Implementar los niveles de seguridad física necesarios para proteger todos los equipos que se encuentran en el centro de cómputo de la sede de Dirección General. Estas medidas de seguridad también aplican en el evento que el ICBF incorporen nuevos equipos propiedad de la Entidad o equipos de terceros para proyectos o pilotos, éstos se reportarán con debida antelación al Contratista para que sean incorporados en su esquema de seguridad.
- Realizar la inspección del control de incendio y en caso de requerirse, realizar la recarga del sistema FM200.

6.9.2 APLICACIONES

6.9.2.1 GENERALIDADES DEL SERVICIO

En la actualidad el ICBF cuenta con aplicaciones que atienden y apoyan las funciones laborales propias de los colaboradores del ICBF e igualmente la atención a los usuarios de los diferentes programas de la Entidad, estas aplicaciones son desarrolladas, ajustadas y complementadas internamente por el ICBF en apoyo con un contrato de fábrica de software, adicional se tienen algunas aplicaciones comerciales instaladas, parametrizadas configuradas y personalizadas de acuerdo con las necesidades del Instituto.

Los sistemas operativos en las cuales están soportadas las aplicaciones son

Sistema Operativo	Cantidad
Red Hat Enterprise Linux Server release 7.9 (Maipo)	2
Red Hat Enterprise Linux release 8.4 (Ootpa)	1
Red Hat Enterprise Linux release 9.5 (Plow)	1
Red Hat Enterprise Linux release 9.6 (Plow)	1
Red Hat Enterprise Linux release 9.7 (Plow)	1
Red Hat Enterprise Linux Server 7.9 (Maipo)	1
Red Hat Enterprise Linux Server release 7.6 (Maipo)	7
Red Hat Enterprise Linux Server release 7.7 (Maipo)	1
Windows Server 2003 R2 Enterprise Ed.	1
Windows Server 2012 R2 estándar edition	8

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Windows Server 2016 R2 Standard Edicion	14
Windows server 2019 Standard Edicion	7
Windows Server 2022	15
Windows server 2025	15
Total general	75

2.Las aplicaciones están desarrolladas en los siguientes lenguajes de programación:

Lenguaje	Cantidad
C# - ASP.NET	1
C# - ASP.NET - DevExpress	2
C# Angular	1
Drupal: 11.3.5 PHP 8.3.29 Nginx:1.20.1	1
Java 1.8.0_161	2
PHP 5.4.16	1
PHP 5.5.38	1
PHP 5.5.38	1
PHP 5.6.25	1
PHP 7.2.10	4
PHP 7.2.24	2
PHP 7.4.27	1
PHP 8.2.25	1
PHP 8.2.28	1
Phyton	1
Servicos en .net 4.5 y las interface en java y c#	1
Visual Studio 2015 C#	2
Visual Studio 2015 VB	1
VS Basic	4
VS C#	46
Total general	**75**

3.Los motores de base de datos sobre las cuales están soportadas las aplicaciones son:

Motor de Base de Datos	Cantidad
SQL Server 2008	1
SQL Server 2012	9
SQL Server 2014	39
SQL Server 2016	13
SQL Server 2019	12
SQL Server 2022	6
Maria DB 8.0.27	1
Maria DB 8.0.26	1
Maria BD 5.5.68	6
MariaDB 10.2.22	2
MariaDB 10.11.14	4
MySQL 8.0.24	1
MySQL 8.4.8	1
MySQL 8.0.35	2
MySQL 8.0.43	1
Oracle 10G	37
Total	136

Nota: Los elementos y características descritas en las tablas anteriores, corresponden a la infraestructura actual del ICBF , sin perjuicio a los anterior dicha infraestructura podrá ser objeto de cambios durante la ejecución del contrato, razón por la cual el contratista deberá adaptar prestación de los servicios contratados a las modificaciones que se implementen, sin afectar la calidad, la oportunidad y continuidad de los mismos.

6.9.2.2 ALCANCE

El alcance para el servicio de administración de aplicaciones tanto misionales como de apoyo y financieras con las que cuenta el ICBF, está enmarcado en la configuración, Instalación, operación, administración, gestión, mantenimiento, remediación sugerida y publicada por los fabricantes, diagnóstico y monitoreo (7X24X365) de las aplicaciones

productivas del ICBF según la operación y necesidades del ICBF. También se requiere contar con el apoyo técnico para implementar los ambientes de prueba o pre productivos para los nuevos sistemas de información cuando se requiera.

El contratista debe garantizar la disponibilidad y optimo desempeño de las aplicaciones, como la continuidad, seguridad y control de las aplicaciones actuales como de las que surjan durante la vigencia del contrato.

El contratista debe realizar una administración integral teniendo en cuenta todos los componentes de software e integración con otros servicios.

En el siguiente cuadro se ilustra la cantidad de aplicaciones que actualmente tiene en producción en ICBF, sin embargo, es importante resaltar que esta cantidad puede aumentar o disminuir, dependiendo de la dinámica del Instituto.

SERVICIO	COMPONENTE	UNIDAD DE MEDIDA
APLICACIONES	Administración de aplicaciones	Número de Aplicaciones administradas 75

6.9.2.3 DESCRIPCIÓN DEL SERVICIO

El contratista debe recibir las aplicaciones del ICBF, y disponer del recurso técnico para la administración y que estas se mantengan en operación y disponibles, además de solucionar incidentes y los requerimientos para modificación o mejora de las aplicaciones; se deben usar buenas prácticas para la gestión de las aplicaciones, y suministrar las mejores recomendaciones del caso de acuerdo con los diagnósticos realizados para mejorar el desarrollo y desempeño de los sistemas de información del ICBF, el Contratista estará participando con su equipo técnico en mesas de trabajo con los líderes del servicio de la Dirección de Tecnologías de la Información (DTI) entre otro personal profesional y técnico del ICBF para mejora del servicio de aplicaciones.

6.9.2.4 REQUERIMIENTOS DEL SERVICIO

El servicio de aplicaciones incluye la configuración, instalación, administración, mantenimiento, gestión y monitoreo (7X24X365) de las aplicaciones en el ambiente de producción. Para el servicio de aplicaciones el ICBF requiere:

- Realizar el dimensionamiento y configuración de la infraestructura de las aplicaciones de acuerdo con mejores prácticas de tecnología de la información.

- Instalación en ambientes de producción de las aplicaciones de acuerdo con el procedimiento definido por el ICBF y apoyo en los ambientes de pruebas y preproducción e interoperabilidad con otras entidades del estado.
- Probar, diagnosticar y monitorear el rendimiento de aplicaciones WEB. IIS, ASP.NET, APIS, Apache, PHP, Drupal, NodeJS, Keepalived, Solr, Nginx, Varnish entre otras que puedan surgir por medio de trazas, contadores de desempeño, rendimiento, herramientas de análisis y diagnóstico u otro método que permita hacer un seguimiento de la ejecución de las aplicaciones.
- Realizar la administración, operación, monitoreo y mantenimiento de la plataforma de aplicaciones, así como la ejecución de todas las tareas recurrentes, programadas y no programadas para mantener en estado de operación óptima las aplicaciones del ICBF. Realizar la gestión y administración de las aplicaciones en granjas de servidores web, azure, con la configuración de parámetros de rendimiento, resolución de problemas e incidentes y configuración de mejores prácticas en todos los componentes de software que se usan para operación de los sistemas de información en todas sus categorías

6.9.3 BASES DE DATOS

6.9.3.1 GENERALIDADES DEL SERVICIO

En la actualidad el ICBF cuenta con diferentes motores de base de datos (SGDB) como son SQL Server, Oracle, MySQL y MariaDB que soportan data estructurada provenientes de las diferentes aplicaciones y/o permite a los usuarios funcionales almacenar información y consultar datos. de los motores de las bases de datos. Los SGDB permiten a los usuarios la relación, estructuración, organización y gestión de los datos (almacenar, modificar, extraer y acceder), garantizando la integridad, confidencialidad, disponibilidad y seguridad de la información que se almacena en las bases de datos.

Adicional a esto permite a los administradores la definición de rutinas de mantenimiento, estructura y métodos de acceso, políticas de respaldos, concesión de autorización de acceso, entre otros.

6.9.3.2 ALCANCE

El alcance para el servicio de administración de base de datos tanto misionales como de apoyo, está enmarcado en la administración en el monitoreo (7X24X365), instalación, implementación, configuración, mantenimiento, aplicación de buenas prácticas y recomendaciones de fabricantes, garantizando la disponibilidad, integridad, confidencialidad, consistencia, seguridad y control de las bases de datos productivas actuales y las que se surjan durante la vigencia del contrato.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

En el siguiente cuadro se ilustra la cantidad de bases de datos en los diferentes SGDB que actualmente tiene en producción el ICBF, sin embargo, es importante resaltar que esta cantidad puede aumentar o disminuir, dependiendo de la dinámica del Instituto.

SERVICIO	COMPONENTE	UNIDAD DE MEDIDA
BASES DE DATOS	Administración de bases de datos (Motor de Base de Datos SQL Server, Oracle, MySQL y MariaDB) y SQL Azure	136

La línea base puede tener modificaciones durante la ejecución del contrato, el cual el proveedor debe asumir los cambios.

El contratista debe mantener la información estructurada bajo una administración profesional y técnica con recursos especializados como los DBAs para la administración, operación, instalación, configuración, mantenimiento y monitoreo de los motores de bases de datos Microsoft SQL Server, Azure SQL Server, Oracle, MySQL y MariaDB, procesamiento de datos.

El contratista debe garantizar y asegurar la disponibilidad, integridad, confidencialidad, consistencia, seguridad y buen desempeño de las bases de datos de los diferentes ambientes con las que cuenta actualmente el ICBF así como aquellas bases de datos que se adquieran durante la vigencia del contrato, que soportarán los sistemas de información del ICBF, así como aquellas bases de datos que se adquieran durante la vigencia del contrato, que soportarán los sistemas de información del ICBF.

6.9.3.3 DESCRIPCIÓN DEL SERVICIO

Las bases de datos con las que se cuenta el ICBF actualmente almacenan la información de los diferentes aplicativos que soportan la operación de las áreas misionales y administrativas, para lo cual se tienen bases de datos en motores: Microsoft SQL Server, Oracle, MySQL y MariaDB.

6.9.3.4 REQUERIMIENTOS DEL SERVICIO

Para las bases de datos el ICBF requiere la administración, operación, instalación, configuración, implementación, mantenimiento, monitoreo, garantizando la disponibilidad, integridad, confidencialidad, consistencia, seguridad y control de las bases de datos en los ambientes productivos. Así mismo como aquellas que se adquieran durante la vigencia del contrato.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- El servicio de administración de base de datos incluye la instalación de motores de Bases de datos, Configuración e implementación con las mejores prácticas, migración (versión, edición u otro SGBD), operación procesamiento de datos, y administración de esquemas de alta disponibilidad para todas las bases de datos actuales y para aquellas nuevas que surjan durante la vigencia del contrato. El ICBF proporcionará las licencias necesarias para los motores de bases de datos.
- Realizar el montaje, implementación, administración, operación, diagnóstico y soporte del motor de base de datos y de componentes tales como reporting services, integration services, analysis services, business Intelligence, Data Ware House, Cubos_,Databricks, Azure Data Factory, Azure SQL Server, Synapse Analytics, Azure Analisis Services, Azure Storage Account en los ambientes, productivo, pre-productivos, pruebas y desarrollo así mismos apoyar en solución de las incidencias presentadas en los ambientes que soportarán los sistemas de información del ICBF.
- Responder por la administración, operación, monitoreo y mantenimiento de la plataforma de base de datos, así como la ejecución de todas las tareas recurrentes, programadas y no programadas para mantener en estado de operación óptima y eficiente las bases de datos del ICBF.
- Realizar un Informe mensual sobre el comportamiento y performance de las bases de datos que incluya como mínimo: informe de bloqueos (deadlock), recomendaciones, comportamiento estadístico de las bases de datos, recomendaciones de mejoras para optimizar las bases de datos, así como también: tablas a particionar, vistas, índices, top 10 de sentencias que consuman más recursos.
- Llevar bitácora de control de las bases de datos y sus componentes del ICBF, incluyendo como mínimo crecimiento mensual, almacenamiento disponible, incidentes, ejecución de backup, tareas automáticas, análisis de errores, optimización de procesos y alertas debe ser un anexo para el informe mensual de gestión.
- Definir, documentar y comunicar las políticas, procedimientos, planes de mantenimiento y estándares de las bases de datos con previa aprobación del ICBF.
- Brindar apoyo técnico y proponer activamente recomendaciones y buenas prácticas tanto de configurar de base de datos como de desarrollo de consultas transact o procedimientos almacenados, tendientes a optimizar el uso de recursos, asegurar la disponibilidad, seguridad, integridad, consistencia, continuidad, operación y buen desempeño de las bases de datos del ICBF.
- Dar respuesta a las consultas técnicas realizadas por el ICBF, asesorando en el mejoramiento y optimización de recursos, con el fin de garantizar la disponibilidad y buen desempeño de las bases de datos en los tiempos definidos por El ICBF.
- Instalar, administrar y soportar bases de datos Oracle 10G o superior, MySQL y MariaDB, administrar y configurar RMAN (Recovery Manager).

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Administrar, configurar y automatizar tareas de mantenimiento y optimización de los motores de bases de datos a través de las herramientas propias del motor de base de datos o que el Contratista suministre.
- Mantener actualizado el inventario de Base de Datos de acuerdo con los formatos establecidos en conjunto con el ICBF.
- Documentar, mantener actualizada y entregar al final del contrato o cuando se requiera, en formatos acordados con el ICBF, la base de datos del conocimiento y de configuraciones en cada servidor de base de datos: Gestión de configuración, Gestión de problemas, Gestión de cambios entre otras.
- Presentar recomendaciones sobre el diseño, configuración, arquitectura de todos los componentes y servicios de los motores de bases de datos.
- Identificar consultas a optimizar y suministrar recomendaciones y mejores prácticas en la construcción de sentencias SQL.
- Generar y presentar un cronograma de las actividades de mantenimiento de las bases de datos con fechas de ejecución y responsables, el cual debe ser validado por el ICBF.
- Realizar los traslados físicos de las bases de datos, bajo solicitud y aprobación del ICBF, mediante un proceso de control de cambios, previa aprobación del comité de control de cambios.
- Realizar pruebas de carga, estrés y seguridad sobre ambientes de prueba o pre productivos para dimensionar su capacidad y concurrencia de usuarios sobre las bases de datos de los sistemas de información actuales y nuevos proyectos que se implementen durante la duración del contrato. El proveedor debe proporcionar software especializado para realizar estas labores.

6.9.4 BIG-DATA

6.9.4.1 GENERALIDADES DEL SERVICIO

El servicio de BIG-DATA tiene como propósito administrar, gestionar, operar, monitorear, controlar y asegurar la disponibilidad de la plataforma de Big Data y Analítica del Instituto Colombiano de Bienestar Familiar – ICBF, garantizando el adecuado funcionamiento de los componentes tecnológicos que soportan la integración, almacenamiento, procesamiento, transformación, explotación, análisis y visualización de los datos institucionales, necesarios para apoyar la operación, la toma de decisiones y el cumplimiento de los objetivos estratégicos de la Entidad.

El servicio comprende la administración integral de los componentes que conforman la plataforma de Big Data del ICBF, tanto en ambientes On-Premise como Cloud, incluyendo los servicios, herramientas, plataformas y recursos tecnológicos destinados a la integración de datos, procesos ETL/ELT, almacenamiento analítico, procesamiento de datos, explotación de información, analítica, inteligencia de negocios (Business Intelligence),

visualización de información y demás componentes que hagan parte de la arquitectura tecnológica institucional durante la ejecución del contrato.

El servicio incorporará capacidades de ingeniería y gestión técnica de datos, extracción y gestión de metadatos, documentación estructurada y técnica, automatización y optimización de los procesos ETL/ELT, monitoreo y mejoramiento de la calidad de los datos, mediante el aprovechamiento de las tecnologías institucionales existentes, incluidos los servicios de datos de Microsoft Azure y Microsoft Fabric, cuando este último se encuentre habilitado por el ICBF.

La prestación del servicio deberá garantizar la continuidad operativa de la plataforma de Big Data, mediante la administración, monitoreo, optimización, mantenimiento preventivo y correctivo, gestión de incidentes, problemas, cambios, requerimientos, capacidad, disponibilidad, continuidad, seguridad y rendimiento de los componentes administrados, asegurando el cumplimiento de los Acuerdos de Niveles de Servicio (ANS) establecidos por el ICBF.

El Contratista será responsable de mantener actualizada la Línea Base del Servicio, la documentación técnica, la configuración de los componentes administrados, los procedimientos operativos, los inventarios, las métricas e indicadores del servicio, así como de proponer e implementar acciones de mejora continua orientadas a optimizar el desempeño, la disponibilidad, la capacidad, la confiabilidad y la eficiencia operativa de la plataforma de Big Data.

Así mismo, el servicio deberá soportar la incorporación de nuevos componentes tecnológicos, servicios, fuentes de información, modelos analíticos, plataformas, herramientas y capacidades que el ICBF requiera durante la ejecución contractual, garantizando su integración con la arquitectura tecnológica institucional, conforme a las mejores prácticas de la industria, los lineamientos de arquitectura empresarial, gobierno de datos, seguridad de la información y gestión de servicios de TI definidos por la Entidad.

La operación del servicio deberá ejecutarse bajo las mejores prácticas de ITIL, los marcos de referencia adoptados por el ICBF y los lineamientos institucionales vigentes, garantizando la trazabilidad de las actividades realizadas, la disponibilidad de la información técnica y la generación de reportes e indicadores que permitan efectuar el seguimiento, control y mejora continua de la plataforma de Big Data.

6.9.4.2 ALCANCE DEL SERVICIO

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

El servicio de **BIG-DATA** comprende la instalación, administración, operación, monitoreo, soporte, mantenimiento (7X24X365), optimización y evolución de los componentes que conforman la plataforma de Big Data y Analítica del ICBF, garantizando su disponibilidad, desempeño, capacidad, continuidad, seguridad e integración con la arquitectura tecnológica institucional.

El servicio incluye la gestión integral de los componentes de la plataforma Big Data, tanto en ambientes **On-Premise** como **Cloud**, abarcando las actividades necesarias para asegurar su correcto funcionamiento durante todo su ciclo de vida, desde su implementación o incorporación hasta su retiro o sustitución, cuando aplique.

Como parte del alcance del servicio, el Contratista deberá administrar los componentes tecnológicos que soportan la integración, almacenamiento, procesamiento, transformación, explotación, análisis y visualización de los datos institucionales, incluyendo las actividades de instalación, configuración, parametrización, monitoreo, actualización, mantenimiento preventivo y correctivo, atención de incidentes, solución de problemas, ejecución de cambios, gestión de requerimientos, control de versiones, optimización del desempeño, administración de la capacidad, respaldo y recuperación de la información, así como la implementación de acciones orientadas al uso eficiente de los recursos tecnológicos, la optimización del consumo de infraestructura y de los servicios asociados a la plataforma Big Data, procurando el aprovechamiento eficiente de la capacidad instalada y la sostenibilidad operativa del servicio.

Así mismo, el Contratista será responsable de la elaboración, actualización, mantenimiento y custodia de la documentación técnica y operativa asociada al servicio, incluyendo, como mínimo, inventarios de componentes, diagramas de arquitectura, procedimientos operativos, manuales técnicos, configuraciones, bitácoras de operación, documentación de procesos de integración y transformación de datos (ETL/ELT), flujos de procesamiento, control de versiones y demás artefactos técnicos requeridos para garantizar la adecuada administración, la transferencia de conocimiento, la continuidad operativa y la trazabilidad del servicio.

El servicio deberá permitir la incorporación, administración y soporte de nuevos componentes tecnológicos que sean implementados durante la ejecución del contrato, manteniendo actualizada la Línea Base del Servicio y asegurando su integración con los demás servicios de infraestructura, bases de datos, redes, seguridad, aplicaciones, interoperabilidad y demás componentes tecnológicos administrados por el Operador.

La unidad de medida del servicio corresponderá al **número de componentes Big Data – instalación, administración, operación y monitoreo**, de conformidad con la Línea Base del Servicio aprobada por el ICBF.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Para efectos del presente contrato, se entenderá por **componente Big Data** cualquier elemento tecnológico que haga parte de la plataforma institucional de Big Data y Analítica, incluyendo, entre otros:

- Plataformas de Big Data.
- Plataformas de Analítica de Datos.
- Data Lake.
- Data Warehouse.
- Bases de datos analíticas.
- Procesos ETL y ELT.
- Pipelines de integración y orquestación de datos.
- Motores de procesamiento de datos.
- Espacios de trabajo (Workspaces) analíticos.
- Herramientas de inteligencia de negocios (Business Intelligence) y visualización de información.
- Catálogos de datos y metadatos.
- Ambientes de Desarrollo, Pruebas y Producción.
- Demás componentes tecnológicos que hagan parte de la arquitectura Big Data implementada por el ICBF durante la ejecución del contrato.

El alcance del servicio podrá ampliarse o modificarse conforme a la evolución de la plataforma tecnológica institucional, mediante la incorporación de nuevos componentes, herramientas, plataformas o capacidades, de acuerdo con las necesidades del ICBF, sin que ello implique la modificación de la naturaleza del servicio.

Unidad de medida del servicio

SERVICIO	COMPONENTE	UNIDAD DE MEDIDA	CANTIDAD
BIG-DATA	**Analítica**	Servicio integral de administración, operación, monitoreo, mantenimiento, soporte y optimización de la plataforma Big Data y Analítica del ICBF	**1**

6.9.4.3 DESCRIPCIÓN DEL SERVICIO

El servicio de **BIG-DATA** comprende la administración integral de la plataforma de Big Data y Analítica del ICBF, mediante la prestación de los servicios especializados requeridos para garantizar la operación, disponibilidad, continuidad, desempeño, capacidad, seguridad, confiabilidad y evolución de los componentes que soportan la gestión del ciclo de vida de los datos institucionales.

El Contratista será responsable de la administración técnica y operativa de los componentes que conforman la plataforma de Big Data, asegurando su correcta instalación, configuración, parametrización, monitoreo, mantenimiento, actualización, optimización y soporte, de acuerdo con las necesidades del ICBF, los Acuerdos de Niveles de Servicio (ANS), las mejores prácticas de la industria y los lineamientos tecnológicos definidos por la Entidad.

El servicio comprende la gestión de los componentes destinados a la integración, almacenamiento, procesamiento, transformación, análisis, explotación y visualización de la información institucional, así como la administración de los procesos de ingesta, integración y orquestación de datos, repositorios analíticos, plataformas de inteligencia de negocios, herramientas de analítica, motores de procesamiento, catálogos de datos y demás componentes tecnológicos que hagan parte de la arquitectura Big Data del ICBF.

Como parte de la prestación del servicio, el Contratista deberá ejecutar las actividades necesarias para garantizar la disponibilidad y el adecuado funcionamiento de la plataforma, incluyendo el monitoreo permanente de los componentes administrados, la atención de incidentes, la gestión de problemas, requerimientos y cambios, el mantenimiento preventivo y correctivo, la optimización del desempeño y la capacidad, la administración de respaldos y recuperación de la información, la implementación de acciones de mejora continua y el soporte técnico especializado requerido para asegurar la continuidad de la operación.

El servicio deberá garantizar la adecuada integración con los demás servicios tecnológicos administrados por el Operador, tales como infraestructura tecnológica, redes, bases de datos, plataformas en la nube, seguridad de la información, aplicaciones, interoperabilidad y demás componentes que soporten la operación institucional, asegurando la interoperabilidad, consistencia y disponibilidad de la información.

Así mismo, el Contratista será responsable de mantener actualizada la documentación técnica y operativa del servicio, incluyendo los inventarios de componentes, configuraciones, procedimientos, diagramas de arquitectura, manuales técnicos, documentación de procesos de integración y transformación de datos, control de versiones, bitácoras de operación y demás artefactos técnicos necesarios para garantizar la trazabilidad, la continuidad operativa, la transferencia de conocimiento y la adecuada gestión del servicio.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Durante la ejecución del contrato, el servicio deberá soportar la incorporación de nuevos componentes tecnológicos, herramientas, plataformas, fuentes de información y capacidades analíticas que requiera el ICBF, garantizando su integración con la arquitectura tecnológica institucional y su administración conforme a los lineamientos de arquitectura empresarial, gobierno de datos, seguridad de la información y gestión de servicios de tecnología adoptados por la Entidad.

La prestación del servicio deberá ejecutarse bajo un enfoque de mejora continua, promoviendo la optimización permanente de la plataforma Big Data, la automatización de procesos, el fortalecimiento de la calidad de los datos, el uso eficiente de los recursos tecnológicos, la optimización del consumo de infraestructura y de los servicios asociados a la plataforma, el aprovechamiento eficiente de la capacidad instalada y la generación de capacidades que contribuyan al aprovechamiento estratégico de la información institucional para apoyar la toma de decisiones y el cumplimiento de la misión del ICBF.

6.9.4.4 REQUERIMIENTOS DEL SERVICIO

El Contratista deberá prestar el servicio de **BIG-DATA** cumpliendo, como mínimo, los siguientes requerimientos operativos:

Administración de la Plataforma Big Data
El Contratista deberá:

- Administrar, operar, monitorear y mantener la plataforma Big Data y Analítica del ICBF durante la ejecución del contrato, garantizando la continuidad y disponibilidad del servicio de conformidad con los Acuerdos de Niveles de Servicio (ANS).
- Instalar, configurar, parametrizar, actualizar y optimizar los componentes tecnológicos que conforman la plataforma Big Data y Analítica.
- Administrar los ambientes de Desarrollo, Pruebas, Calidad y Producción cuando apliquen.
- Ejecutar actividades de mantenimiento preventivo, correctivo y evolutivo de los componentes administrados.
- Gestionar incidentes, problemas, cambios y requerimientos conforme a las prácticas ITIL adoptadas por el ICBF.
- Monitorear permanentemente el estado, disponibilidad, capacidad, desempeño y utilización de los componentes administrados.
- Mantener actualizados los componentes tecnológicos conforme a las recomendaciones del fabricante y las políticas institucionales.
- Presentar recomendaciones para mejorar la disponibilidad, estabilidad, capacidad y desempeño de la plataforma.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Integración de Datos (ETL y ELT)

El Contratista deberá:

- Administrar, operar y monitorear los procesos de extracción, transformación y carga de datos (ETL y ELT).
- Administrar y monitorear los procesos de integración y orquestación de datos.
- Verificar periódicamente la correcta ejecución de los procesos de integración.
- Identificar, analizar y corregir oportunamente las fallas presentadas durante la ejecución de los procesos ETL y ELT.
- Optimizar los tiempos de procesamiento y ejecución de las cargas de datos.
- Garantizar la trazabilidad de los procesos ejecutados.
- Implementar controles para garantizar la integridad de la información durante los procesos de integración.
- Documentar los procesos implementados, modificados o retirados.
- Generar informes periódicos sobre el estado y desempeño de los procesos de integración.

Data Lake, Data Warehouse y Repositorios Analíticos

El Contratista deberá:

- Administrar, operar, monitorear y mantener los componentes de almacenamiento analítico que conforman la plataforma Big Data y Analítica del ICBF.
- Administrar los componentes Data Lake, Data Warehouse y demás repositorios analíticos implementados por el ICBF o que sean incorporados durante la ejecución del contrato.
- Garantizar la disponibilidad, integridad y consistencia de la información almacenada.
- Administrar la capacidad y el crecimiento de los repositorios analíticos.
- Monitorear permanentemente el desempeño y utilización del almacenamiento analítico.
- Ejecutar actividades de mantenimiento preventivo y correctivo sobre los componentes administrados.
- Optimizar el desempeño de consultas y procesos analíticos.
- Atender incidentes, problemas y requerimientos relacionados con los componentes administrados.
- Apoyar las actividades de migración, actualización y evolución tecnológica de los componentes cuando sean requeridas por el ICBF.
- Generar recomendaciones para optimizar el desempeño y utilización de los repositorios analíticos.

Analítica e Inteligencia de Negocios

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

El Contratista deberá:

- Administrar los componentes de inteligencia de negocios, analítica y visualización de información que conforman la plataforma Big Data y Analítica del ICBF.
- Garantizar la disponibilidad y correcto funcionamiento de los componentes de explotación y visualización de la información.
- Brindar soporte técnico especializado a los componentes de analítica e inteligencia de negocios administrados.
- Administrar los procesos asociados a la generación de indicadores e información analítica.
- Apoyar técnicamente la implementación, operación y mantenimiento de modelos analíticos cuando sean requeridos por el ICBF.
- Optimizar el desempeño de los componentes de analítica.
- Gestionar la disponibilidad de los servicios asociados a la explotación de la información.
- Atender incidentes y requerimientos relacionados con los componentes analíticos.

Calidad de Datos

El Contratista deberá:

- Implementar mecanismos para validar la completitud, consistencia, unicidad e integridad de los datos administrados.
- Ejecutar controles de validación sobre los procesos de integración de datos.
- Identificar inconsistencias que afecten la calidad de la información.
- Gestionar incidentes relacionados con la calidad de los datos.
- Generar informes periódicos sobre el estado de la calidad de los datos.
- Presentar recomendaciones para mejorar la calidad de la información institucional.
- Apoyar la implementación de controles de calidad definidos por el ICBF.
- Mantener registro de las incidencias y acciones correctivas implementadas.

Seguridad de la Plataforma

El Contratista deberá:

- Implementar los controles de seguridad aplicables a la plataforma Big Data.
- Administrar usuarios, perfiles y privilegios de acceso conforme a las políticas institucionales.
- Gestionar el acceso a los componentes administrados de acuerdo con los lineamientos definidos por el ICBF.
- Mantener la trazabilidad de las actividades realizadas sobre la plataforma.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Integrar, cuando aplique, los registros de eventos (logs) con las herramientas institucionales de monitoreo y seguridad.
- Gestionar vulnerabilidades identificadas en los componentes administrados.
- Apoyar la gestión de riesgos asociados a la plataforma Big Data.
- Aplicar las políticas de seguridad de la información definidas por el ICBF.
- Implementar las acciones correctivas derivadas de auditorías técnicas relacionadas con el servicio.

Respaldo y Continuidad del Servicio

El Contratista deberá:

- Garantizar la ejecución de los procesos de respaldo definidos para los componentes administrados.
- Verificar periódicamente la correcta ejecución de los respaldos.
- Realizar pruebas periódicas de restauración conforme al plan de continuidad definido por el ICBF.
- Mantener actualizados los procedimientos de recuperación.
- Apoyar la ejecución de pruebas de continuidad y recuperación del servicio.
- Garantizar la disponibilidad de la información respaldada.
- Implementar acciones para minimizar el impacto de incidentes que afecten la continuidad del servicio.
- Gestionar los procesos de recuperación cuando se presenten contingencias que afecten la operación.

Documentación Técnica y Operativa

El Contratista deberá:

- Mantener actualizado el inventario de componentes Big Data.
- Mantener actualizados los diagramas de arquitectura de la plataforma.
- Documentar las configuraciones y parametrizaciones de los componentes administrados.
- Mantener actualizados los procedimientos operativos del servicio.
- Documentar los procesos ETL y ELT implementados.
- Mantener actualizados los manuales técnicos de administración y operación.
- Documentar las modificaciones realizadas sobre la plataforma.
- Gestionar el control de versiones de configuraciones y componentes.
- Mantener actualizadas las bitácoras operativas del servicio.
- Elaborar y actualizar la documentación requerida para la transferencia de conocimiento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Optimización y Mejora Continua

El Contratista deberá:

- Implementar acciones de mejora continua sobre la plataforma Big Data y Analítica.
- Optimizar el desempeño de los componentes administrados.
- Promover el uso eficiente de los recursos tecnológicos.
- Optimizar el consumo de infraestructura y de los servicios asociados a la plataforma.
- Implementar acciones orientadas al aprovechamiento eficiente de la capacidad instalada.
- Optimizar los tiempos de procesamiento y respuesta de la plataforma.
- Automatizar procesos operativos cuando resulte técnica y operativamente viable.
- Identificar oportunidades de mejora tecnológica y funcional de la plataforma.
- Presentar recomendaciones orientadas a mejorar la disponibilidad, desempeño, capacidad y eficiencia operativa del servicio.
- Proponer iniciativas que contribuyan a la evolución tecnológica y al fortalecimiento de la plataforma Big Data y Analítica del ICBF.

6.9.5 INTEGRACION DE SERVICIOS

6.9.5.1 GENERALIDADES DEL SERVICIO:

El ICBF cuenta con diversos sistemas de información, bases de datos, plataformas tecnológicas y servicios digitales que soportan los procesos misionales y administrativos de la entidad. Estos sistemas operan sobre diferentes arquitecturas tecnológicas, incluyendo plataformas tradicionales, servicios en nube, microservicios, contenedores, plataformas de integración y tecnologías de procesamiento y explotación de datos como Big Data.

El servicio de Integración de Servicios tiene como propósito asegurar la interoperabilidad y comunicación entre estos componentes tecnológicos, garantizando el intercambio de información entre sistemas, aplicaciones, plataformas de datos y servicios tecnológicos.

Este servicio incluye la administración y monitoreo de los mecanismos de integración entre sistemas, la gestión de flujos de datos entre plataformas tecnológicas, la integración entre entornos On-Premise y Cloud, así como la integración de fuentes de información que soportan procesos de analítica institucional, procesamiento de datos y generación de información para la toma de decisiones.

6.9.5.2 ALCANCE

El ICBF requiere que el Contratista realice la administración, diseño, gestión, operación, monitoreo (7X24X365) y mantenimiento del servicio de integración de datos y explotación

analítica, garantizando la interoperabilidad entre los sistemas de información, plataformas tecnológicas y repositorios de datos de la entidad.

Dentro del alcance del servicio se incluye la gestión y monitoreo de los procesos de integración y procesamiento de datos, el control de calidad de la información, el seguimiento al uso y aprovechamiento de los datos institucionales, la administración de datasets preparados para análisis y la generación de indicadores y tableros de control que soporten la operación y la toma de decisiones del ICBF.

Así mismo, el servicio contempla la actualización permanente del inventario de activos de información y datasets utilizados para explotación analítica, la gestión de incidentes asociados a la disponibilidad o calidad de los datos, la incorporación de nuevas fuentes de información o servicios de datos que se requieran integrar durante la ejecución del contrato y la formulación de iniciativas de mejora orientadas al aprovechamiento de la información institucional.

6.9.5.3 LINEA BASE DEL SERVICIO

La línea base del servicio de Integración de Servicios y explotación de datos corresponde al estado inicial de los sistemas de información, repositorios de datos, datasets, mecanismos de integración y procesos de procesamiento de datos existentes en el ICBF al momento del inicio de la operación del contrato.

Esta línea base deberá incluir como mínimo:

- Inventario de sistemas de información institucionales que generan o consumen datos para procesos operativos o analíticos.
- Inventario de bases de datos, repositorios de información y plataformas de almacenamiento utilizadas por la entidad.
- Inventario de datasets institucionales disponibles para procesos de análisis o explotación de información.
- Identificación de los procesos de ingesta y procesamiento de datos existentes (ETL, ELT u otros mecanismos de integración).
- Identificación de los flujos de datos entre sistemas de información, plataformas tecnológicas y repositorios de datos.
- Identificación de herramientas o plataformas utilizadas para análisis de información y visualización de datos.
- Identificación de los indicadores y tableros de control existentes que utilizan información institucional.

El Contratista deberá validar, documentar y mantener actualizada la línea base del servicio durante la ejecución del contrato, incorporando las nuevas integraciones, datasets o servicios de datos que se implementen durante la operación.

6.9.5.4 REQUERIMIENTOS DEL SERVICIO

Para la prestación del servicio de Integración de Servicios y explotación de datos institucionales, el Contratista deberá cumplir como mínimo con los siguientes requerimientos:

- Mantener actualizado el inventario de activos de información, fuentes de datos, repositorios y datasets utilizados para procesos de explotación analítica, asegurando su documentación, clasificación, responsables y periodicidad de actualización.
- Realizar el monitoreo periódico de la calidad de los datos institucionales, evaluando criterios como completitud, consistencia, duplicidad e integridad de la información, e identificar hallazgos y recomendaciones de mejora.
- Administrar y monitorear los procesos de ingesta y procesamiento de datos institucionales, incluyendo la ejecución de procesos ETL/ELT u otros mecanismos de integración, verificando su correcta ejecución, tiempos de procesamiento, volúmenes procesados y posibles fallos o reprocesos.
- Realizar seguimiento al uso y explotación de los datos institucionales, identificando los datasets más utilizados, niveles de consumo de información, consultas realizadas y servicios de datos utilizados por las diferentes dependencias del ICBF.
- Monitorear el desempeño y capacidad del repositorio analítico o plataforma de almacenamiento de datos, evaluando el crecimiento de los volúmenes de información, el uso de almacenamiento y el rendimiento de consultas y procesos analíticos.
- Gestionar y reportar los incidentes relacionados con la disponibilidad, integridad o procesamiento de los datos institucionales, tales como pérdidas de información, duplicidad de datos, fallas de carga o indisponibilidad de servicios de datos.
- Diseñar e implementar procesos de integración para nuevas fuentes de información o datasets que deban incorporarse a los procesos de explotación de datos institucionales.
- Generar indicadores derivados del análisis de datos institucionales que permitan evaluar el comportamiento de variables relevantes para la operación del ICBF, incluyendo análisis comparativos y recomendaciones para la toma de decisiones.
- Diseñar, implementar o actualizar tableros de control analíticos que permitan visualizar indicadores, tendencias y comportamiento de la información institucional mediante herramientas de análisis o visualización de datos utilizadas por la entidad.
- Administrar y mantener actualizado el inventario de datasets preparados para procesos de análisis, incluyendo la documentación de su origen, estructura, periodicidad de actualización y responsables.
- Elaborar y presentar el plan mensual de actividades del servicio de gestión, integración y explotación de datos institucionales, incluyendo las actividades programadas, responsables, cronograma y entregables asociados.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Formular propuestas de iniciativas, mejoras o productos de datos orientados al aprovechamiento de la información institucional, optimización de procesos de datos o generación de analítica que apoye la toma de decisiones del ICBF.

6.9.6 HERRAMIENTAS DE GESTIÓN, MONITOREO, ANALÍTICA DE DATOS (POWER BI), GESTIÓN DE DISPOSITIVOS (INTUNE), AZURE ARC Y GESTIÓN DE ITSM.

El ICBF cuenta con herramientas específicas de las plataformas y soluciones de la infraestructura tecnológica institucional para la gestión, administración y monitoreo centralizado de servidores, estaciones de trabajo, dispositivos y servicios tecnológicos, incluyendo soluciones de almacenamiento, respaldo, seguridad y control operativo. Agregar la entrega de una herramienta de monitoreo que será de propiedad del instituto.

Gran parte de la infraestructura operativa del ICBF, tanto a nivel de sistemas operativos como de aplicaciones, se encuentra basada en plataformas Microsoft. Para tal efecto, la Entidad ha adquirido y mantiene licenciamiento de soluciones como Microsoft System Center, Azure Operations Management Suite (AOMS) y Microsoft Intune, las cuales permiten la gestión, monitoreo, control, aseguramiento y administración integral de la infraestructura tecnológica, los dispositivos y los usuarios, tanto en entornos locales como en la nube.

El servicio comprende la gestión de los mecanismos de integración entre aplicaciones, bases de datos y plataformas tecnológicas, incluyendo entornos On-Premise y Cloud, así como la administración de procesos de ingesta, procesamiento y disposición de datos utilizados para la explotación analítica institucional.

Asimismo, la Entidad dispone de la plataforma como herramienta de **Gestión de Servicios de TI (ITSM)** para el soporte, control y operación centralizada de los procesos de la mesa de servicio. Esta solución habilita la gobernanza tecnológica institucional bajo el marco de buenas prácticas de ITIL, permitiendo la automatización, registro, seguimiento y resolución de incidentes, requerimientos, problemas, cambios, gestión de la configuración (CMDB) y control estricto de los niveles de servicio (SLA).

Asimismo, considerando la estrategia de transformación digital, modernización tecnológica y adopción de servicios híbridos y en la nube de la Entidad, resulta necesario fortalecer las capacidades de administración, automatización y actualización de la infraestructura tecnológica mediante el aprovechamiento de las plataformas Microsoft Intune y Microsoft Azure Arc.

En este contexto, Microsoft Intune se constituye como la plataforma estratégica para la gestión moderna de dispositivos (Modern Device Management), permitiendo la administración centralizada de estaciones de trabajo, equipos móviles y dispositivos

corporativos, independientemente de su ubicación física o conexión a la red institucional. A través de esta solución, la Entidad requiere la implementación, administración y mejora continua de políticas de seguridad, cumplimiento normativo, configuración de dispositivos, distribución de aplicaciones corporativas, control de actualizaciones del sistema operativo y adopción de modelos de actualización basados en Windows Update for Business.

En consecuencia, el Contratista deberá garantizar la planeación, implementación, administración y optimización de las políticas de actualización administradas desde Microsoft Intune, incluyendo la definición de anillos de despliegue (deployment rings), grupos piloto, validación previa de actualizaciones, automatización de ventanas de mantenimiento, monitoreo de cumplimiento, remediación de incidentes asociados a actualizaciones fallidas y generación de reportes de adopción y cumplimiento, procurando minimizar riesgos operativos y garantizar la continuidad de los servicios institucionales.

De igual forma, el ICBF dispone de entornos híbridos compuestos por servidores alojados tanto en centros de datos institucionales como en plataformas de nube pública. Para la administración unificada de dichos recursos, se requiere el aprovechamiento de Microsoft Azure Arc como plataforma de gobierno, administración y operación de servidores físicos y virtuales, independientemente de su ubicación.

En este sentido, el Contratista deberá implementar y administrar las capacidades de Azure Arc para la incorporación, administración y monitoreo centralizado de servidores Windows y Linux, facilitando la aplicación homogénea de configuraciones, controles de cumplimiento, inventario tecnológico, administración de recursos híbridos y automatización de procesos operativos.

Adicionalmente, se requiere la utilización de Azure Update Manager y las capacidades de automatización asociadas a Azure Arc para la gestión integral del ciclo de vida de actualizaciones de servidores, permitiendo la evaluación de cumplimiento, programación de despliegues, ejecución de actualizaciones en ventanas controladas, verificación de estados posteriores a la instalación y generación de reportes consolidados. Estas capacidades deberán complementar y, cuando sea técnicamente viable y autorizado por la Entidad, reemplazar progresivamente los esquemas tradicionales de administración de actualizaciones basados en WSUS, con el fin de adoptar modelos modernos de gestión orientados a servicios híbridos y entornos distribuidos.

Igualmente, el Contratista deberá implementar mecanismos de automatización mediante Azure Automation, Azure Policy, Update Manager, PowerShell, Runbooks y demás herramientas nativas del ecosistema Microsoft, orientados a reducir actividades operativas manuales, mejorar la eficiencia de los procesos de administración, fortalecer los controles de seguridad, asegurar la estandarización de configuraciones y optimizar la gestión del ciclo de vida de los activos tecnológicos administrados.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Las actividades asociadas a Microsoft Intune, Azure Arc y las soluciones de automatización deberán contemplar labores de diseño, implementación, administración, soporte, monitoreo, optimización, transferencia de conocimiento, documentación técnica y actualización permanente de procedimientos operativos, garantizando la alineación con las mejores prácticas de Microsoft, los lineamientos institucionales, los requerimientos de seguridad de la información y los Acuerdos de Nivel de Servicio (ANS) definidos por la Entidad.

Finalmente, y como parte integral del servicio de gestión y monitoreo de la infraestructura tecnológica, el ICBF requiere el uso de Microsoft Power BI como herramienta de analítica, visualización y control, orientada a la construcción, administración, actualización y mantenimiento de tableros de control que consoliden la información generada por la herramienta principal de monitoreo y demás fuentes técnicas del servicio. Dichos tableros deberán permitir la visualización en tiempo real y el análisis histórico del cumplimiento de los Acuerdos de Nivel de Servicio (ANS), la disponibilidad, desempeño y capacidad de los servicios de infraestructura, así como facilitar el seguimiento, control y toma de decisiones por parte de las áreas técnicas y de supervisión del ICBF, constituyéndose en un insumo fundamental para el control operativo y contractual del servicio.

El alcance del servicio comprende el uso, implementación, configuración, administración y operación de las herramientas de gestión y monitoreo de los servicios TIC del ICBF, así como la instalación, parametrización y gestión de las herramientas necesarias para el monitoreo, control y administración de los recursos tecnológicos centralizados y distribuidos de la Entidad, las cuales deberán estar en capacidad de monitorear y gestionar el cien por ciento (100 %) de la infraestructura tecnológica del ICBF.

En este contexto, el Contratista deberá suministrar, implementar y poner en operación una herramienta de gestión y monitoreo centralizada, la cual será la herramienta principal y obligatoria para el seguimiento de los servicios TIC, la medición de los Acuerdos de Nivel de Servicio (ANS), la verificación del cumplimiento contractual y la generación de reportes oficiales de desempeño. Dicha herramienta deberá cubrir de manera integral los recursos tecnológicos del ICBF y no dependerá de las herramientas actualmente licenciadas por la Entidad para su operación principal.

El monitoreo y la gestión de los servicios TIC del ICBF deberán permitir, como mínimo, la observación y control de la disponibilidad de los hosts, así como de variables tales como desempeño, latencia, frecuencias, contadores, capacidades, utilización de recursos y eventos operativos, entre otros parámetros técnicos necesarios para garantizar la adecuada operación de la infraestructura tecnológica.

Para el ICBF, se entienden como Puntos Finales (Endpoints) todos los equipos y/o dispositivos que cuenten con conexión a la red institucional, incluyendo, entre otros: computadores, dispositivos móviles, equipos de red, servidores físicos y virtuales,

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

impresoras, sistemas de climatización con conectividad de red, UPS, y demás dispositivos que sean propiedad del ICBF o que se encuentren al servicio de la Entidad. Dichos endpoints deberán ser gestionados y monitoreados de manera centralizada, incluyendo aquellos administrados mediante Microsoft Intune, como plataforma de gestión unificada de dispositivos y aplicaciones (MDM/MAM).

Para el seguimiento de los eventos que ocurren sobre los diferentes objetos de los servicios TIC, se hará uso de la herramienta principal de gestión y monitoreo suministrada por el Contratista, la cual deberá proporcionar visibilidad completa del estado operativo de los recursos tecnológicos del ICBF, permitiendo la atención oportuna y eficiente de incidentes, problemas y eventos durante la operación del servicio.

Como parte integral del alcance del servicio, el Contratista deberá diseñar, construir, administrar, actualizar y mantener tableros de control en Microsoft Power BI, orientados a la visualización, seguimiento y análisis del cumplimiento de los Acuerdos de Nivel de Servicio (ANS) y del desempeño de los servicios de infraestructura tecnológica. Dichos tableros deberán consolidar la información proveniente de la herramienta principal de monitoreo y demás fuentes técnicas del servicio, permitiendo el análisis en tiempo real e histórico y constituyéndose en un insumo oficial para la supervisión, control y toma de decisiones contractuales por parte del ICBF.

Para el adecuado soporte de los procesos de analítica y visualización definidos en el presente servicio, el Contratista deberá contar con conocimientos en Python, orientados al tratamiento, transformación, validación y preparación de datos, que permitan complementar la construcción y mantenimiento de los tableros de Microsoft Power BI, especialmente en escenarios que requieran automatización de cálculos, depuración de información, integración de múltiples fuentes y fortalecimiento de la calidad de los datos utilizados para la medición y control de los Acuerdos de Nivel de Servicio (ANS).

Actualmente, el ICBF cuenta con las siguientes herramientas de gestión y monitoreo, las cuales no constituyen la plataforma principal, pero se mantendrán como herramientas complementarias y de respaldo:

Microsoft System Center, licenciado para los siguientes módulos:

- Configuration Manager + Endpoint Protection + WSUS (Implementado)
- Service Manager (No implementado)
- Operations Manager – SCOM (Implementado)
- Virtual Machine Manager (Implementado)
- Data Protection Manager (No implementado)
- Orchestrator (Implementado)

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Azure Operations Management Suite (AOMS).
Microsoft Intune.
Azure ARC.
Power BI

Adicionalmente, se encuentran en operación Microsoft WSUS para la administración de actualizaciones y KMS para la administración del licenciamiento, con el propósito de consultar, contrastar o verificar información específica cuando se requiera, sin perjuicio de que la herramienta suministrada por el Contratista sea la única plataforma válida para la medición de ANS y el seguimiento del cumplimiento contractual.

6.9.6.1 REQUERIMIENTOS DEL SERVICIO

Las herramientas suministradas por el Contratista, así como aquellas de propiedad del ICBF que se mantengan como complementarias o de respaldo, destinadas al ejercicio de administración, mantenimiento y operación de la infraestructura tecnológica, deberán permitir, como mínimo, el cumplimiento de los siguientes requerimientos funcionales y técnicos:

Requerimientos generales de la herramienta

- Garantizar la gestión y el monitoreo de la infraestructura tecnológica del ICBF desde el primer día de la operación, mediante la herramienta principal de gestión y monitoreo suministrada por el Contratista, asegurando la cobertura del cien por ciento (100 %) de los servicios y componentes incluidos en el alcance del contrato.
- Garantizar que la herramienta principal de monitoreo permita la gestión integral de todos los elementos de la infraestructura tecnológica del ICBF. En caso de requerirse herramientas complementarias para fines específicos de integración o soporte técnico, el Contratista deberá unificar la información y los resultados, de manera que la evidencia del monitoreo, la gestión y el cumplimiento de los ANS sea centralizada, homogénea y trazable, sin fragmentación de la información.Administrar y operar los módulos de Microsoft System Center y Azure Operations Management Suite (AOMS) que se encuentren disponibles en el ICBF, exclusivamente como herramientas complementarias y de respaldo, garantizando su correcta operación, integración y alineación con los procedimientos y lineamientos definidos por el ICBF. Toda configuración, ajuste o información generada sobre estas plataformas será propiedad del ICBF y deberá ser entregada debidamente documentada al finalizar el contrato. Definir, administrar y monitorear las políticas de actualización de parches para servidores, estaciones de trabajo y demás dispositivos actualizables, utilizando WSUS, Microsoft Intune o las herramientas que el ICBF disponga, con el fin de mantener actualizados y seguros los sistemas operativos y componentes tecnológicos durante la ejecución del contrato.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Garantizar el correcto funcionamiento de WSUS, integrado con las herramientas de gestión del ICBF, durante toda la ejecución del contrato, asegurando la correcta distribución y control de las actualizaciones de software.
- Presentar informes mensuales consolidados sobre la gestión y el estado de las herramientas de gestión y monitoreo, incluyendo resultados de operación, eventos relevantes, disponibilidad de servicios y cumplimiento de los ANS.
- Elaborar, actualizar y mantener toda la documentación técnica y operativa relacionada con el servicio de herramientas de gestión y monitoreo, la cual deberá ser almacenada en los repositorios que el ICBF designe para tal fin.
- Utilizar las herramientas propiedad del ICBF, tales como System Center, AOMS e Intune, de manera complementaria, cuando aplique, asegurando su correcta integración con la herramienta principal de monitoreo suministrada por el Contratista, sin que dichas herramientas sustituyan la plataforma principal definida para la medición de ANS y el control contractual.
- Implementar, optimizar o actualizar, cuando sea requerido por el ICBF, las configuraciones técnicas y operativas de las herramientas complementarias del ICBF, garantizando su alineación con las necesidades de la infraestructura tecnológica y con el modelo de operación definido en el presente documento.
- Garantizar que la herramienta principal de monitoreo permita resolver los requerimientos definidos en el presente anexo técnico de manera nativa o mediante integraciones certificadas por el fabricante. Cualquier integración, ajuste o configuración deberá quedar debidamente documentada y alineada con los servicios y contratos vigentes del ICBF.Suministrar las herramientas adicionales que resulten necesarias para el cumplimiento del presente contrato, siempre que se evidencie técnicamente que las herramientas propiedad del ICBF no cubren un requerimiento específico. Dichas herramientas deberán integrarse con la herramienta principal y su uso no afectará la centralización de la información ni la medición de los ANS.
- Suministrar y administrar toda la infraestructura, licenciamiento, bases de datos, sistemas operativos y recursos físicos o lógicos necesarios para el funcionamiento de las herramientas que sean propiedad del Contratista. Las herramientas suministradas deberán ser de uso exclusivo del ICBF durante la ejecución del contrato.Administrar y operar las herramientas de gestión que actualmente se encuentran implementadas en el ICBF, en calidad de herramientas complementarias o de respaldo, garantizando su disponibilidad y correcta articulación con la herramienta principal de monitoreo.
- Garantizar que la herramienta principal suministrada por el Contratista cubra la totalidad de los requerimientos técnicos y funcionales definidos en el presente documento, sin dependencia operativa de las herramientas del ICBF para la medición de ANS y el seguimiento contractual.
- Diseñar, implementar, administrar y actualizar los tableros de control solicitados por el ICBF, utilizando Microsoft Power BI, orientados a la visualización del estado de los servicios, el desempeño de la infraestructura y el cumplimiento de los Acuerdos

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

de Nivel de Servicio (ANS), y publicarlos a través de los medios o dispositivos que el ICBF defina.Permitir la generación de notificaciones y alarmas en tiempo real, integradas con la Mesa de Servicios del ICBF, para la creación automática de tickets y la notificación al personal designado por la Entidad.

- Programar y ejecutar transferencias de conocimiento dirigidas al personal designado por el ICBF, relacionadas con la operación de la herramienta principal de monitoreo, Microsoft Intune, Power BI y las herramientas complementarias utilizadas durante la ejecución del contrato. Dichas transferencias deberán realizarse de manera periódica y documentada.Gestionar la administración y el monitoreo de todos los ítems definidos en el capítulo de herramientas de gestión y monitoreo del presente documento, garantizando esquemas de monitoreo centralizados, personalizables y accesibles, a través de la herramienta principal suministrada por el Contratista.
- Garantizar la alta disponibilidad, continuidad operativa y respaldo de la herramienta principal de gestión y monitoreo suministrada por el Contratista, de tal forma que la indisponibilidad de esta no afecte la medición de ANS ni el seguimiento contractual.
- Alinear la operación de las herramientas de monitoreo, gestión de endpoints y Power BI con las políticas de seguridad de la información, control de accesos y clasificación de la información del ICBF, garantizando el principio de mínimo privilegio.

Requerimientos generales de gestión y monitoreo

- Ejecución de acciones de notificación automáticas e inmediatas ante la aparición de condiciones de anormalidad que afecten la prestación de los servicios TIC.
- Acceso remoto seguro que permita configurar, administrar, consultar el estado del monitoreo en tiempo real y generar reportes, conforme a los perfiles definidos por el ICBF.
- Implementación de mecanismos de autenticación segura, incluyendo cifrado de credenciales y control de accesos.
- Capacidad de integración con el Directorio Activo u otros servicios de identidad institucionales para la gestión de accesos.
- Capacidad de integración con la Mesa de Servicios, permitiendo la creación automática de tickets ante la generación de eventos, alertas o incidentes.
- Generación de reportes de auditoría, operación y desempeño a través de consolas de administración, las cuales deberán estar disponibles para el ICBF de acuerdo con los perfiles definidos por la DIT, con el fin de soportar el seguimiento, control y supervisión contractual.
- Generación de tableros de control (dashboards) por cada uno de los servicios monitoreados y por cada Acuerdo de Nivel de Servicio (ANS) definido.
- De manera complementaria, el Contratista deberá diseñar, construir, administrar, actualizar y mantener tableros de control en Microsoft Power BI, los cuales deberán consolidar la información proveniente de la herramienta principal de monitoreo y demás fuentes técnicas del servicio, permitiendo la visualización en tiempo real y el análisis histórico del cumplimiento de los ANS, así como el seguimiento al

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

desempeño, disponibilidad y capacidad de los servicios de infraestructura. Dichos tableros constituirán un insumo oficial para el control operativo, la supervisión contractual y la toma de decisiones por parte del ICBF.

- Contar con un Centro de Monitoreo y Gestión encargado del monitoreo y atención de primer nivel de cualquier tipo de incidente que se presente en las plataformas de servicios.
- Monitorear los servicios en tiempo real por medio de herramientas automatizadas propias del ICBF y/o Contratista que envíen notificaciones a la herramienta de Mesa de servicio de acuerdo con su nivel de criticidad y cuya información permita generar acciones proactivas.
- Monitorear7X24X365 los recursos de los servidores de las aplicaciones, bases de datos y servicios, identificar disponibilidad e indisponibilidad, tiempos de respuesta y desempeño de cada aplicación. Emitir recomendaciones mensualmente para la optimización, realizar diagnósticos y análisis de seguimiento
- Generar alertas automáticas dirigidas al personal del ICBF bajo determinados eventos. El personal al que se le deben enviar las alertas y el tipo de eventos que las generan serán determinados por el ICBF en la Etapa de Transición y podrán ser modificadas en cualquier etapa del proyecto.
- Configurar las acciones automáticas ante caídas del servicio, mediante envío de popup, e-mail, mensajes de consola, etc. El personal designado por el ICBF deberá recibir mensajes de notificación a los teléfonos móviles (Mensajería Instantánea, Email), cuando se presenten caídas de los Servicios.
- Monitorear el uso de recursos lógicos de los dispositivos a través de los agentes activos instalados para tal efecto.
- Identificar en forma temprana posibles fallas en los sistemas y dispositivos de los servicios.
- Actuar de inmediato ante la aparición de incidentes o alarmas para buscar su solución. El CMG (Centro de Monitoreo y Gestión) constituye un primer nivel de atención y deberá generar un caso para atención de segundo nivel.
- Brindar Información al contratista de Mesa de Servicio y al ICBF en el caso de indisponibilidad de alguno de los servicios, de acuerdo con el procedimiento establecido para tal fin.
- Ejecutar y registrar la gestión realizada en la herramienta de Mesa de Servicio, frente a incidentes, problemas y cambios en el procesamiento, y cumplir con el escalamiento según corresponda y según lo especificado en el Manual de Procedimientos.
- Completar la categorización o recategorizar los incidentes asignados ya sea por Mesa de Servicio o por la Herramienta de gestión en caso de ser necesario.
- Aplicar los parches de mantenimiento de software preventivo y correctivo (parches, fixes o service packs) del software de monitoreo para corregir defectos.
- Definir y mantener actualizada, en asocio con ICBF, la lista de contactos para el escalamiento del servicio de monitoreo.
- Informar al contratista de mesa de servicio que administra la CMDB el ingreso de un nuevo hardware y software que soportan los sistemas de información del ICBF.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Requerimientos de contenerización, automatización y API management

El servicio comprende la gestión de los mecanismos para la contenerización de micorservicios, desplegados en clusters bien sea on-premise o en nube pública.

El servicio de API mnagement consiste en Instalar, configurar y mantener pasarelas de APIs, Diseñar Estrategias de APIs, Gestionar el Ciclo de Vida Completo, Asegurar la Seguridad y Cumplimiento, Soporte y Resolución de Problemas, impulsar la Automatización (CI/CD), Habitar la Estrategia de Integración, Capacitación y Liderazgo Técnico.

El servicio de automatización consiste en analizar los diferentes procesos para implementar y desarrollar soluciones de automatización. Además de actividades de mejoramiento y mantenimiento.

Requerimientos de Gestión y administración de endpoints

- Realizar la **gestión, administración y monitoreo de los Puntos Finales (Endpoints)** del ICBF que se encuentren dentro del alcance del Contrato, siempre que la naturaleza del dispositivo lo permita.
- Realizar el **control de la línea base de software** para servidores y equipos de cómputo.
- Realizar el **despliegue masivo o dirigido de software** en servidores y equipos de cómputo.
- realizar la **preparación y alistamiento masivo de equipos de cómputo**, incluyendo la creación y distribución centralizada de imágenes de sistemas operativos, de acuerdo con las características de cada tipo de equipo.
- Para los dispositivos de usuario final y equipos móviles, la gestión se realizará de manera complementaria mediante **Microsoft Intune**, como plataforma de **gestión unificada de dispositivos y aplicaciones (MDM/MAM)**, permitiendo la aplicación de políticas de seguridad, cumplimiento y control de configuraciones.
- Gestionar el monitoreo integral de todos los Puntos Finales (Endpoints) productivos, activos o de contingencia que el ICBF designe, a través de la herramienta principal de gestión y monitoreo suministrada por el Contratista, permitiendo la definición de esquemas de monitoreo centralizados, personalizables y accesibles, sin perjuicio del uso de herramientas complementarias propiedad del ICBF para fines específicos de gestión o verificación.
- Parametrizar. Administrar y monitorear todos los elementos activos, pasivos y de contingencia que se encuentren operativos en la infraestructura del ICBF, garantizando su correcta incorporación y seguimiento dentro de la herramienta principal de monitoreo, así como su integración con las herramientas complementarias que el ICBF disponga.
- Gestionar el descubrimiento automático de hardware y software de los Endpoints que el ICBF designe, asegurando que la información se almacene y actualice de

manera automática en la CMDB que se encuentre activa en la Entidad. Dicha base de datos deberá contener el detalle de cada ítem o elemento de configuración, permitir la relación entre activos, incidencias, problemas, cambios y demás datos del servicio de TI, y garantizar la disponibilidad de información completa, confiable y actualizada.

- Realizar el despliegue de aplicaciones, configuraciones, scripts y componentes de software a través de Microsoft System Center, Microsoft Intune u otras herramientas dispuestas por el ICBF, de acuerdo con los requerimientos operativos definidos por la Entidad.
- Ejecutar, con periodicidad trimestral, procesos de verificación que permitan identificar en servidores y equipos de usuario final la instalación de componentes de Microsoft SQL Server, indicando versión y edición, y presentar al ICBF un informe detallado de los equipos y servidores en los que se detecten dichas instalaciones.
- En caso de que el ICBF defina un cambio de plataforma de monitoreo, el Contratista deberá realizar la migración integral de los elementos de configuración, incluyendo activos, umbrales, reglas, eventos históricos, relaciones de la CMDB y demás componentes necesarios para garantizar la continuidad del servicio y la trazabilidad de la información.Presentar, cuando aplique, el contrato de adquisición y licenciamiento de las herramientas suministradas por el Contratista, garantizando que dichas herramientas cumplan con las normativas de derechos de autor y licenciamiento de software vigentes, y que su uso se encuentre debidamente autorizado durante la ejecución del contrato.

Requerimientos Monitoreo

- El Contratista deberá monitorear y administrar el licenciamiento del ICBF a través de las herramientas dispuestas por la Entidad para tal fin, tales como KMS Server, System Center y las demás herramientas que el ICBF adquiera durante la vigencia del Contrato.
- Administrar, monitorear y soportar el licenciamiento de los equipos servidores y estaciones de trabajo del ICBF, ya sean productivos, activos o de contingencia, utilizando la herramienta entregada por el ICBF System Center.

El Contratista deberá remitir informes mensuales de gestión de licenciamiento, que incluyan como mínimo:

- Software instalado por máquina.
- Gestión de listas negras de software no autorizado.
- Resultados del cruce entre software adquirido y software instalado.
- Uso de software licenciado por equipo.

Analítica, Visualización y Control de ANS (Power BI)

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Diseñar, construir, implementar, administrar, actualizar y mantener tableros de control en Microsoft Power BI, orientados a la visualización, seguimiento y análisis del cumplimiento de los Acuerdos de Nivel de Servicio (ANS) de todos los servicios de infraestructura tecnológica incluidos en el alcance del contrato.
- Garantizar que los tableros de Power BI consoliden información proveniente de la herramienta principal de monitoreo, así como de las demás fuentes técnicas que el ICBF autorice, asegurando la centralización, homogeneidad y trazabilidad de la información utilizada para la medición de los ANS.
- Asegurar que los tableros de Power BI permitan la visualización en tiempo real y el análisis histórico del desempeño de los servicios, incluyendo métricas de disponibilidad, desempeño, capacidad, eventos, incidentes y cumplimiento de ANS, conforme a los criterios definidos por el ICBF.
- Garantizar la calidad, integridad, consistencia y confiabilidad de los datos utilizados en los tableros de Power BI, de tal forma que la información presentada sea verificable, auditable y consistente con las fuentes técnicas de monitoreo y con los reportes contractuales.
- Configurar los tableros de Power BI de acuerdo con los roles, perfiles y niveles de acceso definidos por el ICBF, garantizando el principio de mínimo privilegio, la protección de la información y el cumplimiento de las políticas de seguridad de la Entidad.
- Permitir la exportación de información, gráficos y datasets desde Power BI en formatos estándar (CSV, Excel, PDF u otros que defina el ICBF), con el fin de soportar procesos de auditoría, supervisión contractual, análisis externo y atención a entes de control.
- Garantizar la actualización periódica y automática de los tableros de Power BI, de acuerdo con la criticidad de los servicios y los requerimientos de medición de los ANS, evitando desalineaciones entre la información visualizada y la operación real del servicio.
- Gestionar el versionamiento, control de cambios y trazabilidad de los tableros, métricas, visualizaciones y modelos de datos en Power BI, asegurando que toda modificación relevante cuente con justificación técnica y quede debidamente documentada.
- Brindar soporte técnico y funcional a los tableros de Power BI durante toda la ejecución del contrato, incluyendo ajustes, correcciones, optimizaciones y adecuaciones requeridas por el ICBF para reflejar cambios en los ANS, en los servicios o en la infraestructura tecnológica.
- Garantizar que los tableros de Power BI constituyan un insumo oficial para la supervisión, seguimiento y control contractual, de tal forma que la información allí presentada sea utilizada como referencia para la evaluación del desempeño del servicio y el cumplimiento de los ANS.
- Realizar transferencias de conocimiento al personal designado por el ICBF sobre la operación, interpretación, administración y uso de los tableros de Power BI, incluyendo modelos de datos, métricas de ANS y buenas prácticas de análisis.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Al finalizar el contrato, entregar al ICBF la documentación técnica y funcional de los tableros de Power BI, incluyendo estructura de datasets, métricas, cálculos, fuentes de información y configuraciones, garantizando la continuidad operativa y la independencia tecnológica de la Entidad.

Herramienta ITSM

El administrador de la plataforma ITSM del ICBF debe garantizar el cumplimiento de las siguientes especificaciones para la prestación del servicio:

1. Gestión de Disponibilidad, Rendimiento y Reglas de Negocio

- **Monitoreo de Alta Disponibilidad:** El proveedor deberá supervisar activamente que la plataforma ITSM mantenga la disponibilidad de operación continua del 99.9% (7x24x365). Ante cualquier interrupción del servicio, activará proactivamente los planes de contingencia operativos de la mesa de servicio y reportará la anomalía de forma inmediata.

- **Control y Optimización de Tiempos de Respuesta:** El proveedor será responsable de realizar las configuraciones lógicas, depuraciones de datos y limpiezas de caché permitidas por la herramienta para garantizar que la interfaz de usuario, las consultas y los reportes operen bajo estándares de baja latencia.

- **Automatización de Reglas de Negocio:** El proveedor debe parametrizar y mantener actualizadas dentro de la herramienta las reglas de asignación automática, los flujos de aprobación, las plantillas de notificación por correo electrónico y los árboles de decisión requeridos para la operación.

- **Cargue de Matrices de Niveles de Servicio (SLA):** El proveedor debe configurar en la herramienta los tiempos acordados de respuesta y solución para cada tipo de incidente o requerimiento, habilitando las alertas tempranas visuales o automáticas que ofrece la aplicación.

2. Seguridad, Gestión de Accesos y Privacidad de la Información

- **Control de Accesos Basado en Roles (RBAC):** El proveedor debe parametrizar, ejecutar la creación, modificación y desactivación de cuentas de usuario dentro de la plataforma, administrando de manera estricta la matriz de perfiles y permisos granulares (Administrador, Supervisor, Especialista, Agente y Usuario Final), asegurando que el acceso a la información confidencial esté restringido según las funciones autorizadas.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- **Vigilancia de Seguridad y Cifrado:** El proveedor debe verificar que se apliquen y mantengan activas las políticas de seguridad digital de la herramienta respecto al cifrado de datos en tránsito (HTTPS/TLS) y en reposo, custodiando la confidencialidad de la información y reportando cualquier riesgo al ICBF.

- **Cumplimiento de Protección de Datos Personales:** El proveedor velará por que todas las parametrizaciones de formularios, captura de datos y tratamiento de la información que cumplan estrictamente con la normativa colombiana.

3. Interfaz, Experiencia de Usuario e Integración Analítica

- **Aseguramiento de Acceso Multicanal:** El proveedor validará y dará soporte funcional para que el ingreso a la plataforma se realice de forma estándar a través de navegadores web compatibles (Edge, Chrome, Firefox) y dispositivos móviles, reportando al fabricante fallas de compatibilidad en las actualizaciones.

- **Modelado y Conexión de Datos (Power BI):** El proveedor debe construir las consultas, extraer los reportes de datos y habilitar los conectores o vistas permitidas por la herramienta ITSM para alimentar y actualizar de forma automatizada los tableros analíticos de Microsoft Power BI del ICBF.

4. Diseño, Estructuración y Gestión del Catálogo de Servicios

- **Definición y Modelado del Catálogo:** El proveedor debe diseñar, estructurar e implementar técnicamente el Catálogo de Servicios de TI dentro de la herramienta, organizando los servicios por categorías, subcategorías y tipos de elementos que respondan a las necesidades del ICBF.

- **Ciclo de Vida del Catálogo:** El proveedor será responsable del mantenimiento continuo del Catálogo de Servicios, incluyendo la creación de nuevos servicios, modificación de los existentes y el retiro de aquellos obsoletos, previa autorización de la supervisión del ICBF.

- **Asociación de Acuerdos de Niveles de Servicio (SLA):** El proveedor debe vincular formalmente cada servicio configurado en el catálogo con su respectiva matriz de tiempos de respuesta y solución parametrizada en la herramienta.

5. Auditoría, Base de Conocimiento y Escalabilidad Operativa

- **Control de Pistas de Auditoría (Logs):** El proveedor asegurará el correcto funcionamiento del registro inalterable de la plataforma sobre el historial cronológico

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

de acciones (creación, modificación, asignación, variaciones de estado y cierres de tickets), identificando fecha, hora y usuario responsable para fines de control interno.

- **Gestión de la Base de Conocimiento:** El proveedor debe alimentar, categorizar y actualizar continuamente el módulo de soluciones conocidas y artículos de ayuda dentro de la plataforma, vinculándolos al catálogo para facilitar la autogestión de los usuarios.

- **Gestión de Escalabilidad Operativa:** El proveedor monitoreará la capacidad transaccional de la instancia consumida en la herramienta de ITSM (volumen de requerimientos, registros históricos y archivos adjuntos), emitiendo alertas tempranas al ICBF si el crecimiento operativo exige una ampliación de capacidades o licencias ante el tercero.

6.9.7 SERVICIO NOC

6.9.7.1 REQUERIMIENTOS SERVICIO NOC

Requerimientos Monitoreo de aplicaciones

La herramienta principal de monitoreo deberá permitir:

- Monitorear **transacciones de aplicaciones** y detectar oportunamente cuellos de botella.
- Monitorear transacciones de usuario y cargas a nivel de servidor, base de datos y back-end.
- Identificar componentes afectados por degradación del servicio.
- Proporcionar **alertas en tiempo real** sobre problemas de disponibilidad y rendimiento.
- Realizar rastreo y seguimiento de transacciones.
- Monitorear contadores de rendimiento de servicios web IIS, incluyendo, entre otros:
    - Bytes enviados y recibidos por segundo
    - Peticiones por segundo
    - Máximo de conexiones
    - Errores HTTP (404)
    - Uso de CPU
    - Caché hit ratio
    - Tiempos de espera
    - Transacciones por segundo

Así como todas aquellas métricas adicionales que el ICBF requiera para garantizar el óptimo funcionamiento de las aplicaciones.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Requerimientos Monitoreo de bases de datos

La herramienta principal deberá permitir el monitoreo integral de bases de datos Oracle, Microsoft SQL Server y MySQL, incluyendo métricas de disponibilidad, rendimiento, uso de recursos, seguridad, capacidad, eventos de error, backups, tendencias históricas y análisis de desempeño, conforme a las mejores prácticas de cada motor y a las necesidades operativas del ICBF.

(Se mantienen los requerimientos específicos ya definidos para cada motor de base de datos, los cuales forman parte integral del presente capítulo.)

Requerimientos Monitoreo de servidores, nube, red y seguridad

La herramienta principal de monitoreo deberá permitir:

- Monitorear servidores **on-premise, virtualizados y en nube**, así como equipos de red y seguridad.
- Monitorear capacidad, disponibilidad y desempeño de componentes de almacenamiento y red.
- Configurar alarmas con niveles de criticidad personalizables.
- Visualizar de forma consolidada el estado de los nodos monitoreados.
- Asociar políticas de monitoreo a servidores o grupos de servidores.
- Monitorear sistemas operativos Microsoft, Linux y otros utilizados por el ICBF.
- Monitorear variables ñde desempeño de sistema operativo, procesos críticos, servicios, memoria, CPU, disco, red y eventos SNMP, durante toda la vigencia del Contrato.

Requerimiento servicio del NOC (Network Operation Center)

- La Entidad requiere la implementación y operación de un Centro de Operaciones de Red de Nueva Generación (Next-Generation NOC) que, a diferencia de los modelos reactivos tradicionales, se fundamente en un enfoque impulsado por datos (Data-Driven) y una arquitectura de Observabilidad Full-Stack. Este servicio deberá estar soportado por una plataforma de vanguardia que trascienda el monitoreo convencional basado en umbrales estáticos, integrando capacidades nativas de Machine Learning (ML) e Inteligencia Artificial para Operaciones de TI (AIOps); lo anterior con el fin de permitir la correlación automatizada y en tiempo real de los tres pilares fundamentales de la visibilidad (métricas, logs y trazas), garantizando así la detección proactiva de anomalías, la reducción del tiempo medio de reparación (MTTR) y la resiliencia operativa de la infraestructura.
- El servicio del NOC debe ofrecer una solución integral de monitoreo y observabilidad.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- El contratista no solo suministrará una plataforma en Alta Disponibilidad (HA), sino que garantizará la integración bidireccional y fluida con la herramienta de monitoreo propia del ICBF, permitiendo el intercambio de eventos y alertas para una gestión unificada.
- Además, el contratista proporcionará los servicios de administración, tunning (afinamiento) de modelos de Machine Learning y operación experta, asegurando que las líneas base de comportamiento se ajusten continuamente a la realidad operativa del Instituto, transformando los datos técnicos en inteligencia estratégica para la toma de decisiones.
- Monitoreo Continuo y Observabilidad Proactiva: Capacidad de monitorear en tiempo real la infraestructura de red y servicios mediante el análisis correlacionado de métricas, logs y trazas. La herramienta debe trascender el estado "up/down" para medir la salud del servicio y la experiencia del usuario, detectando degradaciones sutiles antes de que se conviertan en incidentes.
- Esquema de cobertura por nivel de monitorización Nivel1(Monitoreo Triage inicial,Nivel 2(Analisis Tecnico especializado),Nivel 3 (Ingeniería Avanzada Fabricante).
- Alertas Inteligentes y Notificaciones Basadas en AIOps: Capacidad de enviar alertas a los líderes de servicio del ICBF según matriz de escalamiento definido con anterioridad, en tiempo real. El sistema debe aplicar supresión de ruido y correlación de eventos mediante Machine Learning para agrupar múltiples alertas relacionadas en un único incidente de causa raíz, evitando la saturación de notificaciones.
- Integrar mediante la plataforma ITSM y gestión de incidencias para tener soporte de la gestión y cumplimiento de servicio, generar una bitácora de los casos creado y gestionados.
- Resolución de Problemas y Análisis de Causa Raíz (RCA): Capacidad de resolver incidentes en los tiempos máximos establecidos (SLA). La plataforma de observabilidad debe proporcionar diagnósticos automatizados que identifiquen el origen exacto de la falla (enlace, hardware, aplicación o seguridad), agilizando la resolución y la entrega de informes técnicos detallados.
- Conocimiento Dinámico de la Infraestructura: Capacidad de mantener un inventario y topología de red autodescubierta y dinámica. La herramienta debe mapear automáticamente las dependencias entre los componentes de hardware, software y servicios, permitiendo visualizar el impacto de cualquier cambio o falla en los procesos del ICBF.
- Capacidades de Escalado Predictivo: Capacidad de escalar recursos de manera elástica según la demanda. Mediante el análisis de tendencias y Capacity Planning predictivo, el sistema debe alertar sobre la necesidad de ampliación de capacidades antes de que se alcance el umbral de saturación.
- Seguridad, Confidencialidad y Cumplimiento: Garantizar la seguridad de los datos recolectados (logs y telemetría) mediante cifrado y controles de acceso estrictos, cumpliendo con la Ley de Protección de Datos Personales y las políticas de seguridad de la información del ICBF.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Gestión y Comunicación de Cambios (Observabilidad del Cambio): Capacidad de comunicar cambios con antelación y, tras su implementación, utilizar la herramienta de observabilidad para verificar el impacto inmediato en el rendimiento, asegurando que el cambio no haya generado regresiones en el servicio.
- Soporte, Capacitación y Transferencia de Conocimiento: Provisión de asistencia técnica especializada, documentación técnica actualizada y sesiones de transferencia de conocimiento sobre el uso de la plataforma de observabilidad y las nuevas capacidades de AIOps para el personal del ICBF.
- Comunicación Efectiva y Omnicanalidad: Proporcionar un punto de contacto designado y canales seguros (como portales de autoservicio o Dashboards compartidos) para una interacción fluida y visibilidad total del estado de los servicios.

Requisitos de Rendimiento de la Plataforma (SLA Técnico):

- Capacidad de Ingesta: La plataforma debe soportar la ingesta de al menos 8,000 Eventos por Segundo (EPS) y 50,000 Flujos por Minuto (Flows) sin pérdida de datos ni degradación del rendimiento.
- Tiempo de Respuesta de Consultas: El 95% de las consultas en los Dashboards (visualización de datos de las últimas 24 horas) debe cargar en menos de 3 segundos.
- Granularidad de Telemetría: Capacidad de recolectar métricas con una frecuencia de hasta 10 segundos para servicios críticos.
- Disponibilidad de la Herramienta (Uptime): La plataforma de observabilidad debe garantizar una disponibilidad del 99.9%, operando en esquema de Alta Disponibilidad (HA).

Mapeo Dinámico y Observabilidad de Infraestructura de Red

- Topología de Red e Inventario Dinámico: La herramienta debe realizar un descubrimiento automático (Auto-discovery) y mapeo de toda la infraestructura (Switches, Routers, APs, Controladoras, Firewalls y enlaces). Debe generar una topología interactiva que visualice dependencias entre hardware, software y servicios.
- Análisis de Ruta Salto a Salto (Hop-by-Hop): Capacidad de realizar análisis de ruta de red para identificar el punto exacto de falla o degradación de rendimiento entre un origen y un destino, visualizando cada nodo intermedio (enlaces LAN, WAN o Nube) y alertando específicamente sobre el equipo que causa la caída o el error.
- Salud de Hardware y Capa Física: El sistema debe supervisar y alertar en tiempo real sobre el estado de salud de los activos de red, incluyendo: fallas en fuentes de poder, temperatura excedida, estado de ventiladores, errores en interfaces físicas, saturación de CPU/Memoria en el plano de control y errores de redundancia (STP, LACP).

Requisitos Mínimos de Machine Learning y AIOps

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Establecimiento de Líneas Base (Baselines): La herramienta debe calcular automáticamente el comportamiento normal de la red tras un periodo de aprendizaje máximo de 7 a 14 días.
- Detección de Anomalías: Capacidad de identificar desviaciones estadísticas (picos de tráfico, latencia inusual) sin necesidad de configurar umbrales manuales.
- Reducción de Ruido: El motor de IA debe ser capaz de correlacionar eventos de distintas fuentes.

Requisitos de Infraestructura (Appliance o On-Premise):

- Arquitectura de Procesamiento: Mínimo 32 Cores vCPU (específicos para el motor de análisis de datos).
- Memoria Volátil: Mínimo 128 GB de RAM (requeridos para el procesamiento de modelos de ML en memoria).
- Almacenamiento de Alto Desempeño: Mínimo 10 TB efectivos en discos SSD NVMe o SSD Enterprise (imprescindible para la indexación rápida de logs y trazas).
- Interfaces de Red: Mínimo 2 interfaces de 10 Gbps para la ingesta de tráfico y telemetría.

Requisitos de Interoperabilidad y Seguridad:

- Integración con herramienta propia del icbf: Soporte nativo o vía API (REST/Webhooks) para la integración bidireccional de alertas con la consola actual del ICBF.
- Protocolos Soportados: Debe soportar nativamente: SNMP (v2/v3), NetFlow, IPFIX, Syslog, HTTP/HTTPS, y Streaming Telemetry (gNMI/gRPC).
- Seguridad de Acceso: Integración obligatoria con el Directorio Activo del ICBF y soporte para Autenticación Multifactor (MFA).
- Cifrado: Toda la información recolectada en tránsito y en reposo debe estar cifrada mediante algoritmos AES-256 o superior.
- Reporte de Disponibilidad por Sede y Nodo Crítico: Informe consolidado que detalle el porcentaje de Uptime de cada una de las sedes del ICBF y de los equipos core del Datacenter. Debe incluir el cálculo de cumplimiento del SLA y la justificación técnica de cualquier indisponibilidad detectada.
- Reporte de Saturación de Enlaces WAN e Internet: Análisis del consumo de ancho de banda en los canales MPLS e Internet. Debe resaltar los enlaces que superen el 70% de utilización de forma recurrente (Capacity Planning) para prever necesidades de ampliación antes de que se afecte el servicio.
- Análisis de Ruta y Experiencia del Usuario (Hop-by-Hop): Informe de rendimiento de las rutas críticas (ej. Sede Regional hacia Aplicativo Misional en Datacenter). Debe mostrar la latencia promedio, pérdida de paquetes y los saltos (nodos) que presentaron mayor degradación durante el mes.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Inventario Dinámico y Gestión de Activos: Listado actualizado de todos los equipos de red descubiertos por la herramienta, detallando modelo, versión de firmware/SO, estado de las interfaces y alertas de fin de vida útil (End-of-Life) o fin de soporte del fabricante.
- Informe de Salud de Hardware y Capacidad: Resumen ejecutivo sobre el estado físico de los equipos (uso de CPU, Memoria, Temperatura) y reporte de fallas de componentes (fuentes de poder, ventiladores) que hayan sido mitigadas proactivamente.

Estadísticas de AIOps y Eficiencia del SOC/NOC:

- Tasa de reducción de ruido: Cantidad de alertas totales vs. alertas correlacionadas en incidentes únicos.
- MTTD y MTTR: Tiempo promedio de detección y tiempo promedio de resolución de incidentes de red.
- Incidentes recurrentes: Identificación de los 10 nodos o enlaces que más alertas generaron durante el mes para acciones de mejora definitiva.
- Reporte de Observabilidad de Cambios: Detalle de las ventanas de mantenimiento ejecutadas y el impacto medido por la herramienta antes y después del cambio, certificando que no hubo degradación en los servicios tras las intervenciones.

6.9.8 MICROSOFT 365 - AD

6.9.8.1 GENERALIDADES DEL SERVICIO

Microsoft 365 como servicio (modelo SaaS) es una oferta por suscripción de Microsoft que entrega aplicaciones de productividad (Word, Excel, PowerPoint, Outlook, OneNote) y servicios en la nube (OneDrive, Exchange Online, SharePoint, Teams) con seguridad, cumplimiento y herramientas de gestión, todo accesible desde cualquier dispositivo y actualizado por Microsoft; en un ambiente híbrido se integra con la infraestructura local (Active Directory para identidades y Exchange Server para mensajería) sincronizando usuarios, políticas y datos para ofrecer acceso unificado, continuidad operativa y administración centralizada entre on-premises y cloud.

La plataforma de Microsoft 365 - AD para el ICBF está conformada por los servicios e Infraestructura de:

- Active Directory - DNS
- Certificate Authority
- AD Manager
- Microsoft Entra Connect
- Exchange On-premise
- Microsoft Teams
- Exchange Online

- SharePoint Online
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Entra ID
- Microsoft Purview

6.9.8.2 ALCANCE

El ICBF utiliza Microsoft 365 para la provisión y administración de sus servicios de productividad en línea, complementado por una infraestructura híbrida on-premise que incluye Active Directory, DNS, Certificate Authority, Microsoft Entra Connect y Exchange Server (correo y relay de aplicaciones e impresoras). Estos componentes locales, alojados en los centros de datos del ICBF o en servicios de datacenter contratados, son necesarios para garantizar la disponibilidad, compatibilidad y continuidad operativa de la plataforma.

El contratista será responsable de la administración, gestión operativa y monitoreo continuo de la infraestructura híbrida del ICBF, incluyendo Active Directory y DNS, Certificate Authority, AD Manager, Microsoft Entra Connect, Exchange On-premise, Exchange Online, Microsoft Teams, SharePoint Online, Microsoft Defender for Identity, Microsoft Defender for Office 365, sus tareas incluyen:

- Microsoft 365: administración de licencias y usuarios, configuraciones de seguridad y cumplimiento, gestión de Teams, SharePoint, OneDrive, políticas de retención y cumplimiento, actualizaciones y soporte de usuario final.
- Active Directory (on-prem y/o híbrido): gestión de controladores de dominio, DNS, OU y políticas de grupo (GPO), sincronización Microsoft Entra Connect, ciclo de vida de las cuentas (provisión, cambios, desactivación, baja), gestión de privilegios y cuentas administrativas.
- Exchange (on-prem y/o Exchange Online): administración de buzones, bases de datos, políticas de retención y cumplimiento, reglas de transporte, protección antispam/antimalware, migraciones y coexistencia híbrida cuando aplique.

6.9.8.3 DESCRIPCIÓN DEL SERVICIO

El ICBF tiene suscritos y adquiridos con Microsoft los servicios que se detallan a continuación, los cuales deberán ser administrados por El Contratista, incluyendo la gestión de la correspondiente línea base. A continuación, se presenta información ampliada sobre los servicios de Microsoft 365, Active Directory, Exchange Server y Entra Connect con que cuenta actualmente la Entidad:

Active Directory: Microsoft Active Directory (AD) es un servicio de directorio centralizado para la gestión de identidades, autenticación y autorización en entornos Windows. DNS (Domain Name System) es el servicio de resolución de nombres necesario para la

localización de controladores de dominio y servicios en un dominio AD. AD y DNS son pilares de la infraestructura de identidad y resolución de nombres; su correcta administración asegura autenticación, localización de servicios y aplicación de políticas en la red corporativa.

AD Manager Plus: ADManager Plus es una solución de gestión y automatización para Active Directory, Microsoft 365/Exchange y entornos híbridos, diseñada para simplificar tareas de administración de identidades, provisión/desprovisión, delegación y reporting sin necesidad de scripts.

Certificate Authority: Microsoft Certificate Authority, implementado mediante Active Directory Certificate Services (AD CS), es la solución de Microsoft para emitir, gestionar y revocar certificados digitales en entornos Windows. Proporciona la infraestructura de clave pública (PKI) necesaria para autenticación, cifrado, firma digital y establecimiento de confianza entre usuarios, equipos y servicios.

Microsoft Entra Connect: Microsoft Entra Connect es la herramienta oficial de sincronización y federación entre Active Directory local y Microsoft Entra ID (Azure AD / Microsoft 365). Permite mantener sincronizadas identidades, atributos y credenciales entre el directorio on-premises y la nube, facilitando escenarios híbridos de autenticación y acceso.

Entra ID: Microsoft Entra ID es el servicio de identidad y acceso basado en la nube de Microsoft que centraliza la gestión de identidades, autenticación y autorización para aplicaciones cloud, recursos híbridos y servicios de Microsoft 365.

Correo electrónico: Exchange Server y Exchange Online en entorno híbrido integran la plataforma de mensajería y colaboración onpremises de Microsoft con Exchange Online (Microsoft 365), ofreciendo coexistencia de buzones, enrutamiento de correo y una experiencia de usuario unificada. Proporcionan servicios de transporte y almacenamiento de buzones, acceso mediante protocolos (SMTP, MAPI/HTTP, OWA, ActiveSync) y funcionalidades avanzadas de cumplimiento, protección y gobernanza, permitiendo migraciones escalonadas, políticas centralizadas de retención y eDiscovery, y continuidad operativa entre el entorno local y la nube.

Microsoft Teams: Microsoft Teams es la plataforma de colaboración y comunicación empresarial de Microsoft que integra chat persistente, reuniones en línea, llamadas de voz/video, colaboración en documentos y espacios de trabajo por equipos, tanto en entornos cloud como híbridos.

SharePoint Online: Plataforma de colaboración y gestión documental en la nube integrada en Microsoft 365, que permite crear sitios de equipo y comunicación, bibliotecas de documentos, flujos de trabajo, portales intranet y soluciones de colaboración estructurada.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

OneDrive for Bussiness: Servicio de almacenamiento personal en la nube para usuarios, orientado a archivos de trabajo personales y sincronización/copia de seguridad entre dispositivos, con integración nativa con SharePoint Online y Microsoft 365.

Microsoft Defender: Microsoft Defender para Identity y Microsoft Defender para Office 365 son soluciones de seguridad complementarias dentro del ecosistema Microsoft que protegen identidades, detectan actividades maliciosas y defienden la plataforma de correo y colaboración de Microsoft 365.

Microsoft Purview: Microsoft Purview es la plataforma integral de gobernanza de datos, cumplimiento y protección de la información en el ecosistema Microsoft 365 y fuentes conectadas. Facilita descubrimiento, clasificación, protección, cumplimiento normativo y gestión del ciclo de vida de la información corporativa.

6.9.8.4 REQUERIMIENTOS DEL SERVICIO

Para este servicio se requiere garantizar la administración, configuración, operación, soporte y monitoreo de todas las plataformas y servicios que componen la línea base detallados en el numeral 6.9.6.4 LÍNEA BASE DEL SERVICIO.

- El Contratista será responsable de la administración, gestión operativa, soporte y monitoreo continuo de la infraestructura híbrida de identidad, colaboración y seguridad del ICBF, la cual integra servicios On-Premise y On-Line que conforman el ecosistema de Microsoft 365. Dicha infraestructura incluye, entre otros, Active Directory, DNS, Certificate Authority, Microsoft Entra Connect, Exchange On-Premise, Exchange Online, Microsoft Teams, SharePoint Online, Microsoft Defender for Identity, Microsoft Purview y Microsoft Defender for Office 365, garantizando su operación segura, estable y alineada con los lineamientos institucionales.
- Administrar, operar, soportar, mantener, controlar y monitorear Microsoft 365 (Online) y componentes Onpremises relacionados, incluido Active Directory (AD), DNS y sincronización híbrida (AD – Entra ID).
- Administrar licenciamiento (asignación, optimización, auditoría) conforme políticas ICBF. Reporte de consumo y recomendación mensual.
- Preparar evidencias técnicas y acompañar escalamiento a Microsoft u otros, documentando comunicaciones y resoluciones. Notificar al Líder de Servicio al escalar.
- Garantizar disponibilidad del servicio ≥ 95% mensual (excluyendo mantenimientos programados).
- Administrar cuentas (crear, modificar, deshabilitar, eliminar), políticas de contraseñas, MFA, y controles de mínimo privilegio. Implementar y documentar cambios mediante GPO y políticas.
- Gestionar todas las solicitudes en la herramienta ITSM definida por ICBF, cumpliendo ANS. Registrar diagnóstico, acciones, evidencias y cierre.

- Operar y mantener sincronización híbrida (AD Connect), garantizar integridad y resolución de conflictos. Monitoreo y verificación diaria de replicación y estado de controladores de dominio.
- Proveer solución controlada para envíos de correos externos bajo demanda sin afectar reputación del dominio ICBF; generar reportes por envío (entregados, rechazados, errores detallados, aperturas y cliente/navegador). Integración previa autorización del ICBF.
- Implementar y gestionar política de backup y recuperación para Exchange, OneDrive, SharePoint, Teams y componentes Onpremises.
- Proponer mejoras (plan, beneficios, riesgo), y capacitar al personal designado por ICBF cuando se active nuevas funcionalidades o servicios.
- Mantener documentación técnica actualizada (configuraciones, diagramas, evidencias) y facilitar auditorías. Entregar reportes operativos mensuales y documentación requerida en auditorías.
- Administrar, operar, soportar y monitorear las capacidades de Microsoft Purview implementadas por ICBF, incluyendo etiquetas de sensibilidad, políticas de retención, clasificación de información y controles de protección de datos, garantizando su correcta operación y alineación con los lineamientos institucionales.
- Administrar, monitorear y optimizar las políticas de Prevención de Pérdida de Datos (DLP) implementadas en Exchange Online, SharePoint Online, OneDrive y Microsoft Teams. Analizar alertas, gestionar excepciones autorizadas, investigar eventos y proponer ajustes para minimizar riesgos de fuga o exposición de información institucional.

En este contexto, el Contratista deberá ejecutar, como mínimo, las siguientes actividades:

1. **Administración de Microsoft 365**

- Administrar licencias, usuarios y grupos, de acuerdo con la línea base definida por el ICBF.
- Configurar y gestionar las políticas de **seguridad, cumplimiento, retención de la información y gobernanza**.
- Administrar los servicios de **Microsoft Teams, SharePoint Online y OneDrive**, incluyendo configuración, permisos, sitios, equipos y políticas de uso.
- Gestionar actualizaciones y configuraciones del servicio conforme a los procedimientos establecidos por la Entidad.

2. **Administración de Active Directory (OnPremise y/o Híbrido)**

- Administrar los controladores de dominio, el servicio de DNS, las Unidades Organizativas (OU) y las Políticas de Grupo (GPO), asegurando su correcta configuración, aplicación y alineación con los lineamientos de seguridad definidos por el ICBF.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Gestionar la sincronización de identidades mediante Microsoft Entra Connect, garantizando la coherencia, integridad y disponibilidad de los objetos de identidad entre el entorno On-Premise y la nube, cuando aplique.
- Administrar el ciclo de vida de las cuentas (creación, modificación, suspensión, desactivación y eliminación), así como la gestión de roles, privilegios y cuentas administrativas, bajo el principio de mínimo privilegio.
- Administrar y mantener la estructura lógica del Directorio Activo, incluyendo usuarios, grupos, OU, objetos del esquema y directivas de seguridad, garantizando su consistencia y adecuada operación.
- Configurar y supervisar la replicación entre controladores de dominio, asegurando la consistencia de la información y la disponibilidad del servicio en toda la infraestructura.
- Mantener el Directorio Activo y los controladores de dominio actualizados con parches y actualizaciones de seguridad, conforme a las políticas de cambio y mantenimiento del ICBF.
- Implementar y mantener mecanismos de alta disponibilidad para los servicios de Directorio Activo y DNS, garantizando su operación continua 7x24x365, de acuerdo con los requerimientos institucionales.
- Habilitar y administrar la auditoría y el registro de eventos del Directorio Activo, permitiendo la trazabilidad de actividades, el cumplimiento normativo y el análisis de eventos de seguridad.
- Monitorear el desempeño, capacidad y salud del Directorio Activo y sus componentes, identificando y gestionando oportunamente incidentes o degradaciones del servicio.
- Formular y presentar al ICBF recomendaciones de buenas prácticas relacionadas con políticas de seguridad, administración de usuarios, respaldo, endurecimiento (hardening) y operación del Directorio Activo y DNS.
- Ejecutar las actividades de actualización del nivel funcional del dominio o de migración del Directorio Activo a nuevas versiones, cuando el fabricante (Microsoft) libere dichas versiones y establezca en su documentación oficial la necesidad o recomendación de realizar dichas actualizaciones, garantizando que la ejecución se lleve a cabo de manera planificada, controlada y de bajo impacto, conforme a las buenas prácticas del fabricante y a los lineamientos de operación del ICBF.

3. Administración de Exchange (OnPremise y/o Exchange Online)

- Administrar buzones, bases de datos, y contactos.
- Configurar y gestionar **políticas de retención, cumplimiento normativo y eDiscovery**.
- Administrar reglas de transporte, protección antispam y antimalware, y controles de seguridad del correo electrónico.
- Ejecutar procesos de migración, coexistencia y operación híbrida, cuando aplique.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

4. Seguridad, operación y soporte

- Administrar y operar las soluciones de Microsoft Defender, incluyendo Defender for Identity y Defender for Office 365, garantizando capacidades de protección, detección y respuesta ante amenazas, y seguridad del correo electrónico e identidades.
- Realizar el monitoreo continuo de la plataforma, atendiendo incidentes, requerimientos y eventos de seguridad u operación.
- Gestionar el soporte técnico con el fabricante (Microsoft), incluyendo escalamiento de casos cuando sea requerido.

5. Operación híbrida y buenas prácticas

- Administrar los servicios de Microsoft 365 y los componentes OnPremise relacionados **exclusivamente mediante las herramientas provistas por el fabricante** o disponibles de forma nativa en la plataforma. El uso de herramientas no avaladas deberá contar con **autorización expresa del ICBF**.
- Configurar e implementar **políticas de respaldo (backup)**, tanto incrementales como completos, de los componentes definidos por la Entidad.
- Ejecutar labores de **mantenimiento preventivo y correctivo** sobre los ítems de configuración involucrados en la prestación del servicio.
- Implementar los cambios de configuración, activación, desactivación, actualización o eliminación de usuarios, grupos, recursos y servicios, conforme a las **directrices formales del ICBF** (documentación, actas, correos o comunicaciones oficiales).

6. Administración de Microsoft Purview y Protección de la Información

- Administrar y operar las capacidades de Microsoft Purview implementadas por el ICBF, incluyendo etiquetas de sensibilidad, protección de la información, retención de datos, auditoría, cumplimiento y gobierno de la información.
- Administrar, monitorear y optimizar las políticas de Prevención de Pérdida de Datos (DLP) implementadas en Exchange Online, SharePoint Online, OneDrive y Microsoft Teams, incluyendo la atención de alertas, análisis de incidentes, gestión de excepciones autorizadas y generación de recomendaciones para la protección de la información institucional.
- Monitorear y atender alertas de cumplimiento y protección de datos generadas por Microsoft Purview, ejecutando las acciones de análisis, contención, escalamiento y remediación que sean requeridas por el ICBF.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

6.9.9 REDES LAN

6.9.9.1 GENERALIDADES DEL SERVICIO

El ICBF cuenta con equipos activos de red para conectar los diferentes dispositivos que cuentan con interfaces de red para obtener conectividad a nivel de red LAN del ICBF haciendo uso de los recursos compartidos para el acceso a los servicios de Red con los que cuenta la Entidad como Internet, conectividad entre sedes, Telefonía IP, video conferencia y acceso a los recursos tecnológicos que se encuentran en el datacenter.

Estos equipos activos de red se deben instalar, configurar, administrar, operar, monitorear y gestionar garantizando la disponibilidad del servicio.

6.9.9.2 ALCANCE

El ICBF requiere el servicio contratado comprenda la administración, operación, monitoreo y soporte integral de los equipos activos de la red LAN garantizando la conexión de estaciones de trabajo, impresoras, teléfonos IP, cámaras de videoconferencia, servidores, enrutadores y otros dispositivos que cuenten con interfaz de red y habilitados para funcionar mediante los protocolosIPv4 (Internet Protocol versión 4) e IPv6 (Internet Protocol versión 6) en las sedes de la Dirección General y Sedes Anexas a nivel nacional, las cuales se describen en la Línea Base.

El alcance de servicio será llegar al Rack de Comunicaciones de cada área de la Sede de la Dirección General y de las sedes anexas. Administrar, operar y monitorear los dispositivos de red necesarios para garantizar el servicio.

El alcance también requiere la instalación, configuración, monitoreo y garantizar que se respete las mejores prácticas del fabricante y los estándares definidos por la entidad. En los nuevos switches cuando sea requerido para mejorar el desempeño de la red o cuando fallen y se requiera el reemplazo de estos. Los dispositivos serán entregados por el ICBF al Contratista para dicha instalación y configuración.

Además, el servicio contempla administrar, operar y monitorear de manera remota los Switches de distribución y acceso de las sedes regionales y sedes anexas del ICBF. Este servicio se prestará desde la ciudad de Bogotá de manera centralizada para cubrir las 33 Regionales, Centros Zonales y sedes anexas a nivel nacional y con el apoyo del ICBF para cuando se requiera manos remotas.

El Contratista deberá:

- Contar con el recurso humano profesional, técnico y especializado necesario para garantizar la administración, operación, monitoreo y soporte de la infraestructura LAN del ICBF, conforme a los niveles de servicios establecidos.

- Realizar administración, configuración, monitoreo y gestión centralizada de los switches de Core del ICBF ubicados en el Datacenter principal y centro de cómputo de la Sede Dirección General.
- Administrar, monitoreó y gestionar de manera remota los Switches de distribución y acceso de las sedes regionales, centros zonales, Caivas, Casas de Justicia, Unidad local, CESPA y SRPA (servicio de responsabilidad penal de adolescentes), Casas atrapasueños, CDI (Centros de Desarrollo Infantil) del ICBF.
- Instalar, configurar, administrar y gestionar los Switches de los cuartos de cableado de la sede Dirección General, Datacenter principal y Archivo Documental Sede anexa de la Dirección General del ICBF.
- Administrar el software de gestión, monitoreo y operación de los Switches de manera centralizada.
- Realizar el diagrama topológico de red por cada servicio conectado a la red LAN de las sedes de la Dirección General, Datacenter principal, y Archivo Documental Sede anexa de la Dirección General, sedes regionales, centros zonales Caivas, Casas de Justicia, Unidad local, CESPA y SRPA (servicio de responsabilidad penal de adolescentes), Casas atrapasueños, CDI (Centros de Desarrollo Infantil) del ICBF.
- Actualizar los diagramas topológicos ante cambios, mantenimientos, nuevas instalaciones o requerimientos del ICBF.
- Suministrar, instalar, configurar y mantener sistemas de control de acceso físico en todas las puertas de los centros de cableado definidos Sede de la Dirección General mediante chapas inteligentes operadas por clave numérica, tarjeta de proximidad o ambos mecanismos. Los elementos suministrados e instalados pasarán a ser propiedad de la Entidad al finalizar el contrato
- Realizar los mantenimientos preventivos programados a la totalidad de los equipos activos de red ubicados en los centros de cableado de la Dirección General, Datacenter Principal, Archivo Documental y demás sedes del ICBF, incluyendo Sede Regionales, Centros Zonales, CAIVAS, Casas de Justicia, Unidades Locales, CESPA y SRPA (Sistema de Responsabilidad Penal para Adolescentes), Casas Atrapasueños y Centros de Desarrollo Infantil (CDI), con el fin de garantizar la continuidad operativa, la disponibilidad, el desempeño y la confiabilidad de la infraestructura de redes y comunicaciones institucionales. Las actividades deberán contemplar inspección física, verificación de hardware y software, actualización de firmware cuando aplique, limpieza especializada, validación de configuraciones, revisión de capacidad y generación de informes técnicos con hallazgos y recomendaciones

6.9.9.3 DESCRIPCIÓN DEL SERVICIO

El servicio de red LAN debe permitir a los funcionarios del ICBF de la sede de la Dirección General y sedes Anexas la conectividad a periféricos de salida como impresoras, escáneres y transferencia de datos localmente entre dispositivos y endpoints, a través de la interconexión de dispositivos activos como switches y Access Point, los cuales están

instalados en cada una de las sedes del ICBF. Además, la administración de los balanceadores permitiendo el balanceo de carga y aceleración de las aplicaciones web ubicados en el Datacenter Principal.

El cableado estructurado para interconexión de equipos en el interior de las sedes será responsabilidad del ICBF.

La Sede de la Dirección General cuenta con catorce (14) centros de cableado distribuidos en forma equidistante en sus instalaciones; los catorce (14) de estos se encuentran aislados y cuentan con cerramiento.

6.9.9.4 REQUERIMIENTOS DEL SERVICIO

El servicio de administración de red LAN se requiere como mínimo las siguientes actividades:

- Monitorear permanentemente la red de área local (LAN) mediante herramientas centralizadas, permita conocer en tiempo real el desempeño y la disponibilidad de los equipos que conforman la red y sus componentes asociados a través de un protocolo que permita dar información de administración de los dispositivos de red. El monitoreo deberá incluir, como mínimo las siguientes variables: Fuente de Poder, Ventilador, Procesador, Memoria, Puertos, Disponibilidad del Equipo, Puertos, tráfico sobre sus interfaces y Eventos críticos y alertas de sistema
- Administrar el direccionamiento IP asignación de direcciones dual Stack IPv4 e Ipv6 a los equipos y dispositivos de acuerdo con las mejores prácticas.
- Instalar, configurar y mantener el hardware y software necesario para el buen funcionamiento y servicio de la red LAN, incluido la realización de backups de respaldo de configuración y actualización de firmware, software de los equipos que están relacionados en la línea base de este servicio y los equipos que se adquieran o cambien durante la vigencia del contrato. La información de la configuración de los switches de acceso y switch Core debe estar respaldada en la unidad de almacenamiento que el ICBF disponga.
- Asignar, documentar y gestionar direcciones IP según estándares del ICBF y mejores prácticas de diseño
- Crear nuevas redes, subredes, VLANS, interfaces lógicas y rutas de acuerdo con las necesidades en la infraestructura del ICBF. Mantener actualizada la matriz de direccionamiento y comunicar oportunamente los cambios al ICBF.
- Realizar el diagnóstico para el mejoramiento y ampliación de la red LAN, con el fin de incluir nuevos servicios respondiendo a las necesidades de crecimiento del ICBF.
- Realizar el mapeo de la Red LAN de la sede de la Dirección General, Datacenter y Sedes Anexas, donde se indique por medio de un diagrama topológico y físico los switches interconectados con otros dispositivos de red (servidores, impresoras, Access

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Point, cámaras, entre otros.). Este mapeo debe estar actualizado ante cualquier cambio realizado.

- Configurar en los equipos relacionados en la línea base de este servicio, el protocolo SSH (Secure Shell) y deshabilitar el acceso remoto por Web y por Telnet con el propósito de ofrecer mayor seguridad a la red.
- Realizar las actividades necesarias para segmentar la red LAN de la sede de la Dirección General y sedes Anexas, según los parámetros definidos por el ICBF.
- Bloquear y desbloquear puertos de conexión según los requerimientos del ICBF.
- Administrar y gestionar de manera remota los Switches de distribución y acceso de las sedes regionales, centros zonales, Caivas, Casas de Justicia, Unidad local, CESPA y SRPA (servicio de responsabilidad penal de adolescentes), Casas atrapasueños, CDI (Centros de Desarrollo Infantil) del ICBF a través de la herramienta IMC, de la cual se tiene licenciamiento.
- Realizar las conexiones físicas de red en el centro de cómputo de la sede de la Dirección General, Datacenter principal, Archivo Documental sede alterna a Sede Dirección General entre los diferentes dispositivos que hacen parte de la infraestructura tecnológica de la Entidad o las que sean requeridas por el ICBF.
- Gestionar las garantías del hardware y software que hacen parte de la Red LAN con el respectivo fabricante o proveedor que se encuentren vigentes en la Entidad.
- Realizar el mantenimiento correctivo y preventivo a los equipos de la red LAN instalados en la Sede Dirección General, Datacenter principal y Archivo Documental Sede anexa de la Dirección General, sedes Regionales, Centros Zonales, Caivas, Casas de Justicia, Unidad local, CESPA y SRPA (servicio de responsabilidad penal de adolescentes), Casas atrapasueños, CDI (Centros de Desarrollo Infantil) del ICBF. que se encuentra fuera de soporte por proveedor y se deberá realizar una (1) vez al año durante el periodo del contrato.
- Realizar el diagnóstico de disponibilidad de puertos para los equipos red LAN instalados en la sede de la Dirección Nacional, Datacenter principal, sede Alterna de la dirección General y Sede Gestión Documental en el municipio de Funza.
- Realizar acompañamiento y soporte a las actividades requeridas por el proveedor de comunicaciones conectividad WAN necesarias para el correcto funcionamiento del servicio LAN a los usuarios.
- Administrar, operar y monitorear los equipos activos de la red LAN de las Sedes de la Dirección de Tecnologías de la Información (DTI), en la Ciudad de Bogotá, Archivo documental Sede anexa de la Dirección General a, las sedes regionales (ubicadas en las ciudades capitales de cada departamento), centros zonales, Caivas, Casas de Justicia, Unidad local, CESPA y SRPA (servicio de responsabilidad penal de adolescentes, Casas atrapasueños y Centro de desarrollo infantil (CDI).
- Mantener actualizados los inventarios de la infraestructura de la red LAN en los centros de cableado y centro de cómputo de la sede de la Dirección General, datacenter principal, Sedes Anexas en el formato que el ICBF designe. Dichas actividades deben tener altas, bajas y movimientos de switches.
- Desarrollar actividades periódicas de análisis de tráfico en redes LAN. Dichas

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

actividades se desarrollarán trimestralmente y como resultado de ellas, el Contratista presentará un informe detallando el análisis de protocolos realizado, porcentaje de utilización de ancho de banda por protocolo, hallazgos de seguridad y hallazgos relacionados con configuraciones de switching en las redes y sus respectivos planes de acción para corregir problemas y mejorar las condiciones o configuraciones actuales.

- Mantener actualizada la documentación de la topología de las redes LAN de los centros de cableado y centro de cómputo de la Dirección General, datacenter principal y Sedes Anexas, incluyendo diagramas y planos, en medio magnético y notificar los cambios vía correo electrónico a la persona encargada en el ICBF.
- Realizar el escalamiento de incidentes de los problemas de hardware o software al fabricante o proveedor de los equipos de red administrados.
- Mantener organizado y etiquetado los cables de datos de los racks que se encuentran en los cuartos de cableado de la Sede Dirección General, Datacenter principal, Sede Metrópolis y Archivo Documental Sede anexa de la Dirección General, sedes regionales, centros zonales, Caivas, Casas de Justicia, Unidad local, CESPA y SRPA (servicio de responsabilidad penal de adolescentes), Casas atrapasueños, CDI (Centros de Desarrollo Infantil) del ICBF.
- Realizar la **creación, administración, monitoreo y actualización de los usuarios autorizados** para el ingreso a los centros de cableado de la Sede Dirección General.
- Disponer de un sistema de monitoreo centralizado que permita gestionar todos los equipos LAN de manera proactiva (alertas, disponibilidad, CPU, temperatura, tabla MAC, STP, etc

6.9.10 REDES WLAN

6.9.10.1 GENERALIDADES DEL SERVICIO

El ICBF cuenta con una infraestructura de equipos activos de red Access Point para conectar de forma inalámbrica los diferentes dispositivos que cuentan con interface de red inalámbrica, para que tengan conectividad a la red LAN del ICBF y garantizar el acceso de los recursos compartidos, servicios de red como Internet, entre otros, al servicio de los usuarios del ICBF; estos equipos activos de red inalámbrica se deben instalar, configurar, administrar, operar, monitorear y gestionar, garantizando la disponibilidad del servicio.

6.9.10.2 ALCANCE

El ICBF requiere el servicio de administración, operación, monitoreo de los equipos activos de la red WLAN garantizando la conexión de los equipos inalámbricos a la red LAN de las sedes de la Dirección General y Sedes Anexas, las cuales se describen en la Línea Base.

Adicionalmente se requiere la instalación de nuevos Access Point o reubicación cuando sea

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

requerido para mejorar el desempeño de la red o cuando fallen y se requiera el reemplazo de estos. Estos dispositivos serán entregados por el ICBF al Contratista para dicha instalación y configuración.

El Contratista deberá tener capacidad para administrar con el recurso humano profesional y técnico requeridos para el servicio de WLAN.

El contratista debe asegurar que los funcionarios del ICBF equipados con dispositivos como desktops, laptops, Tablets y dispositivos inteligentes y similares se conecten a la red inalámbrica (WLAN), brindando movilidad y ampliando la cobertura de la red LAN dentro de las instalaciones físicas de la sede de la Dirección General, sedes regionales, centros zonales, Caivas, Casas de Justicia, Unidad local, CESPA y SRPA (servicio de responsabilidad penal de adolescentes) Casas atrapasueños, CDI (Centros de Desarrollo Infantil); de manera centralizada para cubrir las 33 Regionales, Centros Zonales y sedes anexas a nivel nacional y con el apoyo del ICBF para cuando se requiera manos remotas.

El contratista debe:

- Realizar instalación, configuración, administración y gestión centralizada de los Access Point del ICBF ubicados en la Sede Dirección General, sedes regionales, centros zonales, Caivas, Casas de Justicia, Unidad local, CESPA y SRPA (servicio de responsabilidad penal de adolescentes) Casas atrapasueños, CDI (Centros de Desarrollo Infantil).
- Administrar las controladoras y el software de gestión y monitoreo de las soluciones inalámbricas de manera centralizada.

6.9.10.3 DESCRIPCIÓN DEL SERVICIO

El servicio de red WLAN debe permitir a los funcionarios del ICBF de la sede de la Dirección General y sedes Anexas la conectividad inalámbrica entre equipos y pueden formar una red inalámbrica externa (local o internet) con la que interconectar dispositivos móviles o tarjetas de red inalámbricas para el acceso a los diferentes servicios tecnológicos con los que cuenta el ICBF, a través de la interconexión de dispositivos activos como switches y Access Point, los cuales están instalados en cada una de las sedes del ICBF.

6.9.10.4 REQUERIMIENTOS DEL SERVICIO

El ICBF requiere instalación, configuración, administración y soporte del servicio WLAN y los componentes que permiten su funcionamiento para las sedes del ICBF descritas en la línea base de este servicio. Para los Access Point marca HP 560 AM y HP-MSM 430 AM el contratista debe realizar la administración a través de una controladora física ubicada en el Datacenter principal y centro de cómputo de la sede de la Dirección General.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Para los Access Point marca ARUBA 325, 315, 335, 305 el contratista debe realizar la administración a través de una controladora física ubicada en el Datacenter principal y centro de cómputo de la sede de la Dirección General.

Para los Access Point marca CISCO C1260 el contratista debe realizar la administración de manera autónoma sobre el dispositivo.

Se requiere la administración de los Access Points y de las controladoras inalámbricas sin importar su ubicación física dentro de las sedes del alcance de este servicio.

Dentro del servicio y administración se debe garantizar lo siguiente:

- Aplicar políticas de QoS, Seguridad y cobertura (RF) a los Access Points por medio de los Controladores de Puntos de Acceso Distribuidos por la red la red inalámbrica.
- Integrar planos preconfigurados en la herramienta de administración.
- Visualización de Heat Maps y cobertura en radio frecuencia
- Permitir la localización de los Access Points y clientes Wifi que se encuentren en la red inalámbrica (WLAN) mediante planos preconfigurados, incluidos los equipos móviles.
- Consolidar alarmas y reportes de los niveles de radio, interferencia, seguridad, desempeño.
- Incluir herramientas para planificación del crecimiento de la red Wireless, mostrando los sitios más indicados para la instalación de nuevos Puntos de Acceso.
- Implementar IDS (Intrusion Detection System) basado en firmas de radio frecuencia (RF) y reportarlo al SOC.
- Instalar Access Point cuando se requiera para ampliación según el mapa de calor o cuando fallen los dispositivos
- Gestionar las garantías del hardware y software que hacen parte de la red inalámbrica con el respectivo fabricante o proveedor que se encuentren vigentes en la Entidad.
- Administrar, configurar, monitorear y dar soporte de la red inalámbrica (WLAN) para la sede de la Dirección General de la Entidad, metrópolis, sedes anexas de la dirección general, sedes regionales, centros zonales, Caivas, Casas de Justicia, Unidad local, CESPA y SRPA (servicio de responsabilidad penal de adolescentes), Casas atrapasueños y Centro de desarrollo infantil (CDI).
- Mantener actualizados los inventarios de la infraestructura de la red WLAN en las sedes de la Dirección General, metrópolis, sedes anexas de la dirección general, sedes regionales, centros zonales, Caivas, Casas de Justicia, Unidad local, CESPA y SRPA (servicio de responsabilidad penal de adolescentes), Casas atrapasueños y Centro de desarrollo infantil (CDI) en el formato que el ICBF designe.
- Entregar un informe de zonas de cobertura bimestral como mínimo o cuando el ICBF lo requiera.
- Llevar control y actualización del inventario de Access Points de acuerdo con el formato establecido por el ICBF.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Configurar y dar soporte al portal cautivo para ingreso de visitantes a la red WLAN del ICBF de acuerdo con las políticas establecidas por el ICBF.
- Realizar el escalamiento de incidentes de los problemas de hardware o software al fabricante o proveedor de los equipos de red inalámbricos administrados.
- Disponer de un sistema de monitoreo centralizado que permita gestionar todos los equipos WLAN.

6.9.11 RESPALDOS

6.9.11.1 GENERALIDADES DEL SERVICIO

El Contratista deberá prestar el servicio integral de administración, operación, configuración, monitoreo, soporte, respaldo, restauración y recuperación de la información institucional, sobre las soluciones tecnológicas de respaldo con las que cuenta el ICBF y aquellas que sean incorporadas durante la ejecución del contrato.

El servicio deberá garantizar la disponibilidad, integridad, confidencialidad, trazabilidad y recuperabilidad de la información respaldada, mediante la aplicación de las políticas, procedimientos, estándares de seguridad, esquemas de retención y lineamientos definidos por el ICBF, así como las buenas prácticas aplicables de los fabricantes de las soluciones implementadas.

La prestación del servicio deberá garantizar monitoreo 7x24x365, gestión integral de las plataformas, atención de incidentes, ejecución y seguimiento de las políticas de respaldo, gestión de medios, custodia externa, restauración de información, pruebas de recuperación, gestión de capacidad y generación de informes técnicos y ejecutivos.

6.9.11.2 ALCANCE

El servicio incluye la ejecución de los procesos de respaldo en los medios magnéticos asociados a las soluciones implementadas tanto por el ICBF como por el Contratista. Los medios magnéticos deberán ser suministrados por el Contratista y ser plenamente compatibles con las soluciones de respaldo utilizadas por la Entidad. Adicionalmente, todo medio magnético y flujo de datos asociado al proceso de respaldo deberá implementar protocolos de cifrado robustos, tales como AES-256 para cifrado en reposo y TLS 1.2 o superior para la transferencia de información, garantizando la integridad, confidencialidad y protección de los datos durante su manipulación, transporte y almacenamiento.

El Contratista deberá garantizar el servicio de custodia externa, asegurando que los medios magnéticos y/o documentos que requieran almacenamiento seguro sean transportados bajo medidas de seguridad física y lógica, incluyendo la verificación de sellos de seguridad, registro de cadena de custodia y uso de contenedores certificados, manteniendo en todo momento el cifrado de la información almacenada en los medios.

A continuación, se presenta el inventario en el ***Anexo 03 - Linea Base de Servicios TI*** actual del ICBF que servirá como referencia para la operación a cargo del Contratista. Dicho inventario podrá variar conforme a las necesidades de actualización tecnológica de la Entidad, por lo cual el Contratista deberá ajustar la prestación del servicio según los cambios implementados. La gestión deberá ejecutarse con el personal profesional y técnico requerido, garantizando el cumplimiento de los lineamientos operativos, de seguridad de la información y de los protocolos de cifrado definidos.

De igual manera, el Contratista será responsable de realizar las restauraciones de información provenientes tanto de los medios magnéticos como de las soluciones de respaldo, asegurando que todos los datos restaurados mantengan el cifrado correspondiente durante el proceso y que únicamente sean descifrados bajo los procedimientos autorizados por el ICBF. Estas actividades deberán realizarse conforme a los planes, protocolos de recuperación, procedimientos establecidos y mejores prácticas vigentes, utilizando para ello el recurso humano profesional y técnico necesario.

El contratista debe:

- Mantener al ICBF dentro de una política de gestión de soluciones de respaldo con alternativas de salvaguardar y restaurar información de archivos de datos estructurados, no estructurados e imágenes, que estén disponibles para cualquier eventualidad o necesidad en que se requiera recuperar la información. Mantener al ICBF dentro de una política integral de gestión de soluciones de respaldo que garantice alternativas confiables para la salvaguarda y restauración de información correspondiente a archivos de datos estructurados, no estructurados e imágenes. Estas soluciones deberán asegurar la disponibilidad, integridad y recuperabilidad de la información ante cualquier eventualidad, incidente operativo o requerimiento institucional de recuperación.

- Garantizar la política de rotación de medios utilizada por la Entidad. El ICBF cuenta con una política de rotación de medios GFS (ABUELO, PADRE, HIJO), donde el backup anual se rota cada 25 años, el backup mensual se rota entre 1 a 10 años y el backup diario se rota cada 3 meses, las anteriores políticas pueden ser ajustadas durante la vigencia del contrato. Garantizar la aplicación y cumplimiento de la política de rotación de medios definida por el ICBF para la solución de respaldo Veeam Backup. La Entidad utiliza un esquema de retención GFS (Grandfather–Father–Son), en el cual los respaldos anuales (Grandfather) se conservan por un ciclo de 25 años, los respaldos mensuales (Father) se mantienen entre 1 y 10 años, y los respaldos diarios (Son) se rotan cada 3 meses. Estas políticas podrán ser ajustadas por el ICBF durante la vigencia del contrato, por lo que el Contratista deberá actualizar la configuración correspondiente en Veeam Backup, garantizando el cumplimiento de los parámetros de retención y conservación establecidos.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

El Contratista deberá tener capacidad para administrar el servicio de respaldos con el recurso humano profesional y técnico requeridos en el ***Anexo 01 - Personal mínimo requerido***, para todos los elementos relacionados en el siguiente inventario: El Contratista deberá contar con la capacidad operativa y técnica necesaria para administrar el servicio de respaldos, disponiendo del recurso humano profesional y técnico definido en el ***Anexo 01 – Personal mínimo requerido***. Dicho personal será responsable de la gestión, operación, monitoreo y soporte de todos los elementos incluidos en el inventario relacionado a continuación, garantizando su adecuado funcionamiento dentro del marco de la solución de respaldo implementada por el ICBF.

6.9.11.3 DESCRIPCIÓN DEL SERVICIO

El futuro contratista deberá ejecutar la **administración, operación, configuración y monitoreo** de la solución de respaldo institucional basada en **Veeam Backup & Replication**, atendiendo las siguientes condiciones:

- **Respaldos en cinta y disco de servidores del ICBF**: Veeam Backup se integrará con las librerías físicas y virtuales disponibles, garantizando la protección de la información crítica mediante políticas de respaldo programadas y verificadas.
- **Integración con librerías físicas**: la solución deberá gestionar respaldos hacia las librerías de cinta de alta capacidad (LTO6 y LTO8), asegurando la correcta administración de slots, drives y ciclos de retención.
- **Respaldos en disco con deduplicación**: Veeam Backup aprovechará las capacidades de equipos especializados como Exagrid y plataformas híbridas (Libreria IBM), configuradas como librerías virtuales de cintas, optimizando el uso de espacio mediante deduplicación y compresión de datos.
- **Monitoreo y reportes centralizados**: el contratista deberá garantizar la supervisión continua de los procesos de respaldo, validando la integridad de los datos y generando reportes de cumplimiento para auditoría y control interno.
- En este contexto, **Veeam Backup & Replication** se consolida como la herramienta central de protección de datos del ICBF, garantizando continuidad operativa, recuperación ante desastres y cumplimiento de las políticas de seguridad y disponibilidad de la información.

El servicio ejecuta al mes aproximadamente 410 políticas de respaldo, con 20 copias de seguridad esporádicas, dando un peso total aproximado de 307.7 terabytes; se reciben aproximadamente 60 solicitudes de restauración que equivalen a 155 restauraciones, las cuales deberán ser atendidas por el Contratista.

6.9.11.4 REQUERIMIENTOS DEL SERVICIO

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Para este servicio el ICBF requiere la administración, operación, configuración, y monitoreo de las soluciones de respaldo con las que cuenta el ICBF y las que se adquieran durante la ejecución del contrato.

- El servicio incluye la implementación, actualización y ejecución de las políticas de backup y recuperación para servidores en los diferentes ambientes (desarrollo, pruebas, capacitación, pilotos y producción) y mantener actualizada mensualmente esta información.
- El servicio de custodia de medios debe comprender tanto el almacenamiento del medio, como el transporte desde el sitio de custodia hasta las instalaciones donde el ICBF tenga su infraestructura de respaldos y/o donde se requiera el recojo/entrega de información (por ejemplo, CD en la Sede de la Dirección General). Además, debe contar con la opción de servicio de transporte de emergencia disponible 7X24X365 con un tiempo no superior a 4 horas continuas en caso de que se requiera. En caso de no poder realizar backup de la información de forma centralizada, el servicio de custodia deberá operar en las regionales con dificultades de comunicación en las mismas condiciones establecidas.
- De igual forma este servicio contempla el mantener y garantizar la política de rotación de medios utilizada por la Entidad, la cual se entregará durante la etapa de entrada.
- El servicio de respaldos incluye la custodia de medios y a su vez contiene: almacenamiento, transporte de medios magnéticos, bóvedas especiales, personal capacitado en la manipulación de información y estrictas medidas de seguridad, que permitan garantizar la conservación y seguridad de la información. Los requerimientos mínimos que se deben cumplir con el servicio de custodia externa son:

    - La temperatura y humedad relativa del ambiente en el que se deben encontrar almacenados los medios para su custodia están en el siguiente rango:
    - Temperatura Impermeabilizada: 15°C a 25°C
    - Humedad Relativa: 40% a 60% y ambiente controlado.
    - Las cintas o medios resguardados deben colocarse en estantes o armarios adecuados en una biblioteca de cintas en sus respectivos Case.
    - Los medios resguardados deben contar con un único código de identificación de la empresa de custodia de medios, que permita su identificación y ubicación en los inventarios.
    - Contar con la opción de asignar códigos diferenciados.
    - Efectuar la marcación de medios magnéticos de acuerdo con la nomenclatura y/o estándar del ICBF.
    - Recibir como mínimo una (1) vez a la semana los medios a ser enviados en custodia.
- Administrar la(s) herramienta(s) de respaldo con la(s) que cuenta el ICBF.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Cumplir a cabalidad con lo definido por el ICBF respecto a la gestión de copias de seguridad y a la gestión para la restauración de copias de seguridad vigentes, junto a sus eventuales cambios que puedan presentarse durante el desarrollo del contrato.
- Realizar el monitoreo 7X24X365 de las soluciones de respaldo y el registro de incidencias presentadas, tales como fallos en la ejecución de una tarea de respaldo.
- Desarrollar las actividades relacionadas con respaldo (backups) y restauración (restore) dejando registradas las acciones realizadas en la herramienta de gestión suministrada por el ICBF.
- Realizar, en coordinación con el servicio de administración de aplicaciones, el levantamiento de aplicativos y bases de datos a nivel nacional, para determinar con los diferentes responsables la pertinencia de la creación, modificación o eliminación de las políticas de respaldo asociadas a estas.
- Realización de copias de seguridad exitosas de todas las aplicaciones, bases de datos, correo electrónico, repositorios del ICBF y plataforma de virtualización, así como la verificación y certificación de la correcta realización de estas con la(s) herramienta(s) de respaldo con la(s) que cuenta la Entidad de acuerdo con las políticas de Backups vigentes en el ICBF.
- Atender las solicitudes respectivas a las políticas de Backups de la Entidad (inclusión, modificación, retiro), especificadas a través del procedimiento descrito para tal fin y de acuerdo con los tiempos allí descritos.
- Revisar mensualmente las Políticas de Backups configuradas verificando Retención, Configuración, Ejecución, Rotación y las que solicite el supervisor del contrato.
- Coordinar internamente con el ICBF y la empresa encargada de la custodia externa de los medios, los tiempos de respuesta para la restauración de copias de seguridad en casos de contingencia como: daños de equipos, desastres naturales, robos, ataques malintencionados, siniestros, fortuitos o en los casos en que el ICBF lo requiera.
- Recibir medios magnéticos (CD provenientes de las regionales y cintas de las tareas de respaldo centralizado), y remitirlos a la empresa de custodia externa de medios.
- Suministrar las cintas requeridas (1800TB de almacenamiento en cintas anuales) para realizar tareas de backups, las cuales deberán ser proporcionadas de manera granular previa solicitud del supervisor del contrato, de tipo LTO8 o en la máxima referencia en uso por la Entidad.
- Mantener actualizada, en documentación previamente concertada con el ICBF, la información correspondiente como mínimo de:
    - Inventario de medios
    - Políticas de backups
    - Información respaldada
    - Reporte Consumo de almacenamiento (Cintas y Discos)
- Realizar por lo menos una (1) vez por semestre, tareas de mantenimiento preventivo

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

sobre las soluciones de backups con las que cuenta el ICBF, registrando las actividades realizadas en una bitácora y se presentarán en el informe del respectivo mes.

- Realizar actividades de restauración de pruebas, tanto a nivel de base de datos como de aplicación de los backups realizados, basado en un cronograma presentado anualmente y aprobado por la supervisión del ICBF.
- Prestar el servicio de Backups con las herramientas con la(s) herramienta(s) de respaldo con la(s) que cuenta la Entidad, para realizar las copias de seguridad de todas las aplicaciones, sistemas operativos de servidor, bases de datos, correo electrónico, repositorios de información y plataforma de virtualización.
- Realizar la migración de los respaldos desde la plataforma Networker hacia la nueva plataforma Veeam Backup & Replication, asegurando que los procesos de copia y retención en cinta se ejecuten en la librería IBM TS4300.
- Proveer y mantener vigente durante la ejecución del contrato el servicio de custodia de medios que cuente con: almacenamiento, transporte de medios magnéticos, bóvedas especiales, personal capacitado en la manipulación de información y estrictas medidas de seguridad, que permitan garantizar la conservación y seguridad de la información.
- Informar al líder del servicio del ICBF sobre extravío, hurto o deterioro de los medios dentro de las 24 horas de ocurrido el suceso. En estos casos el Contratista deberá asumir los costos de reposición respectivos.

6.9.12 SERVICIOS DE NUBE

6.9.12.1 GENERALIDADES DEL SERVICIO

El ICBF cuenta con servicios de infraestructura en la nube de Microsoft Azure, los cuales actúan como extensión de su plataforma tecnológica institucional y soportan la operación de aplicaciones, sistemas de información y servicios digitales de la Entidad. Azure proporciona capacidades de cómputo, almacenamiento, redes, bases de datos y seguridad, permitiendo el despliegue, administración y escalabilidad de los recursos tecnológicos requeridos para el cumplimiento de las funciones misionales y administrativas.

Estos servicios son provistos bajo un esquema de suscripción en la nube, alojados en centros de datos de Microsoft, lo que permite al ICBF disponer de una infraestructura flexible, segura y de alta disponibilidad, alineada con las necesidades operativas y los lineamientos de arquitectura tecnológica institucional.

6.9.12.2 ALCANCE

El ICBF utiliza los servicios de Microsoft Azure como una extensión de su infraestructura tecnológica institucional, para soportar los ambientes de Producción, Pruebas y Desarrollo,

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

permitiendo el despliegue, operación y escalabilidad de aplicaciones y servicios requeridos para el cumplimiento de sus funciones misionales y administrativas.
Así mismo, los servicios de Azure son utilizados como parte integral de la arquitectura de aseguramiento del acceso, soportando mecanismos de control, gestión y protección de los recursos tecnológicos, así como de los usuarios y dispositivos que acceden a las plataformas institucionales, en concordancia con los lineamientos de seguridad de la información de la Entidad.

El Contratista deberá administrar, soportar, gestionar y mantener los servicios de Microsoft Azure antes mencionados, garantizando su correcta operación y disponibilidad, así como su integración con los demás componentes tecnológicos de la Entidad, en escenarios de operación en línea, en sitio (onpremise) o bajo esquemas de operación híbrida, según aplique.

6.9.12.3 DESCRIPCIÓN DEL SERVICIO

El ICBF cuenta con servicios de Microsoft Azure suscritos y adquiridos con la empresa Microsoft Corporation, los cuales constituyen la base de su infraestructura tecnológica en la nube y deben ser administrados por el Contratista, de acuerdo con la línea base de usuarios, recursos y servicios definidos por la Entidad.

- En particular, el ICBF dispone de los siguientes servicios en la nube:
- Microsoft Azure Cloud Services: Plataforma de servicios de infraestructura y plataforma en la nube que permite al ICBF extender y complementar su infraestructura tecnológica local, soportando cargas de trabajo institucionales mediante servicios de cómputo, almacenamiento, redes, bases de datos y seguridad. Azure facilita la operación de los ambientes de producción, pruebas y desarrollo, garantizando escalabilidad, alta disponibilidad y continuidad del servicio conforme a las necesidades de la Entidad.

6.9.12.4 REQUERIMIENTOS DEL SERVICIO

Para la adecuada prestación del servicio, el ICBF requiere la administración integral de la plataforma Microsoft Azure, lo cual comprende las actividades de configuración, operación, soporte, monitoreo y mantenimiento de la infraestructura en la nube que soporta los sistemas de información y servicios institucionales.

El Contratista deberá asumir, como mínimo, los siguientes requerimientos y responsabilidades:

- Administrar, operar, monitorear y soportar de manera continua los servicios de Microsoft Azure contratados por el ICBF, garantizando su disponibilidad,

desempeño, estabilidad, capacidad, seguridad y correcta operación en los ambientes de Producción, Pruebas y Desarrollo.

- Gestionar el soporte técnico especializado de los servicios de Microsoft Azure, incluyendo la atención, seguimiento y escalamiento ante Microsoft de incidentes, requerimientos, problemas, fallas y eventos que afecten la infraestructura, los servicios en la nube o los entornos híbridos de la Entidad.
- Administrar, mantener y optimizar la arquitectura Cloud del ICBF, incluyendo la Landing Zone de Azure, suscripciones, grupos de administración, grupos de recursos, redes, almacenamiento, bases de datos, máquinas virtuales, servicios PaaS, componentes de integración y demás recursos que hagan parte del entorno tecnológico administrado.
- Administrar y mantener la integración entre los servicios de Microsoft Azure y la infraestructura On-Premise del ICBF, incluyendo la gestión de entornos híbridos, sincronización de servicios, conectividad, interoperabilidad y operación de los recursos tecnológicos que interactúen con la plataforma.
- Administrar los servicios de identidad, control de acceso y gobierno de recursos de Microsoft Azure, incluyendo usuarios, grupos, roles, permisos, RBAC, identidades administradas, políticas de acceso, segregación de funciones y demás mecanismos de control que permitan garantizar la seguridad y gobernabilidad de la plataforma.
- Implementar, administrar y mantener los mecanismos de gobierno de Azure mediante Azure Policy, Management Groups, Landing Zone, etiquetas (Tags), estándares de configuración, clasificación de recursos, organización de suscripciones y demás controles requeridos para asegurar la adecuada administración, trazabilidad y cumplimiento de los lineamientos definidos por el ICBF.
- Ejecutar actividades de mantenimiento, actualización, optimización, migración, reorganización, consolidación, transformación o traslado de recursos y servicios de Microsoft Azure que sean requeridas o autorizadas por el ICBF, garantizando la continuidad operativa, la minimización de riesgos y la documentación correspondiente de los cambios realizados.
- Administrar, configurar y operar los servicios de continuidad del negocio, respaldo, recuperación y recuperación ante desastres implementados sobre Microsoft Azure, garantizando la ejecución de copias de seguridad, recuperación de información y protección de recursos críticos conforme a los lineamientos establecidos por el ICBF.
- Administrar, mantener y optimizar Microsoft Azure Arc, así como los servicios asociados para la gestión centralizada de servidores y recursos híbridos, incluyendo la administración de configuraciones, inventario, extensiones, actualizaciones, parches de seguridad y demás funcionalidades habilitadas por la Entidad.
- Administrar y optimizar los servicios de monitoreo, observabilidad, registros, diagnóstico y alertamiento de Microsoft Azure, incluyendo herramientas como Azure Monitor, Log Analytics Workspace, Application Insights y demás servicios

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

equivalentes, garantizando la supervisión permanente de la plataforma y la atención oportuna de eventos operativos y de seguridad.

- Administrar y operar Microsoft Defender for Cloud, Microsoft Defender for Servers y demás servicios de seguridad habilitados por el ICBF, realizando el monitoreo, análisis, gestión y seguimiento de alertas, vulnerabilidades, recomendaciones, hallazgos, controles de cumplimiento, Secure Score y actividades de remediación que se requieran dentro del alcance del servicio.
- Realizar el control y seguimiento del consumo de los servicios de Microsoft Azure, manteniendo actualizado el inventario de recursos, la documentación técnica y de arquitectura, así como generando informes periódicos y recomendaciones orientadas a la optimización del servicio, el fortalecimiento de la seguridad, la mejora continua y la eficiencia en el uso de los recursos contratados.
- Gestionar todas las solicitudes de Incidentes, Requerimientos, Problemas y Cambios a través de los mecanismos definidos por el ICBF, garantizando el cumplimiento de los Acuerdos de Nivel de Servicio (ANS), el acceso a la información requerida para supervisión y auditoría, la participación en mesas técnicas cuando sea requerido y la ejecución de todas las actividades conforme a las mejores prácticas del fabricante, los lineamientos de arquitectura, seguridad y gobierno definidos por el ICBF y la normatividad vigente aplicable.

6.9.13 SERVIDORES Y ALMACENAMIENTO

6.9.13.1 GENERALIDADES DEL SERVICIO

El ICBF cuenta con una plataforma de servidores físicos, virtuales y en Cloud, en arquitecturas de alta disponibilidad y redundancia, en infraestructura tradicional, convergente e hyperconvergente que soportan los servidores de bases de datos, aplicaciones y herramientas de gestión en todos sus ambientes.

6.9.13.2 ALCANCE

El ICBF requiere la administración, gestión, operación, monitoreo, control y mantenimiento de la plataforma de servidores físicos, virtuales y en Cloud, en arquitecturas de alta disponibilidad y redundancia, en infraestructura hiperconvergente, así como la ejecución de todas las tareas recurrentes, programadas y no programadas para mantener en estado de operación óptima la plataforma de servidores que soportan servicios, aplicaciones y bases de datos del ICBF. La plataforma de servidores debe estar disponible, administrada, monitoreada y en operación 7X24X365. De igual forma se requiere la administración, monitoreo, ejecución de actualizaciones y garantizar la adecuada operación de los servicios, Dynamic Host Configuration Protocol (DHCP), File Server, FTP Server y Terminal Server.

El Contratista deberá tener capacidad para administrar con el recurso humano profesional y técnico requeridos para el servicio de servidores con una capacidad mínima, así:

SERVICIO	COMPONENTE	UNIDAD DE MEDIDA
SERVIDORES	Productivos	Número de Servidores de ambiente Productivo (Incluye 4 servidores de Almacenamiento).
	No Productivos	Número de Servidores de ambiente pre productivo.

Nota: Los elementos y características descritas en la tabla anterior, corresponden a la infraestructura actual del ICBF (Anexo 03 línea base) la cual podrá modificarse durante la ejecución del contrato, en consecuencia, el futuro contratista deberá adaptar la prestación de servicios a los cambios que se puedan dar sobre la infraestructura.

De otra parte, el contratista deberá proporcionar y operar durante toda la vigencia del contrato una infraestructura hiperconvergente en alta disponibilidad, nuevo no remanufacturada, incluyendo licencias, soporte técnico, mantenimiento y garantía.

Aunque la infraestructura se utilice bajo un esquema de servicio durante la ejecución del contrato, al finalizar este, el contratista deberá entregarse a la entidad todos los equipos, componentes, licencias y documentación asociada, de manera que la infraestructura pase a ser propiedad plena y definitiva de la entidad.

La transferencia de propiedad estará incluida dentro del valor del contrato, sin generar costos adicionales para la entidad, y se formalizará mediante las actas de entrega y recibo a satisfacción correspondientes. Asimismo, el contratista deberá garantizar que los bienes se entreguen libres de gravámenes o limitaciones y cumplir las obligaciones de garantía y calidad que resulten aplicables, que cumpla como mínimo la siguiente capacidad de cómputo:

Diez (10) nodos de última generación tipo rack que ocupen máximo dos (2) unidades de rack cada uno. Cada nodo deberá tener las capacidades y características relacionadas en la siguiente tabla:

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Ítem	Descripción propuesta agnóstica	Cantidad total
1.	Nodo de cómputo de arquitectura x86-64, de generación vigente al momento de presentación de la oferta, diseñado para centro de datos y montaje en rack, con una ocupación máxima de dos (2) unidades de rack por nodo. La configuración suministrada deberá estar soportada y certificada por el fabricante de la solución para operar como plataforma de virtualización e infraestructura hiperconvergente objeto del contrato.	10 nodos
1.1.	Procesamiento: Cada nodo deberá disponer de procesadores para centro de datos de generación vigente, con arquitectura x86-64 y una capacidad mínima agregada de sesenta y cuatro (64) núcleos físicos por nodo. La solución deberá garantizar capacidad de procesamiento empresarial, virtualización por hardware, eficiencia energética y capacidades de seguridad integradas. No se establece restricción respecto del fabricante, modelo, número de sockets o frecuencia específica del procesador, siempre que se cumpla o supere la capacidad y desempeño requeridos.	≥ 640 cores físicos
1.2.	Memoria: Cada nodo deberá contar con mínimo 2 TB de memoria RAM instalada, de tecnología DDR5 ECC RDIMM o tecnología de servidor vigente equivalente o superior, con mecanismos de detección y corrección de errores. La distribución, capacidad y cantidad de módulos será definida por el fabricante o proponente de acuerdo con la arquitectura del servidor, preservando el rendimiento y las mejores prácticas de configuración.	≥ 20 TB
1.3.	Almacenamiento: Cada nodo deberá proporcionar almacenamiento de estado sólido de alto rendimiento basado en tecnología NVMe o superior, con una capacidad bruta mínima equivalente a 215 TB por nodo. El proponente podrá determinar libremente la cantidad y capacidad individual de las unidades, siempre que garantice como mínimo la capacidad total requerida, compatibilidad certificada con la plataforma propuesta y características empresariales de disponibilidad, desempeño, resistencia y protección de datos.	≥ 2,15 PB brutos agregados
1.4.	Conectividad de datos: Cada nodo deberá disponer de conectividad redundante para tráfico de datos, con mínimo cuatro (4) interfaces físicas por nodo y velocidad mínima de 10 Gbps por interfaz, admitiendo interfaces de 10/25 GbE o superiores. Se deberán incluir todos los transceptores, DAC, AOC, cables o elementos de interconexión necesarios para la operación integral de la solución.	≥ 40 interfaces

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

1.5.	Alimentación eléctrica: Cada nodo deberá disponer de mínimo dos (2) fuentes de alimentación redundantes, dimensionadas de acuerdo con la configuración ofrecida, y suministrarse con los cables y conectores requeridos para su integración con la infraestructura eléctrica del centro de cómputo de la Entidad.	≥ 20 fuentes / conexiones redundantes
1.6.	Seguridad de hardware: Cada nodo deberá incorporar capacidades de seguridad basadas en hardware compatibles con TPM 2.0 o tecnología funcionalmente equivalente o superior, así como mecanismos de arranque seguro, protección de firmware y establecimiento de una cadena de confianza entre hardware y firmware.	≥ 1 por nodo
1.7.	Administración fuera de banda: Cada nodo deberá contar con una interfaz física dedicada para administración remota Out-of-Band (OOB), independiente del sistema operativo y de las interfaces de producción, con velocidad mínima de 1 GbE. Deberá permitir, como mínimo, encendido/apagado remoto, monitoreo de hardware, acceso remoto a consola, gestión de firmware, generación de alertas y administración segura. Se aceptarán tecnologías equivalentes independientemente de la denominación comercial utilizada por cada fabricante.	≥ 1 por nodo
1.8.	Conectividad adicional: Cada nodo deberá disponer de capacidad adicional de conectividad Ethernet con mínimo dos (2) puertos físicos y velocidad mínima de 10 GbE por puerto, mediante interfaces Base-T, SFP+, SFP28 o tecnología equivalente o superior, siempre que sea compatible con la arquitectura de red de la Entidad. Deberán incluirse los elementos necesarios para su conexión y puesta en funcionamiento.	≥ 2 puertos por nodo

La solución de infraestructura ofrecida deberá corresponder a un fabricante con reconocimiento y trayectoria comprobada en el mercado de infraestructura empresarial. Para efectos de garantizar la madurez tecnológica, capacidad de ejecución, evolución de producto, soporte y sostenibilidad de la solución, el fabricante de la plataforma principal de infraestructura deberá encontrarse ubicado en el cuadrante de Líderes (Leaders) del Magic Quadrant de Gartner correspondiente al mercado de Distributed Hybrid Infrastructure (DHI), o la categoría que lo sustituya o resulte equivalente para este tipo de soluciones, tomando como referencia la publicación vigente o la última publicada disponible a la fecha de cierre del proceso.
El oferente deberá aportar como parte de su propuesta documentación pública, certificación, comunicación del fabricante o referencia documental verificable que permita a la Entidad validar el cumplimiento de esta condición.
La exigencia anterior no implica la selección de una marca, fabricante o referencia específica, y se aceptarán soluciones de cualquier fabricante que satisfaga el criterio de

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

posicionamiento establecido y que, adicionalmente, cumpla o supere integralmente los requerimientos mínimos de capacidad de procesamiento, memoria, almacenamiento, conectividad, disponibilidad, interoperabilidad, administración, seguridad, soporte y demás características técnicas definidas por la Entidad.
La ubicación del fabricante en el cuadrante señalado constituye un criterio complementario de madurez y posicionamiento tecnológico y no sustituye la obligación del oferente de demostrar el cumplimiento integral de cada una de las especificaciones técnicas, funcionales y de servicio requeridas por el ICBF.

Nota: Las especificaciones técnicas establecidas corresponden a requerimientos mínimos de capacidad y funcionalidad. Se aceptarán arquitecturas, tecnologías y configuraciones equivalentes o superiores, independientemente del fabricante, siempre que el proponente demuestre técnicamente su cumplimiento y garantice la interoperabilidad, estabilidad, soporte, seguridad y operación integral de la solución. No se considerará como incumplimiento una configuración que utilice diferente número de procesadores, módulos de memoria, unidades de almacenamiento, tarjetas de red o componentes internos, cuando la capacidad total ofrecida sea igual o superior a la requerida y la configuración se encuentre soportada por el fabricante.

Tipo de Licenciamiento requerido:

SKU	Quantity	Product Description
SW-NCM-STR-PR	640	Subscription, Nutanix Cloud Manager (NCM) Starter Software License & Production Software Support Service for 1 CPU Core
SW-NCI-PRO-PR	640	Subscription, Nutanix Cloud Infrastructure (NCI) Pro Software License & Production Software Support Service for 1 CPU Core
SWA-NCI-SEC-PR	640	Subscription, Nutanix Cloud Infrastructure (NCI) Security add-on Software License & Production Software Support Service for 1 CPU Core

Para la puesta en funcionamiento e interconexión de la infraestructura requerida, el Contratista deberá suministrar dos (2) switches para centro de datos, cada uno con mínimo veinticuatro (24) puertos, con velocidad mínima de 10 Gbps por puerto. Se podrán utilizar interfaces ópticas, eléctricas o de conexión directa, tales como SFP+, SFP28, DAC, AOC o tecnologías equivalentes o superiores, siempre que garanticen la capacidad, desempeño, disponibilidad e interoperabilidad requeridos.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Con el propósito de garantizar madurez tecnológica, capacidad de ejecución, soporte y sostenibilidad de la solución, tanto el fabricante de los servidores o nodos de cómputo como el fabricante de los switches deberán encontrarse ubicados como Líderes (Leaders) en el Magic Quadrant de Gartner aplicable a su respectiva categoría tecnológica, tomando como referencia la última publicación disponible a la fecha de cierre del proceso.

Los servidores y switches podrán ser de fabricantes diferentes, siempre que cumplan individualmente el requisito anterior y garanticen su interoperabilidad con los demás componentes de la solución y con la infraestructura de red Core del ICBF. El oferente deberá aportar documentación verificable que permita acreditar el posicionamiento requerido. Esta condición no constituye referencia a una marca o fabricante específico ni sustituye el cumplimiento de las demás especificaciones técnicas.

El Contratista deberá incluir todos los transceptores, cables, interfaces, adaptadores, módulos, licencias y demás elementos de hardware y software necesarios para la instalación, configuración, integración y puesta en funcionamiento de la solución. También deberá incluir el licenciamiento o derechos de uso requeridos para los sistemas operativos y funcionalidades contratadas, sin generar costos adicionales para la Entidad durante la vigencia contractual.

Durante la ejecución del contrato, el Contratista deberá mantener los componentes de hardware, firmware y software en versiones soportadas por sus respectivos fabricantes y aplicar las actualizaciones y controles necesarios para garantizar la seguridad, disponibilidad, estabilidad y continuidad de la plataforma, conforme con los lineamientos establecidos por el ICBF.

Al finalizar el contrato, los equipos y demás elementos físicos suministrados deberán quedar bajo propiedad plena y definitiva del ICBF, libres de gravámenes, reservas de dominio o restricciones que limiten su administración, operación, actualización, soporte o disposición.

Las licencias perpetuas, cuando aplique, deberán quedar registradas, cedidas o transferidas al ICBF. Para modelos de suscripción, término o consumo, los derechos de uso deberán quedar registrados a nombre de la Entidad o permitir su administración directa, incluyendo continuidad, soporte y renovación.

Finalmente, el Contratista deberá entregar los equipos, componentes, licencias o derechos de uso, garantías, credenciales institucionales, configuraciones, respaldos, diagramas, inventarios, manuales y documentación técnica necesaria para garantizar la administración y continuidad de la infraestructura por parte del ICBF.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

6.9.13.3 DESCRIPCIÓN DEL SERVICIO

El ICBF cuenta actualmente con 576 servidores de los cuales 34 son físicos y se encuentran distribuidos en el Centro de Cómputo de la Sede de la Dirección General, el Data Center Externo y las 33 sedes regionales a nivel nacional. Los 542 servidores virtualizados son a través de la herramienta de virtualización Acrópolis Hypervisor y se encuentran alojados en los servidores físicos ubicados en el Datacenter, Centro de cómputo y en las 33 sedes regionales a nivel nacional y 1 servidores en plataforma Azure.

PRODUCCION	397
PRUEBAS	179
TOTAL	**576**

El ICBF cuenta con el licenciamiento de todos los sistemas operativos que estos equipos utilizan tanto en Windows Server, como Linux CentOS, RedHat y Oracle Linux.

En la actualidad ICBF cuenta con:

- Infraestructura de convergencia para 6 sedes regionales con configuración de File Server que comparten información con las estaciones de trabajo a través de la red LAN (Red de Área Local).
- Infraestructura de Hiperconvergencia 3 Clúster (1 de 4 nodos, 1 de 6 nodos y 1 de 10 nodos) para el Datacenter principal y 1 Clúster en el centro de cómputo en la sede nacional (compuesto por 3 nodos) del ICBF, basado en clúster de NUTANIX.
- Infraestructura de dos (2) PowerEdge R540, un (1) PROLIANT DL360 G8 y un (1) GOOGLE SEARCH APPLIANCE.

6.9.13.4 REQUERIMIENTOS DEL SERVICIO

- Realizar un plan de mejora continua donde se analice, diseñe, coordine y optimice las operaciones relacionadas con el sistema operativo e hipervisores; esto incluye las mejores prácticas del fabricante, actualizaciones, renombramiento de servidores, redistribución de clúster.
- Ejecutar el plan de mejora continua de las operaciones relacionadas con el sistema operativo e hipervisores, una vez analizados y aprobados por el ICBF y el Comité de Cambios del ICBF.
- Administrar los parámetros de los sistemas operativos de acuerdo con las mejores prácticas del fabricante y lineamientos dados por el ICBF.
- Generar toda la documentación relacionada con bitácoras, fichas técnicas, seguimientos de control, manuales de procedimientos y hojas de vida de los equipos servidores y las máquinas virtuales.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Mantener actualizados los servidores y sus sistemas operativos con los últimos niveles de firmware, parches y fixes ajustándose a cronogramas previamente aprobados con el ICBF.
- La realización de pruebas tanto para la instalación, como para actualización y configuración de software de sistema operativo, siguiendo los lineamientos establecidos por el ICBF y mejores prácticas del fabricante.
- El servicio de migración de los sistemas de información del ICBF a servidores en Nube pública y/o Privada y continuar con la administración en la nueva infraestructura tecnológica de propiedad o contratada por el ICBF.
- La administración y monitoreo del almacenamiento físico y lógico (Interno y externo) asignado al sistema operativo y a datos. Comprende actividades de planeación y ejecución de administración del almacenamiento de los servidores.
- El escalamiento, seguimiento continuo y solución del soporte reactivo y proactivo del hardware en garantía, para velar por las óptimas condiciones de la infraestructura tecnológica.
- Realizar mantenimientos preventivos de equipos servidores y diagnóstico de condiciones e infraestructura mínimo una vez al año o cuando el ICBF lo requiera.
- El análisis y ejecución de las configuraciones y arreglos de servidores necesarios para garantizar la alta disponibilidad de la plataforma central de servicios básicos de red (File Server, FTP Server, Terminal Server, DHCP); de tal forma que se garantice la disponibilidad 7X24X365 de los recursos de la red (DHCP, FTP Server, Terminal Server y File Server)
- La realización por parte del Contratista de recomendaciones sobre mejores prácticas para la definición e implementación de políticas de seguridad, administración de usuarios, políticas de backup, políticas particulares de administración y otras que apliquen para la correcta administración de los servidores, sistemas operativos, File Server, FTP Server, Terminal Server DHCP.
- Para los servidores en Cloud que el ICBF adquirió a través del acuerdo marco de precio de centro de datos/nube privada, será responsabilidad del contratista:
  - Administración de sistema operativo
  - Administración de las bases de datos instaladas
  - Administración de las aplicaciones instaladas
  - Administración de los demás componentes y elementos que se encuentren instalados
- El ICBF requiere la administración, operación, configuración y monitoreo del almacenamiento con el que cuenta el ICBF, así como también se requiere de la administración, operación, configuración y monitoreo del nuevo software y hardware que adquiera el ICBF durante la vigencia del contrato para mejorar el desempeño del almacenamiento. De igual forma se requiere de la implementación de las recomendaciones y solicitudes realizadas por parte de la Entidad. Administrar, gestionar, operar, monitorear, controlar y realizar mantenimientos a las plataformas hiperconvergentes, convergentes y físicas del ICBF, así como instalar las ultimas

actualizaciones (firmware, fixes, versiones) estables liberadas por el fabricante de acuerdo con las mejores prácticas.

- Instalar y configurar adecuadamente el software de Sistema Operativo y de aplicaciones de acuerdo con los requerimientos del ICBF y las mejores prácticas del fabricante.
- Generar un plan con el fin de que los logs de seguridad de los servidores queden en un repositorio centralizado el cual pueda ser indexado por una herramienta para la búsqueda de soluciones a incidentes presentados o consultados por el especialista del Contratista.
- Verificar las bitácoras de errores, problemas y logs para búsqueda de causas de incidentes ocurridos y/o para prevenir su ocurrencia.
- Instalar, configurar, administrar y monitorear nuevo hardware y software para servidores que entren en operación durante el contrato, cuando el ICBF así lo requiera.
- Realizar la instalación, configuración, administración y monitoreo a nivel de servidores, servicios DHCP, DNS, FTP Server, Terminal Server, File Server, FailOver Clúster, políticas GPO.
- Generar un plan y realizar la aplicación de actualizaciones a firmware, fixes y parches de sistemas operativos en servidores de producción el cual debe someterse a una fase de prueba en máquinas dedicadas para ello, las cuales son suministradas por el ICBF.
- Realizar la marcación de los servidores físicos de acuerdo con los lineamientos dados por el ICBF.
- Administrar, monitorear y mantener durante la ejecución del contrato los espacios en disco, realizando depuración y/o generando la notificación al ICBF a que haya lugar para prevenir incidentes.
- Generar y entregar al líder de servicio vía correo electrónico informe trimestral con la lista de servidores sin utilizar en un período igual o mayor a 3 meses.
- Configurar en todos los servidores objeto de monitoreo los agentes necesarios para la notificación en la herramienta de gestión que se encuentre en operación en el ICBF para la apertura de tickets.
- Notificar al líder del servicio del ICBF cualquier incidente que afecte la prestación del servicio, a través de correo electrónico y/o telefónicamente o por otro medio disponible según la hora de aparición del incidente, y actuar proactivamente en la búsqueda y aplicación de la solución.
- Proponer cambios en caso de requerirse, documentar y mantener actualizados los procesos, procedimientos, lineamientos e instructivos del servicio de Servidores.
- Analizar, diseñar, proponer y ejecutar las configuraciones y arreglos de servidores necesarios para dotar de alta disponibilidad la plataforma de clusterización de servidores.
- Instalar, configurar, administrar, monitorear y/o brindar apoyo a los proveedores sobre el nuevo hardware de servidores y software que entre en operación durante el contrato cuando el ICBF lo requiera.
- Analizar, diseñar, proponer y ejecutar las configuraciones necesarias previa verificación del ICBF de nuevos sistemas que optimicen procedimientos.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Generar los mapas lógicos de interconexión de servidores de aplicaciones y base de datos y mantenerlos actualizados.
- Dar respuesta a las consultas técnicas realizadas por el ICBF por el medio definido en acta de comité técnico y el tiempo establecido en ella, asesorando en el mejoramiento, estructura y ampliación de los servidores, con el fin de incluir nuevos servicios tanto para el cliente externo (servicios en Internet) como para el cliente interno, y respondiendo a las necesidades de crecimiento del ICBF en servicios y aplicaciones.
- Documentar cada ticket en la herramienta que disponga el ICBF (llamada de servicio, incidente o problema) relacionado con fallos en los servidores. Dar apoyo en el diagnóstico de las causas de estos, independientemente del ambiente del servidor (Piloto, Desarrollo, Pruebas, Producción) y presentar el informe respectivo.
- Mantener actualizado el listado de servidores, sus componentes y software instalado y suministrar la información al contratista de mesa de servicio con el fin de mantener la CMDB actualizada. Además, mantendrá actualizadas las hojas de vidas de los servidores en un formato diseñado para ello en conjunto y presentarlas al ICBF cuando este lo requiera.
- Llevar a cabo el análisis, diagnóstico y corrección de fallos y problemas técnicos presentados en hardware y en sistemas operativos y/o hacer seguimiento al proveedor o fabricante en el evento de que alguna solución requiera de tal escalamiento y presentar los informes correspondientes en un tiempo no superior a las 24 Horas siguientes al incidente.
- Cuando se presente una falla en los servidores y no sea posible la solución remota, El Contratista deberá desplazarse a los Datacenter y dar soporte en sitio.
- Permitir el acceso a ficheros compartidos por la red de área local.
- Mantener la disponibilidad de las soluciones de almacenamiento y File Server del ICBF.
- Mantener y presentar carpetas gestionando el acceso y permisos a los colaboradores del ICBF.
- Entregar en calidad de servicio y durante toda la etapa de operación una infraestructura tipo hiperconvergente en alta disponibilidad que incluya su licenciamiento, soporte técnico y garantía hasta la vigencia del contrato, que cumpla con las capacidades requeridas. En la implementación de la infraestructura como servicio el Contratista debe tener en cuenta todos los equipos o dispositivos necesarios para que la infraestructura requerida como servicio quede en operación, incluido el licenciamiento del sistema operativo de los servidores que requiera aprovisionar el ICBF sobre las versiones de Windows o Linux.

6.9.14 TELEFONIA

6.9.14.1 GENERALIDADES DEL SERVICIO

El ICBF cuenta con una plataforma de servidores físicos y virtuales en arquitecturas de alta disponibilidad y redundancia, en infraestructura tradicional, convergente e

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

hyperconvergente que soportan la plataforma de telefonía IP la cual está conformada por 14 servidores donde se centralizan los servicios a nivel Nacional y se cubren 7.500 extensiones.

6.9.14.2 ALCANCE

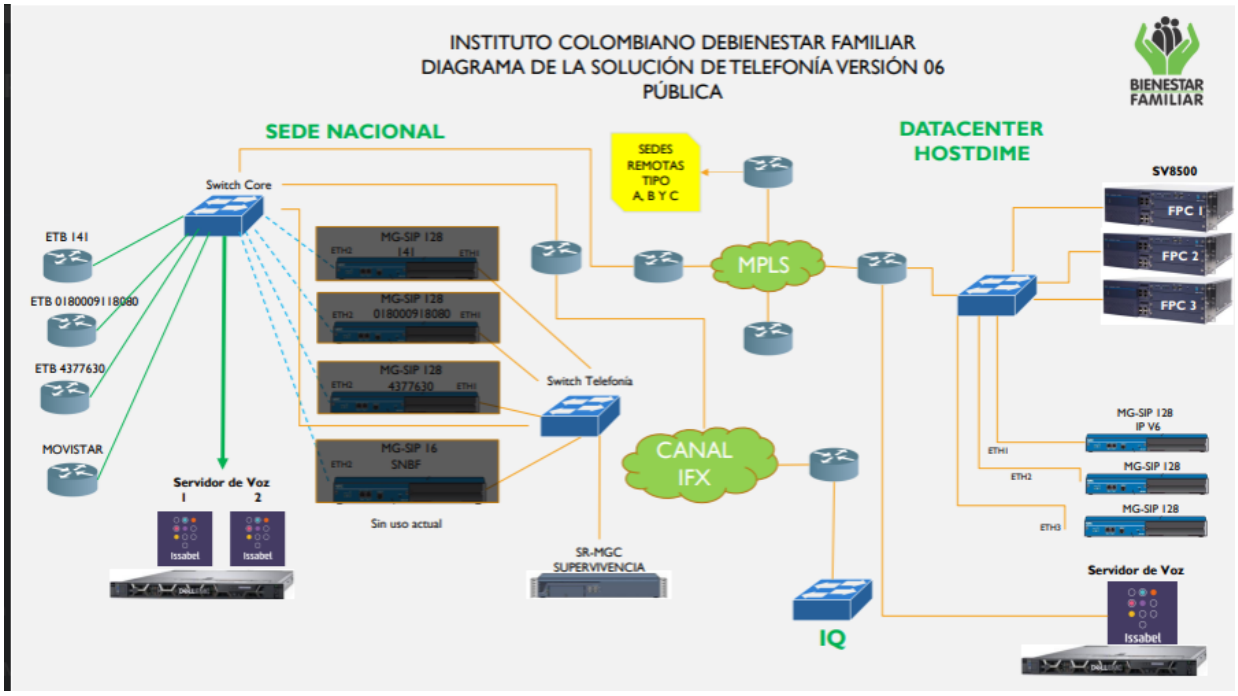
El ICBF requiere la administración, gestión, operación, monitoreo, control y mantenimiento de la plataforma de telefonía IP, en arquitecturas de alta disponibilidad y redundancia, en infraestructura tradicional, convergente e hyperconvergente, así como la ejecución de todas las tareas recurrentes, programadas y no programadas para mantener en operación continua la plataforma que soportan los servicios de VoIP del ICBF. La plataforma debe estar disponible, administrada, monitoreada y en operación 7X24X365.

6.9.14.3 DESCRIPCIÓN DEL SERVICIO

El servicio de Telefonía IP del ICBF está conformado por tres servidores de voz marca NEC modelo Univerge SV8500, los cuales se encuentran fusionados para operar como un solo servidor, dos servidores virtuales para el servicio de tarificación, un servidor NEC AVST LE2900 para el servicio de correo de voz, seis servidores virtuales para los servicios ISSABEL PBX en alta disponibilidad, los cuales se encuentran integrados con la solución NEC de manera activa al servicio, en estos se encuentran los servicios para las líneas de atención al ciudadano 141 y 018000918080, servidor de voz para enrutamiento de llamadas. Adicional a esto se cuentan con periféricos (Gateway, Supervivencias, MG-SIP, etc.) marca NEC distribuidos en diferentes centros zonales, regionales, datacenter externo y el datacenter de Sede Dirección General, los cuales dan servicio local de salida a la PSTN y de supervivencia en caso de una falla de canal ya que toda la plataforma se encuentra centralizada en Datacenter Principal y centro de cómputo sede Nacional.

Arquitectura actual del servicio

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012



6.9.14.4 REQUERIMIENTOS DEL SERVICIO

- Realizar un plan de mejora continua donde se analice, diseñe, administre, coordine y optimice las operaciones relacionadas con la plataforma de telefonía IP.
- Arquitectura actualizada del servicio.
- El contratista debe contar con un soporte de tercer nivel para la atención de incidentes o requerimientos para los que el especialista del servicio no pueda dar solución o respuesta.
- Administrar los parámetros de los sistemas operativos de acuerdo con las mejores prácticas del fabricante y lineamientos dados por el ICBF.
- Generar toda la documentación relacionada con bitácoras, fichas técnicas, seguimientos de control, manuales de procedimientos y hojas de vida de los equipos servidores y las máquinas virtuales.
- La administración y monitoreo del almacenamiento físico y lógico (Interno y externo) asignado al sistema operativo y a datos. Comprende actividades de planeación y ejecución de administración del almacenamiento de los servidores.
- Generación de reportes y estadísticas de funcionamiento de los equipos y sistemas a nivel de alarmas, fallas y niveles de utilización.
- Administración y gestión centralizada de la infraestructura de equipos telefónicos de usuario (teléfonos).
- Coordinar las actualizaciones de versiones e instalación de parches del firmware y sistema operativo recomendados por fabricantes o desarrolladores de ISSABEL PBX.

- Gestión de disponibilidad de las líneas análogas y digitales de todas las sedes.
- Gestionar backup de los servidores físicos y virtuales de manera periódica.
- Remitir informes de control de costos de telefonía mediante la utilización del sistema tarificador a la supervisión. El contratista deberá presentar las estadísticas de uso del sistema telefónico, discriminando por cada extensión por demanda durante la prestación de los servicios objeto de este contrato. Esta información deberá incluir una sección de análisis de tendencias y recomendaciones para la racionalización de los costos asociados a la telefonía.
- Administración, operación y gestión remota de la infraestructura de los servidores de telefonía IP y sistemas complementarios del ICBF a nivel de:
  - Consola de administración.
  - Sistema de correo de voz.
  - Consola de operadora.
  - Operadora automática
  - Centro de Atención Telefónica (Call Center)
  - Activación y desactivación de usuarios.
  - Programación de los servicios de los usuarios.
  - Actualización y modificaciones a la programación de los servidores de telefonía IP.
  - Backus de los servidores de telefonía IP.
  - Administración del plan de numeración telefónica.
- El escalamiento, seguimiento continuo y solución del soporte reactivo y proactivo del hardware en garantía, para velar por las óptimas condiciones de la infraestructura tecnológica.
- Administrar, gestionar, operar, monitorear, controlar y realizar mantenimiento a la plataforma de telefonía de manera centralizada atendiendo sus incidentes, requerimientos, cambios y problemas que se presenten a la misma.
- Realizar mantenimientos preventivos de equipos servidores y diagnóstico de condiciones e infraestructura mínimo dos (2) veces al año o cuando el ICBF lo requiera.
- Instalar, administrar, configurar y mantener actualizada la plataforma de telefonía IP, incluyendo servidores físicos, servidores virtualizados y aplicaciones de acuerdo con los requerimientos del ICBF y las mejores prácticas del fabricante.
- Generar un plan de integración con SIEM y un repositorio centralizado para los logs de seguridad de los servidores, el cual pueda ser indexado por una herramienta para la búsqueda de soluciones a incidentes presentados, correlación de eventos o consultados por el especialista de El Contratista. El análisis de éstos debe ser responsabilidad del SOC.
- Administrar, Verificar y mantener las troncales SIP, asegurando su registro, disponibilidad, calidad y correcta autenticación.
- Generar alertas por degradación de calidad de las llamadas, realizar escalamientos con operadores SIP
- Gestionar, configurar y/o actualizar de manera oportuna las extensiones, IVR, rutas entrantes y salientes, buzones de voz y demás elementos del plan de marcación.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Instalar, configurar, administrar y monitorear nuevo hardware y software para servidores de telefonía que entren en operación durante el contrato, cuando el ICBF así lo requiera.
- Realizar la marcación de los servidores etiquetado y documentación de los servidores de telefonía físicos y virtuales de acuerdo con los lineamientos dados por el ICBF.
- Aplicar parches de seguridad, actualizaciones controladas y procedimientos de mantenimiento preventivo y correctivo
- Configurar en todos servidores físicos y virtuales de telefonía objeto de monitoreo los agentes necesarios para la notificación en la herramienta de gestión que se encuentre en operación en el ICBF.
- Monitorear 7X24X365
- Documentar cada ticket en la herramienta que disponga el ICBF (llamada de servicio, incidente, requerimiento, problema) relacionado con fallos en los servidores Físicos o virtuales de telefonía.
- Notificar al líder del servicio del ICBF cualquier incidente que afecte la prestación del servicio, a través de correo electrónico y/o telefónicamente o por otro medio disponible según la hora de aparición del incidente, y actuar proactivamente en la búsqueda y aplicación de la solución.

6.9.15 MESA DE SERVICIO

6.9.15.1 GENERALIDADES DEL SERVICIO

El Instituto Colombiano de Bienestar Familiar (ICBF) requiere implementar una Mesa de Servicio de Tecnologías de la Información (TI) que opere como Punto Único de Contacto (SPOC) para todos los usuarios internos y externos. Este servicio garantizará la continuidad operativa y el adecuado desarrollo de las funciones misionales de la Entidad.

El servicio debe operar bajo mejores prácticas ITIL, asegurando la gestión integral del ciclo de vida de los servicios de TI.

6.9.15.2 ALCANCE

En el marco de la prestación del servicio de Mesa de Servicio, el CONTRATISTA deberá asegurar no solo la gestión integral de incidentes, requerimientos y solicitudes, sino también la articulación directa con las actividades de soporte técnico y mantenimiento de los equipos tecnológicos asociados a la operación del servicio.

6.9.15.3 DESCRIPCIÓN DEL SERVICIO

Se deberá prestar los servicios establecidos en el presente documento en estricto cumplimiento de las mejores prácticas del marco de referencia ITIL, así como de los

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

lineamientos técnicos, operativos y administrativos definidos por el ICBF. En este contexto, el CONTRATISTA será responsable de la gestión integral del servicio, garantizando su correcta operación, continuidad y calidad, mediante la ejecución de las actividades y obligaciones detalladas en los apartados correspondientes.

Operación de la Mesa de Servicio – Nivel 1

Recepción, registro, categorización, priorización y clasificación de incidentes, requerimientos y solicitudes de información, en la herramienta helppeople propiedad de la entidad.

Entrega de soluciones iniciales conforme con los procedimientos, guías, bases de conocimiento y lineamientos establecidos por el ICBF.

Atención telefónica, remota y por los canales definidos por la Entidad.

Gestión de Soporte en Sitio

Prestación del soporte técnico en sitio para los servicios TIC incluidos en el presente documento.

Ejecución de actividades de diagnóstico, resolución y verificación técnica según los procedimientos definidos.

Gestión y Escalamiento

Escalamiento oportuno de incidentes y requerimientos a los líderes técnicos y funcionales responsables, siguiendo los flujos establecidos.
Seguimiento continuo al avance de los casos escalados hasta su resolución final.

Cierre y Validación con el Usuario

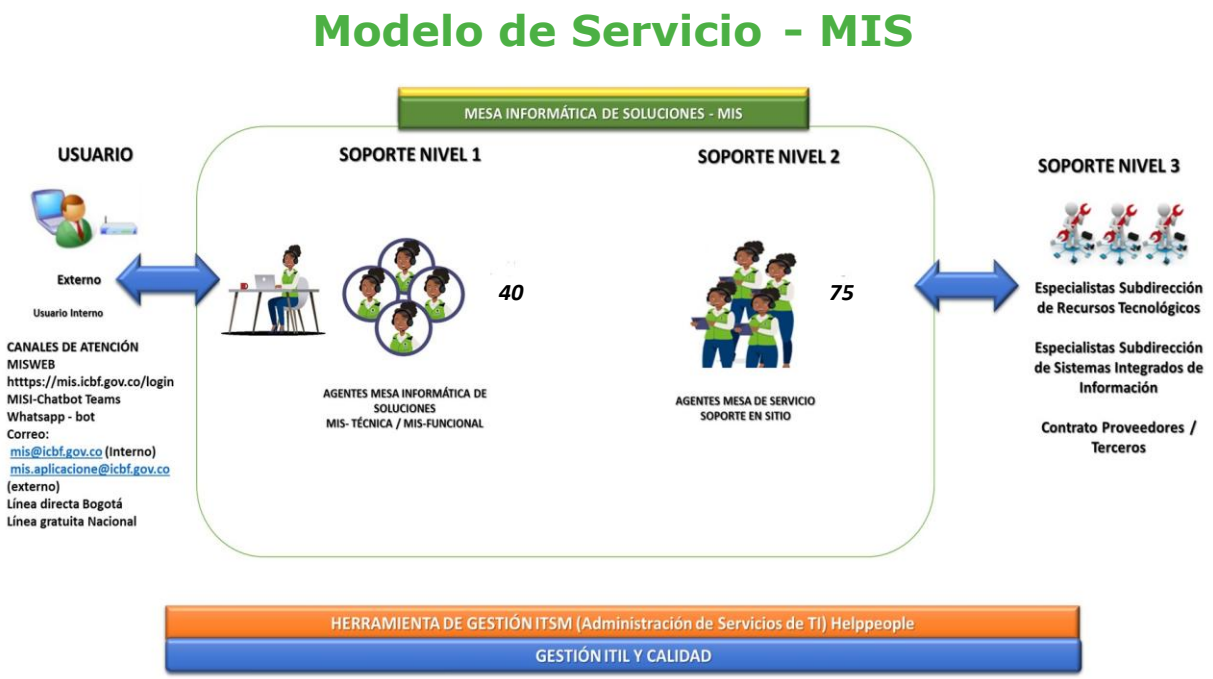
Confirmación con el usuario final sobre la solución implementada y la conformidad para proceder al cierre del caso.
Registro y gestión de la encuesta de satisfacción asociada a cada solicitud atendida.

Cumplimiento de Acuerdos de Niveles de Servicio (SLA)

Asegurar que todas las actividades operativas y de soporte se ejecuten conforme con los niveles de servicio, tiempos de respuesta y tiempos de solución definidos en este Pliego de Requisitos en el *Anexo 02 - Acuerdos de Nivel de Servicio.*
Calidad, Control y Mejora Continua

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Implementar prácticas de mejora continúa alineadas con ITIL.
- Mantener actualizada la documentación operativa requerida para la correcta gestión del servicio.



6.9.15.4 CONDICONES BASICAS

Niveles de escalamiento

El modelo de escalamiento se define en forma específica por cada servicio, solución y aplicación, para lo cual el ICBF suministrará el modelo de servicio actual, dentro de la ejecución del contrato se espera que el modelo de servicio sea actualizado para cumplir con las mejores prácticas de ITIL.

Dentro del modelo de servicio actual se tienen contemplados los siguientes niveles de escalamiento:

Nivel 1 - Mesa de Servicio.

Estará conformado por los Agentes de primer nivel, quienes recibirán, registrarán y gestionarán las solicitudes a través de los canales habilitados (llamadas telefónicas, portal

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

web, chat, correo electrónico, WhatsApp y Microsoft Teams). Sus responsabilidades incluyen, entre otras, las siguientes actividades:

- Recepción, registro y atención inicial de solicitudes, incidentes, requerimientos e inquietudes reportadas por los usuarios.
- Clasificación, categorización y priorización de cada solicitud conforme a los modelos establecidos por el ICBF (informativa, peticiones, problemas, incidentes, accesos).
- Suministro de información general sobre procesos, lineamientos y servicios institucionales del ICBF.
- Orientación funcional y técnica básica sobre el uso adecuado de aplicaciones, servicios y componentes tecnológicos requeridos por el ICBF.
- Gestión de creación, activación, desactivación y cambio de contraseñas en Directorio Activo, como parte del soporte de primer nivel y en cumplimiento de los procedimientos de seguridad definidos por la Entidad.
- Cierre de tiquetes durante la atención cuando la solicitud sea resuelta en primer nivel.

En los casos en los cuales la solicitud no pueda ser resuelta en el primer nivel o cuando el modelo de servicio correspondiente exija la intervención de equipos especializados, el ticket deberá ser escalado oportunamente con toda la información técnica y funcional necesaria para su correcta atención por parte de los agentes de Nivel 2 y/o especialistas.

Dentro de las funciones de la Mesa de Servicio se incluye también el seguimiento integral al ciclo de vida de los tickets, así como la verificación del cumplimiento de los niveles de servicio (SLA) definidos para todos los niveles de atención.

Nivel 2 - Soporte en sitio

Encargados de atender y resolver los incidentes y requerimientos técnicos que no pueden ser gestionados por el Nivel 1. Este equipo está conformado por agentes con conocimientos avanzados en sistemas operativos, redes, hardware, software institucional y plataformas tecnológicas.

Sus funciones incluyen la ejecución de diagnósticos técnicos **detallados**, la administración remota de equipos, la aplicación de configuraciones específicas y el seguimiento de incidentes que requieren análisis presencial.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Adicionalmente, el Nivel 2 documenta las soluciones aplicadas, propone mejoras a la Mesa de Servicio y, cuando la criticidad o naturaleza del incidente lo requieren, realiza la escalación formal a los especialistas (Nivel 3) para su atención y gestión, este nivel está conformado por la siguiente estructura operativa:

Coordinador de Soporte en Sitio (1): Responsable de la coordinación nacional del equipo, la planificación operativa, la distribución de cargas de trabajo y el seguimiento al cumplimiento de los niveles de servicio (SLA).

Agentes de Soporte en Sitio (92) distribuidos a nivel nacional: Estos agentes atienden incidentes y requerimientos técnicos de manera presencial en las sedes del ICBF de acuerdo con el Anexo 07 sedes de soporte en sitio.

El número de agentes corresponde a los recursos asignados para la prestación del servicio y no a personal permanente en cada sede. Los agentes de soporte en sitio deberán desplazarse a las sedes con atención presencial según las necesidades operativas. Por su parte, las sedes con atención remota serán atendidas a través de los canales definidos y, en caso de requerirse una intervención presencial, esta será coordinada y escalada a los ingenieros regionales.

En consecuencia, la cantidad de perfiles relacionados no debe interpretarse como una asignación individual y permanente por sede, sino como la definición de la cobertura operativa requerida para atender las diferentes ubicaciones de acuerdo con el modelo de prestación del servicio establecido.

El ICBF suministra los puestos de trabajo para estos agentes de acuerdo con la distribución a nivel nacional.

Nota: En caso de que alguna de las sedes definidas en el Anexo 07 – Sedes de soporte en sitio sea modificada o reubicada durante la vigencia del contrato, y dicha nueva ubicación se encuentre dentro del casco urbano de la regional correspondiente, el proveedor deberá garantizar la cobertura mediante soporte presencial en sitio.

Cuando la nueva ubicación se encuentre por fuera del casco urbano de la regional, la atención se realizará de manera remota, sin que ello implique incumplimiento de los niveles de servicio establecidos, salvo que el ICBF disponga expresamente lo contrario.

Distintivo Institucional

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

El servicio comprende el suministro del uniforme con la imagen institucional del ICBF, asignado por Agente, y deberá cumplir con las características que se describen a continuación:

El Proveedor deberá suministrar una (1) chaqueta convertible en chaleco, elaborada en material impermeable, poliéster u otro material de características equivalentes definido por EL CONTRATISTA. La prenda deberá incluir:

- Cierre frontal en cremallera.
- Bolsillos funcionales.
- Diseño y combinación de colores según las especificaciones definidas por el ICBF.
- Aplicación de la imagen institucional conforme a los lineamientos vigentes del Instituto.

Cada uniforme deberá ser entregado completamente nuevo al inicio de la operación, previa coordinación entre el ICBF y el Proveedor. La entrega deberá quedar documentada mediante acta de recibo o mecanismo equivalente aprobado por el ICBF.

La prenda deberá tener una vida útil mínima de doce (12) meses bajo condiciones normales de uso.

En caso de que la vigencia de la orden de compra exceda dicho periodo o se requiera continuidad del servicio de uniformidad institucional, deberá garantizarse la reposición correspondiente.

Al vencimiento de la orden de compra, o cuando se presente cambio de Agente durante su ejecución, cada uniforme suministrado deberá ser devuelto al Proveedor.

El Proveedor será responsable de realizar la destrucción controlada del uniforme, asegurando la eliminación adecuada de la imagen institucional y evitando su uso posterior.

La destrucción deberá ser soportada mediante certificado o evidencia documental entregada al ICBF.

Canales de Comunicación o de Atención al Usuario.

El servicio será atendido mediante los siguientes medios, los cuales deberán ser provistos y operados integralmente por EL CONTRATISTA, salvo donde se indique lo contrario:

a) Número único nacional (018000).

b) Número fijo local.

c) Herramienta de tickets web — la plataforma será provista por el ICBF; el CONTRATISTA debe asegurar su uso operativo.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

d) Chat en línea, WhatsApp y Microsoft Teams.

e) Correos institucionales:

mis@icbf.gov.co

mis.aplicaciones@icbf.gov.co

Canal telefónico

EL CONTRATISTA deberá suministrar las líneas telefónicas solicitadas por el ICBF, incluyendo:

Línea fija local directo.

Extensión telefónica (si aplica).

Al finalizar la vigencia de la orden de compra, EL CONTRATISTA deberá ceder las líneas a la Entidad Compradora, salvo que esta decida no recibirlas.

Nota técnica: La extensión telefónica aplica únicamente cuando la Mesa de Servicios opere fuera de instalaciones del ICBF y la comunicación hacia el centro de soporte requiera enrutamiento externo (instalaciones del CONTRATISTA o terceros).

Canal Web

El CONTRATISTA deberá gestionar La herramienta de tickets: la creación, gestión y consulta de casos vía página web.

Integrarse con los lineamientos técnicos y de seguridad del Instituto.

Correo electrónico

EL CONTRATISTA deberá gestionar el canal de correo de atención, las cuentas de correo institucional asociadas a la Mesa de Servicios:

mis@icbf.gov.co

mis.aplicaciones@icbf.gov.co

Chat en línea / WhatsApp / Teams

El CONTRATISTA será responsable de gestionar, registrar, clasificar y realizar seguimiento a todas las solicitudes recibidas a través de los canales de atención habilitados, asegurando su registro y trazabilidad en la herramienta de gestión de tickets definida por el ICBF.

Los canales digitales implementados deberán cumplir con los requisitos de accesibilidad digital y diseño universal establecidos en la normatividad vigente, permitiendo su uso por

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

parte de personas con discapacidad y demás grupos de interés, en concordancia con lo establecido en la Ley 1346 de 2009, la Ley 1618 de 2013, la Norma Técnica Colombiana NTC 5854 y las Pautas de Accesibilidad para el Contenido Web (WCAG) en su versión vigente.

• Chat en línea con agente (suministrado por la herramienta de gestión definida por la Entidad).

• WhatsApp empresarial, incluyendo línea telefónica, configuración y soporte suministrados por el CONTRATISTA.

• Microsoft Teams, cuando se requiera integración interna.

Al finalizar el contrato, y cuando el ICBF lo requiera, el CONTRATISTA deberá adelantar el proceso de cesión o transferencia de la línea de WhatsApp utilizada para la prestación del servicio a favor de la Entidad, garantizando la continuidad del canal de atención.

EL CONTRATISTA será responsable de gestionar, registrar, clasificar y dar seguimiento a todas las solicitudes que se reciban a través de cualquiera de estos canales, asegurando su trámite en la herramienta de gestión de tickets definida por el ICBF y manteniendo la trazabilidad completa del proceso.

Chat en línea con agente. (Suministrado por la herramienta de gestión de la entidad)

Microsoft Teams (si se requiere integración interna).

6.9.15.5 REQUERIMIENTOS DEL SERVICIO

- La herramienta de gestión de Mesa de Servicio dispuesta por el ICBF – HelpPeople en su última versión deberá ser utilizada para registrar, documentar y administrar la totalidad de los tickets derivados de incidentes, requerimientos y controles de cambio.
- EL CONTRATISTA deberá cumplir estrictamente con los horarios, tiempos de atención y tiempos de respuesta establecidos por el ICBF.
- EL CONTRATISTA deberá entregar, durante la etapa de transición de entrada, un procedimiento detallado de atención, que incluya:
  - Metodología para diagnóstico, atención y solución de incidentes, problemas, solicitudes y requerimientos.
  - Proceso de seguimiento, cierre y registro en la herramienta de Mesa de Servicio.

  Este procedimiento estará sujeto a revisión y aprobación del Supervisor del Contrato.
- Los tiempos máximos de atención y resolución para incidentes, problemas y solicitudes estarán determinados por la severidad o criticidad asignada a cada caso.
- La prioridad de atención será establecida por el ICBF conforme al Modelo de la Mesa de Servicio institucional y el anexo de ANS.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Todos los incidentes, problemas y solicitudes deberán quedar registrados obligatoriamente en la herramienta de Mesa de Servicio, ya sea a través de mecanismos automáticos o mediante registro manual.
- Para cada uno de los servicios descritos en el numeral 6.7 se requiere que en la herramienta de gestión de mesa de servicio que disponga el ICBF se gestione y documenten los tickets que por incidentes, requerimientos y controles de cambios que se generen. En el caso de requerimientos, el Contratista deberá ajustarse a los horarios y tiempos de respuesta establecidos en el modelo ITSM.
- Debe contar con un procedimiento detallado de atención, diagnóstico, solución de solicitudes, problemas e incidentes y seguimiento, el cual será entregado durante la etapa de transición de entrada y estará sujeto a aprobación por parte del supervisor del contrato. Dentro de dicho procedimiento se debe detallar todos los datos de contacto telefónicos, correo electrónico u otros existentes, también de centro(s) de atención, ubicación y datos de contacto del equipo de trabajo que ofrece el soporte y niveles de escalamiento.
- El Contratista deberá ofrecer soporte telefónico, remoto, presencial, vía web y acceso a bases de conocimiento.
- Los tiempos máximos de atención para los incidentes, problemas y solicitudes dependerán de su severidad, esta prioridad será establecida por la Entidad en el Modelo de la Mesa de Servicio y/o en el Anexo 02 - Acuerdos de Niveles de Servicio.
- Es responsabilidad del contratista realizar el registro en caso de haber sido informado de una manera alterna o haber sido quien identifico el incidente.
- El contratista deberá documentar cada ticket en la herramienta que disponga el ICBF (llamada de servicio, incidente, requerimiento o solicitud o problema) relacionado con fallos en los servicios. Adelantar el diagnóstico de las causas de estos y presentar el informe respectivo.
- Todo incidente, problema o solicitud será cerrado de común acuerdo entre el ICBF y el Contratista siempre y cuando la situación presentada se haya resuelto satisfactoriamente para la entidad, y se darán por terminados o cerrados cuando la entidad informe que el problema, incidente o solicitud quedo solucionado. Además, se debe realizar soporte técnico presencial o remoto, todos con previo aval del supervisor y su acompañamiento para realizar actividades programadas y de visitas técnicas periódicas.
- Se requiere que en la herramienta de gestión de mesa de servicio que disponga el ICBF HelpPeople se gestione y documenten los tickets que por incidentes, requerimientos y controles de cambios se generen. En el caso de requerimientos, EL CONTRATISTA deberá ajustarse a los horarios y tiempos de respuesta establecidos en el modelo ITSM.
- Debe contar con un procedimiento detallado de atención, diagnóstico, solución de solicitudes, problemas e incidentes y seguimiento, el cual será entregado durante la etapa de transición de entrada y estará sujeto a aprobación por parte del supervisor del contrato.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Dentro de dicho procedimiento se debe detallar todos los datos de contacto telefónicos, correo electrónico u otros existentes, también de centro(s) de atención, ubicación y datos de contacto del equipo de trabajo que ofrece el soporte y niveles de escalamiento.
- EL CONTRATISTA deberá ofrecer soporte telefónico, remoto, presencial, vía web y acceso a bases de conocimiento.
- Los tiempos máximos de atención para los incidentes, problemas y solicitudes dependerán de su severidad, esta prioridad será establecida por la Entidad en el Modelo de la Mesa de Servicio y/o en el Anexo 02 - Acuerdos de Niveles de Servicio.
- Todo incidente, problema y/o solicitud deberá estar registrado en la herramienta de Mesa de Servicio ya sea a través de procesos manuales o automáticos, es responsabilidad de EL CONTRATISTA realizar el registro en caso de haber sido informado de una manera alterna o haber sido quien identifico el incidente.
- El soporte de nivel 1 y en sitio serán suministrados por la mesa de servicio y el soporte de nivel 3 corresponderá al servicio que será atendido por la operación de infraestructura tecnológica.
- El soporte en sitio deberá verificar y mantener actualizada la CMDB cada vez que realice un servicio.
- El Contratista deberá gestionar, tramitar y hacer seguimiento de las garantías con los diferentes proveedores que tenga la entidad.
- La estrategia de infraestructura y calidad de servicio de EL CONTRATISTA deberá cumplir con los ANS indicados para este contrato.
- En el modelo de prestación de los servicios EL CONTRATISTA deberá adoptar las mejores prácticas de ITIL en cuanto a la entrega y soporte de estos. Deberá acompañar a la Dirección de Tecnologías de la Información (DTI) en actividades de adaptación, actualización, implementación y mejora de los procesos implementados con el proveedor actual (Gestión de Incidentes, Gestión de Requerimientos, Gestión de Configuraciones, Gestión de Problemas y de ser necesario Gestión de Cambios).
- EL CONTRATISTA deberá contemplar con carácter obligatorio, los requerimientos realizados por el ICBF y debe garantizar los servicios con la calidad ofertada, la cual no puede ser inferior a la solicitada en documentos y anexos.
- EL CONTRATISTA deberá ofrecer y facturar el servicio según la demanda real para lo cual el ICBF entregará el Anexo 06 - Catalogo de Servicios para el dimensionamiento de los servicios con las proyecciones anuales de crecimiento sobre las líneas base.
- EL CONTRATISTA debe prestar los servicios con personal calificado, especializado que cumpla con los perfiles y experiencia exigidos por el ICBF como se indica en el Anexo 01 - Personal mínimo requerido. EL CONTRATISTA deberá Diseñar, Entregar y Aplicar los formatos, Procesos y Procedimientos para la prestación del servicio con el detalle que el ICBF lo exija.
- El CONTRATISTA deberá implementar y ejecutar mensualmente un mecanismo de evaluación de la calidad de la atención y gestión realizada por los agentes de Mesa de Servicio y Soporte en Sitio, mediante criterios objetivos relacionados con el

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

cumplimiento de ANS, calidad y documentación de los tickets, adherencia a procedimientos, resolución en primer contacto cuando aplique, casos reabiertos, satisfacción del usuario y calidad de la atención. Los resultados deberán consolidarse en el informe mensual del servicio e incluir hallazgos, tendencias, oportunidades de mejora y planes de acción cuando se identifiquen desviaciones.

6.9.16 SEGURIDAD INFORMÁTICA

El Instituto Colombiano de Bienestar Familiar (ICBF), en su rol de entidad pública responsable de la protección integral de primera infancia, niñez, adolescencia y el bienestar de las familias colombianas, administra información altamente sensible, datos personales de menores de edad y plataformas tecnológicas críticas que soportan procesos misionales del Estado. Esta condición exige la adopción de un modelo de ciberseguridad moderno, robusto, escalable y alineado con las mejores prácticas internacionales.

En cumplimiento de sus obligaciones legales y regulatorias, el ICBF ha definido una estrategia integral de ciberseguridad basada en el modelo Zero Trust (Confianza Cero), alineada con el MSPI de MinTIC, los CONPES 3995 y 4144, la Ley 1581 de 2012, la Ley 1712 de 2014, así como con estándares internacionales tales como ISO/IEC 27001:2022, NIST SP 800-207 (Zero Trust Architecture), NIST Cybersecurity Framework 2.0, MITRE ATT&CK, MITRE D3FEND y CIS Controls v8.

Adopción del modelo Zero Trust

El ICBF ha evolucionado desde el modelo tradicional de seguridad perimetral basado en “confiar, pero verificar” hacia un modelo Zero Trust fundamentado en el principio “nunca confiar, siempre verificar”, en el cual ninguna entidad usuario, dispositivo, aplicación, servicio, sesión o flujo de datos es considerada confiable por defecto, independientemente de su ubicación dentro o fuera del perímetro institucional.
Este modelo se sustenta en principios estratégicos tales como:

- Verificación continua de identidades, dispositivos, aplicaciones y sesiones.
- Aplicación del principio de mínimo privilegio.
- Segmentación y microsegmentación de la red.
- Reducción sistemática de la superficie de ataque.
- Autenticación fuerte y adaptativa.
- Autorización contextual basada en riesgo.
- Monitoreo continuo y respuesta automatizada.
- Protección integral de datos en reposo, en tránsito y en uso.
- Resiliencia operativa frente a amenazas avanzadas y de día cero.

Inteligencia Artificial como capacidad transversal

Frente al crecimiento de amenazas impulsadas por Inteligencia Artificial Generativa, malware polimórfico, phishing automatizado, deepfakes y ataques adaptativos, el ICBF ha determinado que las tecnologías de ciberseguridad deberán incorporar de forma transversal capacidades avanzadas de IA, Machine Learning, analítica de comportamiento, correlación inteligente, automatización de respuesta y aprendizaje continuo, alineadas con los Lineamientos de Seguridad y Privacidad de la Información para Sistemas de Inteligencia Artificial publicados por MinTIC.

Todas las plataformas que soportan los servicios objeto del presente proceso deberán incorporar capacidades de Inteligencia Artificial y Aprendizaje Automático, de forma nativa o mediante módulos licenciados del propio fabricante, habilitadas y en operación durante toda la vigencia contractual. Estas capacidades deberán estar orientadas a la detección de comportamientos anómalos, la identificación de amenazas desconocidas, la correlación inteligente de eventos, la priorización de alertas por riesgo y contexto, la reducción de falsos positivos y la recomendación o ejecución de acciones de respuesta, incluyendo la protección frente a amenazas generadas, automatizadas o potenciadas mediante inteligencia artificial.
Para efectos del presente anexo, se entiende acreditada la existencia de dichas capacidades cuando el fabricante las documenta en su hoja de datos pública, manual oficial o documentación técnica vigente del modelo ofertado. El oferente acreditará este requisito mediante dicha documentación, sin que se exija denominación comercial, arquitectura, modelo algorítmico ni tecnología específica de un fabricante determinado.
La provisión del licenciamiento no constituye, por sí sola, cumplimiento de este requisito. El cumplimiento se acredita mediante la habilitación efectiva de las capacidades, su parametrización conforme a la realidad operativa, los activos y los procesos misionales del ICBF, su afinamiento periódico y la entrega de evidencias verificables de su operación, conforme a las actividades, entregables y criterios de verificación.

Resiliencia digital y continuidad operativa

La estrategia Zero Trust se complementa con un enfoque integral de resiliencia digital que garantiza la continuidad de los servicios institucionales mediante alta disponibilidad, arquitecturas redundantes, planes de contingencia (DRP/BCP), análisis de impacto al negocio (BIA), protección frente a ransomware, monitoreo continuo y gestión integral de crisis cibernéticas.

Gobierno y cumplimiento

El modelo Zero Trust se soporta en un marco de gobierno, cumplimiento y cultura fundamentado en el SGSI ISO/IEC 27001:2022, el MSPI de MinTIC, la gestión de riesgos bajo ISO 27005, el cumplimiento normativo, la sensibilización institucional, la coordinación con el ColCERT y el CSIRT Gobierno, y la participación activa en iniciativas nacionales de ciberseguridad.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

6.9.16.1 GENERALIDADES DEL SERVICIO

Dada la gran cantidad de servicios TIC que ofrece el Instituto Colombiano de Bienestar Familiar y la gran demanda de los funcionarios y la ciudadanía en general, la Entidad se ve en la obligación de salvaguardar y asegurar la infraestructura tecnológica que componen los aplicativos misionales y de apoyo, servidores, bases de datos y todos los servicios internos y externos que operan la red de la Entidad. Adicional a esto, la Entidad adopta los lineamientos establecidos por el MinTIC con referencia a la adopción del protocolo IPv6.

El creciente uso de internet ha impulsado al ICBF a permitir a sus proveedores, funcionarios y otras Entidades gubernamentales acceder a los sistemas de información desde sedes externas impulsando iniciativas de movilidad en el trabajo, por lo cual se han configurado accesos VPN (Virtual Private Network) para mantener y mejorar los niveles de seguridad exigidos en la política de seguridad de las Información de la Entidad. Dichos accesos son de tipo sitio a sitio y cliente a sitio y son protegidos mediante cifrado SSL para VPN estándar y también VPN con IPSEC, actualmente los enlaces VPN son:

CANTIDAD	TIPO VPN
19	Site to Site
6800 usuarios	SSL
5	IpSec Client to Site

El ICBF cuenta con licenciamiento de antivirus Microsoft System Center 2012 Endpoint Protection con cobertura a 1.000 usuarios con administración centralizada desde consola System Center Configuration Manager (SCCM), Antivirus Microsoft Defender con 28.000 licencias de Endpoint y 900 licencias para servidores. licencias que funcionan de forma recurrente y bajo arquitectura de consola de administración centralizada en la nube, agente para servidores (Windows / Linux) la cual permite acceso a herramientas de gestión del antivirus, generación de reportes y atención de alertas tanto en servidores como en endpoints contando con módulos de Protección Contra Amenazas, Control de periféricos, Restricción de aplicaciones, Prevención de perdida de datos (DLP), Control WEB, Gestión de actualizaciones, Firewall de Windows, las actualizaciones de definiciones se distribuyen mediante cache servers distribuidos en las sedes Regionales del ICBF.

6.9.16.2 ALCANCE

El servicio de seguridad informática y seguridad digital se encarga de proteger los sistemas de información digital que maneja el ICBF para cumplir con su misión y objetivos institucionales. Todas las actividades del servicio giran en torno a mantener la disponibilidad, confidencialidad, integridad, no repudio, análisis y tratamiento de riesgos a los que se expone la información institucional. A su vez este servicio debe garantizar la

protección y correcto acceso y uso de todos los servicios informáticos, evitando la divulgación, intercepción o destrucción no autorizada de la información.

Prestar al ICBF un servicio administrado e integral de seguridad informática y seguridad digital, que incluya la administración, operación, monitoreo, soporte especializado, mantenimiento, optimización y mejora continua de las capacidades de ciberseguridad de la entidad, sin suministro de equipos, sobre la infraestructura y plataformas tecnológicas definidas por el ICBF dentro del alcance contractual.

Alcance técnico mínimo

El servicio deberá incluir como mínimo:

- Administración y operación de la seguridad endpoint en equipos de usuario final.
- Administración y fortalecimiento de la seguridad de aplicaciones, sistemas operativos, servidores y bases de datos.
- Administración y operación de controles de seguridad para correo electrónico.
- Detección, análisis y respuesta frente a amenazas avanzadas y APT.
- Administración y operación de controles de seguridad de red y apoyo a la protección perimetral e interna.
- Operación de acceso seguro para usuarios externos mediante ZTNA/SSE y autenticación multifactor por software.
- Gestión de vulnerabilidades y gestión de parches.
- Virtual patching en los componentes que soporten esta funcionalidad.
- Protección de marca y monitoreo de exposición digital.
- Gestión forense digital y apoyo a la respuesta ante incidentes.
- Operación integral del SOC del ICBF.
- Gestión de accesos privilegiados mediante PAM.
- Generación de reportes técnicos, ejecutivos y de cumplimiento.
- Acompañamiento especializado, transferencia de conocimiento y mejora continua.

Condiciones de prestación del servicio

El contratista deberá ejecutar, como parte del servicio, las siguientes actividades:

- Parametrización, configuración y afinamiento de políticas, reglas, firmas, alertamientos y casos de uso.
- Monitoreo continuo de eventos, alertas, incidentes e indicadores de seguridad.
- Administración operativa y técnica de las plataformas incluidas en el alcance.
- Soporte técnico especializado.
- Mantenimiento preventivo, correctivo y evolutivo a nivel lógico y funcional.
- Actualización de configuraciones, políticas y capacidades técnicas.
- Recomendaciones de hardening y mejora continua.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Acompañamiento en investigación, contención, erradicación y recuperación ante incidentes.
- Gestión de hallazgos y seguimiento a planes de remediación.
- Elaboración de informes periódicos de operación, incidentes, vulnerabilidades, tendencias, indicadores y oportunidades de mejora.

Nota: La solución de antivirus será provista por la entidad.

El Contratista deberá prestar al ICBF un servicio integral administrado de seguridad informática y seguridad digital en todas sus sedes, que incluya la administración, configuración, operación, monitoreo, soporte técnico especializado, mantenimiento, optimización y mejora continua de las plataformas, herramientas de software y componentes tecnológicos de seguridad que hagan parte del alcance contractual. Para tal efecto, deberá realizar el análisis periódico y permanente del tráfico y de las comunicaciones digitales de la entidad, identificar vulnerabilidades, amenazas, eventos e incidentes de seguridad, y formular recomendaciones, buenas prácticas, planes de acción y medidas de mejora orientadas al fortalecimiento de la postura de ciberseguridad institucional.

Así mismo, deberá apoyar la definición, actualización e implementación de lineamientos, políticas, procedimientos y estándares asociados al SGSI, Seguridad Digital y Continuidad de la Operación, en articulación con los lineamientos establecidos por el ICBF. También deberá ejecutar las actividades de migración, parametrización, integración, reconfiguración, administración, monitoreo, soporte y mejoramiento continuo de las herramientas y plataformas de seguridad incluidas en el alcance del servicio, así como apoyar la gestión, mitigación, análisis y atención forense de incidentes de seguridad.

Toda la infraestructura y las soluciones de seguridad incluidas en el alcance del servicio deberán integrarse al SIEM de próxima generación con capacidades SOAR, garantizando la recolección, correlación, análisis y trazabilidad de logs y eventos de seguridad, cuyo tratamiento operativo será responsabilidad del SOC. El Contratista deberá contar con la capacidad técnica y el personal especializado necesario para adelantar, dentro de los dos (2) meses siguientes a la suscripción del contrato, las actividades de alistamiento, migración, integración y puesta en operación del servicio, así como su posterior administración, operación y monitoreo continuo. El alcance aquí descrito corresponde a un servicio administrado, por lo que no comprende suministro de equipos, salvo estipulación expresa en contrario.

CANTIDAD	SERVICIO	UBICACIÓN
1	Servicio de Firewall Perimetral redundante y en alta disponibilidad.	Datacenter principal
1	Servicio de Firewall interno redundante y en alta disponibilidad.	Datacenter principal

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

CANTIDAD	SERVICIO	UBICACIÓN
1	Servicio de Firewall Perimetral redundante y en alta disponibilidad.	Centro de cómputo - Sede Nacional
1	Servicio de Firewall interno redundante y en alta disponibilidad.	Centro de cómputo - en Sede Nacional
1	Servicio de Protección/Detección de Intrusos IPS/IDS.	Datacenter principal
1	Servicio de Control de Aplicaciones.	Datacenter principal
1	Servicio de Proxy Trasparente y Filtrado Web.	Datacenter principal
1	Servicio de Protección contra Malware.	Datacenter principal
1	Servicio de Manejo de tráfico y calidad de servicio.	Datacenter principal
1	Servicio de VPN IPSec y SSL.	Datacenter principal
1	Servicio de protección contra Amenazas Persistentes Avanzadas.	Datacenter principal
1	Servicio de Firewall de aplicaciones redundante y en alta disponibilidad con capacidad de servicio para mínimo 78 aplicaciones.	Datacenter principal
1	Servicio de gestión acceso privilegiadas (PAM)	Datacenter principal
1	Servicio de Firewall de Bases de Datos con capacidad de servicio para mínimo las bases de datos descritas en el **Anexo 03 - Linea Base de Servicios TI**	Datacenter principal
1	Servicio de seguridad y DLP en correo electrónico para 28000 cuentas Office 365.	On premise
1	Servicio de protección frente a ataques DDOS (Distributed Denial of Service)	On Premise
1	Servicio de logs y reportes	Datacenter principal
1800	Servicio de correlación de eventos para hosts, seguimiento y gestión de eventos y alertas para el servicio de SOC	Datacenter principal y a nivel nacional
1	Servicio de SOC (Centro de Operaciones de Seguridad) 7x24x365	Instalaciones que el contratista designe para tal fin
1	Servicio de virtual patching	Datacenter principal

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

CANTIDAD	SERVICIO	UBICACIÓN
1	Servicio de detección y gestión de vulnerabilidades	A nivel nacional
1	Servicio de administración de Antivirus Microsoft Defender. 28000 licencias de usuario + 900 licencias de servidores. Incluye todos sus módulos (control de dispositivos, control de aplicaciones, firewall, Data Loss Prevention (DLP) para Endpoint, Red y Storage. Entre otros) nota: la cantidad de licencias puede aumentar a 28000 licencias de usuario + 800 licencias de servidor.	A nivel nacional
1	Servicio de administración de Antivirus Microsoft System Center 2012 Endpoint Protection. 1000 licencias	A nivel nacional
1	Servicio de análisis y protección de marca ICBF	A nivel nacional
1	Servicio de etical hacking de por lo menos 2 veces al año	A nivel nacional

6.9.16.3 SEGURIDAD PERIMETRAL

El servicio de seguridad perimetral suministrado deberá garantizar la protección integral de la infraestructura tecnológica del ICBF, la disponibilidad de los servicios institucionales, la continuidad operativa, la confidencialidad, integridad y trazabilidad de la información, así como la prevención, detección, contención y respuesta oportuna frente a amenazas, eventos e incidentes de ciberseguridad.

El servicio deberá estar alineado con un modelo de ciberseguridad moderno basado en Zero Trust, bajo el principio de “nunca confiar, siempre verificar”, incorporando validación continua de usuarios, dispositivos, aplicaciones, tráfico, identidades, postura de seguridad y contexto de acceso, tanto en el perímetro externo como en los segmentos internos de la red institucional. Este enfoque es coherente con la estrategia institucional descrita en el PETI, donde se plantea la evolución desde el modelo tradicional de seguridad hacia una estrategia de confianza cero.

Adicionalmente, el servicio deberá incorporar capacidades de Inteligencia Artificial (IA), Machine Learning (ML), analítica avanzada y automatización, orientadas a fortalecer la detección proactiva, el análisis de comportamiento, la identificación de amenazas desconocidas, la reducción de falsos positivos, la correlación inteligente de eventos y la respuesta automatizada frente a amenazas avanzadas, incluyendo aquellas generadas,

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

automatizadas o potenciadas mediante inteligencia artificial. Este enfoque se encuentra alineado con los lineamientos de MinTIC para sistemas de IA, los cuales contemplan monitoreo continuo, análisis de anomalías, correlación de eventos y gestión de riesgos.

Aprovisionamiento, entrega e implementación

El contratista deberá disponer en el Datacenter Principal Externo y en el Centro de Cómputo de la Sede Dirección General del ICBF los elementos de seguridad contratados, dentro de los treinta (30) días calendario siguientes a la fecha de inicio de ejecución del contrato, con el propósito de adelantar la configuración, integración, pruebas de operación, validación funcional y actividades de transición controlada.

El servicio deberá estar soportado en plataformas totalmente nuevas, de clase Enterprise/Datacenter, cuya fecha de fabricación no podrá ser superadas doce (12) meses respecto de la fecha de inicio la etapa de operacion o, en todo caso, no podrá superar un (1) año de antigüedad respecto de la fecha de inicio de la etapa de operación. Estas plataformas deberán corresponder a Firewalls de Nueva Generación NGFW con capacidades avanzadas de IA/ML, análisis contextual, inspección profunda de tráfico, prevención de amenazas, segmentación, automatización e integración con ecosistemas de seguridad.

Para lo anterior, el contratista deberá entregar, dentro de los cuarenta y cinco (45) días calendario siguientes a la fecha de inicio de ejecución del contrato, como mínimo, los siguientes documentos:

- Certificación del fabricante donde se indique la fecha de fabricación de las plataformas.
- Datasheet oficial del fabricante.
- Manifiesto de importación, cuando aplique.
- Factura de compra o documento equivalente.
- Certificación de soporte, garantía y licenciamiento vigente.
- Documentos complementarios que determine el ICBF para validar autenticidad, capacidad, soporte y trazabilidad de los componentes suministrados.

Compatibilidad, interfaces y conectividad

El servicio deberá estar soportado por plataformas que cuenten con todas las interfaces de red necesarias para garantizar una prestación óptima, escalable y segura del servicio. Deberá contar con compatibilidad nativa con IPv6, manteniendo paridad funcional en políticas, inspección, registro, administración, seguridad y monitoreo para tráfico IPv4 e IPv6.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

El proveedor deberá presentar carta firmada por el fabricante en la cual se certifique que la plataforma soporta IPv6 de forma nativa y funcional en sus capacidades de seguridad, administración y operación.

Cada plataforma deberá contar, como mínimo, con cuatro (4) interfaces ópticas de 10 Gbps para conexión hacia el switch core de la Entidad, sin perjuicio de las interfaces adicionales requeridas para alta disponibilidad, segmentación, administración, monitoreo, sincronización, enlaces WAN, zonas desmilitarizadas, enlaces dedicados o arquitecturas híbridas.

Arquitectura de seguridad

El servicio deberá ser implementado con appliances o plataformas de seguridad perimetral instaladas en el Datacenter Principal Externo y en el Centro de Cómputo de la Sede Dirección General del ICBF. Los componentes deberán quedar completamente implementados dentro de los dos (2) meses siguientes a la fecha de inicio de ejecución del contrato, incluyendo la configuración de políticas de seguridad requeridas por el ICBF, pruebas de operación, pruebas de alta disponibilidad, validación de conectividad, integración con plataformas de monitoreo y entrega de documentación técnica.
El servicio deberá garantizar los mismos niveles de seguridad en ambas ubicaciones. Para ello, el ICBF requiere contar, tanto en el Datacenter Principal Externo como en la Sede Dirección General, con dos capas de protección:

- Una capa dedicada a la función de firewall perimetral externo.
- Una capa dedicada a la función de firewall interno o de segmentación, pudiendo ser física o virtual, siempre que cumpla con los requerimientos técnicos, de rendimiento, disponibilidad, aislamiento, registro y seguridad exigidos por la Entidad.

Esta arquitectura deberá permitir la implementación de controles de seguridad perimetral, segmentación interna, microsegmentación, inspección de tráfico norte-sur y este-oeste, reducción de superficie de ataque, contención de movimiento lateral y aplicación de políticas basadas en identidad, contexto, riesgo y criticidad del activo.

La arquitectura aquí descrita se considera referencial; sin embargo, el contratista deberá garantizar el diseño, recomendación, reconfiguración, implementación y puesta en operación de la arquitectura más adecuada, conforme a las mejores prácticas de seguridad informática, ciberseguridad, continuidad operativa, alta disponibilidad y Zero Trust.

Migración y transición

El contratista deberá tener en cuenta la migración controlada de políticas, reglas, rutas, objetos, perfiles de seguridad, NAT, VPN, listas, configuraciones, zonas, certificados, integraciones, parámetros lógicos y físicos desde el servicio de seguridad perimetral actual hacia el nuevo servicio entregado.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

La migración deberá realizarse conforme a las mejores prácticas del fabricante, garantizando la continuidad de los servicios institucionales, la mínima afectación operativa, la integridad de las configuraciones, la trazabilidad de los cambios y la validación previa mediante pruebas técnicas.

El contratista deberá presentar un plan de migración que incluya, como mínimo:

- Inventario de configuraciones a migrar.
- Matriz de equivalencia de políticas.
- Identificación de reglas obsoletas, duplicadas o inseguras.
- Plan de pruebas.
- Plan de reversa.
- Ventanas de cambio.
- Riesgos y controles asociados.
- Evidencias de validación.
- Aprobaciones requeridas por el ICBF.

Al finalizar el contrato, el contratista deberá entregar al ICBF las políticas, reglas, objetos, rutas, configuraciones, parámetros técnicos, respaldos, diagramas, inventarios, reportes y documentación detallada de los dispositivos y servicios administrados, garantizando la confidencialidad, integridad, disponibilidad y reutilización de dicha información por parte de la Entidad.

Las configuraciones realizadas por el **contratista** durante la vigencia contractual serán propiedad del ICBF para su libre utilización, continuidad, auditoría, verificación, migración o transferencia operativa.

Disponibilidad y alta disponibilidad

Tanto el servicio de firewalls del Datacenter Principal Externo como el servicio de firewalls de la Sede Dirección General deberán estar totalmente aprovisionados en esquema de Alta Disponibilidad (HA), con mecanismos de sincronización de políticas, sesiones, objetos, configuraciones y estado operativo, según las capacidades del fabricante y la arquitectura aprobada por el ICBF.

El servicio deberá permitir la ejecución de pruebas de continuidad y conmutación cuando el ICBF lo requiera, con el fin de validar el correcto funcionamiento del esquema HA, la recuperación ante fallas, la resiliencia de la plataforma y la disponibilidad efectiva de los servicios.

Se deberá contar con configuración que permita Alta Disponibilidad Geográfica entre el Datacenter Principal Externo y el Centro de Cómputo de la Sede Dirección General,

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

garantizando continuidad, supervisión, monitoreo, recuperación ante desastres y operación segura.

Nota técnica: Para garantizar una implementación exitosa de firewalls en alta disponibilidad geográfica, las plataformas instaladas en la Sede Dirección General y en el Datacenter Principal Externo deberán contar con características técnicas equivalentes o compatibles, de forma que permitan ejecutar pruebas de continuidad, sincronización, administración centralizada, conectividad, monitoreo, recuperación ante desastres y aplicación homogénea de políticas de seguridad.

Rendimiento mínimo requerido

Datacenter Principal Externo

Las plataformas que soportan el servicio de seguridad perimetral en el Datacenter Principal Externo deberán cumplir, como mínimo, con los siguientes rendimientos:

- Rendimiento mínimo de firewall: Entre 145 Gbps y 400 Gbps (o superior)
- Rendimiento IPS/IDS en tráfico mixto productivo / enterprise: Entre 55 Gbps y 85 Gbps (o superior).
- Rendimiento de control de aplicaciones: Entre 50 Gbps y 75 Gbps (o superior).
- Rendimiento de protección contra amenazas con IPS, control de aplicaciones y antimalware activos: Entre 45 Gbps y 65 Gbps (o superior).
- Rendimiento de inspección SSL/TLS Deep Inspection: Entre 28 Gbps y 45 Gbps (o superior).
- Acceso Remoto Seguro en Túneles Cifrados (VPN IPsec AES-256 / VPN SSL / ZTNA): Entre 25 Gbps y 50 Gbps (o superior)
- Capacidad VPN SSL: Entre 12.000 y 20.000 usuarios (o superior) usuarios concurrentes con autenticación multifactor.
- Conexiones concurrentes: Entre 10.000.000 y 30.000.000 de sesiones (o superior).
- Nuevas sesiones por segundo: Entre 500.000 y 900.000 CPS (o superior).
- Soporte de filtrado de contenido sin licenciamiento limitado por usuario.
- Entre 4 y 8 puertos de 40 GE (QSFP+) o 100 GE (QSFP28), y mínimo 4 puertos de 10 GE / 25 GE (SFP+/SFP28).

Sede Dirección General del ICBF

Las plataformas que soportan el servicio de seguridad perimetral en la Sede Dirección General deberán cumplir, como mínimo, con los siguientes rendimientos:

- Rendimiento mínimo de firewall: Entre 145 Gbps y 400 Gbps (o superior)
- Rendimiento IPS/IDS en tráfico mixto productivo / enterprise: Entre 55 Gbps y 85 Gbps (o superior).
- Rendimiento de control de aplicaciones: Entre 50 Gbps y 75 Gbps (o superior).

- Rendimiento de protección contra amenazas con IPS, control de aplicaciones y antimalware activos: Entre 45 Gbps y 65 Gbps (o superior).
- Rendimiento de inspección SSL/TLS Deep Inspection: Entre 28 Gbps y 45 Gbps (o superior).
- Acceso Remoto Seguro en Túneles Cifrados (VPN IPsec AES-256 / VPN SSL / ZTNA): Entre 25 Gbps y 50 Gbps (o superior)
- Capacidad VPN SSL: Entre 12.000 y 20.000 usuarios (o superior) usuarios concurrentes con autenticación multifactor.
- Conexiones concurrentes: Entre 10.000.000 y 30.000.000 de sesiones (o superior).
- Nuevas sesiones por segundo: Entre 500.000 y 900.000 CPS (o superior).
- Soporte de filtrado de contenido sin licenciamiento limitado por usuario.
- Entre 4 y 8 puertos de 40 GE (QSFP+) o 100 GE (QSFP28), y mínimo 4 puertos de 10 GE / 25 GE (SFP+/SFP28).

Componentes y características técnicas mínimas - NGFW con IA/ML

La solución deberá contar, como mínimo, con los siguientes componentes y características de seguridad, integrados de manera nativa o mediante módulos licenciados del mismo ecosistema tecnológico, garantizando administración centralizada, interoperabilidad, trazabilidad e integración con las plataformas de seguridad del ICBF.

Firewall de Nueva Generación NGFW con IA/ML

La plataforma deberá permitir inspección profunda de tráfico desde la capa de red hasta la capa de aplicación L3 a L7, con análisis contextual de usuarios, aplicaciones, dispositivos, contenido, destino, reputación, geolocalización, postura de seguridad y comportamiento.
Deberá incorporar capacidades de IA/ML para análisis de tráfico entrante y saliente, detección dinámica de aplicaciones, identificación de comportamientos anómalos, detección de intentos de evasión, recomendación de políticas y priorización de eventos de seguridad.

IPS/IDS avanzado

La solución deberá contar con capacidades de prevención y detección de intrusos para proteger contra amenazas conocidas, emergentes y desconocidas, incluyendo exploits, intentos de explotación, ataques de día cero, escaneos, anomalías de protocolo, ataques DoS y técnicas de evasión.

Deberá emplear firmas, análisis heurístico, decodificadores de protocolo, análisis de comportamiento y modelos asistidos por IA/ML para mejorar la detección y reducir falsos positivos.

Control avanzado de aplicaciones

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

La plataforma deberá identificar y controlar aplicaciones independientemente del puerto, protocolo, cifrado, técnica de ocultamiento u ofuscación utilizada. Deberá permitir políticas granulares basadas en usuario, grupo, aplicación, categoría, riesgo, dispositivo, zona, horario, ubicación y criticidad del servicio.

Protección contra malware, ransomware y amenazas persistentes

La solución deberá contar con capacidades de detección, prevención y mitigación de malware, ransomware, troyanos, botnets, spyware, amenazas persistentes avanzadas y archivos maliciosos, incluyendo análisis en tiempo real sobre protocolos HTTP/S, SMTP/S, FTP, SMB/CIFS y demás protocolos soportados.

Deberá integrarse con una plataforma de sandboxing local o en la nube para el análisis de archivos desconocidos, URLs, scripts y objetos sospechosos, mediante análisis estático, dinámico, conductual y modelos de IA/ML.

Filtrado web y proxy transparente

La solución deberá permitir filtrado de navegación web mediante bases de datos de reputación, categorización dinámica, análisis de riesgos, control por usuario, grupo, categoría, horario y política institucional.

Deberá operar en modo transparente, sin requerir agentes en los equipos de usuario, y permitir control de URLs, categorías, reputación, dominios maliciosos, sitios de phishing, descarga de malware y contenido no permitido.

Inspección SSL/TLS

La plataforma deberá contar con capacidad de inspección profunda de tráfico cifrado entrante y saliente, incluyendo soporte para estándares modernos como TLS 1.3, de acuerdo con las capacidades del fabricante.

La solución deberá permitir inspección total tipo Full Proxy/MITM cuando sea autorizado por la Entidad y técnicamente viable, así como inspección basada en SNI o metadatos cuando existan restricciones de privacidad, cumplimiento, criticidad o imposibilidad técnica de descifrado.

La inspección deberá soportar motores de IPS, antimalware, DLP, filtrado web, control de aplicaciones y análisis de amenazas, minimizando el impacto en el rendimiento mediante aceleración por hardware cuando aplique.

QoS y gestión de tráfico

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

La plataforma deberá permitir priorización, limitación, clasificación y control de tráfico basado en criticidad del negocio, aplicaciones, servicios, perfiles de usuario, sedes, segmentos y niveles de servicio, garantizando ancho de banda para flujos de misión crítica.

SD-WAN seguro

La solución deberá contar con capacidades de gestión inteligente de enlaces, selección dinámica de rutas, balanceo de carga, failover automático y toma de decisiones basada en latencia, jitter, pérdida de paquetes, disponibilidad y calidad del enlace.

El motor de conectividad WAN deberá estar integrado con el motor de seguridad, permitiendo que las decisiones de enrutamiento y acceso estén alineadas con políticas de protección y riesgo.

Firewall interno y microsegmentación

La solución deberá soportar segmentación lógica y control de tráfico este-oeste, permitiendo aislar dominios de seguridad internos, proteger activos críticos, contener movimiento lateral y aplicar políticas basadas en identidad, rol, criticidad, aplicación, zona y nivel de riesgo.

VPN IPsec y VPN SSL con autenticación fuerte

- La plataforma deberá soportar VPN sitio-a-sitio y cliente-a-sitio, con algoritmos robustos como AES-256, SHA-256 y grupos Diffie-Hellman 14 o superiores.
- La VPN SSL deberá soportar autenticación multifactor 2FA/MFA, validación de postura del equipo, políticas de acceso condicional y capacidades compatibles con modelos ZTNA/SSE para usuarios externos.

Identidad, autenticación y Zero Trust

La solución deberá integrarse con servicios de identidad basados en estándares abiertos, incluyendo LDAP, RADIUS, SAML, OAuth, OpenID Connect y Microsoft Entra ID/Azure AD, según aplique.

Deberá permitir políticas basadas en identidad, grupo, dispositivo, postura, ubicación, aplicación, riesgo y contexto, bajo un enfoque Zero Trust.

Convergencia con SSE/ZTNA

La solución deberá integrarse o interoperar con plataformas de Security Service Edge (SSE) y Zero Trust Network Access (ZTNA) para extender el control de acceso, la protección de

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

aplicaciones, la visibilidad de usuarios remotos, la inspección segura y la protección frente a amenazas en arquitecturas híbridas y distribuidas.

Administración, logging y analítica

La solución deberá contar con consola centralizada para administración unificada, configuración, monitoreo, generación de reportes, trazabilidad, gestión de eventos, visualización de amenazas, análisis de tráfico y operación del servicio.

Deberá permitir exportación de logs hacia plataformas SIEM, SOAR, XDR, SOC y herramientas de monitoreo mediante protocolos estándar como Syslog, API, IPFIX u otros soportados por el fabricante.

Actualización tecnológica y resiliencia

El servicio deberá incluir actualización periódica, automática y controlada de firmas, motores de detección, reputación, inteligencia de amenazas, motores de IA/ML, bases de datos de seguridad, listas de bloqueo, indicadores de compromiso, parches, hotfixes y versiones recomendadas por el fabricante.

Estas actualizaciones deberán garantizar la protección frente a amenazas recientes reportadas globalmente, sin afectar la continuidad operativa de los servicios institucionales.

Componentes Core de Firewall de Nueva Generación

La solución deberá soportar control de tráfico multizona, permitiendo aplicar políticas entre interfaces físicas, lógicas, zonas de seguridad, VLAN, segmentos, túneles VPN y entornos virtuales.

Deberá contar con políticas basadas en identidad, integradas con AD, LDAP, SAML 2.0 u otros mecanismos equivalentes, permitiendo combinar usuario, grupo, tipo de dispositivo, ubicación, postura y aplicación dentro de una misma regla.

La plataforma deberá permitir visibilidad y control de dispositivos mediante identificación automática, fingerprinting, clasificación por sistema operativo, categoría, fabricante, comportamiento y nivel de riesgo. Esta capacidad deberá estar licenciada para brindar inventario y visibilidad sin costos ocultos durante la vigencia contractual.

La solución deberá contar con modo de aprendizaje o recomendación asistida por IA/ML, que permita analizar tráfico real, identificar patrones, detectar reglas permisivas, recomendar endurecimiento de políticas y apoyar la reducción de superficie de ataque.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Deberá soportar IPv6 de forma nativa, con paridad funcional en reglas, inspección, administración, monitoreo, registro y seguridad mediante GUI y CLI.

Protección avanzada contra amenazas

La solución deberá soportar operación en línea para bloqueo inmediato y, cuando aplique, operación fuera de línea mediante puertos SPAN/Mirror para análisis sin impacto productivo.
Deberá permitir prevención adaptativa mediante firmas, decodificadores de protocolo, análisis heurístico, reputación, inteligencia de amenazas, IA/ML y actualizaciones automáticas mediante esquemas Push y Pull.

La plataforma deberá permitir acciones de mitigación como bloqueo, reseteo de sesiones, cuarentena de origen, aislamiento lógico, captura de paquetes, generación de alertas y exportación de eventos hacia SIEM/SOAR/XDR/SOC.

Deberá identificar anomalías de protocolo, exploits, ataques de denegación de servicio, escaneos de puertos, buffer overflow, conexiones sospechosas, tráfico anómalo y patrones asociados a técnicas, tácticas y procedimientos de atacantes.

La plataforma deberá permitir la mitigación de vulnerabilidades conocidas mediante firmas referidas a su código CVE, bloqueando los intentos de explotación dirigidos a servidores y servicios alcanzables a través del perímetro, sin requerir modificación del código, cambio de configuración ni reinicio de los sistemas protegidos. Deberá permitir la aplicación selectiva de dichas firmas por activo, segmento o zona de seguridad, el registro y la trazabilidad de cada bloqueo, y la exportación de los eventos asociados hacia las plataformas SIEM, SOAR y SOC de la Entidad. Esta capacidad se entiende comprendida dentro de la suscripción de IPS e inteligencia de amenazas exigida para la plataforma, sin que genere ítem de precio independiente, y el contratista deberá garantizar su vigencia y actualización permanente durante toda la ejecución contractual.

Control de aplicaciones y filtrado web

La solución deberá permitir identificación granular de aplicaciones, independientemente del puerto o protocolo utilizado, incluyendo aplicaciones SaaS, colaboración, almacenamiento en nube, streaming, redes sociales, mensajería, acceso remoto y demás categorías relevantes para la Entidad.

Deberá permitir filtrado web transparente, control por categorías, reputación, riesgo, contenido, usuario, grupo, horario, dispositivo y política institucional.

Deberá soportar Safe Search, filtrado de scripts, control de descargas, control de navegación por cuotas o categorías y generación de reportes detallados.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Protección contra malware y sandboxing

La solución deberá permitir análisis antivirus y antimalware en tiempo real sobre protocolos HTTP/S, SMTP/S, FTP, SMB/CIFS y demás protocolos soportados.

Deberá integrarse de forma nativa o interoperable con una plataforma de sandboxing para envío, análisis y clasificación de archivos sospechosos, con capacidad de bloqueo en línea cuando se determine comportamiento malicioso.

La solución deberá permitir detección y bloqueo automático de conexiones hacia servidores de comando y control C2/C&C, botnets, dominios maliciosos, URLs sospechosas e infraestructura asociada a campañas activas.

Módulo de protección DoS/DDoS, Scrubbing y WAF

La solución deberá incorporar o integrarse con capacidades de mitigación DoS/DDoS, protección contra ataques volumétricos, ataques de aplicación, ataques de amplificación, reflexión, SYN Flood, UDP Flood, HTTP Flood y demás vectores soportados por el fabricante o por el servicio asociado.

Deberá permitir umbrales configurables, detección de tráfico anómalo, alertamiento automatizado, mitigación adaptativa y generación de reportes.
El servicio deberá contemplar capacidad de Scrubbing en línea o bajo demanda para limpieza de tráfico malicioso, con el fin de neutralizar ataques masivos sin interrumpir la infraestructura productiva del ICBF.

Adicionalmente, la solución deberá contar con motor básico o estándar de protección para reglas de tráfico expuestas hacia Internet o zona DMZ. No obstante, cuando se trate de aplicaciones críticas expuestas públicamente, deberá integrarse con un WAF especializado que permita protección contra ataques de capa 7, OWASP Top 10, bots maliciosos, explotación de vulnerabilidades web y tráfico automatizado.

Nota Técnica:

Como criterio de validación técnica, el oferente deberá acreditar que las soluciones de seguridad perimetral propuestas para las categorías de firewall (FW), firewall de aplicaciones web (WAF), seguridad de correo electrónico (ANTISPAM), mitigación de ataques de denegación de servicio distribuido (DDoS), análisis de amenazas en entornos aislados (SANDBOX) y firewall de bases de datos cuentan con reconocimiento o evaluación verificable en al menos uno (1) de los informes publicados durante los últimos veinticuatro

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

(24) meses por firmas analistas independientes reconocidas, correspondientes a la categoría tecnológica aplicable a cada solución ofertada.

La acreditación podrá sustentarse en informes de diferentes firmas analistas independientes, siempre que se pueda verificar la fuente, la fecha de publicación y la correspondencia entre el informe y la categoría tecnológica evaluada.

Operación, mantenimiento y mejora continua del servicio

Administración y operación continua

El contratista deberá asumir la administración integral, operación continua, monitoreo proactivo, soporte técnico especializado, gestión de disponibilidad, ajuste funcional, atención de incidentes, gestión de requerimientos y operación segura de todos los componentes de seguridad perimetral, garantizando desempeño, estabilidad, trazabilidad y correcta prestación durante la vigencia contractual.

Actualizaciones y parches

El servicio deberá incluir gestión, aplicación, validación y seguimiento de actualizaciones de seguridad, mejoras de versión, hotfixes, parches, firmas, reputación, motores de IA/ML y bases de inteligencia de amenazas liberadas por el fabricante.

Estas actividades deberán ejecutarse procurando no afectar la continuidad operativa ni la disponibilidad de los usuarios, aplicando controles de cambio cuando corresponda.

Mantenimiento preventivo, correctivo y evolutivo

El contratista deberá ejecutar actividades de mantenimiento preventivo, correctivo y evolutivo sobre configuraciones, políticas, integraciones, licenciamiento, componentes lógicos, componentes físicos, reglas, objetos, perfiles de seguridad, certificados, respaldos, monitoreo y reportes.

Estas actividades deberán incluir afinamiento de reglas, optimización de desempeño, eliminación de configuraciones obsoletas, fortalecimiento de controles, adopción de mejores prácticas y mejora continua de la postura de seguridad.

Pruebas de seguridad y validación técnica

El servicio deberá contemplar la coordinación, ejecución o gestión de evaluaciones periódicas de seguridad, tales como análisis de vulnerabilidades, revisión de configuración segura, pruebas de alta disponibilidad, validación de reglas críticas, revisión de exposición

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

externa, pruebas de continuidad, simulaciones controladas y validaciones técnicas sobre los componentes que soportan el servicio.

Detección, respuesta y seguimiento

El contratista deberá generar y presentar informes periódicos, como mínimo mensuales, sobre eventos, incidentes, alertas, accesos sospechosos, acciones de respuesta, estado de plataformas, disponibilidad, desempeño, indicadores de operación, hallazgos relevantes, cumplimiento de políticas, cambios ejecutados, riesgos identificados y oportunidades de mejora.

Mejora continua

El contratista deberá proponer e implementar, previa validación del ICBF, acciones de mejora continúa orientadas al fortalecimiento de la postura de seguridad, optimización de políticas, reducción del riesgo, aumento de visibilidad, mejora de experiencia de usuario autorizado, reducción de falsos positivos, endurecimiento de controles y madurez operativa del servicio.

Certificados digitales

El contratista deberá administrar para el adecuado funcionamiento de los servicios incluidos en el contrato, incluyendo certificados wildcard SSL/TLS, certificados SAN, certificados para aplicaciones web, portales públicos, servicios de correo, colaboración, autenticación, publicación segura y demás servicios institucionales definidos por el ICBF.

La administración de certificados deberá incluir inventario, fechas de vencimiento, alertas tempranas, renovación oportuna, instalación, validación, documentación, custodia segura y entrega de evidencias.

Tabla – Certificados Digitales

TIPO DE CERTIFICADO	SERVICIO	CADUCIDAD
Wildcard	Aplicaciones	02/01/2027
SAN	Exchange Server	15/06/2027

- Todos los servicios relacionados con la seguridad informática deben poder integrarse con la herramienta de SIEM-SOAR deben ser monitoreados por el SOC en tiempo real.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

6.9.16.4 SERVICIO DE PROTECCIÓN CONTRA AMENAZAS PERSISTENTES AVANZADAS(SANDBOXING).

El contratista deberá prestar al ICBF un servicio administrado de protección contra amenazas persistentes avanzadas (APT) y análisis de malware de día cero (0-day), el cual deberá incluir la administración, configuración, operación, monitoreo, soporte especializado, mantenimiento, optimización y mejora continua de una plataforma de sandboxing de última generación.

Dicha plataforma deberá ser capaz de analizar archivos, URLs, scripts, objetos sospechosos y demás artefactos potencialmente maliciosos en entornos aislados, controlados y altamente instrumentados, garantizando la ejecución segura de muestras y la detección de comportamientos maliciosos no evidentes mediante técnicas tradicionales.

El servicio deberá permitir la detección, análisis y clasificación de amenazas avanzadas, incluyendo malware desconocido, evasivo y polimórfico, así como su integración con las demás plataformas de seguridad de la Entidad, garantizando la generación de alertas, indicadores de compromiso (IoC), reportes técnicos y ejecutivos, así como la exportación de logs y resultados hacia plataformas SIEM de próxima generación, SOAR y SOC.

En el marco de un modelo de ciberseguridad basado en Zero Trust, el servicio deberá contribuir a la validación continua de artefactos y contenidos que ingresan o transitan por la infraestructura tecnológica, fortaleciendo los controles de prevención, detección y respuesta frente a amenazas avanzadas.

Como parte de las capacidades de nueva generación, la plataforma de sandboxing deberá integrar de manera obligatoria mecanismos avanzados de Inteligencia Artificial (IA) y Machine Learning (ML), orientados al fortalecimiento de la detección proactiva, el análisis conductual y la respuesta automatizada frente a amenazas sofisticadas, incluyendo aquellas generadas o potenciadas mediante inteligencia artificial. En este sentido, el servicio deberá contemplar, como mínimo, las siguientes capacidades:

- Análisis conductual basado en IA: Capacidad de identificar comportamientos maliciosos mediante el estudio dinámico de la ejecución de archivos, independientemente de firmas conocidas.
- Detección de amenazas desconocidas y de día cero: Mediante modelos de aprendizaje automático capaces de identificar patrones anómalos, técnicas de evasión y comportamientos sospechosos.
- Clasificación inteligente de malware: Utilizando algoritmos de IA que permitan categorizar variantes de malware, familias y niveles de riesgo.
- Correlación avanzada de eventos: Integración con plataformas de seguridad para enriquecer eventos con contexto, priorizar alertas y reducir falsos positivos.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Automatización de respuestas (orquestación): Capacidad de ejecutar acciones automáticas tales como bloqueo, cuarentena, aislamiento o generación de reglas de protección, conforme a políticas definidas.
- Capacidad de autoaprendizaje (auto-learning): Mejora continua de los modelos de detección a partir de nuevos datos, eventos y muestras analizadas.
- Análisis de amenazas avanzadas basadas en IA: Detección de técnicas modernas como malware adaptativo, scripts generados dinámicamente, ataques sin archivo (fileless) y campañas automatizadas.

Adicionalmente, la solución deberá permitir el análisis de amenazas en diferentes entornos (sistemas operativos, navegadores, arquitecturas), así como la generación de inteligencia de amenazas (threat intelligence) reutilizable para el fortalecimiento de controles en otros componentes del ecosistema de seguridad.

El servicio deberá garantizar tiempos de respuesta acordes a la criticidad de los eventos, así como la trazabilidad completa de los análisis realizados, facilitando procesos de auditoría, cumplimiento normativo, análisis forense y gestión de incidentes.

Finalmente, el servicio deberá alinearse con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, incorporando capacidades de monitoreo continuo, análisis de anomalías, correlación de eventos y gestión de riesgos en entornos que integran tecnologías de inteligencia artificial.

Capacidad de Procesamiento y Análisis

- Rendimiento de Extracción de Archivos (Sniffer Mode): Entre 6 Gbps y 12 Gbps (o superior) (Capacidad de procesar el tráfico de red para identificar y extraer objetos sospechosos).
- Capacidad de Análisis Dinámico (Sandbox): Entre 800 y 1.500 archivos/hora (o superior) archivos por hora (Rendimiento de detonación y análisis de comportamiento en entornos virtuales).
- Procesamiento de Correo Electrónico: Entre 45.000 y 80.000 correos/hora (o superior) correos por hora (Integración con gateways de mensajería para análisis de adjuntos y URLs).
- Análisis de Archivos en Paralelo: Entre 16 y 40 entornos concurrentes en configuración base, con capacidad de expansión por licenciamiento, hardware o nube híbrida

Hardware y Almacenamiento Forense

- Almacenamiento Interno: Entre 3 TB y 6 TB (o superior) (Destinados al sistema operativo, máquinas virtuales de análisis y, especialmente, a la retención de evidencias forenses, trazas de red y muestras de malware).

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Memoria RAM de Sistema: Entre 48 GB y 128 GB (o superior) (Para soportar la ejecución fluida de múltiples sistemas operativos de análisis de forma concurrente).

Conectividad y Resiliencia

- Interfaces de Red:
  - Mínimo 4 puertos 1 GbE (RJ45/SFP) y entre 2 y 4 puertos 10 GbE (SFP+).
- Fuentes de poder redundantes (1+1) intercambiables en caliente (Hot-swappable), chasis rackeable.

NOTA TÉCNICA: El fabricante de la solución de Sandboxing/Protección contra Amenazas Avanzadas debe estar clasificado en evaluaciones recientes de firmas analistas independientes internacionalmente reconocidas (Gartner, Forrester, IDC o equivalentes) dentro de las categorías de Seguridad de Red, Prevención de Amenazas Avanzadas, Detección y Respuesta de Amenazas o Sandboxing Empresarial.

6.9.16.5 REQUERIMIENTOS DEL SERVICIO

Como parte del servicio, el contratista deberá cumplir, como mínimo, con los siguientes requerimientos:

- Realizar la configuración, administración, operación, monitoreo y mantenimiento de la solución de protección contra amenazas persistentes avanzadas, asegurando su funcionamiento continuo, estabilidad operativa, disponibilidad, trazabilidad e integración con los demás componentes de seguridad del ICBF.
- Ejecutar actividades de afinamiento, actualización, optimización y mejora continua de políticas, perfiles de análisis, motores de detección, reglas, flujos de tratamiento e integraciones, con el propósito de fortalecer la capacidad de detección, reducir falsos positivos o negativos y mejorar la efectividad del servicio.
- Configurar, administrar y mantener la herramienta de monitoreo necesaria para medir la disponibilidad, desempeño, eventos, alertas y estado operativo del servicio durante cada periodo de operación, de forma que el ICBF pueda verificar el cumplimiento de los Acuerdos de Niveles de Servicio (ANS) aplicables.
- Garantizar la generación, conservación, consulta y trazabilidad de registros, eventos, evidencias y resultados de análisis asociados al servicio, permitiendo su correlación e integración con plataformas institucionales como SIEM NG, SOAR, SOC, IA o aquellas definidas por la Entidad.
- Presentar informes periódicos de operación y seguridad, con frecuencia mensual y/o por demanda, los cuales deberán ser entregados dentro de las veinticuatro (24) horas siguientes a la solicitud realizada por la Entidad, acompañados del respectivo análisis técnico desde la gestión de seguridad informática.

Los informes deberán contener, como mínimo, los siguientes componentes:

- Reporte de archivos día cero (0-day) identificados, analizados o bloqueados.
- Reporte de archivos maliciosos conocidos detectados por la solución.
- Reporte de carpetas compartidas comprometidas, incluyendo análisis asociado a eventos de alteración, cifrado, borrado o afectación de información, cuando aplique.
- Reporte de redes, segmentos o activos en los que se hayan identificado indicadores de malware avanzado o comportamientos asociados a amenazas persistentes avanzadas.
- Reportes correlacionados con otras plataformas de seguridad, en especial las asociadas a seguridad en red y seguridad en aplicaciones web, cuando exista integración o relación directa con los eventos detectados.
- Top 10 de malwares identificados durante el periodo reportado.
- Top 10 de amenazas o archivos día cero (0-day) detectados durante el periodo reportado.
- Top 10 de dominios, páginas, activos o servicios del ICBF que hayan sido objeto de ataques asociados a APT o malware avanzado.
- Reporte de usuarios, equipos o sesiones relacionados con eventos de malware día cero (0-day), incluyendo su respectivo análisis y nivel de criticidad.

Adicionalmente, cada informe deberá incluir el análisis técnico correspondiente, contemplando como mínimo el contexto del evento, criticidad, alcance, activos afectados, indicadores de compromiso identificados, tendencias observadas, acciones ejecutadas, estado de contención o mitigación y recomendaciones orientadas al fortalecimiento de la postura de seguridad del ICBF.

6.9.16.6 SERVICIO DE SEGURIDAD EN APLICACIONES WEB NGWAF

El contratista deberá prestar al ICBF un servicio administrado de seguridad en aplicaciones web, orientado a la administración, operación, monitoreo, mantenimiento, soporte técnico especializado, optimización y mejora continua de los mecanismos de protección de las aplicaciones web institucionales alojadas en el datacenter externo del ICBF.

El servicio deberá garantizar la protección permanente de las aplicaciones web frente a amenazas, ataques, explotación de vulnerabilidades, alteraciones no autorizadas y afectaciones a la disponibilidad, mediante una arquitectura especializada de Firewall de próxima generación de aplicaciones Web (WAF), operando en esquema de proxy reverso y bajo alta disponibilidad, con cobertura suficiente para las aplicaciones definidas por la Entidad dentro del alcance contractual.

Rendimientos Mínimos de las Plataformas que soportan el Servicio Seguridad en aplicaciones Web:

- Rendimiento HTTP: Entre 4 Gbps y 10 Gbps (o superior).
- Rendimiento HTTPS: Entre 4 Gbps y 8 Gbps (o superior).

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Capacidad mínima de conexiones HTTP concurrentes: Entre 1.000.000 y 2.000.000 de conexiones (o superior).
- Interfaces de Red de Alta Velocidad aprovisionadas : Entre 4 y 8 puertos de 10 Gbps (SFP+) y mínimo 2 puertos de 1 Gbps (SFP o RJ45).
- Almacenamiento mínimo: Entre 2 TB y 4 TB (o superior).

Soporte para protocolos TLS 1.2 y TLS 1.3,Permitir la aplicación de políticas de seguridad sobre el tráfico de las aplicaciones protegidas y disponer de soporte para IPv6.

- Implementación en Alta Disponibilidad (HA) con fuentes de alimentación redundantes reemplazables en caliente (Hot-swappable) y soporte nativo IPv6.
- El licenciamiento de la plataforma no deberá estar limitado por la cantidad de aplicaciones web protegidas que hagan parte del alcance definido por el ICBF.

Así mismo, la solución deberá proporcionar capacidades de inspección, análisis y protección contra amenazas dirigidas a aplicaciones web, incluyendo como mínimo protección frente a ataques de capa de aplicación tales como:

- SQL Injection.
- Cross-Site Scripting (XSS).
- Cross-Site Request Forgery (CSRF).
- Ataques de secuestro y manipulación de sesión.
- Inclusión local o remota de archivos (LFI/RFI).
- Inyección de comandos.
- Ataques automatizados basados en bots.
- Y demás categorías de amenazas contempladas en el estándar OWASP Top 10 vigente.

Requerimientos mínimos del servicio:

- El contratista deberá disponer, administrar, operar, monitorear, mantener y optimizar el servicio de seguridad en aplicaciones web, soportado sobre plataformas especializadas de Firewall de Aplicaciones Web (NGWAF) de propósito específico, con vigencia tecnológica adecuada para garantizar la correcta prestación del servicio.
- Como parte de la etapa de transición, el contratista deberá acreditar ante el ICBF las condiciones técnicas de la plataforma que soportará el servicio, incluyendo la documentación que permita validar su vigencia tecnológica, trazabilidad, compatibilidad y capacidad de operación.
- El servicio no deberá estar limitado por el número de aplicaciones web protegidas dentro del alcance definido por la Entidad, permitiendo su crecimiento, ajuste y administración conforme a las necesidades operativas del ICBF.
- El contratista deberá garantizar que la plataforma que soporta el servicio cuente con las interfaces de red, capacidades de procesamiento, disponibilidad de recursos y

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

compatibilidad técnica necesarias para la operación continua, segura y eficiente del servicio.

- El servicio deberá ser totalmente compatible con protocolos de última generación, incluyendo IPv6, garantizando su adecuada administración, operación e integración con la infraestructura tecnológica del ICBF.
- El contratista deberá garantizar la protección de las aplicaciones web alojadas en el datacenter externo del ICBF, así como de aquellas que sean incorporadas al alcance del servicio durante la ejecución contractual, previa validación de la Entidad.
- El servicio deberá mantenerse integrado con el servicio histórico de logs y reportes, así como con las plataformas institucionales de monitoreo, correlación y gestión de eventos de seguridad, con el fin de asegurar trazabilidad, visibilidad, análisis y generación de reportes.

Administración, operación, mantenimiento y mejora continua

El contratista deberá ejecutar de manera continua las actividades de administración, operación, monitoreo, soporte técnico especializado, mantenimiento preventivo, correctivo y evolutivo, así como el afinamiento, actualización, hardening, optimización de reglas, perfiles, firmas, políticas y parámetros de inspección del servicio.

Así mismo, deberá realizar acciones permanentes de mejora continua, orientadas al fortalecimiento de la postura de seguridad de las aplicaciones web, la reducción de falsos positivos, la optimización del desempeño, la mejora de la cobertura de protección y la adaptación del servicio frente a cambios en el entorno tecnológico, nuevas amenazas, hallazgos de seguridad o necesidades del ICBF.

La operación del servicio deberá generar la trazabilidad, evidencia técnica y reportabilidad necesarias para soportar actividades de monitoreo, auditoría, análisis de incidentes, gestión de vulnerabilidades y toma de decisiones por parte del ICBF.

Funciones y Características de Nueva Generación (IA/ML)

Como parte del servicio administrado de seguridad en aplicaciones web, el contratista deberá garantizar la administración, operación, monitoreo, mantenimiento, optimización y mejora continua de capacidades avanzadas de Inteligencia Artificial (IA) y Machine Learning (ML), orientadas a fortalecer la detección proactiva, el análisis de amenazas, la reducción de falsos positivos y la protección continua de los aplicativos webs institucionales.

En ese sentido, el servicio deberá contemplar, como mínimo, las siguientes capacidades funcionales:

- Análisis basado en Machine Learning: El servicio deberá permitir la administración y operación de mecanismos capaces de construir, ajustar y mantener modelos de

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

comportamiento de las aplicaciones web, con el fin de identificar anomalías, patrones atípicos y amenazas de día cero, sin depender exclusivamente de firmas estáticas. Autoaprendizaje (Auto-Learning):

El contratista deberá gestionar capacidades de autoaprendizaje que permitan la generación, ajuste y afinamiento continuo de perfiles de seguridad basados en el tráfico real de las aplicaciones, contribuyendo a la disminución de falsos positivos y al fortalecimiento de la precisión de los controles de protección.

- Protección contra el Top 10 de OWASP: El servicio deberá incluir la operación continua de controles especializados para la mitigación de las principales amenazas sobre aplicaciones web, incluyendo como mínimo Cross-Site Scripting (XSS), SQL Injection, Remote File Inclusion (RFI), Local File Inclusion (LFI), OS Command Injection y demás riesgos contemplados en el OWASP Top 10, conforme a las mejores prácticas y actualizaciones del fabricante.
- Protección avanzada de aplicaciones web: El contratista deberá garantizar la administración y operación de mecanismos de protección avanzada, incluyendo capacidades de Anti-Defacement sin agentes, mitigación de ataques DoS y DDoS en capa 7, contención de ataques basada en geolocalización y protección frente a bots maliciosos, con ajuste continuo conforme al comportamiento observado y al contexto institucional.
- Análisis integrado de vulnerabilidades: El servicio deberá contemplar la ejecución, administración y seguimiento de capacidades de análisis de vulnerabilidades sobre las aplicaciones web protegidas, permitiendo la identificación continua de debilidades de seguridad, malas configuraciones y oportunidades de fortalecimiento, sin limitación por número de análisis dentro del alcance del servicio.
- Los hallazgos del análisis de vulnerabilidades sobre las aplicaciones protegidas deberán poder traducirse en reglas de mitigación aplicadas por la propia plataforma, que neutralicen la explotación de la vulnerabilidad identificada sin modificar el código de la aplicación ni requerir su redespliegue. La plataforma deberá permitir la generación de dichas reglas a partir de los resultados del análisis propio o de una herramienta de análisis dinámico de seguridad de aplicaciones (DAST) integrada, su aplicación por aplicación o por conjunto de aplicaciones, y el registro y trazabilidad de cada mitigación. Esta capacidad se entiende comprendida dentro de la suscripción de firmas y actualizaciones del WAF, sin que genere ítem de precio independiente.

REQUERIMIENTOS DEL SERVICIO

El contratista deberá prestar al ICBF un servicio administrado de seguridad en aplicaciones web, que incluya la administración, configuración, operación, monitoreo, soporte técnico especializado, mantenimiento preventivo, correctivo y evolutivo, optimización y mejora continua de los mecanismos de protección requeridos para salvaguardar los aplicativos webs institucionales publicados en Internet, Intranet y WAN de la Entidad.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Como parte de la prestación del servicio, el contratista deberá cumplir, como mínimo, con los siguientes requerimientos:

- Administrar, operar, configurar, monitorear, mantener y optimizar las plataformas y capacidades de Firewall de Aplicaciones Web (NGWAF) requeridas para la protección de los aplicativos webs del ICBF entregadas como servicio.
- Garantizar la protección continua de los aplicativos webs que el ICBF tenga expuestos o disponibles a través de Internet, Intranet y la WAN institucional, asegurando cobertura, trazabilidad, control y capacidad de respuesta frente a amenazas y ataques sobre dichos activos.
- Configurar, administrar y mantener las herramientas de monitoreo necesarias para medir la disponibilidad, desempeño, eventos, alertas y estado operativo del servicio de seguridad en aplicaciones web durante cada periodo de operación, de manera que el ICBF pueda verificar el cumplimiento de los Acuerdos de Niveles de Servicio (ANS) aplicables.
- Ejecutar actividades permanentes de ajuste, afinamiento, actualización, fortalecimiento de políticas, optimización de perfiles, revisión de reglas y mejora continua del servicio, con el propósito de incrementar la efectividad de la protección, reducir falsos positivos y mantener alineación con la evolución de las amenazas y de las aplicaciones protegidas.
- Garantizar la integración del servicio con las plataformas de monitoreo, gestión de logs, análisis de eventos, SIEM, SOC o demás componentes de seguridad definidos por la Entidad, asegurando trazabilidad y capacidad de correlación.

Informes del servicio

El contratista deberá presentar informes con periodicidad mensual y/o por demanda, los cuales deberán ser entregados dentro de las veinticuatro (24) horas siguientes a la solicitud realizada por la Entidad. Dichos informes deberán ser emitidos desde la gestión de seguridad informática y acompañarse del respectivo análisis técnico.

Como mínimo, los informes deberán contener los siguientes componentes:

- Top 10 de malwares identificados durante el periodo reportado, cuando exista correlación con eventos asociados a las aplicaciones protegidas.
- Top 10 de ataques dirigidos a los aplicativos webs durante el periodo reportado.
- Top 10 de ataques web de día cero (0-day) detectados o mitigados.
- Top 10 de direcciones IP de origen asociadas a eventos o intentos de ataque sobre las aplicaciones protegidas.
- Consumo de canal de las aplicaciones, con reporte filtrado entre direcciones IP internas y externas, conforme a la información suministrada por las plataformas de monitoreo y análisis definidas por la Entidad. Este reporte podrá presentarse con periodicidad trimestral o la que establezca el ICBF.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Reporte de intentos de defacement detectados, mitigados o investigados durante el periodo.
- Informe de vulnerabilidades de aplicaciones web, incluyendo hallazgos, criticidad, estado, tendencia y recomendaciones de tratamiento.

Adicionalmente, cada informe deberá incluir como mínimo el análisis del comportamiento observado, tendencias, nivel de criticidad, aplicativos afectados, acciones ejecutadas, hallazgos relevantes, estado de mitigación y recomendaciones orientadas al fortalecimiento de la postura de seguridad del ICBF.

NOTA TÉCNICA: El fabricante de la solución Web Application Firewall (NGWAF) de Próxima Generación deberá estar posicionado en los informes más recientes del Cuadrante Mágico de Gartner para WAF, demostrando capacidad de ejecución, visión estratégica e innovación tecnológica en la protección de aplicaciones web y API.

6.9.16.7 SERVICIO DE SEGURIDAD EN BASES DE DATOS (DAM)

La Entidad requiere una solución de Monitoreo de Actividad de Bases de Datos (Database Activity Monitoring – DAM) que permita auditar, proteger, monitorear y gestionar los riesgos de seguridad asociados a los motores de bases de datos institucionales.

El servicio deberá permitir la supervisión continua de la actividad sobre las bases de datos, la identificación de comportamientos anómalos, la detección de accesos no autorizados, la gestión de vulnerabilidades, la trazabilidad de transacciones críticas, la protección de información sensible y el fortalecimiento permanente de los controles de seguridad asociados a estos activos.

Adicionalmente, la solución deberá incorporar capacidades de analítica avanzada, aprendizaje automático (Machine Learning), Inteligencia Artificial (IA) y mecanismos de detección basados en comportamiento, orientados a fortalecer la detección temprana de amenazas, la reducción de falsos positivos, la identificación de actividades anómalas y la respuesta frente a eventos de seguridad dirigidos contra los activos de datos de la Entidad.

Modalidad de la Solución

La plataforma deberá ser provista mediante un appliance físico o virtual de propósito específico.
Para garantizar la integridad y el desempeño de los servicios críticos, el monitoreo principal deberá realizarse en modo Sniffer (pasivo), asegurando que no se genere latencia ni degradación del rendimiento de los motores de base de datos monitoreados.
La solución deberá soportar adicionalmente modos de monitoreo mediante agentes y mecanismos de protección en línea cuando la Entidad lo requiera.

Alcance y Compatibilidad

Suministro Integral
El oferente deberá incluir hardware, software, soporte, mantenimiento, instalación, configuración, parametrización, puesta en operación y licenciamiento requerido durante toda la vigencia contractual.

Cobertura de Motores de Base de Datos
La solución deberá soportar de forma nativa la auditoría, monitoreo y protección de las siguientes plataformas:

- Oracle Database.
- Microsoft SQL Server.
- MySQL.
- MariaDB.

La solución deberá soportar implementaciones On-Premise, entornos virtualizados, híbridos y servicios desplegados en nube pública o privada.

Interfaces de Red
La plataforma deberá contar con la densidad de puertos necesaria para capturar tráfico replicado mediante SPAN, TAP o puertos Mirror provenientes de los segmentos de red donde operan los servicios de bases de datos.

Rendimientos Mínimos de la Plataforma
Para garantizar el procesamiento de grandes volúmenes de consultas y transacciones, la solución deberá cumplir como mínimo con las siguientes capacidades:

- Capacidad de Procesamiento : Entre 25.000 y 40.000 SQL/TPS (o superior).
- Latencia de análisis: Entre 0.1 ms y 5 ms.
- Mínimo 2 puertos 10 GbE (SFP+) y 4 puertos 1 GbE (RJ45).
- Almacenamiento local entre 8 TB a 12 TB (o superior) brutos para la retención de registros de auditoría y evidencias.
- Fuentes de alimentación redundantes y licenciamiento suficiente para cubrir la totalidad de instancias de bases de datos definidas por la Entidad.

Funciones de Monitoreo, Protección y Auditoría (DAM)

La solución deberá permitir:

Centralización
Capacidad de centralizar la auditoría y monitoreo de múltiples motores de bases de datos mediante una consola unificada de administración.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Alertamiento en Tiempo Real
Generación de alertas en tiempo real sobre:
Comandos DML
- SELECT
- INSERT
- UPDATE
- DELETE

Comandos DDL
- CREATE
- ALTER
- DROP

Comandos DCL
- GRANT
- REVOKE

Autenticación
- Accesos exitosos.
- Accesos fallidos.
- Bloqueos de cuentas.
- Cambios de privilegios.

Monitoreo de Actividad
La solución deberá monitorear y registrar:
- Consultas realizadas.
- Modificaciones sobre estructuras de bases de datos.
- Actividades administrativas.
- Acciones de cuentas privilegiadas.
- Transferencias masivas de información.
- Accesos a datos sensibles.
- Intentos de evasión de controles.

Detección Basada en IA y Analítica de Comportamiento
La solución deberá incorporar capacidades de IA y Machine Learning que permitan:
- Detectar comportamientos anómalos de usuarios, administradores, aplicaciones y cuentas de servicio.
- Identificar accesos fuera del patrón habitual.
- Detectar posibles amenazas internas.
- Detectar movimientos laterales asociados a cuentas comprometidas.
- Identificar consultas masivas o inusuales sobre información sensible.
- Detectar posibles intentos de exfiltración de datos.
- Asignar niveles dinámicos de riesgo a usuarios, sesiones y transacciones.
- Reducir falsos positivos mediante aprendizaje continuo (Auto-Learning).

Integración con Inteligencia de Amenazas

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

La solución deberá permitir la correlación con:

- Indicadores de Compromiso (IoC).
- Indicadores de Ataque (IoA).
- Fuentes de Threat Intelligence.
- Plataformas SIEM, SOAR y SOC.

Gestión de Vulnerabilidades y Postura de Seguridad (DSPM)

La solución deberá incorporar capacidades de evaluación continua de postura de seguridad para bases de datos permitiendo:

- Descubrimiento de instancias de bases de datos.
- Identificación de configuraciones inseguras.
- Identificación de privilegios excesivos.
- Identificación de cuentas huérfanas.
- Detección de vulnerabilidades conocidas.
- Clasificación de información sensible.
- Recomendaciones de hardening y remediación.
- Generación de reportes de cumplimiento.

Gestión de Accesos Privilegiados (PAM)

La solución deberá permitir el control, monitoreo, auditoría y protección de cuentas privilegiadas en ambientes On-Premise, híbridos y Cloud.

La plataforma deberá:

- Centralizar la administración de credenciales privilegiadas mediante bóvedas seguras (Vaults).
- Implementar controles RBAC.
- Gestionar credenciales de:
    - Sistemas operativos.
    - Bases de datos.
    - Aplicaciones.
    - Equipos de red.
    - Servicios Cloud.
- Implementar rotación automática de credenciales.
- Mantener trazabilidad completa de actividades privilegiadas.
- Grabar sesiones administrativas cuando aplique.
- Integrarse con MFA y proveedores de identidad corporativos.

Accesos Temporales y Controlados

La solución deberá soportar:

- Accesos Just-In-Time (JIT).
- Accesos temporales.
- Aprobación multinivel.
- Segregación de funciones (SoD).
- Principio de mínimo privilegio.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Compatibilidad con sistemas legacy y servicios críticos.

Integración con Ecosistema de Seguridad
La solución deberá integrarse con:
- SIEM.
- SOAR.
- MDE-XDR.
- ITSM.
- SOC.

Informes y Reportes
La solución deberá generar informes técnicos y ejecutivos que incluyan:
- Actividad de usuarios.
- Actividad privilegiada.
- Vulnerabilidades identificadas.
- Riesgos detectados.
- Alertas generadas.
- Hallazgos de comportamiento anómalo.
- Indicadores de cumplimiento.
- Tendencias de seguridad.
- Resumen ejecutivo para toma de decisiones.

Alineación con Zero Trust
La solución deberá alinearse con una estrategia de seguridad basada en Zero Trust, garantizando:
- Verificación continua de identidades.
- Aplicación de acceso de mínimo privilegio.
- Monitoreo permanente de actividades.
- Evaluación continua del riesgo.
- Protección de información sensible.
- Auditoría integral de operaciones.
- Respuesta oportuna frente a eventos de seguridad.

Gestión de Vulnerabilidades y Virtual patching

La Entidad requiere un servicio especializado de Parcheo Virtual (Virtual Patching) orientado a proteger de manera proactiva los activos tecnológicos del ICBF frente a la explotación de vulnerabilidades conocidas y desconocidas, mientras se ejecutan de manera formal los procesos de parcheo oficial, remediación definitiva o actualización de los sistemas afectados.

Los procesos de parcheo tradicional pueden requerir ventanas de mantenimiento, pruebas de regresión, validaciones funcionales y coordinación operativa que, en algunos casos, no

permiten una remediación inmediata. Durante ese periodo, los activos permanecen expuestos a la explotación de vulnerabilidades críticas.
El parcheo virtual permite reducir la ventana de exposición mediante controles compensatorios que bloquean o mitigan los intentos de explotación, fortaleciendo la postura de seguridad y garantizando la continuidad operativa de los servicios institucionales, especialmente en:

- Sistemas críticos que no pueden ser reiniciados de inmediato.
- Sistemas legacy o sin soporte del fabricante.
- Aplicaciones que requieren pruebas de regresión antes del parcheo oficial.
- Servicios expuestos a Internet.
- Bases de datos y aplicaciones misionales.

Alcance del servicio
El servicio deberá permitir la protección mediante parcheo virtual sobre:

- Servidores físicos y virtuales.
- Sistemas operativos Windows, Linux y Unix.
- Aplicaciones web y servicios expuestos.
- Bases de datos institucionales.
- Servicios en la nube y entornos híbridos.
- Contenedores y cargas de trabajo cloud (cuando aplique).
- Sistemas legacy o sin soporte.
- Protocolos y servicios de red críticos.

El servicio deberá integrarse con los componentes de seguridad existentes y contratados, incluyendo NGFW, WAF, IPS/IDS, EDR/XDR, SOC, SIEM y SOAR.

Capacidades funcionales mínimas
La solución deberá permitir como mínimo:

- Detección y bloqueo de intentos de explotación de vulnerabilidades conocidas (CVE).
- Protección frente a exploits de día cero mediante análisis de comportamiento.
- Aplicación de firmas virtuales y reglas de protección.
- Inspección profunda de tráfico (DPI) hacia los activos protegidos.
- Protección a nivel de red, host y aplicación.
- Correlación con inteligencia de vulnerabilidades y amenazas.
- Priorización de protección según criticidad del activo y severidad de la vulnerabilidad.
- Aplicación de controles sin necesidad de reiniciar los sistemas protegidos.
- Protección de sistemas legacy sin soporte del fabricante.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Registro y trazabilidad de eventos de protección.
- Generación de alertas y reportes.

Alineación con la estrategia Zero Trust

El servicio de parcheo virtual deberá contribuir a la estrategia Zero Trust del ICBF mediante:

- Reducción continua de la superficie de ataque.
- Protección permanente independientemente de la ubicación del activo.
- Aplicación de controles compensatorios basados en riesgo.
- Validación continua del estado de exposición de los activos.
- Contención automatizada frente a intentos de explotación.
- Protección de activos críticos y legacy dentro del modelo de mínimo privilegio.

Adicional el servicio de virtual Patching deberá:

- Vulnerability Assessment (VA): Realización de análisis de vulnerabilidades sobre los motores de BD a través de la red, identificando debilidades de configuración, privilegios excesivos o contraseñas débiles.
- Mapeo CVE: Los hallazgos deben hacer referencia a bases de datos de vulnerabilidades públicas (CVE) y reportar niveles de severidad (Alto, Medio, Bajo).
- Descubrimiento Automático: Capacidad de identificar nuevos motores de base de datos instalados en la red de forma automática.
- Parcheo Virtual (Virtual Patching): Capacidad de mitigar vulnerabilidades conocidas mediante reglas de seguridad en el DAM que bloqueen el exploit antes de que el motor sea actualizado físicamente.
- El sistema debe permitir implementar parcheo virtual, entendido como la mitigación de vulnerabilidades mediante reglas de seguridad (WAF, IPS, EDR, RASP o firewall) sin modificar el código o instalar parches en el sistema afectado.
- Esta tecnología debe actuar como un escudo que bloquee intentos de explotación a nivel de red, aplicación o endpoint mientras se planifica el parche definitivo.
- Su operación de bloqueo de exploits no debe modificar el sistema original.
- De permitir integrarse con soluciones SIEM para gestion de SOC.

Seguridad Avanzada y Prevención de Fugas

- Prevención de Intrusiones: Capacidad de alertar y bloquear ataques dirigidos a bases de datos (como SQL Injection avanzado) y actividades no autorizadas en tiempo real.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Control de Exfiltración: Monitoreo para detectar fugas de información, transacciones inusuales o accesos sospechosos por parte de usuarios con privilegios elevados (DBAs).
- Reportabilidad: Generación de reportes predefinidos para cumplimiento regulatorio y reportes personalizables según la necesidad del ICBF.

NOTA TECNICA: La solución de seguridad y monitoreo de bases de datos (Database Activity Monitoring – DAM) deberá acreditar capacidades especializadas para la supervisión, auditoría y detección de actividades anómalas o no autorizadas sobre los motores de bases de datos incluidos en el alcance contractual.

El oferente deberá presentar documentación técnica verificable que evidencie la compatibilidad de la solución con los motores de bases de datos requeridos por la entidad, incluyendo, según corresponda, Oracle, Microsoft SQL Server, MariaDB y otros motores existentes en la infraestructura del ICBF. Asimismo, deberá acreditar la disponibilidad de mecanismos de actualización y mantenimiento de firmas, reglas de detección, decodificadores de protocolos y demás componentes necesarios para mantener la compatibilidad con las versiones soportadas de dichos motores.

La solución deberá contar con soporte vigente del fabricante, un ciclo documentado de actualización tecnológica y procedimientos para incorporar nuevas versiones de motores de bases de datos, de acuerdo con la hoja de ruta y las políticas de soporte publicadas por el fabricante.

La acreditación podrá sustentarse en documentación oficial del fabricante, matrices de compatibilidad, notas de versión, políticas de soporte y demás evidencias técnicas verificables.

6.9.16.8 SERVICIO DE SEGURIDAD EN CORREO ELECTRÓNICO.

La Entidad requiere un servicio especializado de protección de mensajería electrónica de propósito específico, capaz de mitigar amenazas avanzadas y garantizar la higiene de la comunicación institucional.
La solución deberá incorporar de manera nativa capacidades avanzadas de Inteligencia Artificial (IA), Machine Learning (ML), analítica de comportamiento y automatización, orientadas a fortalecer la protección de la mensajería electrónica institucional frente a amenazas modernas, incluyendo aquellas generadas o potenciadas mediante inteligencia artificial.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Alcance y Arquitectura del Servicio

- Protección Integral: El servicio debe proteger la totalidad de los buzones descritos en el Anexo técnico, con capacidad de escalamiento dinámico. Debe cubrir tanto el correo entrante como el saliente.
- Defensa Multi-amenaza: Capacidad de detección y bloqueo de SPAM, Virus, Malware, Phishing, Ransomware y amenazas de día cero (*0-day*).
- Alta Disponibilidad: La solución debe estar arquitectada en un esquema de Alta Disponibilidad (HA) y balanceo de carga para garantizar la continuidad del servicio sin puntos únicos de falla.
- Integridad de Ecosistema: El fabricante del hardware, software y las firmas de seguridad deberá ser el mismo, asegurando una conexión en tiempo real a su base de datos de inteligencia de amenazas global.
- Compatibilidad: Debe funcionar como SMTP Mail Gateway y poseer compatibilidad nativa para proteger entornos de Office 365 y nubes híbridas.

Funciones Avanzadas de Seguridad

- Análisis de Malware de Día Cero: El servicio debe incluir de forma inmersa la capacidad de enviar adjuntos y URLs sospechosas a un Sandbox para análisis dinámico. Dicho Sandbox debe ser provisto por el mismo fabricante del servicio de correo.
- Inspección de Contenido: Análisis en tiempo real de encabezados, cuerpo del mensaje, enlaces y archivos adjuntos mediante múltiples motores antimalware y heurísticos.
- Cifrado e Identidad: Capacidad de cifrado basado en la identidad (IBE) o estándares equivalentes para asegurar la confidencialidad de la información saliente.
- Prevención de Fuga de Información (DLP): Módulo DLP integrado y funcional para la creación de políticas basadas en patrones (ej. números de identificación, tarjetas de crédito) sin requerir licenciamiento adicional.

Rendimientos Mínimo de las Plataforma

- Capacidad de Procesamiento e Inspección de Mensajería Electrónica: Entre 50.000 y 100.000 correos/hora (o superior).
- Interfaces: Mínimo 4 interfaces 1 GbE (RJ45/SFP) y/o mínimo 2 interfaces 10 GbE (SFP+).
- Fuente: Redundante, balanceo de carga.
- Almacenamiento: Entre 4 TB y 8 TB usables configurados bajo esquema RAID redundante empresarial (RAID 5, RAID 6 o RAID 10).
- Capacidad de análisis antispam, antimalware, protección contra phishing y protección frente a amenazas avanzadas.
- El licenciamiento de la plataforma no deberá estar limitado por cantidad de dominios protegidos de la entidad.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- La solución deberá incluir módulo de bypass físico (Fail-Open) para garantizar la continuidad del flujo de correo electrónico ante fallas de hardware, software, energía o mantenimiento programado de la plataforma.

NOTA TECNICA: Como criterio de validación técnica, la solución de Seguridad de Correo Electrónico de Nueva Generación (SEG – Secure Email Gateway) deberá contar con reconocimiento o evaluación verificable en al menos uno (1) de los informes publicados durante los últimos veinticuatro (24) meses por firmas analistas independientes reconocidas internacionalmente, correspondientes a la categoría tecnológica aplicable.

La acreditación podrá sustentarse en informes de diferentes firmas analistas independientes, siempre que se pueda verificar la fuente, la fecha de publicación y la correspondencia con la categoría tecnológica evaluada.

6.9.16.9 SERVICIO DE SEGURIDAD PARA ATAQUES DE DENEGACIÓN DE SERVICIO DISTRIBUIDO (DDOS).

La Entidad requiere un servicio especializado para la detección, análisis y mitigación de ataques de Denegación de Servicio Distribuido (DDoS), orientado a proteger la disponibilidad, continuidad operativa y resiliencia de la infraestructura tecnológica expuesta a Internet y de los servicios críticos institucionales.
La solución deberá consistir en un Appliance físico de propósito específico (On-Premise) con capacidad de procesamiento a velocidad de cable (Wire-Speed), incorporando mecanismos avanzados de Inteligencia Artificial (IA), Machine Learning (ML), analítica de comportamiento y automatización, orientados a detectar y mitigar amenazas conocidas, desconocidas y de día cero dirigidas contra los servicios institucionales.

Arquitectura y alta disponibilidad del servicio

El equipo propuesto deberá integrar un módulo de Bypass mecánico (Fail-to-Wire) o contar con un switch de bypass externo gestionado. Esta capacidad será obligatoria para garantizar que, ante fallas de hardware, software o pérdida de energía del appliance, el tráfico continúe fluyendo de manera transparente, evitando interrupciones de conectividad hacia los servicios institucionales.
Resiliencia de Hardware
El equipo deberá contar con:

- Fuentes de alimentación redundantes (1+1).
- Componentes Hot-Swappable.
- Alta disponibilidad nativa.
- Capacidad de recuperación automática ante fallos.

Paridad de Protocolos

La solución deberá soportar de forma nativa la inspección, detección y mitigación de ataques tanto sobre IPv4 como IPv6, manteniendo los mismos niveles de protección y desempeño.

Modos de Implementación

La plataforma deberá operar en los siguientes modos:

- In-Line transparente.
- SPAN / Port Monitoring.
- Out-of-Path.
- Redireccionamiento dinámico de tráfico.
- Integración con mecanismos de Scrubbing cuando aplique.

Rendimientos Mínimos:

Para garantizar la protección eficaz frente a ataques volumétricos, de agotamiento de recursos, amplificación, reflexión y ataques híbridos multicapa, la solución deberá cumplir como mínimo con las siguientes capacidades:

- Rendimiento de procesamiento (Throughput): Entre 15 Gbps y 25 Gbps (o superior) de tráfico bidireccional inspeccionado y mitigado de forma continua.
- Capacidad de mitigación: Entre 14 Mpps y 22 Mpps (o superior).
- Capacidad de sesiones concurrentes: Entre 20.000.000 y 45.000.000 de sesiones concurrentes (y >= 400.000 CPS) en arquitecturas stateful, o capacidad equivalente de mitigación a velocidad de cable (Wire-Speed) en arquitecturas stateless/híbridas.
- Latencia de procesamiento: Entre 1 microsegundo y 100 microsegundos.
- Conectividad: Entre 4 y 8 puertos de 10 GbE (SFP+) compatibles con esquema Fail-to-Wire / Bypass.
- Escalabilidad: Capacidad de crecimiento mediante expansión modular o licenciamiento sin requerir reemplazo de chasis

La solución deberá integrar mecanismos avanzados de Inteligencia Artificial (IA), Machine Learning (ML) y análisis de comportamiento para fortalecer la detección temprana, correlación y mitigación automatizada de amenazas.

Detección Basada en Comportamiento (Behavioral Analysis)

El sistema deberá construir automáticamente líneas base (Baseline) del comportamiento normal del tráfico institucional y detectar desviaciones mediante modelos de aprendizaje automático.

La solución deberá identificar:

- Anomalías de tráfico.
- Ataques de día cero.
- Variaciones atípicas de protocolos.
- Comportamientos asociados a botnets.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Ataques distribuidos coordinados.

Sin depender exclusivamente de firmas estáticas.

Protección DDoS Multicapa (L3–L7)

La solución deberá mitigar ataques dirigidos a:

Capa de Red

- SYN Flood.
- UDP Flood.
- ICMP Flood.
- TCP State Exhaustion.
- Fragmentation Attacks.

Capa de Aplicación

- HTTP Flood.
- HTTPS Flood.
- DNS Flood.
- DNS Query Attacks.
- Slowloris.
- Slow Post.
- Web Session Exhaustion.

Protección contra Reflexión y Amplificación

La solución deberá detectar y mitigar ataques que utilicen:

- DNS.
- NTP.
- SSDP.
- CLDAP.
- Memcached.
- SNMP.
- Protocolos emergentes utilizados para amplificación.

Inteligencia de Reputación Global

La solución deberá integrarse con fuentes globales de inteligencia de amenazas que permitan:

- Identificar botnets activas.
- Detectar centros de comando y control (C2/C&C).
- Bloquear infraestructura maliciosa conocida.
- Identificar campañas coordinadas a nivel global.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

IA Aplicada a Mitigación Adaptativa

La plataforma deberá permitir:

- Aprendizaje continuo (Auto-Learning).
- Ajuste dinámico de umbrales.
- Clasificación automática de amenazas.
- Priorización inteligente de eventos.
- Reducción de falsos positivos.
- Generación de recomendaciones automáticas de mitigación.
- Adaptación automática frente a cambios de comportamiento de los atacantes.
- Detección de ataques impulsados o automatizados mediante IA.

Risk Scoring y Analítica Avanzada

La solución deberá asignar niveles dinámicos de riesgo a:

- Direcciones IP.
- Sesiones.
- Servicios.
- Segmentos.
- Aplicaciones protegidas.

Con base en reputación, comportamiento, geolocalización, inteligencia de amenazas y contexto operacional.

Gestión Multitenancy

La plataforma deberá permitir:

- Segmentación lógica de servicios.
- Políticas independientes por aplicación.
- Administración diferenciada.
- Reportes separados por servicio o dependencia.
- Protección específica para portales críticos y aplicaciones misionales.

Dashboard y Reportabilidad

La solución deberá proporcionar tableros ejecutivos y técnicos con:

- Visibilidad en tiempo real.
- Ataques mitigados.
- Volumen de tráfico.
- Vectores de ataque.
- Top IPs atacantes.
- Indicadores de riesgo.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Tendencias de amenazas.
- Eventos detectados mediante IA.
- Efectividad de las mitigaciones implementadas.

Integración con Ecosistema de Seguridad
La solución deberá integrarse con:

- SIEM.
- SOAR.
- XDR.
- SOC.
- NGFW.
- WAF.
- Sistemas de monitoreo institucional.

La plataforma deberá exportar logs utilizando Syslog, APIs, JSON o mecanismos estándar soportados por el fabricante.

Generación de Inteligencia de Amenazas
La solución deberá permitir generar y exportar:

- Indicadores de Compromiso (IoC).
- Indicadores de Ataque (IoA).
- Direcciones IP maliciosas.
- Firmas de comportamiento.
- Información de reputación.
- Artefactos de inteligencia reutilizables por otras plataformas de seguridad.

Alineación con Arquitectura Zero Trust
La solución deberá contribuir a una estrategia de seguridad basada en Zero Trust mediante:

- Monitoreo continuo de tráfico.
- Evaluación permanente del riesgo.
- Controles adaptativos basados en comportamiento.
- Integración con sistemas de identidad y analítica avanzada.
- Automatización de respuestas frente a amenazas de alto riesgo.

NOTA TECNICA: Como criterio de validación técnica, la solución de mitigación de ataques de denegación de servicio distribuido (DDoS) deberá contar con reconocimiento o evaluación verificable en al menos uno (1) de los informes publicados durante los últimos veinticuatro (24) meses por firmas analistas independientes reconocidas internacionalmente, correspondientes a la categoría tecnológica aplicable.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

La acreditación podrá sustentarse en informes de diferentes firmas analistas independientes, siempre que se pueda verificar la fuente, la fecha de publicación y la correspondencia con la categoría tecnológica evaluada

6.9.16.10 HISTÓRICO, LOGS Y REPORTES.

El oferente deberá suministrar una plataforma de análisis, gestión, correlación y visualización de logs de propósito específico, encargada de la centralización, indexación, análisis avanzado, correlación de eventos, generación de inteligencia y reportabilidad integral de todo el ecosistema de seguridad contratado, incluyendo, entre otros:

- Firewalls de Nueva Generación (NGFW) internos y externos.
- WAF y protección de aplicaciones web.
- Sandboxing.
- Correo electrónico seguro (SEG).
- Protección DDoS.
- DAM y PAM.
- Endpoint y XDR (cuando aplique).
- Servicios SSE/ZTNA.
- Componentes de red y seguridad relacionados.

La plataforma deberá incorporar capacidades avanzadas de Inteligencia Artificial (IA), Machine Learning (ML), analítica de comportamiento (UEBA) y automatización, orientadas a fortalecer la detección temprana, correlación inteligente, priorización de eventos, reducción de falsos positivos, generación de inteligencia de amenazas y soporte para la operación del SOC.

Rendimientos mínimos de la plataforma

Para garantizar el procesamiento eficiente de telemetría institucional, el cumplimiento de los periodos de retención y el soporte a operaciones de análisis forense, la plataforma deberá cumplir con los siguientes umbrales mínimos:

- Capacidad de ingesta de logs: Entre 600 GB/día y 1.000 GB/día (o superior), con capacidad de crecimiento escalable.
- Eventos por segundo (EPS): Entre 18.000 EPS y 28.000 EPS sostenidos (o superior), con soporte para picos superiores.
- Almacenamiento usable de alto desempeño: Entre 24 TB y 35 TB usables (o superior) dedicados a bases de datos de logs, índices y analítica.
- Mínimo un (1) año de retención disponible para consultas, auditorías y análisis forense, con capacidad de expansión modular o externa.
- Gestión de discos: Soporte para esquemas de redundancia de nivel empresarial (RAID 5, RAID 6, RAID 10 o arquitectura de almacenamiento distribuido con tolerancia a fallos).

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Mínimo cuatro (4) interfaces de red, incluyendo al menos dos (2) puertos 10 GbE (SFP+) y dos (2) puertos 1 GbE (RJ45/SFP), con soporte nativo IPv6 certificado por el fabricante.
- Fuentes de alimentación redundantes y componentes críticos intercambiables en caliente (Hot-Swappable).
- Componentes intercambiables en caliente: discos, ventiladores y fuentes.
- Rendimiento de indexación: capacidad de indexar en tiempo real sin degradación del desempeño.
- Rendimiento de búsqueda: motor optimizado para consultas forenses sobre grandes volúmenes de datos.

Capacidades de Inteligencia Artificial, Machine Learning y Analítica Avanzada

La plataforma deberá incorporar capacidades nativas de IA/ML orientadas a fortalecer la detección, correlación y respuesta ante amenazas modernas, incluyendo amenazas automatizadas o impulsadas mediante Inteligencia Artificial. Estas capacidades deberán permitir como mínimo:

- Correlación inteligente de eventos multi-fuente.
- Detección de comportamiento anómalo de usuarios y entidades (UEBA).
- Identificación de patrones asociados a técnicas del marco MITRE ATT&CK.
- Priorización automática de alertas por criticidad, contexto y riesgo.
- Reducción significativa de falsos positivos mediante aprendizaje continuo.
- Aprendizaje continuo (Auto-Learning) del comportamiento del entorno institucional.
- Detección de amenazas persistentes avanzadas (APT).
- Detección de movimientos laterales.
- Detección de campañas coordinadas.
- Identificación de posibles compromisos de credenciales.
- Enriquecimiento automático de eventos con inteligencia de amenazas.
- Recomendaciones automatizadas de mitigación y respuesta.
- Generación de indicadores de riesgo (Risk Scoring) para usuarios, sesiones, dispositivos y aplicaciones.
- Detección de anomalías estadísticas y variaciones de comportamiento.
- Análisis predictivo de amenazas.

Integración con el Ecosistema de Seguridad

La plataforma deberá permitir integración nativa o interoperable con:

- SIEM.
- SOAR.
- XDR.
- SOC.
- NGFW.
- WAF.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- SEG.
- DDoS.
- Sandbox.
- DAM y PAM.
- Servicios SSE/ZTNA.
- Servicios de identidad (AD, Entra ID, LDAP, SAML).
- Servicios de inteligencia de amenazas (Threat Intelligence).
- Servicios ITSM para gestión de incidentes.
- Herramientas de automatización institucional.

La integración deberá permitir:

- Ingesta bidireccional.
- Exportación de eventos.
- Ejecución de acciones automatizadas.
- Enriquecimiento cruzado.
- Correlación centralizada.

Capacidades de Reportabilidad y Cumplimiento

El sistema deberá generar reportes de manera nativa, sin requerir desarrollos adicionales, cumpliendo con:

Formatos y Personalización

- Reportes tabulares y gráficos (pie-chart, bar-chart, líneas de tendencia, mapas de calor, dashboards personalizados).
- Personalización por fuentes, destinos, servicios, aplicaciones, usuarios y ubicaciones.
- Selección de periodos absolutos o relativos.
- Reportes ejecutivos, técnicos, operativos y de cumplimiento.

Automatización

- Calendarización de reportes.
- Envío automático por correo electrónico.
- Publicación en repositorios seguros.
- Ejecución bajo demanda.

Multilingüe

- Soporte para reportes en español e inglés.

Categorías de Reportes Predefinidos

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

La solución deberá incluir plantillas listas para uso en:

Seguridad y Amenazas

- Ataques web.
- Intrusiones (IPS).
- Malware de día cero.
- Ataques DDoS.
- Amenazas identificadas por IA.
- Comportamientos anómalos.

Aplicaciones y Tráfico

- Consumo de ancho de banda.
- Uso de aplicaciones.
- Riesgos por aplicación.
- Reputación de clientes.
- Sesiones críticas.

Correo Electrónico

- Correo malicioso.
- SPAM.
- Phishing.
- BEC.
- Cuarentenas.
- Actividad de usuarios de correo.

Acceso y Uso Web

- Categorías de URL visitadas.
- Uso de VPN.
- Actividades de usuarios.
- Actividades administrativas.
- Actividades privilegiadas.

Reportes de Cumplimiento

- Cumplimiento ISO 27001.
- Cumplimiento MSPI de MinTIC.
- Cumplimiento normativo colombiano.
- Cumplimiento operacional.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Arquitectura, Retención y Disponibilidad

Retención

La plataforma deberá garantizar el almacenamiento y disponibilidad de la información histórica durante un periodo mínimo de un (1) año en almacenamiento activo, permitiendo consultas, auditorías y análisis forense sobre la totalidad del periodo.
Se recomienda contemplar retención extendida en almacenamiento secundario cuando sea requerido por normativa.

Disponibilidad

Debido a que la plataforma opera de forma pasiva recibiendo telemetría, se deberá implementar en un esquema Standalone de alto rendimiento o en modalidad de Alta Disponibilidad según se defina en el diseño, asegurando que su operación no genere impacto o latencia en los servicios de seguridad perimetral.

Ambiente de Análisis Controlado (Sandbox de Análisis DDoS)

El proveedor deberá garantizar la implementación y operación de un entorno controlado tipo sandbox orientado a la protección, análisis y mitigación de ataques de denegación de servicio distribuido (DDoS), incluyendo la generación de logs, registros de actividad, inteligencia de amenazas y reportes analíticos para el seguimiento técnico y operativo del servicio.

Alta Disponibilidad del Servicio

Se deberá suministrar un servicio en alta disponibilidad para la detección, contención, mitigación y análisis de ataques DDoS dirigidos contra la infraestructura web y los componentes de seguridad perimetral de la Entidad, asegurando que el sandbox mantenga capacidad continua de análisis y correlación.

Monitoreo y Medición del Servicio

Se deberán configurar y mantener operativas herramientas de monitoreo capaces de recopilar, consolidar y analizar:

- Logs.
- Trazas de eventos.
- Métricas de desempeño.
- Indicadores de disponibilidad.
- Indicadores de efectividad del servicio anti-DDoS.
- Analítica basada en IA.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Estos indicadores deberán permitir al ICBF validar el cumplimiento de los Acuerdos de Nivel de Servicio (ANS).

Entrega de Informes y Reportes

El contratista deberá presentar informes mensuales, o bajo demanda dentro de las 24 horas siguientes a la solicitud realizada por la Entidad.
Los reportes deberán incluir análisis técnico y evidencias generadas por el sandbox y por los componentes de seguridad asociados.
Como mínimo, los reportes deberán incluir:

- Ataques L3 (Capa de Red).
- Ataques L4 (Capa de Transporte).
- Ataques L7 (Capa de Aplicación).
- Ataques HTTP/HTTPS.
- Ataques DNS.
- Anomalías detectadas.
- Comportamientos identificados mediante IA.
- Análisis conductual.
- Consolidado de logs, eventos, alertas e indicadores.
- Indicadores de compromiso e indicadores de ataque.

Cada reporte deberá incluir análisis técnico completo, con:

- Hallazgos.
- Tendencias.
- Comportamiento del tráfico.
- Niveles de riesgo.
- Recomendaciones de fortalecimiento.
- Acciones preventivas.
- Recomendaciones basadas en analítica avanzada.

Nota Tecnica: Como criterio de validación técnica, la plataforma propuesta para el análisis, correlación y gestión de registros de eventos de seguridad deberá contar con reconocimiento o evaluación verificable en al menos uno (1) de los informes publicados durante los últimos veinticuatro (24) meses por firmas analistas independientes reconocidas internacionalmente, correspondientes a las categorías de Gestión de Información y Eventos de Seguridad (SIEM), Gestión y Analítica de Logs de Seguridad u Operaciones de Seguridad (SecOps), según corresponda a las capacidades de la solución ofertada.

La acreditación podrá sustentarse en informes de diferentes firmas analistas independientes, siempre que se pueda verificar la fuente, la fecha de publicación y la correspondencia con la categoría tecnológica evaluada.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

6.9.16.11 SERVICIO DE CENTRO DE OPERACIÓN DE SEGURIDAD (SOC - Security Operation Center).

- El Contratista deberá suministrar herramientas tecnológicas para este fin, incluyendo (Hardware/software/licenciamiento) garantizando su instalación, configuración, administración, integración, actualización y gestión de reportes durante toda la vigencia del servicio.
- El servicio deberá integrar de manera nativa capacidades de SIEM, SOAR, UEBA, Threat Intelligence, Machine Learning, Inteligencia Artificial (IA), Threat Hunting, Automatización y Orquestación, alineado a marcos internacionales tales como NIST CSF 2.0, ISO/IEC 27001:2022, MITRE ATT&CK, MITRE D3FEND y a los lineamientos del MSPI de MinTIC.
- Se requiere un servicio integral el cual permita monitorear la Seguridad de las plataformas tecnológicas del ICBF mediante el servicio SOC - Security Operation Center, el cual implemente una tecnología de SOAR y Plataforma de Defensa Activa y Caza de Amenazas Mediante Engaño y Señuelos Distribuidos para automatización de respuestas frente a orquestación de incidentes el cual debe cumplir con los siguientes requerimientos mínimos:
- El contratista para dar cumplimiento a la solución de seguridad debe contar con un SOC (Centro de Operaciones de Seguridad) en Colombia. El mismo deberá cumplir con certificación ISO 27001/2013 y versión superior durante el plazo de ejecución del contrato. Adicionalmente, debe estar soportado en un datacenter certificado en al menos TIER III.
- El servicio requerido deberá alinearse con las mejores prácticas definidas por la versión más actualizada de ITIL. Se implementará en los dos (2) primeros meses desde el inicio del contrato, se configurará y estabilizará los componentes SOAR , actividades que se ejecutarán desde el inicio del contrato, para lo cual es importante que el contratista presente el plan de configuración y estabilización del SOAR al inicio de la operación. El servicio deberá contar con:
- El SIEM de próxima generación con características SOAR deberá contar con capacidad de monitorear componentes e infraestructura (On-premise–infraestructura Hibrida-Cloud)
- El SIEM de próxima generación con características SOAR deberá tener capacidad de detección y respuestas extendidas a incidentes de seguridad.
- El SIEM de próxima generación deberá realizar depuración automática de falsos positivos y a su vez el SOC deberá realizar una segunda depuración que permita disminuir el volumen de información a correlacionar.
- El SOC debe garantizar el monitoreo, compatibilidad e interoperabilidad entre todos los dispositivos de seguridad informática, servidores, servicios web, con los que cuente el ICBF En sus diferentes ambientes (On-premise–Hibrido-Cloud).
- El servicio debe contar con la capacidad de efectuar automatización en la contención de amenazas, entre los diferentes componentes de seguridad del servicio a saber FIREWALLS DE APLICACIONES, ANTIVIRUS, WEB, DISPOSITIVO DE SEGURIDAD

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

EN CORREO ELECTRÓNICO, APPLIANCE DDOS, ANTIVIRUS y NAC TANTO PARA EL PARSING DE EVENTOS COMO PARA LA EJECUCIÓN DE PLAYBOOKS DE SOAR y demás dispositivos de seguridad con los que cuente el ICBF.

- Las plataformas SIEM de próxima generación y SOAR deberá contener casuística acorde a las características avanzadas de los componentes de seguridad, el contratista deberá realizar ajustes y afinamiento constante que permitan el correcto aprovechamiento de las características avanzadas de respuesta y automatización de estas.
- Implementar y probar casos de uso personalizados, utilizando pruebas de escritorio y técnicas de machine learning, para asegurar que las soluciones SIEM de próxima generación y SOAR funcionen como se esperaba y se adapten a los procesos y requisitos de la entidad.
- Desarrollar y probar playbooks de automatización de seguridad aplicando pruebas de escritorio, utilizando casos de uso específicos y personalizados, para asegurar que las respuestas y mitigaciones se realicen de manera eficiente y efectiva.
- Implementar y probar mecanismos de retroalimentación y seguimiento de incidentes, utilizando casos de uso específicos y personalizados, para realizar análisis post-ataque y mejorar las defensas.
- Capacidades de rastreo y seguimiento de la evolución de la presencia digital de la marca ICBF, para identificar tendencias y posibles amenazas emergentes
- El SOAR deberá contar como mínimo con ciento cincuenta (150) playbooks personalizables orientados a los casos de uso de seguridad definidos por el ICBF, e incluir conectores para integrarse con SIEM, EDR/XDR, Firewall, WAF, antivirus, correo electrónico, servicios de identidad, gestión de vulnerabilidades, inteligencia de amenazas y sistemas de gestión de tickets, según aplique.
- El servicio, mediante la herramienta de SIEM de próxima generación debe hacer el monitoreo de estado de salud de infraestructura de cómputo, conectividad, servidores, aires acondicionados, UPS, dispositivos de seguridad, dispositivos UEBA mínimo 1200 agentes, integrarlos en una CMDB, y hacer la correlación de eventos de dichas fuentes de información, para la generación de alertas y disparo de libretos de respuesta a incidentes manuales y automáticos en la plataforma de SOAR, mediante la interacción de esta con diferentes componentes de la infraestructura de la entidad. Debe contar con integración al menos con las plataformas de seguridad perimetral ofertadas.
- Realizar análisis de vulnerabilidades internas y externas dos veces al año.
- Análisis de riegos.
- El servicio deberá ser prestado bajo un esquema gestionado, operado y administrado por personal con certificaciones vigentes durante toda la ejecución contractual. El equipo de monitoreo SOC asignado al ICBF deberá contar con dedicación exclusiva para la operación del servicio durante la vigencia del contrato, garantizando la atención continua, el seguimiento oportuno de los eventos de seguridad y el cumplimiento de los niveles de servicio establecidos. El incumplimiento de esta obligación dará lugar a la aplicación de las sanciones contractuales correspondientes.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Realizar una consultoría de al menos 30 horas hábiles para evaluar riesgos generales basados en las nuevas tendencias en ciberseguridad indicando las respectivas recomendaciones y buenas prácticas. El profesional del equipo de trabajo debe tener mínimo las siguientes certificaciones:
- CISM (Certified Information Security Management).
- LEAD Auditor ISO 27001:2022.
- El SIEM deberá contar con capacidades avanzadas de:
    - Recolección de logs multiplataforma y multi-fabricante.
    - Normalización, enriquecimiento y categorización de eventos.
    - Correlación en tiempo real e histórica sobre eventos ya almacenados.
    - Detección basada en firmas, comportamiento, Machine Learning e Inteligencia Artificial.
    - Análisis de comportamiento de usuarios y entidades (UEBA).
    - Correlación con inteligencia de amenazas (Threat Intelligence).
    - Mapeo automático de eventos al framework MITRE ATT&CK.
    - Detección de amenazas persistentes avanzadas (APT).
    - Detección de movimientos laterales, escalamiento de privilegios y compromiso de credenciales.
    - Depuración automática de falsos positivos mediante IA.
    - Priorización dinámica basada en Risk Scoring.
    - Cálculo de riesgo considerando importancia del evento, criticidad del activo, vulnerabilidades asociadas y antecedentes de origen/destino.
    - Correlación cruzada entre múltiples fuentes.

      Análisis contextual mediante abstracción de datos (día, hora, ubicación, patrón de acceso, etc.).

- Diseño del Servicio: El servicio requerido deberá contar con las características mínimas descritas en el presente documento, sin embargo, las definiciones adicionales específicas deberán contemplarse en esta fase del servicio, de tal forma que se detallen y acuerden los alcances técnicos detallados entre la Entidad y el prestador del servicio. Esta fase deberá ser previa a la puesta en producción del servicio contratado y contará con el visto bueno de la Entidad, de tal forma que se cubran las expectativas que la Entidad requiere a nivel de ingeniería de detalle.
- El Contratista deberá presentar la metodología que utilizará para dimensionar, instalar, implementar y hacer transferencia de conocimiento (funcional y técnica) del servicio SOC. El servicio de monitoreo objeto del presente documento, especificando etapas, recursos, entregables, herramientas, técnicas y metodologías a utilizar.
- Transición del Servicio: En esta fase del servicio se deberán analizar todas las actividades necesarias para aprovisionar correctamente el servicio, de tal forma que todas las programaciones, ventanas, información requerida, configuraciones detalladas y demás adicionales, se contemplen y se dejen claras para que los tiempos y el

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

cronograma sea ejecutado correctamente y se cumplan con los tiempos acordados para cada fase.

- Operación del Servicio: Esta fase permitirá la puesta en producción del servicio, contando con la operatividad de la modalidad de servicios, subservicios y características detalladas en el presente documento, garantizando el cumplimiento de los ANS definidos para el servicio.
- Mejora Continua del Servicio: Se deberá contar con una fase que garantice la mejora continua de todos los servicios, subservicios, procesos y características requeridas para la prestación del servicio. Garantizando que las configuraciones, reportes, características y demás requerimientos en los servicios y plataformas que lo soportan, se encuentren totalmente afinados y configurados acorde a las definiciones acordadas en el Diseño del servicio.
- La plataforma que soporte el servicio de SOC deberá cumplir como mínimo con las siguientes funcionalidades:
- La plataforma deberá colectar los eventos de seguridad de múltiples marcas para lo cual se deberá incluir el licenciamiento necesario para esto.
- Deberá ser nueva en su totalidad y con las últimas versiones de software liberadas por el fabricante.
- No se aceptarán dentro de la oferta soluciones basadas en software libre.
- Deberá ser con pares redundantes o unidades de respaldo y con mecanismos internos que ofrezcan alta disponibilidad.
- Deberá tener una arquitectura de última generación, para llevar a cabo la colección, gestión y correlación de eventos.
- El servicio deberá permitir una arquitectura flexible y escalable, en la cual sea posible adicionar incrementos de capacidad de procesamiento de eventos por segundo sobre el licenciamiento base.
- Deberá soportar la cantidad de Eventos Por Segundo (EPS) generados por las fuentes descritas en el Anexo 03 - Línea Base de Servicios TI de las cuales se obtendrán eventos.
- Deberá contemplar la instalación y puesta a punto por personal certificado por parte del fabricante.
- El servicio de correlación deberá utilizar infraestructura dedicada en appliance o servidor que centralice los componentes del motor de correlación. Los componentes que colectan los eventos deberán estar separados del motor de correlación. En caso de que la plataforma sea del tipo Virtual Appliance el proveedor del servicio deberá aprovisionar los recursos de hardware y software necesarios para garantizar la prestación del servicio.
- Los componentes que realizan la recolección de eventos deberán ser aprovisionados en servidores o appliance de propósito específico para el servicio SIEM de próxima generación, así mismo se requiere el aprovisionamiento de una unidad redundante que sirva como respaldo en caso de falla.
- El conjunto de herramientas para recolectar eventos de fuentes no soportadas por la plataforma de correlación deberá permitir la creación y distribución de dichos

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

componentes de forma gratuita para la Entidad, sin importar el número de conectores desplegados.

- Se requiere que hagan uso de la base de datos de conocimiento (Adicionar, modificar, consultar la KDB) de la herramienta de gestión del ICBF.
- El servicio de correlación deberá ser capaz de realizar la correlación en tiempo real y en memoria (sobre el flujo entrante de eventos), así como correlación histórica para eventos que han sido colectados fuera de línea. Ambos mecanismos deberán operar de manera concurrente, esto es correlación en tiempo real y correlación histórica.
- La solución debe estar en capacidad de hacer análisis usando métodos de aprendizaje de máquina (Machine Learning), con el fin de detectar desviaciones de la línea base y generar incidentes en concordancia.
- El servicio de correlación deberá contar con una fórmula parametrizable que evalúe el nivel de riesgo de todos los eventos que son recibidos por el motor de correlación considerando como mínimo los siguientes factores:
    - Importancia del evento
    - Criticidad del activo
    - Vulnerabilidades asociadas
    - Antecedentes sobre el origen, destino o ambos.
- El servicio de correlación deberá tener la capacidad de abstraer datos a partir de los eventos base provenientes de los dispositivos, tales como derivar algún dato particular (ej.: día del mes, hora del día) que permita realizar un análisis de eventos basándose en el contexto (ej. Generar una alerta si el evento se reporta en un horario no productivo a partir de la hora del día).
- El servicio de Correlación de Eventos deberá proporcionar un módulo integrado para la gestión de casos (tickets) de seguridad permitiendo asociar eventos a acciones tales como enviar una notificación al equipo de operadores, abrir y asignar un caso a un usuario para su investigación o ejecutar un script a partir de la identificación de un incidente de seguridad.
- Integrar las alertas de Microsoft Defender XDR con la plataforma SIEM/SOC del ICBF para mejorar la detección y respuesta a incidentes.
- Monitoriar y reportar las incidencias detectadas en la plataforma de Microsoft Defender XDR para activar de manera eficiente y oportuna la respuesta a incidentes.
- El servicio de correlación deberá permitir realizar correlación histórica, es decir de eventos que ya se encuentran almacenados en la base de datos o que incluso pueden ser reactivados. Este método de correlación deberá ser adicional a las capacidades de correlación en tiempo real realizadas por la herramienta.
- La plataforma deberá proveer la capacidad de integrar fuentes de eventos que no sean soportadas actualmente “fuera de la caja” (tales como aplicaciones o desarrollos hechos en casa) a través de la incorporación de un conjunto de herramientas que permitan definir la lógica para extraer, obtener, normalizar y categorizar los eventos registrados en las siguientes fuentes:
    - Archivos de logs (bitácoras) con campos delimitados
    - Archivos de logs (bitácoras) de longitud variable (no delimitados).

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Bases de datos relacionales por conexión ODBC (Open DataBase Connectivity) o Bases de datos relacionales por conexión JDBC (Java Database Connectivity)
- Traps de protocolo SNMP
- Eventos enviados por protocolo Syslog
- Archivos con formato XML

- Deberá monitorear los sistemas vía Ping, SNMP, WMI, así como análisis del reinicio o caída de interfaces críticas, procesos y servicios críticos, cambios en BGP/OSPF/EIGRP o caídas de puertos del tipo Storage, con el fin de evaluar posibles comportamientos sospechosos o ataques a la infraestructura Tecnológica.
- Deberá poder Monitorear Infraestructura VoIP vía IPSLA, SNMP, CDR y CMR, en busca de comportamientos anómalos de la plataforma de telefonía.
- Deberá hacer modelamiento de transacciones sintéticas vía Ping, HTTP, HTTPS, Scripts JAVA, DNS, LDAP, SSH, SMTP, IMAP, POP3, FTP, JDBC, ICMP, traceroute y puertos TCP/UDP genéricos, con el fin de evaluar el impacto a los servicios y/o aplicaciones de la Entidad, en caso de un ataque.
- Deberá poder Monitorear sistemas del tipo Directorio Activo y Exchange basado en WMI y PowerShell.
- La plataforma al ser un SIEM de nueva generación deberá contar con características SOC, por lo cual deberá realizar actualización constante de la base de datos de contextos, configuraciones, software instalado y servicios corriendo de los dispositivos monitoreados.
- Visor personalizado de log de tráfico. Herramienta de búsqueda sobre los logs de tráfico.

Disponibilidad

El servicio deberá ser prestado 7x24x365.

Rendimientos

Rendimientos Mínimos de la Plataforma

El servicio deberá garantizar la recolección de logs de los dispositivos de seguridad, servidores, aplicaciones, bases de datos, dispositivos activos de red y cualquier otro definido por la Entidad, garantizando todo el licenciamiento, software y hardware necesario para su prestación, sin que esto genere costos adicionales para la Entidad, cumpliendo con las siguientes especificaciones:

Número de dispositivos a monitorear

Capacidad mínima para monitorear mil ochocientos (1.800) dispositivos, incluyendo, entre otros:

- Dispositivos de seguridad.

- Servidores físicos y virtuales.
- Aplicaciones.
- Bases de datos.
- Dispositivos activos de red.
- Cualquier otro activo definido por la Entidad.
- Número de agentes UEBA Capacidad para soportar como mínimo mil doscientos (1.200) agentes o entidades de análisis de comportamiento (UEBA), debidamente licenciados y operativos.

Interfaces y fuentes de eventos

- Capacidad de integrar múltiples interfaces, fuentes y tipos de logs, sin limitación por licenciamiento, permitiendo la incorporación progresiva de nuevas fuentes durante la vigencia del contrato.

Eventos por segundo (EPS)

- Capacidad mínima para procesar entre 20.000 EPS y 30.000 EPS sostenidos (con escalabilidad horizontal/vertical sin reimplementación).

La plataforma deberá permitir escalabilidad horizontal o vertical, de tal forma que pueda:

- Procesar un volumen superior de EPS cuando la operación lo requiera.
- Ajustarse a crecimientos en la infraestructura y en el volumen de eventos sin reimplementaciones complejas.
- Normalización y correlación de eventos en tiempo casi real.

Capacidad de análisis avanzado, incluyendo:

- Reglas de correlación.
- Análisis de comportamiento (UEBA).
- Detección de eventos de seguridad y anomalías.
- Capacidad de generación de alertas configurables según criticidad y contexto.
- Almacenamiento de eventos conforme a los requerimientos de la Entidad y normatividad aplicable.
- Capacidad de búsqueda, consulta y análisis histórico de logs.
- Generación de reportes operativos, técnicos y ejecutivos.

Integración con plataformas de seguridad, sistemas operativos, aplicaciones y bases de datos mediante:

- Agentes.
- Protocolos estándar.
- APIs u otros mecanismos equivalentes.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Capacidad de exportar eventos y alertas a otras plataformas de seguridad o respuesta a incidentes (SOAR, ticketing, entre otros).

Numero de Interfaces a Monitorear: No Limitadas por Licenciamiento.

Funciones y características

El servicio de monitoreo de la infraestructura a nivel de seguridad, disponibilidad y recursos deberá cumplir como mínimo con las siguientes características:

- Realizar el monitoreo y la correlación de eventos tipo (SOC) y la administración y soporte delegados desde la sede SOC del Contratista de mil ochocientos (1800) activos de la plataforma de red y cómputo del ICBF, con capacidad dentre 20.000 EPS y 30.000 EPS (Eventos Por Segundo) y debe estar en la capacidad de procesar más EPS en función de la necesidad de operación de la entidad. Entiéndase por activo una única dirección IP de un dispositivo como un Switch, un servidor, una URL, un enrutador, etc.
- La totalidad del software, el licenciamiento, el hardware de cómputo y almacenamiento necesarios para soportar los servicios definidos, deberán ser provistos por el Contratista con herramientas licenciadas (no open source), sin que ello acarre costos adicionales para la Entidad.
- Entregar al supervisor del contrato dentro de la etapa de transición, un plan de trabajo en el cual se indiquen las actividades a realizar y las fechas complementadas para la instalación de los servicios contratados.
- El proveedor deberá contar con una capacidad operativa dedicada al SOC para brindar un soporte 7x24x365 con el personal especializado solicitado y prestar el servicio acorde al modelo operativo definido en el presente documento.
- Para la prestación del servicio de monitoreo y la correlación de eventos, el Contratista debe proveer las herramientas tecnológicas especializadas propias para la recopilación, correlación y análisis de eventos. Por lo tanto, el proveedor pondrá al servicio del ICBF, la infraestructura que sea necesaria para el cumplimiento técnico del servicio, sin que esto implique costos adicionales para la Entidad.
- La plataforma utilizada para el servicio de monitoreo SOC deberán ser propietarias, de propósito específico y con soporte del respectivo fabricante.
- Con el fin de mantener la homogeneidad de las soluciones que prestan en el servicio de SOC, se requiere que las mismas estén totalmente integradas y que desde un mismo dashboard se puedan ver los eventos de SOC, lo cual le garantiza a la Entidad los tiempos de repuesta en temas de soporte y garantía.
- Se debe garantizar el monitoreo 7x24x365 del estado de los activos objeto del servicio SOC y se deben generar las alertas correspondientes en caso de eventos que puedan afectar a la seguridad de la información de la plataforma TI del ICBF.
- Se debe proporcionar un servicio (integrando el concepto de solución SIEM) que permita realizar análisis, gestión de logs y correlación de eventos de seguridad que se presenten.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

La herramienta que soporte este servicio de correlación debe ser especializada para esta función y administrada por personal calificado.

- Se deben parametrizar una serie de alertas específicas, clasificarlas, priorizarlas sobre la plataforma tecnológica que se está monitoreando y reportarlas a las personas designadas por el ICBF cada vez que se encuentre en riesgo la integridad, la disponibilidad o la confidencialidad de la información. Estas alertas deben suministrar información de valor para ser analizadas en la gestión de riesgos e incidentes que hace parte del Sistema de Gestión de Seguridad de la Información, esta información debe responder como mínimo las siguientes preguntas; ¿Quién?, ¿Qué?, ¿Cuándo?, Donde?, ¿Por qué?, ¿categoría?,¿tipo de ataque? el cual permita a la Entidad conocer la trazabilidad detallada de un incidente de seguridad.
- La información de logs que se generen en la actividad de monitoreo será propiedad del ICBF y, por ende, el almacenamiento de esta al finalizar el contrato será provisto por el Entidad. Sin embargo, el Contratista deberá garantizar el almacenamiento de logs en su plataforma con retención en línea de al menos seis (6) meses con retención fuera de línea como mínimo doce (12) meses, esto durante toda la vigencia del contrato.
- Se deben elaborar reportes de monitoreo, estadísticas, alertas/eventos, trazabilidad de históricos de alertas/eventos, hallazgos/recomendaciones, remediación de vulnerabilidades, entre otros y se entregarán de manera periódica según requerimiento, los cuales estarán customizados de acuerdo con los requerimientos de la Entidad, por lo menos con una frecuencia mensual. El servicio debe incluir un Dashboard donde se permita ver el estado de seguridad, indicadores, reportes y datos en tiempo real con disponibilidad 7x24x365, de la siguiente manera:Los Dashboard deben soportar diferentes vistas acordes a las diferentes partes interesadas, incluyendo; alta dirección, equipo de operaciones, departamento de seguridad de la información.
- Los Dashboard deberán tener la capacidad de ser modificados, de tal forma que permitan configurar estilos para cada tipo de usuario del sistema.
- El portal debe presentar el estado de seguridad de la infraestructura de IT que hace parte del servicio.
- Se deberá establecer un procedimiento y un plan de comunicaciones (matriz de escalamiento) claro y preciso para notificación de eventos y gestión de alarmas. Este procedimiento definirá el trabajo conjunto entre el SOC y los especialistas como base para operar el servicio y entregar los resultados solicitados.
- Se deberá actualizar, documentar, implementar y verificar el procedimiento de gestión de eventos y alertas del ICBF. Teniendo en cuenta las mejores prácticas existentes y parámetros del SGSI ICBF.
- Será responsabilidad del Contratista, realizar el acompañamiento debido en la implementación de medidas de remediación de vulnerabilidades que se deriven de eventos de seguridad detectados por el SOC, acorde al modelo operativo definido en el presente documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Sera responsabilidad del SOC realizar la respuesta y seguimiento correspondiente ante un incidente o evento de seguridad que se presente en los equipos incluidos en el servicio.
- El Contratista debe entregar informes extraordinarios originados por los incidentes de seguridad informática de categoría crítica y realizar la respectiva gestión de remediación y/o recomendaciones acordes al modelo operativo definido en el presente documento.
- Para todos los equipos requeridos para la prestación del servicio, deberá asegurarse por parte del Contratista, que estos cuentan con el debido mantenimiento, soporte y garantía en caso de fallas, con lo cual se asegura su reemplazo inmediato.
- El proponente deberá realizar todas las conexiones físicas entre los dispositivos que soportan el servicio y los elementos activos de red, garantizando los elementos y accesorios necesarios para realizar las mismas, sin que esto genere costos adicionales para la Entidad.
- Gestión Inteligente de Eventos y Alertas
- Actualización y Estandarización: El Contratista deberá actualizar, documentar, implementar y verificar el procedimiento de gestión de eventos y alertas, alineado con las mejores prácticas (ISO 27001, NIST) y el SGSI del ICBF.
- Enriquecimiento mediante IA: La gestión de alertas deberá integrar algoritmos de Inteligencia Artificial para la correlación avanzada de eventos. El sistema debe ser capaz de realizar un triage automático, priorizando alertas críticas y reduciendo el ruido de falsos positivos mediante el aprendizaje del comportamiento normal de la red institucional.
- Análisis de Línea Base: La solución debe utilizar Machine Learning para establecer líneas base de comportamiento de usuarios y entidades (UEBA), permitiendo la detección de amenazas persistentes avanzadas (APT) que evaden las reglas de detección estáticas.
- Remediación y Acompañamiento Técnico
- Remediación Post-Incidente: Será responsabilidad del Contratista realizar el acompañamiento técnico y la implementación de medidas de remediación ante vulnerabilidades que se deriven de eventos detectados.
- Priorización Predictiva: El SOC debe utilizar herramientas de IA para correlacionar las vulnerabilidades detectadas con las amenazas activas en el panorama global, priorizando la remediación de aquellos activos que presenten un riesgo real y latente para la Entidad.
- Modelo Operativo: La respuesta debe ejecutarse acorde al flujo de trabajo definido, asegurando que cada remediación sea documentada y verificada para evitar la reincidencia del riesgo.
- Respuesta e Informes de Incidentes Críticos
- Gestión de Incidentes: El SOC realizará la respuesta, contención y seguimiento de incidentes de seguridad en todos los activos incluidos en el servicio.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Informes Extraordinarios con IA: Ante incidentes de categoría crítica, el Contratista entregará informes técnicos detallados que incluyan:
- Análisis de Causa Raíz (RCA): Apoyado en herramientas de IA para identificar el vector de entrada y el movimiento lateral.
- Mapeo MITRE ATT&CK: Clasificación de las tácticas y técnicas utilizadas por el atacante.
- Recomendaciones de Seguridad: Plan de acción inmediato y recomendaciones de endurecimiento (hardening) de largo plazo.
- Mantenimiento, Soporte y Garantía de Infraestructura
- Continuidad Tecnológica: El Contratista garantizará que todos los equipos (hardware/software/appliances) destinados a la prestación del servicio cuenten con mantenimiento preventivo, soporte técnico del fabricante 24x7 y garantía vigente.
- Reemplazo Inmediato (NBD): En caso de fallas de hardware, se debe asegurar el reemplazo del equipo bajo la modalidad Next Business Day (NBD) o superior, asegurando que la ventana de indisponibilidad no afecte la postura de seguridad de la Entidad.
- Gestión de Ciclo de Vida: Incluye la actualización de parches de seguridad, firmas y motores de IA de manera regular y programada durante toda la vigencia del contrato.

REQUERIMIENTOS DEL SERVICIO

- Suministrar, licenciar, configurar, gestionar y monitorear la plataforma de propósito específico de SIEM de próxima generación y SOAR, soportadas con datasheet del fabricante.
- Presentar informe técnico de los servicios en monitoreo teniendo en cuenta el alcance aplicaciones e infraestructura. (On-premise – infraestructura Hibrida - Cloud)
- Garantizar compatibilidad e interoperabilidad entre todos los dispositivos de seguridad informática y el SIEM de próxima generación (SOAR)
- Efectuar automatización entre los diferentes componentes de seguridad del servicio (SIEM de próxima generación SOAR– FIREWALLS) Para llevar a cabo contención automatizada de amenazas aplicando las mejores prácticas del fabricante.
- Realizar configuración y casuística del componente SOAR con el fin de contar con automatización aplicando las mejores prácticas del fabricante.
- Presentar informe mensual de estado de la configuración, casuística y eventos relevantes a la automatización para la contención de amenazas.
- El SOC debe presentar informes regulares y auditar la solución de SOAR para garantizar que cumpla con los estándares de seguridad y sea eficaz en la protección de la organización.
- El SOC debe implementar características para obtener visibilidad y detección de amenazas en toda la organización, incluyendo la nube, aplicaciones y dispositivos móviles, y responder de manera efectiva a amenazas e incidentes.
- El SOC debe implementar procesos de SOAR para automatizar tareas de seguridad

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

y responder rápidamente a amenazas e incidentes, reduciendo la carga de trabajo manual y aumentando la eficiencia en la respuesta a incidentes.

- El SOC debe evaluar regularmente la solución de SOAR y realizar mejoras y ajustes necesarios para mantener la eficacia y eficiencia en la protección de la organización contra amenazas cibernéticas.
- Presentar el plan de trabajo, especificando etapas, resultados esperados, estrategias para asegurar el logro de los productos en los tiempos establecidos y describir las técnicas y herramientas que utilizará en la ejecución del contrato, previa aprobación del ICBF.
- Garantizar el servicio de monitoreo de la gestión integrada de seguridad compuesto por:

    - Gestión de Bitácoras y Correlación de Eventos de Seguridad en tiempo real
    - Gestión de eventos en tiempo real
    - Gestión de Configuraciones en tiempo real

- Administrar y monitorear componentes principales y segundarios (HA) 7X24X365 la gestión integrada de seguridad del ICBF.
- Proporcionar el mantenimiento de hardware y actualizaciones de software (parches y upgrades de versión) por la duración del contrato.
- Proporcionar Soporte técnico del fabricante con atención mínimo 8x5 por la duración del contrato.
- Mantener actualizadas las definiciones de ataques, vulnerabilidades y categorización de eventos en el correlacionador de eventos durante la vigencia del contrato y contar con un servicio de suscripción para la actualización de contenidos de seguridad.
- Garantizar en toda circunstancia la posibilidad de escalamiento del servicio con el fabricante para una oportuna solución de incidentes relacionados con la infraestructura como servicio implementado.
- Proporcionar entrenamiento sobre la infraestructura implementada para la prestación del servicio a nivel administrador y usuario final.
- Presentar un informe mensualmente o por demanda (el tiempo de generación y entrega de este no deberá exceder 4 horas) de la Entidad, este informe deberá contener como mínimo los siguientes ítems y será entregado desde el servicio de SOC con su respectivo análisis:

    - Reporte de Incidentes de Seguridad.
    - Reporte de Actividades Sospechosas de Usuarios / Equipos / Aplicaciones.
    - Reporte de Integridad de Archivos.
    - Reporte de Cambios de Configuraciones.
    - Reporte de Cambios no Autorizados en los Registros de Windows.
    - Reporte de Violaciones de Políticas en Bases de Datos.
    - Reporte de Violaciones de Políticas de Control de Acceso.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- El SIEM de próxima generación debe soportar y cumplir como mínimo 70 casos de uso personalizados y probados mediante pruebas de escritorio, como condición necesaria para la aceptación y funcionamiento del servicio.
- El SIEM de próxima generación debe demostrar el cumplimiento de estos requisitos mediante pruebas de escritorio y documentación técnica, y mantener este cumplimiento durante toda la ejecución del contrato.
- El contratista para dar cumplimiento a la solución de seguridad debe contar con un SOC (Centro de Operaciones de Seguridad) en Colombia. El mismo deberá cumplir con certificación ISO 27001/2022 y versión superior durante el plazo de ejecución del contrato. Adicionalmente, debe estar soportado en un datacenter certificado en al menos TIER III.

NOTA TÉCNICA: El fabricante de la solución SIEM de próxima generación propuesta deberá encontrarse clasificado como Líder (Leader) o jugador principal en evaluaciones recientes de firmas analistas independientes internacionalmente reconocidas (tales como el Cuadrante Mágico de Gartner para Security Information and Event Management - SIEM, Forrester Wave para Security Analytics Platforms o IDC MarketScape equivalente).

6.9.16.12 PLATAFORMA DE ORQUESTACIÓN, AUTOMATIZACIÓN Y RESPUESTA (SOAR)

La solución de SOAR deberá actuar como el centro de inteligencia y respuesta automatizada del ICBF, permitiendo la integración de todo el ecosistema de seguridad para reducir los tiempos de respuesta ante incidentes (MTTR).

Capacidad de Integración y Fuentes Inteligentes

- Interoperabilidad Universal: La plataforma debe integrarse de forma nativa mediante protocolos estándar y APIs con los siguientes componentes mínimos:
    - Ecosistema de Seguridad: SIEM de próxima generación, Firewalls (NGFW), WAF, IDS/IPS, Mitigación DDoS, Seguridad de Correo (SEG), Sandboxing (ATP), Plataformas de Decepción y Protección de Marca y demás soluciones que el ICBF indique.
    - Gestión de Identidad: Directorios de identidad (AD, LDAP) y plataformas de autenticación (MFA/SSO).
    - Gestión Operativa: Herramientas de Ticketing (ITSM) y gestión de incidentes.
    - Inteligencia de Amenazas: Capacidad de ingesta de indicadores de compromiso (IoC) mediante estándares STIX/TAXII y otros *feeds* de inteligencia.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Densidad de Conectores: Capacidad técnica para soportar y mantener al menos 200 integraciones activas simultáneas entre plataformas de seguridad, TI y servicios externos de inteligencia.

Rendimiento de Automatización y Orquestación IA-Driven

Para garantizar una respuesta ágil y eficiente, la plataforma deberá cumplir con los siguientes umbrales de rendimiento:

- Ejecución de Playbooks: Entre 120 y 200 playbooks predefinidos y personalizables incluidos.
- Procesamiento Concurrente: Entre 100 y 200 playbooks ejecutándose simultáneamente en paralelo.
- Respuesta Ultra-Rápida: Capacidad de iniciar acciones automatizadas en un tiempo inferior a 30 segundos tras la recepción y correlación de la alerta proveniente del SIEM u otra fuente de telemetría.
- Correlación Asistida por IA: La plataforma debe utilizar algoritmos de Inteligencia Artificial para correlacionar automáticamente múltiples eventos aislados en un único incidente unificado, realizando un *triage* inteligente que identifique la severidad real del evento sin limitación por licenciamiento.

Escalabilidad y Arquitectura Flexible

- Modalidad de Despliegue: La solución debe ser agnóstica a la infraestructura, permitiendo su implementación en formato Appliance (On-premise), entorno Virtualizado, Nube nativa (SaaS) o esquemas Híbridos.
- Alta Disponibilidad: Operación en esquemas de redundancia y failover para asegurar la disponibilidad del motor de automatización 24x7.
- Crecimiento Orgánico: Capacidad de escalabilidad horizontal y vertical según el volumen de eventos e incidentes gestionados por la operación.

Almacenamiento, Trazabilidad y Análisis Forense

- Evidencia Integral: Capacidad de almacenamiento y retención para bitácoras completas de cada playbook, incluyendo evidencias de incidentes, decisiones automatizadas (IA) y manuales (analista), así como las acciones de remediación ejecutadas.
- Auditoría de Acciones: Trazabilidad completa y sellado de tiempo (*timestamping*) de cada acción ejecutada por la plataforma, garantizando la cadena de custodia de la información ante investigaciones forenses.

Cumplimiento, Reportabilidad y Reporte Externo

- Reporting Multinivel: Generación automatizada de reportes técnicos (para el SOC), operativos (gestión de vulnerabilidades) y ejecutivos (indicadores de riesgo).

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Intercambio de Información: Capacidad de exportar información estructurada para auditorías, cumplimiento normativo y reportes oficiales hacia autoridades o grupos de respuesta externos (CSIRT Nacional, CERT, etc.).
- Asistente de IA Generativa: La solución debe permitir la generación de resúmenes de incidentes en lenguaje natural para facilitar la toma de decisiones por parte de los niveles directivos de la Entidad.

NOTA TÉCNICA: Como criterio de validación técnica, la solución de Orquestación, Automatización y Respuesta de Seguridad (SOAR) propuesta deberá contar con reconocimiento o evaluación verificable en al menos uno (1) de los informes publicados durante los últimos veinticuatro (24) meses por firmas analistas independientes reconocidas internacionalmente, correspondientes a las categorías de SOAR, automatización de seguridad u operaciones de seguridad (SecOps), según corresponda a las capacidades de la solución ofertada.

La acreditación podrá sustentarse en informes de diferentes firmas analistas independientes, siempre que se pueda verificar la fuente, la fecha de publicación y la correspondencia con la categoría tecnológica evaluada

Adicionalmente, el oferente deberá acreditar mediante documentación técnica las capacidades de integración con las herramientas de seguridad requeridas por la entidad, la automatización de flujos de trabajo, la ejecución de acciones de respuesta, la gestión de incidentes y la trazabilidad de las acciones realizadas.

6.9.16.13 SERVICIO DE ADMINISTRACIÓN DE ANTIVIRUS

Actualmente el ICBF cuenta con el Antivirus Microsoft Defender y System Center End Point, en producción, que utilizan servidores cache server para la optimización de distribuciones y actualizaciones a sus agentes clientes en toda la infraestructura del ICBF. La periodicidad de aplicación es por demanda, es decir depende de las actualizaciones que Microsoft Defender y Microsoft liberen. La solución de antivirus comprende:

Descripción	Cantidad
System Center Endpoint Protection	1.000
Antivirus Microsoft defender for EndPonit	28000
Antivirus Microsoft defender for server	740
Consola de administración en nube	1

Las dos soluciones anteriores estarán bajo la administración del Contratista. Es posible que por licenciamiento se tenga que administrar los dos antivirus a nivel general.

Disponibilidad

Se debe garantizar que toda la plataforma tecnológica de servidores y parque computacional del ICBF se encuentre con antivirus instalado y actualizado.

Rendimiento

La plataforma de antivirus se encuentra actualmente instalada, configurada y en funcionamiento.

Funciones y Características

Las funciones y características son propias de los productos Microsoft Defender, sin embargo, el oferente deberá contar con preparación para brindar soporte, gestión y reportes a versiones superiores del antivirus como lo podrían ser (XDR) y System Center Endpoint Protection, el futuro contratista será notificado con anterioridad por el ICBF ante un posible cambio de licenciamiento y/o características del antivirus.

La cobertura de servicios de antivirus deberá estar asegurada al total del parque computacional del ICBF incluyendo (servidores / desktops / laptops) En caso de que ICBF cuente con equipos con sistema operativo fuera de soporte del fabricante (4 versiones anteriores a la versión vigente S.O), se deberán contemplar métodos alternativos para garantizar la protección de dichos equipos.

- La gestión, integración y monitoreo de antivirus endpoint (incluyendo todos sus módulos) deberá ser suministrado por el contratista del servicio de seguridad siguiendo los lineamientos y especificaciones del producto de antivirus que determine ICBF, en las versiones vigentes durante la vigencia del contrato. Optimizando su configuración con las mejoras prácticas que recomiende el fabricante del antivirus.
- Administrar Microsoft Defender XDR integrando las alertas provenientes de Defender for Endpoint, Defender for Identity y Defender for Office 365.
- Realizar la gestión (análisis/inclusión/edición/eliminación) de índices de compromiso (IOC) de manera automática en la herramienta de antivirus que provea la entidad durante la vigencia del contrato. En caso de no contar con la capacidad automatizada el futuro contratista deberá de manera manual hacer las actualizaciones de IOC conforme a los reportes IOC liberados, para realizar la gestión del servicio.
- Administrar Microsoft Defender for Endpoint para la protección, investigación y respuesta frente a amenazas en estaciones de trabajo y servidores.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Configurar, mantener, monitorear, gestionar, soportar y actualizar las plataformas de las soluciones de antivirus que el ICBF tenga a disposición.

- Garantizar el despliegue y actualización del Antivirus que se tenga en producción, e informar quincenalmente el estado general de actualización y amenazas detectadas por el mismo.
- Documentar y aplicar sobre el servicio de antivirus del ICBF las políticas y reglas de seguridad asociadas a la infraestructura tecnológica. Además, realizará la revisión, mantenimiento y actualización de políticas y de la plataforma de antivirus de común acuerdo y con la autorización del líder del servicio de seguridad informática del ICBF.
- Configurar las herramientas de monitoreo para medir la disponibilidad del servicio de antivirus del ICBF durante cada periodo de operación con el fin de que el ICBF pueda determinar la aplicación o no del ANS asociado.
- Configurar, administrar y monitorear todos los módulos del antivirus del ICBF: DLP, control de aplicaciones, firewall, entre otros, bajo las mejores prácticas del fabricante. Adicional, de todas las características recomendadas por el especialista para el correcto funcionamiento del servicio. Esto debe aplicar para todas las plataformas de antivirus con las que cuente la Entidad.
- Presentar informe mensual de cobertura de servicios de antivirus del ICBF el cual deberá al menos 99.8% del parque computacional del ICBF incluyendo (servidores / desktops / laptops). En caso de que ICBF cuente con (servidores / desktops / laptops) con sistema operativo fuera de soporte por el fabricante del sistema operativo (4 versiones anteriores a la versión vigente S.O) se deberán contemplar métodos alternativos para garantizar la protección de dichos equipos.
- Presentar informe mensual de gestión de (IOC) con temas relevantes a la IOC “conjunto de datos sobre un objeto o una actividad que indica acceso no autorizado al equipo o red.”
- Presentar un informe mensualmente o por demanda estos deberán ser entregados dentro de las 24 horas siguientes a la solicitud por parte de la Entidad, este informe deberá contener como mínimo los siguientes ítems y será entregado desde la gestión de antivirus con su respectivo análisis:
  - Top 10 de malware.
  - Top 10 de usuarios con malware.
  - Equipos actualizados por regional
  - Servidores actualizados.
  - Top 10 ataques.

REQUERIMIENTOS DEL SERVICIO

- Configurar, mantener, monitorear, gestionar, soportar y actualizar las plataformas de las soluciones de antivirus que el ICBF tenga a disposición.
- Garantizar el despliegue y actualización del Antivirus que se tenga en producción, e informar quincenalmente el estado general de actualización y amenazas detectadas por

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

el mismo.

- Documentar y aplicar sobre el servicio de antivirus del ICBF las políticas y reglas de seguridad asociadas a la infraestructura tecnológica. Además, realizará la revisión, mantenimiento y actualización de políticas y de la plataforma de antivirus de común acuerdo y con la autorización del líder del servicio de seguridad informática del ICBF.
- Configurar las herramientas de monitoreo para medir la disponibilidad del servicio de antivirus del ICBF durante cada periodo de operación con el fin de que el ICBF pueda determinar la aplicación o no del ANS asociado.
- Configurar, administrar y monitorear todos los módulos del antivirus del ICBF: DLP, control de aplicaciones, firewall, entre otros, bajo las mejores prácticas del fabricante. Adicional, de todas las características recomendadas por el especialista para el correcto funcionamiento del servicio. Esto debe aplicar para todas las plataformas de antivirus con las que cuente la Entidad.
- Presentar informe mensual de cobertura de servicios de antivirus del ICBF el cual deberá al menos 99.8% del parque computacional del ICBF incluyendo (servidores / desktops / laptops). En caso de que ICBF cuente con (servidores / desktops / laptops) con sistema operativo fuera de soporte por el fabricante del sistema operativo (4 versiones anteriores a la versión vigente S.O) se deberán contemplar métodos alternativos para garantizar la protección de dichos equipos.
- Presentar informe mensual de gestión de (IOC) con temas relevantes a la IOC “conjunto de datos sobre un objeto o una actividad que indica acceso no autorizado al equipo o red.”
- Presentar un informe mensualmente o por demanda estos deberán ser entregados dentro de las 24 horas siguientes a la solicitud por parte de la Entidad, este informe deberá contener como mínimo los siguientes ítems y será entregado desde la gestión de antivirus con su respectivo análisis:
    - Top 10 de malware.
    - Top 10 de usuarios con malware.
    - Equipos actualizados por regional
    - Servidores actualizados.
    - Top 10 ataques.

6.9.16.14 SERVICIO DE DETECCIÓN Y GESTIÓN DE VULNERABILIDADES.

El ICBF requiere herramientas tecnológicas para la detección y gestión de vulnerabilidades, a para los servidores y aplicaciones del ICBF y sobre plataformas suministradas por el Contratista.

REQUERIMIENTOS DEL SERVICIO

- El oferente deberá suministrar y operar una solución para realizar análisis de vulnerabilidades sobre las aplicaciones web protegidas, de tal forma que se identifiquen

vulnerabilidades existentes en los servidores y aplicaciones del ICBF y sobre plataformas suministradas por El Contratista. de forma ilimitada, sin requerir licenciamiento adicional durante toda la vigencia del servicio.

- El oferente deberá contar con un programa semestral para la ejecución de pruebas de vulnerabilidades ethical hacking en sus diferentes modalidades (caja blanca / caja gris /caja negra) pruebas ejecutadas de manera interna y externa previo acuerdo con el ICBF y acorde a la infraestructura y aplicativos de la entidad.
- El oferente deberá suministrar un dashboard intuitivo que permita el seguimiento y auditoria a los resultados obtenidos de los diferentes análisis planteados anteriormente.
- Los resultados y datos obtenidos en la detección de vulnerabilidades se deben almacenar en contenedores encriptados y controlados garantizando que los datos nunca salgan de la red interna del ICBF.
- Establecer un programa semestral de actividades a desarrollar con el fin de detectar vulnerabilidades de seguridad sobre toda la plataforma de seguridad informática, configuraciones erróneas o susceptibles de mejora y uso indebido de los recursos informáticos, y trazará planes de acción en conjunto con el ICBF para aplicar las correcciones necesarias, cual deberá ser aprobado por el ICBF.
- El oferente deberá entregar evidencia de instalación y operación de una herramienta tecnológica para realizar análisis de vulnerabilidades sobre las aplicaciones web protegidas, de tal forma que se identifiquen vulnerabilidades existentes en los servidores y aplicaciones del ICBF y sobre plataformas suministradas por el contratista de forma ilimitada, garantizando licenciamiento durante toda la vigencia del servicio.
- Establecer un programa semestral para la ejecución de pruebas de vulnerabilidades ethical hacking en sus diferentes modalidades (caja blanca/caja gris/caja negra) acorde a la infraestructura que incluya los aplicativos que la entidad defina. Presentando de manera mensual el seguimiento al programa, el avance y evidencias de ejecución de las labores planteadas.
- Realizar semestralmente un test de penetración (Pen Test) para servidores, dispositivos de red, bases de datos y aplicaciones según línea base definida por el ICBF. El alcance y la metodología del Pen Test deberá acordarse y ser aprobado por el ICBF previa a su ejecución. El Contratista debe presentar un plan de mitigación y realizar el seguimiento debidamente documentado del ciclo de vida de la vulnerabilidad (descubrimiento, tratamiento y mitigación).
- Realizar análisis de vulnerabilidades con la herramienta suministrada por el proveedor sobre los dispositivos que el ICBF defina. El Contratista debe presentar un plan de remediación y realizar el seguimiento debidamente documentado del ciclo de vida de la vulnerabilidad (descubrimiento, remediación y retest.) El seguimiento debe estar incluido dentro del informe de la gestión de seguridad informática junto con el plan de mitigación de reincidencia de las vulnerabilidades encontradas.
- Creación y actualización de un dashboard intuitivo que permita el seguimiento y auditoria a los resultados obtenidos de pruebas de vulnerabilidades y SERVICIO DE PROTECCION DE MARCA ICBF.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Suministrar, configurar gestionar y monitorear herramientas tecnológicas que permitan realizar labores de análisis y protección de marca ICBF. El servicio deberá estar disponible durante toda la vigencia del contrato.
- Configurar, mantener, monitorear, gestionar, soportar y actualizar la herramienta de análisis de vulnerabilidades que el ICBF o el futuro proveedor tengan a disposición.
- Realizar informe mensual con el estado y las acciones realizadas bajo el contexto del análisis y protección de marca ICBF

6.9.16.15 SERVICIO DE PROTECCION DE MARCA ICBF.

La Entidad requiere un servicio especializado de Protección de Marca y Protección de Riesgos Digitales (Digital Risk Protection – DRP) orientado a la identificación, monitoreo, análisis, alertamiento, mitigación y neutralización de amenazas dirigidas contra la marca, la identidad institucional, la reputación digital, los dominios, los activos expuestos y la presencia en línea del ICBF, en Internet, redes sociales, tiendas de aplicaciones, Deep Web y Dark Web.

El servicio deberá incorporar de forma nativa capacidades avanzadas de Inteligencia Artificial (IA), Machine Learning (ML), analítica de comportamiento, correlación con inteligencia de amenazas y automatización, orientadas a fortalecer la detección temprana de amenazas, la reducción de falsos positivos y la respuesta rápida frente a incidentes de exposición digital.

Este servicio se enmarca en la estrategia de ciberseguridad Zero Trust del ICBF y se alinea con los lineamientos del MSPI de MinTIC, la norma ISO/IEC 27001:2022, el NIST Cybersecurity Framework 2.0 y el framework MITRE ATT&CK.

Alcance del servicio
El oferente deberá suministrar, configurar, gestionar, operar y monitorear herramientas tecnológicas especializadas que permitan realizar labores de análisis, monitoreo y protección de la marca ICBF en:

- Internet y sitios web.
- Motores de búsqueda.
- Redes sociales oficiales y no oficiales.
- Perfiles falsos y cuentas fraudulentas.
- Tiendas de aplicaciones móviles (oficiales y no oficiales).
- Dominios y subdominios.
- Certificados digitales.
- Deep Web.
- Dark Web.
- Foros, mercados ilegales y canales de mensajería (cuando aplique).
- Repositorios de código y filtraciones de datos.
- Servicios expuestos e infraestructura asociada a la Entidad.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Alcance mínimo requerido

- Protección mínima de 250 dominios.
- Protección mínima de 500 activos críticos de la Entidad.
- Ejecución mínima de 200 take downs anuales.
- Monitoreo continuo 7x24x365.
- Capacidad de escalamiento dinámico de dominios, activos y take downs según necesidad de la Entidad.

Capacidades funcionales mínimas

La solución deberá permitir como mínimo:

- Monitoreo continuo de la exposición digital de la marca ICBF.
- Detección de suplantación de identidad institucional.
- Detección de dominios fraudulentos y typosquatting.
- Detección de sitios de phishing que suplanten al ICBF.
- Detección de perfiles y cuentas falsas en redes sociales.
- Detección de aplicaciones móviles fraudulentas.
- Detección de campañas de desinformación y fraude.
- Detección de filtraciones de información institucional.
- Detección de credenciales expuestas.
- Detección de menciones maliciosas en Deep y Dark Web.
- Detección de infraestructura maliciosa asociada a la Entidad.
- Gestión y ejecución de take downs (retiro de contenido malicioso).
- Alertamiento temprano de amenazas emergentes.
- Priorización de amenazas según riesgo e impacto reputacional.

Capacidades transversales de Inteligencia Artificial y Machine Learning

La solución deberá incorporar de forma nativa capacidades de IA/ML orientadas a fortalecer la detección y respuesta, incluyendo como mínimo:

- Análisis automatizado de grandes volúmenes de información en Internet, redes sociales y Deep/Dark Web.
- Detección de patrones de suplantación y fraude mediante Machine Learning.
- Análisis de contenido, imágenes, logos y texto mediante IA (reconocimiento de marca).
- Detección de campañas coordinadas de desinformación.
- Detección de amenazas generadas mediante IA generativa (deepfakes, contenido sintético, campañas automatizadas).
- Priorización inteligente de amenazas según riesgo e impacto.
- Reducción de falsos positivos mediante aprendizaje continuo (Auto-Learning).
- Correlación automática con inteligencia de amenazas global.
- Análisis predictivo de amenazas emergentes contra la marca.
- Generación de indicadores de compromiso (IoC) e indicadores de ataque (IoA).
- Mapeo de amenazas al framework MITRE ATT&CK cuando aplique.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Integración con el ecosistema de seguridad
El servicio deberá integrarse de forma nativa o interoperable con:

- SOC / SIEM / SOAR.
- XDR.
- Threat Intelligence.
- NGFW / WAF / SEG.
- ITSM.
- Servicios de correo seguro (para correlación de phishing).

Mediante mecanismos estándar tales como APIs REST/JSON, STIX/TAXII, Syslog y protocolos soportados por la plataforma, permitiendo el enriquecimiento de eventos y la contención coordinada de amenazas.

Alineación con la estrategia Zero Trust
El servicio de protección de marca deberá contribuir a la estrategia Zero Trust del ICBF mediante:

- Monitoreo continuo de la exposición y riesgo digital.
- Validación permanente de la identidad y presencia digital institucional.
- Detección temprana de amenazas externas.
- Reducción de la superficie de ataque externa.
- Correlación de amenazas externas con eventos internos de seguridad.
- Respuesta rápida y coordinada frente a incidentes reputacionales.

Operación, mantenimiento y mejora continua

- Administración integral, monitoreo proactivo y soporte especializado durante la vigencia del contrato.
- Actualización continua de fuentes de inteligencia, motores de IA/ML y capacidades de detección.
- Afinamiento permanente para reducir falsos positivos.
- Validación periódica de la efectividad del servicio.
- Mejora continua de la postura de protección de marca.

REQUERIMIENTOS DEL SERVICIO

- El oferente deberá suministrar, configurar, gestionar y monitorear herramientas tecnológicas que permitan realizar labores de análisis y protección de marca ICBF en internet, redes sociales y Deep web, buscando proteger como mínimo 250 dominios y 500 activos críticos de la entidad esperando como mínimo 2000 take downs anuales.
- El oferente deberá entregar informe mensual de las acciones realizadas bajo el contexto del análisis y protección de marca ICBF.
- Ofrecer asesoramiento y capacitación a los equipos internos de la entidad, sobre buenas prácticas y estrategias para proteger y mantener una sólida reputación en línea de la marca ICBF.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Desarrollar estrategias de mitigación y respuesta rápida ante situaciones críticas o potenciales problemas de reputación que puedan afectar negativamente la marca ICBF.

6.9.17 SISTEMA DE CORRIENTE REGULADA

6.9.17.1 GENERALIDADES DEL SERVICIO

El Instituto Colombiano de Bienestar Familiar -ICBF- requiere para el normal funcionamiento, Desarrollo de su misionalidad la adquisición, instalación, configuración, puesta en funcionamiento, mantenimiento preventivo, correctivo y traslados de equipos especiales de suplencia energética (UPS) para las sedes regionales y centros zonales de la entidad. Estos dispositivos son elementos que regulan y controlan las fluctuaciones eléctricas de la red externa, además de suministrar energía eléctrica regulada por un tiempo limitado y durante una falla en el fluido eléctrico a todos los equipos de red y parque computacional.

6.9.17.2 CONSIDERACIONES A TENER EN CUENTA EN EL SUMINISTRO DE PARTES O SERVICIOS DE LAS UPS

- Si del resultado de los diagnósticos y mantenimientos preventivos realizados, se identifica la necesidad de realizar la entrega, instalación, configuración, pruebas y puesta en funcionamiento de las UPS requeridas para garantizar la continuidad y adecuada operación de la infraestructura tecnológica del ICBF, las mismas o estas serán adquiridas con cargo a la Bolsa de Servicios, previa autorización del supervisor del contrato. La adquisición estará sujeta al cumplimiento a lo establecido en el capítulo 6.9.18. del presente documento.
- El contratista deberá contemplar dentro de su cotización los valores asociados a la adquisición e instalación de los repuestos todos los costos directos e indirectos necesarios para garantizar su correcta implementación y puesta en operación, incluyendo, entre otros, el transporte hasta la sede correspondiente, cargue, descargue, desplazamiento y disponibilidad del personal técnico especializado, herramientas, equipos, materiales, elementos de instalación, configuración, pruebas, adecuaciones menores que resulten necesarias y demás recursos requeridos para asegurar el adecuado funcionamiento de las UPS.
- En consecuencia, la entrega, instalación, configuración y puesta en funcionamiento de las UPS deberá realizarse de manera integral, garantizando que los equipos queden correctamente instalados, configurados, probados y operativos en cada una de las sedes donde sean requeridos, sin que el ICBF deba asumir costos adicionales diferentes a los previamente autorizados y establecidos dentro de la Bolsa de Servicios.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- El contratista será responsable de coordinar y ejecutar todas las actividades logísticas, técnicas y operativas asociadas a la instalación y puesta en servicio de los equipos, hasta lograr su completa operatividad y entrega a satisfacción del supervisor del contrato.
- El servicio de mantenimiento preventivo de las UPS propiedad del ICBF: El contratista deberá realizar mantenimiento preventivo en sitio a las UPS de la entidad que no se encuentran cubiertas por garantía y de las UPS que la entidad requiera, por demanda, en las diferentes sedes del ICBF, previa autorización del supervisor del contrato. Las UPS de la Entidad se relacionan, en el **Anexo 09 – UPS Nuevas y Mantenimientos.**

6.9.17.3 MANTENIMIENTO PREVENTIVO SEMESTRAL DE SISTEMAS UPS

Con el propósito de garantizar la continuidad operativa de los servicios tecnológicos y la protección de los equipos de infraestructura crítica, se ejecutarán dos jornadas de mantenimiento preventivo a los sistemas de Alimentación Ininterrumpida (UPS) anual.

Las actividades para realizar estarán orientadas a verificar el correcto funcionamiento de los equipos, identificar posibles riesgos de falla y asegurar el cumplimiento de las condiciones técnicas requeridas para la operación de las UPS instaladas en las diferentes sedes.

Primer mantenimiento semestral

Durante la primera jornada de mantenimiento se llevarán a cabo las siguientes actividades:

Inspección visual del estado general de las UPS y sus componentes.

- Verificación de conexiones eléctricas, terminales, cableado y sistemas de protección.
- Limpieza interna y externa de los equipos para eliminar acumulación de polvo y agentes contaminantes.
- Revisión de baterías, validando voltajes, estado físico, temperatura y vida útil estimada.
- Verificación de parámetros de operación como voltaje de entrada, voltaje de salida, frecuencia, carga y autonomía.
- Comprobación del correcto funcionamiento de alarmas, indicadores y sistemas de monitoreo.
- Identificación y registro de novedades encontradas durante la intervención.
- Elaboración de informes técnicos con las recomendaciones correspondientes.

Segundo mantenimiento semestral

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

En la segunda jornada de mantenimiento preventivo se efectuarán las siguientes labores:

- Seguimiento a las observaciones y recomendaciones generadas en el primer mantenimiento.
- Revisión integral de los módulos de potencia y sistemas de respaldo.
- Verificación del desempeño de las baterías mediante pruebas operativas.
- Evaluación de la capacidad de respaldo y autonomía del sistema.
- Comprobación del adecuado funcionamiento del bypass manual y automático.
- Ajuste y reapriete de conexiones eléctricas cuando fue requerido.
- Actualización del registro de inventario y control de activos asociados a las UPS.
- Emisión de conceptos técnicos sobre el estado de los equipos y necesidades futuras de mantenimiento o reemplazo.

6.9.17.4 SERVICIO DE MANTENIMIENTO CORRECTIVO DE LAS UPS PROPIEDAD DEL ICBF:

El contratista deberá realizar el mantenimiento correctivo en sitio de las UPS de propiedad del ICBF, cuando como resultado de las actividades de diagnóstico y mantenimiento preventivo se identifique la necesidad de intervenir, reparar, sustituir o reemplazar componentes, partes, baterías u otros elementos necesarios para garantizar su adecuado funcionamiento y condiciones de operación.

Como resultado de los mantenimientos preventivos y de los diagnósticos técnicos efectuados, el contratista deberá identificar, documentar y reportar oportunamente los repuestos, partes, baterías requeridas para atender las actividades de mantenimiento correctivo. Estos elementos serán adquiridos, cuando corresponda, a través de la Bolsa de Servicios, previa justificación técnica de la necesidad, validación y autorización del supervisor del contrato, de conformidad con las condiciones establecidas para la utilización de dicha Bolsa.

El contratista deberá disponer del personal técnico, herramientas, equipos y demás recursos necesarios para ejecutar los mantenimientos correctivos en sitio y deberá realizar las actividades requeridas hasta lograr que las UPS intervenidas queden operativas, funcionales y en condiciones adecuadas de servicio, siempre que la intervención corresponda a una necesidad técnicamente identificada y autorizada.

Cuando durante el mantenimiento preventivo se identifique una condición que pueda afectar el funcionamiento, confiabilidad o continuidad operativa de una UPS, el contratista deberá presentar al supervisor del contrato el correspondiente diagnóstico técnico, indicando como mínimo la identificación del equipo, condición encontrada, causa probable, componentes requeridos, cantidades, actividades correctivas propuestas y justificación técnica. Una vez validada y autorizada la necesidad, se procederá con la adquisición de los elementos que correspondan y con la ejecución del mantenimiento correctivo.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

6.9.17.5 GARANTÍA Y SOPORTE TÉCNICO

Todos los componentes que se oferten deben contar con soporte y garantía, para lo cual la entidad requiere que se coticen las siguientes opciones:

Opción	Descripción	Característica Técnica Mínima
COMPONENTES ELECTRONICOS		
1	Renovación Garantía y Soporte por 24 meses	Garantía y Soporte por 24 meses de Fabrica para todo el hardware, software y componentes de la solución.
BATERIAS		
1	Renovación Garantía y Soporte por 12 meses	Garantía y Soporte por 12 meses de Fabrica para todo el hardware, software y componentes de la solución.

6.9.17.6 ITEMS NO PREVISTOS

Para los ítems no previstos en el ***Anexo 09 – UPS Nuevas y Mantenimientos***, o adicionales que se presenten durante la ejecución, el contratista deberá realizar las especificaciones técnicas de cada uno de dichos ítems, así como sus respectivos análisis de precios unitarios (APU) los cuales deberán ser aprobados por la supervisión del contrato previo a la ejecución de la actividad. Por lo anterior, y para la aprobación e inclusión de ítems y/o actividades no previstas requeridos durante la ejecución del contrato, se deberá seguir el procedimiento establecido a continuación:

Para definir el precio de las actividades o Ítems que no se encuentren relacionados en la ficha de condiciones técnicas, se deberá realizar el siguiente procedimiento:

1. El contratista deberá entregar a la supervisión del contrato la justificación de la necesidad de ejecutar dicha actividad, la especificación técnica, el Análisis de Precio Unitario (APU) con su valor propuesto, soportado en dos (2) cotizaciones de diferentes proveedores presentadas por el contratista.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

2. El Supervisor del contrato solicitará mínimo dos (2) cotizaciones de proveedores que estén legalmente constituidos por medio de correo electrónico, las cuales se podrán comparar con la cotización solicitada al contratista, con el fin de realizar un estudio comparativo.
3. El valor de la actividad o ítem no previsto se fijará por el menor valor de las cotizaciones.
4. Si el valor de la cotización se encuentra acorde al mercado, el supervisor del contrato procederá a aprobar el valor de la Actividad No Prevista, mediante la suscripción de un Acta de Fijación de Ítems o Actividades No Previstos, la cual será suscrita por el Contratista y entregada al supervisor del contrato para su aprobación.

En ningún caso los Ítems no Previstos podrán ser ejecutados sin la suscripción del Acta de Fijación de Precios no Previstos, y en caso de ser necesario, sin la respectiva adición al contrato.

Para la ejecución de las actividades no previstas del contrato, se establecerá una bolsa de servicios y repuestos por demanda. Estas actividades se pagarán de la forma establecida en el numeral 10. FORMA DE PAGO DEL VALOR DEL CONTRATO.

El contratista debe brindar el soporte técnico y garantía del hardware y software, para todos los casos el soporte y garantía debe prestarse en ventanas de 7x24 (7 días a la semana de lunes a domingo, 24 horas al día) que debe contemplar las siguientes características:

Soporte técnico telefónico y/o vía correo electrónico en un esquema 7x24 (7 días a la semana de lunes a domingo, 24 horas al día). El tiempo de atención a la solicitud de soporte no debe superar un máximo de 3 horas.

6.9.18 BOLSA DE SERVICIOS, CONSUMIBLES PARA MANTENIMIENTOS CORRECTIVOS Y REPUESTOS, PARTES Y ACCESORIOS

En el marco de la presente contratación, se establece la creación de una Bolsa de Servicios, Consumibles, Repuestos, Partes y Accesorios. Esta bolsa estará destinada exclusivamente a atender requerimientos que surjan durante la ejecución contractual y que, de manera objetiva, no correspondan al alcance, obligaciones, riesgos ni costos definidos en el objeto, las obligaciones contractuales, las especificaciones técnicas, los niveles de servicio, los acuerdos de nivel de servicio (ANS), la matriz de riesgos y la oferta económica presentada, los cuales deben ser asumidos integralmente por el contratista.

Dichos requerimientos, no previsibles al momento de la estructuración del proceso contractual, deberán ser debidamente justificados técnica y económicamente por el ICBF, y su atención será indispensable para garantizar la continuidad, disponibilidad, estabilidad y seguridad de la infraestructura tecnológica y de los servicios institucionales.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

En consecuencia, la existencia de esta Bolsa no limita, sustituye, complementa ni modifica la responsabilidad integral del contratista respecto de la gestión, operación, administración, monitoreo, soporte, mantenimiento, suministro, instalación, configuración, puesta en funcionamiento, reposición y demás actividades requeridas para garantizar la continuidad, disponibilidad, estabilidad, seguridad y adecuada prestación de los servicios TIC que hacen parte del objeto contractual.

La Bolsa de Servicios, Consumibles, Repuestos, Partes y Accesorios constituye un mecanismo de apoyo operativo destinado exclusivamente a atender necesidades excepcionales, sobrevinientes y no previsibles durante la ejecución contractual, cuya atención resulte indispensable para garantizar la continuidad de los servicios institucionales y la adecuada operación de los activos tecnológicos de propiedad o bajo responsabilidad del ICBF.

Su utilización no constituye una ampliación del objeto contractual, una modificación del alcance de los servicios contratados, ni un mecanismo para reconocer actividades que correspondan a las obligaciones ordinarias del contratista. En consecuencia, no podrá ser empleada para financiar actividades de operación, soporte, mantenimiento preventivo o correctivo, reposición de componentes, actualización tecnológica, garantías o cualquier otra obligación asociada a la infraestructura, plataformas, software, herramientas, equipos o servicios que sean suministrados, administrados o de responsabilidad del contratista, cuyos costos deberán estar incorporados en la propuesta económica presentada.

La bolsa tendrá como destino exclusivo la adquisición de consumibles, repuestos, partes, accesorios o servicios técnicos especializados asociados a activos de propiedad o bajo administración del ICBF, cuya necesidad sea debidamente justificada, no haya sido razonablemente previsible durante la etapa de planeación y no se encuentre cubierta dentro de las obligaciones contractuales ordinarias.

Su ejecución estará sujeta a la previa cuantificación de la necesidad, la respectiva justificación técnica, la validación presupuestal y la autorización expresa del supervisor del contrato, garantizando en todo momento la trazabilidad, razonabilidad y control de los recursos, así como la observancia de los principios de planeación, eficiencia y responsabilidad contractual.

La Bolsa de Servicios, Consumibles, Repuestos, Partes y Accesorios no podrá utilizarse para financiar, complementar o reconocer actividades, bienes, componentes, servicios o recursos que deban ser suministrados, administrados, soportados, mantenidos o reemplazados por el contratista en cumplimiento de las obligaciones derivadas del contrato y de su oferta económica. Su aplicación se limitará a requerimientos excepcionales, sobrevinientes y debidamente justificados por la Entidad, garantizando que no exista

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

duplicidad de pagos ni traslape de responsabilidades entre las obligaciones contractuales del contratista y los conceptos susceptibles de atención mediante la Bolsa.

La Bolsa tendrá como finalidad exclusiva atender necesidades adicionales, extraordinarias y sobrevinientes de la Entidad, relacionadas con bienes, partes, accesorios, consumibles o servicios técnicos especializados requeridos para activos de propiedad o bajo responsabilidad del ICBF, siempre que se determine de manera previa, expresa y verificable que dichos requerimientos:

- No hacen parte del alcance ni de las obligaciones ordinarias asignadas al contratista.
- No corresponden a actividades, bienes, componentes, repuestos, consumibles o servicios que deban estar incluidos en la propuesta económica del contratista.
- No se originan en incumplimientos, deficiencias, omisiones, errores de dimensionamiento, fallas de gestión o riesgos que correspondan al contratista.
- No corresponden a actividades de operación, administración, monitoreo, soporte, mantenimiento preventivo o correctivo, instalación, configuración, puesta en funcionamiento o reposición que sean responsabilidad del contratista.
- Se relacionan con una necesidad que se presenta durante la ejecución contractual y cuya ocurrencia o magnitud no podía ser razonablemente determinada en la etapa de planeación.
- Resultan necesarias para atender una situación que pueda afectar o comprometer la continuidad, disponibilidad, seguridad, estabilidad o adecuada operación de los servicios tecnológicos institucionales.
- Cuentan con la correspondiente justificación técnica, económica y presupuestal por parte de la Entidad y con la autorización previa de la supervisión contractual.

DELIMITACIÓN DE LAS OBLIGACIONES DEL CONTRATISTA FRENTE A LA BOLSA

La Bolsa no constituye una fuente alternativa de financiación de las obligaciones del contratista. En tal sentido, el contratista deberá efectuar, durante la ejecución contractual, la gestión y provisión de todos los recursos necesarios para cumplir integralmente con el objeto contratado, sin que pueda condicionarse la prestación de los servicios a la disponibilidad o autorización de recursos de la Bolsa.

Para efectos de establecer si un requerimiento puede ser atendido mediante la Bolsa, la Entidad realizará previamente un análisis de delimitación de responsabilidades, mediante el cual se verificará que el bien, repuesto, parte, accesorio, consumible o servicio solicitado no se encuentre incluido, directa o indirectamente, dentro de las obligaciones contractuales, los ANS, las especificaciones técnicas, la matriz de riesgos o la oferta económica del contratista.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Cuando exista duda respecto de la responsabilidad de asumir un determinado costo o requerimiento, prevalecerá la obligación contractual del contratista, siempre que del análisis técnico, contractual y económico se determine que el elemento o actividad resulta necesario para el cumplimiento de una obligación que le fue asignada. En ningún caso la Bolsa podrá utilizarse para generar un reconocimiento económico adicional por obligaciones que ya fueron consideradas dentro del precio ofertado.

De igual manera, la utilización de la Bolsa no podrá generar duplicidad de pagos, doble reconocimiento de costos, traslape de responsabilidades o desagregación artificial de obligaciones que, por su naturaleza, deben ser atendidas integralmente por el contratista.

NATURALEZA DE LAS NECESIDADES SUSCEPTIBLES DE ATENCIÓN MEDIANTE LA BOLSA

Se entenderá que existe una necesidad susceptible de ser atendida con cargo a la Bolsa únicamente cuando concurran, como mínimo, las siguientes condiciones:

- Que corresponda a un requerimiento extraordinario, adicional y sobreviniente respecto del alcance ordinario de la contratación.
- Que su necesidad no haya podido ser razonablemente identificada, cuantificada o incorporada en la estructuración de la oferta económica del contratista.
- Que no corresponda a un riesgo asignado al contratista ni a una obligación que este deba asumir integralmente.
- Que no tenga origen en una falla, omisión, deficiencia, desgaste, obsolescencia, inadecuada gestión, insuficiencia de capacidad o deficiente planeación atribuible al contratista.
- Que se encuentre relacionada con activos, componentes, plataformas o servicios cuya responsabilidad corresponda al ICBF y que no hayan sido incorporados al alcance de suministro, administración, operación o mantenimiento del contratista.
- Que su atención sea necesaria para mitigar un riesgo técnico u operativo o evitar una afectación sobre la continuidad, disponibilidad, seguridad o estabilidad de los servicios TIC institucionales.
- Que exista una justificación técnica y económica suficiente que permita establecer la necesidad y la imposibilidad de atenderla mediante las obligaciones ordinarias del contrato.

PROCEDIMIENTO PARA LA UTILIZACIÓN DE LA BOLSA

La utilización de los recursos de la Bolsa requerirá, de manera previa a la adquisición o prestación del bien o servicio, el cumplimiento de las siguientes etapas:

1. Identificación y solicitud del requerimiento, con la descripción detallada de la necesidad, alcance, cantidades, características técnicas, justificación y soportes correspondientes.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

2. Análisis de responsabilidad contractual, mediante el cual la Entidad verificará que el requerimiento no corresponda a una obligación, riesgo o costo que deba ser asumido por el contratista.
3. Concepto técnico del área competente y de la supervisión, en el que se sustente la naturaleza extraordinaria, adicional y sobreviniente de la necesidad.
4. Validación económica y presupuestal, que permita establecer la razonabilidad del valor solicitado frente a las condiciones y precios de mercado.
5. Autorización expresa y previa del ICBF, antes de la adquisición, suministro, instalación o prestación del servicio con cargo a la Bolsa.
6. Ejecución y recepción, de conformidad con las condiciones técnicas y económicas previamente autorizadas.
7. Verificación y trazabilidad, mediante los soportes correspondientes que permitan identificar el requerimiento, su justificación, autorización, ejecución, valor y recibo a satisfacción.

Para el manejo de esta bolsa, el ICBF a través del supervisor, realizará solicitud de tres (3) cotizaciones, preliminares (incluida la del contratista) para su comparación. El valor de la actividad o ítem no previsto se fijará por el menor valor de las cotizaciones. Una vez recibida la facturación, se registrará el valor de la misma, descontándolo del saldo de la bolsa, y así sucesivamente hasta agotar el valor del presupuesto reservado para la correspondiente vigencia para este fin; si los recursos de la bolsa no son consumidos en su totalidad estos serán reembolsados al Tesoro Nacional.

La autorización de un requerimiento con cargo a la Bolsa no implicará, por sí misma, una modificación del objeto contractual ni una ampliación de las obligaciones ordinarias del contratista, y se limitará exclusivamente al bien, repuesto, accesorio, consumible o servicio específicamente autorizado, dentro de las condiciones y valores previamente aprobados.

EXCLUSIONES EXPRESAS

En ningún caso podrán ser atendidos con cargo a la Bolsa los costos asociados a:

- La operación ordinaria de los servicios TIC.
- La administración y gestión de la infraestructura bajo responsabilidad del contratista.
- El monitoreo y soporte de los servicios contratados.
- Los mantenimientos preventivos que correspondan al contratista.
- La atención de incidentes y requerimientos incluidos en los ANS.
- La reposición de equipos, partes o componentes cuya provisión o reemplazo corresponda al contratista.
- Los consumibles requeridos para la prestación ordinaria de los servicios a cargo del contratista.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Las herramientas, equipos o recursos necesarios para que el contratista cumpla sus obligaciones.
- Las actividades derivadas de fallas o deficiencias imputables al contratista.
- Los costos derivados de errores de dimensionamiento o estimación efectuados por el contratista al estructurar su oferta.
- Los costos asociados a riesgos que hayan sido asignados contractualmente al contratista.
- Las actualizaciones, renovaciones, ampliaciones o sustituciones que correspondan a obligaciones expresamente previstas dentro del alcance contractual.
- Cualquier actividad o suministro que haya sido considerado, explícita o implícitamente, en la estructuración de la propuesta económica presentada por el contratista.

El valor de cada requerimiento que se pretenda atender con cargo a la Bolsa estará sujeto a viabilidad técnica y financiera previa por parte del ICBF, incluyendo la verificación de los precios de referencia del mercado, la pertinencia de las cantidades requeridas y la razonabilidad económica de la adquisición.

El contratista no podrá adquirir, suministrar o ejecutar bienes o servicios con cargo a la Bolsa sin contar previamente con la autorización expresa correspondiente. La ejecución sin dicha autorización será responsabilidad exclusiva del contratista y no generará obligación de reconocimiento o pago por parte del ICBF.

La supervisión contractual realizará el seguimiento permanente a la ejecución de la Bolsa, verificando que cada utilización corresponda estrictamente a su finalidad, que exista trazabilidad documental y financiera y que no se produzcan duplicidades, traslapes o reconocimientos de obligaciones que correspondan al contratista.

En consecuencia, la Bolsa se constituye como un mecanismo excepcional para atender necesidades extraordinarias del ICBF que se encuentren fuera del alcance y responsabilidad económica y operativa del contratista, y en ningún caso podrá entenderse como una provisión destinada a cubrir costos inciertos de la operación global delegada, trasladar riesgos contractualmente asignados al contratista o complementar una oferta económica insuficiente.

6.9.18.1 CONSIDERACIONES A TENER EN CUENTA EN EL SUMINISTRO DE LA BOLSA DE SERVICIOS, CONSUMIBLES PARA MANTENIMIENTOS CORRECTIVOS Y REPUESTOS:

- Todas las partes y elementos suministrados en el marco del contrato a celebrar deberán ser nuevos.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- El contratista deberá entregar la documentación que certifique la garantía y soportes para cada elemento o parte que suministre, así mismo el protocolo para brindar dicho soporte.
- El contratista deberá garantizar la prestación del servicio de soporte técnico de garantía de los repuestos, partes, dispositivos, herramientas y/o elementos tecnológicos que suministre. En los casos en que la garantía brindada por el fabricante sea superior a la garantía mínima definida en el contrato, prima la garantía del fabricante.
- Garantía de repuestos o partes importadas: la garantía de bienes importados será responsabilidad entre el productor e importador. El proveedor será solidariamente responsable por la aplicación de la garantía a los bienes, repuestos o partes importados y suministrados en el marco del contrato de bolsa tecnológica.
- Se define como servicio técnico de garantía, el servicio prestado por el contratista para reemplazar partes, piezas, equipos por defectos de fabricación de los mismos, durante el período de garantía otorgado a cada parte, contado a partir de la fecha de su entrega y recibido a satisfacción por parte del ICBF.
- La prestación del servicio de la garantía será sin ningún costo adicional del valor del contrato, por lo tanto, el ICBF no asumirá costo alguno por la asistencia de la garantía.
- Reemplazo y corrección de cualquier componente que presente defecto imputable a fallas en su proceso de fabricación o que no cumpla con las especificaciones ofrecidas originalmente, lo cual incluirá mano de obra y repuestos, con el fin de garantizar el correcto funcionamiento de los equipos durante el periodo de garantía. En el evento en que un equipo o uno de los componentes fallen más de tres (3) veces durante el periodo de garantía, el contratista deberá reemplazar el repuesto por uno nuevo de igual o superiores características al ofertado, siempre y cuando el daño persistente no obedezca a causas diferentes a las cubiertas por la garantía.
- La atención deberá prestarse dentro del día hábil siguiente a la fecha en que el ICBF lo solicite, en caso de reemplazo del elemento o parte, ésta se realizará dentro de los tres (3) días hábiles siguientes al reporte efectuado al proveedor. La garantía debe ser otorgada por el fabricante.
- El contratista deberá entregar un reporte por cada caso atendido, en el evento de ser aplicada la garantía.
- El contratista deberá entregar un reporte mensual hasta la terminación del contrato de los elementos que fueron reportados por garantía, como mínimo el reporte debe contener: Clasificación, nombre del elemento o parte, serial y tipo de daño.
- En el evento en que el ICBF realice la devolución en igual o más de dos (2) oportunidades de algún elemento o parte adquirida a través del presente contrato y que la calidad del mismo compromete la integridad de los servicios TI o del equipo sobre el cual se esté utilizando la parte, el ICBF a través del supervisor del contrato podrá exigir el reemplazo de la parte por una marca diferente a la ofertada por el Contratista que cumpla con las especificaciones mínimas técnicas exigidas por la

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

entidad. Los valores unitarios ofertados por el proponente, no podrá comprometer la garantía y calidad de los bienes suministrados y solicitados por el ICBF.

Nota: Teniendo en cuenta la naturaleza de la presente contratación y el alcance de los servicios requeridos, no resulta técnica ni financieramente posible determinar de manera anticipada y con precisión los bienes, repuestos, partes, accesorios, consumibles o servicios que podrán requerirse durante la ejecución del contrato, así como las cantidades, características, marcas, referencias, condiciones de instalación, sedes de destino o frecuencia con la que eventualmente deberán ser atendidos. Lo anterior obedece a que las necesidades de mantenimiento correctivo y atención de requerimientos por demanda estarán determinadas por las condiciones reales que presente la infraestructura tecnológica durante la ejecución contractual, las cuales dependerán, entre otros factores, del estado y comportamiento de los equipos, resultados de los mantenimientos preventivos, diagnósticos técnicos, fallas sobrevinientes, necesidades de continuidad operativa y condiciones particulares de los activos ubicados en las diferentes sedes del ICBF a nivel nacional.

6.9.18.2 SUMINISTRO DE PARTES, REPUESTOS, DISPOSITIVOS Y/O ELEMENTOS:

ÍTEM	REQUERIMIENTO	TIEMPO MÁXIMO DE SOLUCIÓN DESPUÉS DE REPORTADO EL CASO
1	Cada requerimiento del ICBF deberá ser estudiado técnicamente por el contratista y presentar en un plazo no mayor a cinco (5) días hábiles la oferta que dé solución al requerimiento.	5 días hábiles
2	Una vez el ICBF haya estudiado la oferta y a partir de su aprobación, el contratista tendrá ocho (8) días hábiles para la entrega del servicio por demanda requerido.	8 días hábiles
3	Suministro de partes, repuestos y componentes tecnológicos, que el ICBF identifique como necesarios para operar.	4 días hábiles
4	Solución a las solicitudes de aplicación de garantía de las repuestos, partes y componentes tecnológicos y de soporte técnico que sea necesario adelantar para hacerla efectiva, una vez comunicada al contratista.	5 días hábiles

Nota 1: Las horas hábiles serán en el horario de 8:00 a.m a 5:00 p.m de lunes a viernes, no incluye festivos. Los tiempos empezarán a contar a partir de la aprobación por escrito por parte del ICBF previa presentación de oferta por parte del contratista.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Nota 2: Si una parte o repuesto requiere ser importada, el contratista deberá aportar al supervisor el soporte que evidencie que la parte fue adquirida, mediante factura u orden de compra debidamente radicada en el proveedor, donde se evidencie el tiempo de entrega.

GLOSARIO TÉCNICO

Administración: Conjunto de actividades técnicas, operativas y de control mediante las cuales se organizan, configuran, mantienen y gobiernan los recursos tecnológicos del ICBF, incluyendo infraestructura, plataformas, aplicaciones, datos y licenciamiento, garantizando su adecuada utilización conforme a los lineamientos institucionales y contractuales.

Gestión: Proceso integral y sistemático orientado a planificar, dirigir, coordinar, supervisar y mejorar continuamente los servicios TIC del ICBF, mediante el uso de métricas, indicadores, procesos, controles y acciones de mejora, asegurando su alineación con los objetivos misionales de la Entidad.

Operación: Ejecución permanente y continua de las actividades necesarias para garantizar el funcionamiento estable, eficiente y seguro de los servicios TIC del ICBF, incluyendo la atención de incidentes, requerimientos, tareas programadas y no programadas, bajo esquemas de disponibilidad acordados.

Monitoreo: Proceso continuo de observación, medición y seguimiento del estado, desempeño, disponibilidad, capacidad y seguridad de la infraestructura tecnológica, plataformas, aplicaciones y servicios TIC del ICBF, mediante herramientas que permiten la detección temprana de fallas y generación de alertas.

Control: Conjunto de mecanismos, procedimientos y actividades de verificación orientadas a asegurar que la administración, gestión y operación de los servicios TIC se ejecuten conforme a los lineamientos contractuales, normativos y técnicos definidos por el ICBF.

Mesa de Servicio: Función organizacional que actúa como Punto Único de Contacto (SPOC) entre los usuarios y los servicios TIC del ICBF, encargada de recibir, registrar, clasificar, escalar y dar seguimiento a incidentes, requerimientos y solicitudes hasta su cierre.

Acuerdos de Niveles de Servicio (ANS): Compromisos formales que establecen los niveles mínimos de calidad, disponibilidad, tiempos de atención y solución de los servicios TIC, cuya medición y cumplimiento permiten evaluar el desempeño del contratista.

Incidente: Interrupción no planificada, reducción en la calidad o indisponibilidad de un servicio TIC del ICBF, que requiere atención para restablecer la operación normal en el menor tiempo posible.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Requerimiento: Solicitud de un usuario relacionada con información, acceso, provisión, modificación o soporte de un servicio TIC, que no implica una interrupción del servicio.

Cambio: Adición, modificación o eliminación autorizada que puede afectar directa o indirectamente los servicios TIC del ICBF, su infraestructura, configuración o componentes asociados.

NOC (Network Operations Center): Centro especializado encargado del monitoreo continuo de la infraestructura de red y comunicaciones, con el fin de detectar, analizar y atender eventos operativos que puedan afectar la disponibilidad y desempeño de los servicios.

SOC (Security Operations Center): Centro especializado encargado de la supervisión, detección, análisis y respuesta a incidentes de seguridad de la información y ciberseguridad, asegurando la protección de los activos de información del ICBF.

CMDB: Repositorio centralizado que almacena información actualizada y controlada sobre los Ítems de Configuración (CI) que soportan los servicios TIC, permitiendo su trazabilidad y gestión integral.

Seguridad de la Información: Conjunto de medidas, controles y prácticas destinadas a proteger la confidencialidad, integridad y disponibilidad de la información administrada por el ICBF, así como a prevenir accesos no autorizados.

Alta Disponibilidad: Capacidad de un sistema, servicio o componente tecnológico para mantenerse operativo con niveles mínimos de indisponibilidad, mediante esquemas de redundancia y tolerancia a fallos.

Respaldo (Backup): Proceso de copia, almacenamiento y conservación de información crítica con el fin de permitir su recuperación ante pérdida, daño, incidente o contingencia.

Restauración: Proceso mediante el cual se recupera información, aplicaciones o servicios a partir de respaldos previamente generados, garantizando la continuidad operativa.

Analítica: Conjunto de técnicas y procesos orientados al análisis sistemático de datos con el fin de extraer información útil, generar indicadores, identificar patrones, tendencias y apoyar la toma de decisiones operativas, tácticas y estratégicas del ICBF.

Analítica Institucional: Uso estructurado de datos institucionales del ICBF mediante herramientas, modelos y procesos analíticos para apoyar la gestión, el seguimiento, el control y la toma de decisiones en los procesos misionales, estratégicos y administrativos.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Observabilidad: Capacidad de medir, comprender y analizar el estado interno y el comportamiento de la infraestructura, servicios y aplicaciones TIC del ICBF a partir de métricas, logs, eventos y trazas, permitiendo la detección proactiva de anomalías y fallas.

SIEM: Sistema de Gestión de Información y Eventos de Seguridad que consolida, correlaciona y analiza logs y eventos provenientes de diferentes componentes de la infraestructura TIC, con el fin de detectar incidentes de seguridad, generar alertas y soportar procesos de análisis forense y cumplimiento.

ETL: Conjunto de procesos de Extracción, Transformación y Carga de datos que permiten recopilar información desde diversas fuentes, depurarla, transformarla y almacenarla en repositorios destinados a análisis y explotación de datos institucionales.

Línea Base: Estado inicial validado y documentado de los servicios TIC, infraestructura, volúmenes, capacidades o indicadores, que sirve como punto de referencia para el seguimiento, control y medición de cambios durante la ejecución contractual.

Línea Base del Servicio: Conjunto de características técnicas, operativas y cuantitativas que describen la situación inicial de cada servicio TIC del ICBF al inicio de la operación, y que permite medir la evolución del servicio y su impacto contractual.

Indicador (KPI): Métrica definida para medir el desempeño, calidad, eficiencia o efectividad de un proceso, servicio o actividad TIC, utilizada como insumo para la gestión, el seguimiento y la toma de decisiones.

Tablero de Control: Herramienta visual que consolida y presenta indicadores, métricas y resultados relevantes de los servicios TIC, permitiendo el seguimiento operativo, el control contractual y el análisis histórico del desempeño.

Logs: Registros generados automáticamente por sistemas, aplicaciones, dispositivos y herramientas TIC, que contienen información detallada sobre eventos, transacciones, errores y actividades, y que soportan procesos de monitoreo, auditoría y seguridad.

Gestión de Eventos: Proceso orientado a la detección, análisis y respuesta a eventos generados por la infraestructura y los servicios TIC, con el fin de identificar condiciones normales o anómalas y prevenir incidentes.

Gestión de Vulnerabilidades: Proceso continuo de identificación, análisis, clasificación, priorización y tratamiento de vulnerabilidades técnicas que puedan afectar la seguridad de la información y la infraestructura TIC del ICBF.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Integración de Servicios: Conjunto de procesos y mecanismos técnicos que permiten la interoperabilidad y comunicación entre sistemas de información, plataformas tecnológicas y servicios, garantizando el intercambio consistente de datos e información.

Explotación de Datos: Proceso mediante el cual los datos institucionales son analizados, transformados y utilizados para generar información estratégica, conocimiento y valor para la toma de decisiones del ICBF.

Coordinador de Calidad: El responsable de calidad es el encargado de supervisar todos los procesos, prácticas y acciones durante todo el proyecto para conseguir que los productos, documentos y servicios se entreguen con los estándares de calidad y los tiempos establecidos requeridos por el ICBF.

Gestor de la Capacidad: El responsable de la capacidad se encarga de asegurar de manera preventiva que los servicios y la infraestructura de TI sean capaces de cumplir con los objetivos de capacidad y desempeño de manera equilibrada con el aprovisionamiento de recursos y necesidades a corto y mediano plazo.

Gestor de la Continuidad: El Gestor de la continuidad del servicio de TI es responsable de gestionar aquellos riesgos que podrían afectar severamente la prestación de servicios de TI. Establece estrategias para que la infraestructura cumpla los requisitos mínimos del nivel de servicio en casos de desastre, mediante reducción del riesgo a un nivel aceptable y la planificación de la restauración de los servicios de TI.

Gestor de la Disponibilidad: El Gestor de la disponibilidad es responsable de definir, analizar, planificar, medir y mejorar todo lo concerniente a la disponibilidad de los servicios tecnológicos en cumplimiento de los niveles de servicio establecidos por la Entidad.

Gestor de la Seguridad de TI: El Gestor de la seguridad de TI se ocupa de salvaguardar la confidencialidad, integridad y disponibilidad de los activos, información, datos y servicios de TI de la Entidad, correspondientes al alcance de la presente ficha de condiciones técnicas.

Gestor de Riesgos: El Gestor de riesgos se ocupa de identificar, evaluar y controlar riesgos. Esto incluye el análisis de criticidad de los activos de información de la Entidad, la identificación de amenazas a esos activos y la evaluación de la vulnerabilidad de cada activo ante dichas amenazas, para diseñar estrategias de tratamiento de riesgos y verificación continua de su efectividad para disminuir la probabilidad o impacto asociado a la materialización de riesgos.

Gestor del Nivel de Servicio: El Gestor del nivel de servicio es responsable de monitorear que los procesos y acciones de los recursos humanos

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

asignados al proyecto sean adecuados para cumplir los Acuerdos de Niveles de Servicio descritos en el Anexo 02 - Acuerdos de Niveles de Servicio

Gestor de Portafolio y Catálogo de Servicios: El gestor debe asegurar de que se realice y se edite debidamente el portafolio y catálogo de Servicios, que contenga información precisa y actualizada de todos los servicios operacionales y de los próximos a ofrecerse. Este es información fundamental para el resto de los procesos de Gestión de Servicios: detalles de servicios, estatus actual e interdependencia de estos.

Ciberinteligencia (Cyber Threat Intelligence - CTI): Proceso continuo de recolección, correlación, análisis y producción de inteligencia sobre amenazas cibernéticas mediante información proveniente de fuentes internas y externas, con el propósito de identificar actores maliciosos, tácticas, técnicas y procedimientos (TTP), indicadores de compromiso (IoC), indicadores de ataque (IoA) y riesgos emergentes, apoyando los procesos de prevención, detección, respuesta y mejora continua de la postura de ciberseguridad.

7. OBLIGACIONES DEL CONTRATISTA

7.1 Obligaciones generales

7.1.1 Cumplir con el objeto del contrato con plena autonomía técnica y administrativa y bajo su propia responsabilidad, por lo tanto, no existe ni existirá ningún tipo de subordinación, ni vínculo laboral alguno entre EL CONTRATISTA y el ICBF.

7.1.2 Constituir y allegar al ICBF las garantías requeridas dentro de los tres (3) días hábiles siguientes a la suscripción del contrato o antes de iniciar la etapa de operación del contrato. Considerando esta última como la fecha límite máxima correspondiente a la fecha de finalización de la etapa de transición de entrada, para presentar las pólizas que son requeridas.

7.1.3 Participar y apoyar al ICBF en todas las reuniones a las que éste lo convoque relacionadas con la ejecución del contrato.

7.1.4 Disponer de los medios necesarios para el mantenimiento, cuidado y custodia de la documentación objeto del presente contrato. Toda la información que resulte del contrato debe ser almacenada en el sitio web que disponga la entidad para tal fin y su acceso se monitoreara y se ajustarán los permisos necesarios.

7.1.5 Atender los requerimientos, instrucciones y/o recomendaciones que durante el desarrollo del Contrato le imparta el ICBF a través del supervisor de este, para una correcta ejecución y cumplimiento de sus obligaciones y que se encuentren relacionados con el objeto y alcance contrato.

7.1.6 Entregar al supervisor del Contrato los informes que se soliciten sobre cualquier aspecto y/o resultados obtenidos relacionado con el objeto y alcance contratado, cuando así se requiera.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

7.1.7 Presentar la factura de conformidad con la forma de pago estipulada en el contrato, junto con el informe de las actividades realizadas para cada pago y cualquier otro soporte que considere necesario el supervisor del contrato.

7.1.8 Guardar estricta reserva sobre toda la información y documentos que tenga acceso, maneje en desarrollo de su actividad o que llegue a conocer en desarrollo del contrato y que no tenga carácter de pública. En consecuencia, se obliga a no divulgar por ningún medio dicha información o documentos de terceros, sin la previa autorización escrita del ICBF.

7.1.9 Devolver al ICBF, una vez finalizada la ejecución del contrato, los documentos que en desarrollo del contrato se hayan producido, e igualmente todos los archivos que se hayan generado en cumplimiento de sus obligaciones, debidamente organizado de conformidad con las reglas del Archivos General de la Nación y los lineamientos de la Dirección Administrativa.

7.1.10 Colaborar con el ICBF en el suministro y respuesta de la información correspondiente, a los requerimientos efectuados por los organismos de control del Estado Colombiano en relación con la ejecución, desarrollo o implementación del contrato objeto del presente documento.

7.1.11 No se le permite al contratista utilizar la imagen del ICBF en sus correos electrónicos u otro tipo de comunicación, no se podrá utilizar el nombre, emblema o sello oficial del ICBF para fines publicitarios o de cualquier otra índole, salvo autorización expresa y escrita de las partes y con un objetivo específico.

7.1.12 Realizar los pagos al SISS (salud, pensión y riesgos laborales) y parafiscales, de acuerdo con la normatividad vigente, aportando los soportes de pago correspondientes.

7.1.13 Respetar la política medioambiental del ICBF, política que incluye todas las normas internas sobre el uso de los recursos ambientales, como el agua y la energía, racionamiento de papel, norma sobre parqueaderos y manejo de desechos residuales.

7.1.14 Cumplir con las disposiciones establecidas en el Capítulo “Buenas prácticas en la Gestión Contractual” del Manual de Contratación vigente.

7.1.15 Remitir al supervisor del contrato, dentro de los tres (3) días siguientes a la consignación, copia del documento donde conste la operación que, por concepto de reintegros, rendimientos financieros, multas o cualquier otro, se causen a favor de la Entidad en razón a la ejecución del contrato. PARÁGRAFO: Las consignaciones a que hace referencia esta obligación deben realizarse únicamente en la cuenta informada por escrito por el supervisor del contrato.

7.1.16 Gestión de Requerimientos de Información: Preparar y entregar la información solicitada por el ICBF en un plazo máximo de veinticuatro (24) horas siguientes a la recepción del requerimiento. En caso de que la complejidad de la solicitud impida su cumplimiento en dicho término, el Contratista deberá remitir, dentro del mismo plazo original (24 horas), una comunicación formal que incluya: i) el soporte o justificación técnica de la imposibilidad de entrega inmediata; ii) la razón detallada del retraso; y iii) un plan de trabajo con la fecha definitiva de entrega.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

En ninguna circunstancia este nuevo plazo podrá exceder los cinco (5) días hábiles siguientes al requerimiento inicial. El incumplimiento de los términos aquí previstos se entenderá como una inobservancia de las obligaciones contractuales."

7.1.17 Elaborar la documentación requerida para la presentación de solicitudes de cambio ante el Comité de Control de Cambios de la Entidad, de acuerdo con los procedimientos definidos en tal sentido

7.1.18 El contratista Outsourcing deberá asegurar el borrado de seguro de toda información propiedad del ICBF que pudiera encontrarse en dispositivos de seguridad, dispositivos de almacenamiento, dispositivos de red, dispositivos de procesamiento, dispositivos de virtualización, clústeres etc. Entregando al ICBF evidencias del procedimiento de borrado seguro ejecutado de todos y cada uno de los dispositivos antes mencionados y que pudieran ser suministrados en préstamo a la entidad como parte de la ejecución servicio plasmado. Esta obligación se debe cumplir en la etapa de transición de salida y con el fin de garantizar la integridad del proceso de borrado seguro, el contratista debe:

- Utilizar herramientas de Borrado Seguro de fabricantes reconocidos.
- Entregar un reporte detallado del proceso de borrado, que incluya mínimo fecha, hora y método utilizado.
- Entregar un certificado que confirme que los datos han sido eliminados de manera segura y conforme a la normatividad vigente.
- Entregar documentación con registro fotográfico del procedimiento que se llevó a cabo.

7.2 **Obligaciones específicas**

7.2.1 **Relacionadas con los servicios**

- Garantizar el correcto funcionamiento de todos los servicios contratados, comprometiéndose a subsanar las fallas que le sean atribuibles durante la vigencia del contrato. (en coordinación con los demás operadores de tecnología para ICBF, si se requiere).
- En caso de presentarse algún daño a algún elemento de la plataforma tecnológica que sea atribuible al contratista durante la ejecución del contrato, el contratista deberá reponer de manera inmediata el elemento por uno idéntico o de mejores características cuyo costo sea por lo menos el del elemento afectado, lo anterior sin generar costos adicionales para la Entidad. En todo caso, el contratista será responsable de la afectación a cualquiera de los servicios durante el periodo de reposición.
- Mantener monitoreados los servicios 7X24X365, durante la duración del contrato.
- Garantizar la operación en los servicios bajo los horarios, tiempos de respuesta y condiciones establecidas en el presente documento y en el Anexo 02 -

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Acuerdos de Niveles de Servicio.

- Garantizar al ICBF que cumple y conoce la normatividad, reglas y lineamientos técnicos y legales para la prestación de la operación y los servicios contratados.
- Garantizar que tiene establecidos los controles de calidad sobre los servicios contratados.
- Todo hardware y software suministrado por el Contratista debe estar debidamente licenciado, con los certificados expedidos por el fabricante, es de obligación del Contratista presentar los soportes de las renovaciones y/o adquisiciones realizadas durante la ejecución del contrato.
- Monitorear y administrar el desempeño de toda la infraestructura de tecnología informática expuestos en este documento para el ICBF.
- Apoyar en la implementación de soluciones nuevas relacionadas con los servicios, adquiridas a través de este contrato u otros inclusive.
- Ejecutar cualquier tipo de actualización y mejora sobre la infraestructura, sin que esto genere costos adicionales a la Entidad. El ICBF suministrara los recursos de hardware y licenciamiento necesarios para tal fin a excepción de la infraestructura que provea el contratista
- Todo cambio que se realice deberá contar con su respectiva RFC de acuerdo con el formato de calidad establecido para tal fin y aprobado por la gestoría de cambios.
- Apoyar a la DTI en el diseño, implementación, medición y administración de pruebas piloto relacionadas con los servicios, contratadas a través de este contrato u otros inclusive.
- Proponer recomendaciones y acciones de mejora que, sobre los servicios, basado en las nuevas tendencias tecnológicas, planes de capacidad y consulta a expertos realizadas.
- Ejecutar actividades programadas y no programadas propias sobre la infraestructura y los servicios.
- Acatar las instrucciones que imparta el ICBF para el cabal cumplimiento del contrato, a través del Supervisor del contrato.
- Garantizar la confidencialidad de la información de los datos de los usuarios contenida en las herramientas o aplicaciones que administran, así cómo, el de las contraseñas y demás datos de la administración de los servicios. Esto incluye, la aplicación de las políticas de seguridad y privacidad de la información para la gestión y control de usuarios definidas por el ICBF.
- Responder por los daños y/o perjuicios ocasionados en las instalaciones de terceros ocasionados por el contratista durante la prestación del servicio de operación global en la ejecución del presente contrato.
- Cumplir con lo establecido en el *Anexo 01 - Personal mínimo requerido.*
- Cumplir con lo establecido en el *Anexo 05 - Entregables*
- Llevar el registro continuo durante la ejecución del contrato de fallas, problemas, soluciones, acciones desarrolladas, respaldos, recuperaciones, trabajos

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

realizados y en general todos los detalles de la operación en la herramienta de gestión HelpPeople donde se registran los incidentes, requerimientos, problemas y cambios. Adicionalmente el contratista debe generar la CMDB (Configuration Management Database o Base de Datos de Gestión de la Configuración) y promover el uso de la CMDB en las operaciones diarias para asegurar que se mantenga actualizada y precisa, para ello debe poner en práctica procesos de gestión asociados a ITIL como son gestión de cambios y gestión de incidentes y problemas, para todos los servicios prestados.

- Diseñar, documentar y mantener actualizados los procesos, procedimientos, lineamientos e instructivos de todos los servicios.
- Cumplir con todas y cada una de las condiciones definidas para cada uno de los servicio así como lo definido en el ítem" Requerimientos de servicio" definidos para cada uno de los servicios contratados.

7.2.1.1 MESA DE SERVICIO

- Prestar el servicio como punto único de contacto (SPOC) para la recepción, registro, categorización, priorización, seguimiento y cierre de incidentes, requerimientos, consultas y solicitudes de los usuarios.
- Garantizar la atención de los casos a través de los canales definidos por la Entidad, tales como herramienta de gestión de servicios, correo electrónico, portal de autoservicio, atención telefónica, chat y demás mecanismos habilitados durante la ejecución contractual.
- Registrar la totalidad de los tickets en la herramienta de gestión de servicios dispuesta para tal fin, incluyendo la trazabilidad completa de las actividades realizadas hasta su cierre.
- Cumplir los Acuerdos de Niveles de Servicio (ANS) establecidos por la Entidad para los procesos de atención, escalamiento, solución y cierre de incidentes y requerimientos.
- Realizar la clasificación, priorización y escalamiento funcional o técnico de los casos conforme a los procedimientos definidos por el ICBF y las matrices de criticidad aprobadas.
- Proporcionar soporte de primer nivel, ejecutando las actividades necesarias para la resolución de incidentes y requerimientos que puedan ser atendidos desde la Mesa de Servicio.
- Coordinar el escalamiento oportuno a los grupos resolutores de segundo y tercer nivel, efectuando el seguimiento hasta la normalización efectiva del servicio.
- Mantener actualizada la base de conocimiento, documentando procedimientos, soluciones conocidas, preguntas frecuentes y demás información que contribuya a mejorar la eficiencia del servicio.
- Implementar mecanismos de monitoreo y control sobre la calidad de la atención prestada, orientados a garantizar la satisfacción de los usuarios y el cumplimiento de los objetivos del servicio.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Identificar tendencias y causas recurrentes de incidentes, proponiendo acciones preventivas y correctivas que permitan reducir su frecuencia e impacto.
- Garantizar la disponibilidad y continuidad operativa del servicio, de acuerdo con los horarios de atención y cobertura establecidos contractualmente.
- Cumplir las políticas de seguridad de la información, protección de datos personales, gestión de accesos y confidencialidad definidas por el ICBF.
- Mantener la documentación operativa actualizada, incluyendo procedimientos, instructivos, guías de atención, matrices de escalamiento, catálogos de servicios y demás documentos asociados al servicio.
- Brindar acompañamiento y orientación a los usuarios en el uso adecuado de las herramientas tecnológicas y servicios de TI.
- Participar en reuniones de seguimiento, comités técnicos y sesiones de revisión del servicio cuando sea requerido por la supervisión del contrato.
- Entregar mensualmente los informes de gestión y los soportes asociados, incluyendo evidencias de cumplimiento de ANS, estadísticas de atención, indicadores de desempeño, análisis de tendencias y planes de mejora.
- Transferir el conocimiento y entregar la documentación del servicio al finalizar el contrato Fase de Transición de Salida, garantizando la continuidad operativa y la adecuada gestión de la información.

7.2.1.2 SOPORTE EN SITIO

- Prestar el servicio de soporte técnico en sitio a los usuarios del ICBF para la atención de incidentes, requerimientos, consultas y demás solicitudes asociadas a los servicios y componentes tecnológicos.
- Realizar actividades de diagnóstico, atención, solución, configuración, mantenimiento correctivo de los equipos de cómputo, periféricos y demás elementos tecnológicos cubiertos por el contrato.
- Atender los requerimientos asignados por la Mesa de Servicio dentro de los tiempos establecidos en los Acuerdos de Niveles de Servicio (ANS) definidos por el ICBF.
- Ejecutar la instalación, configuración, actualización y desinstalación de sistemas operativos, aplicaciones, controladores, herramientas y demás componentes autorizados por el ICBF.
- Realizar la configuración y soporte de equipos de escritorio, computadores portátiles, impresoras, escáneres, dispositivos móviles, cámaras, diademas y demás dispositivos tecnológicos.
- Efectuar la validación, diagnóstico y solución de fallas relacionadas con hardware, software, conectividad, accesos, impresión y demás componentes de la infraestructura tecnológica del usuario final.
- Gestionar el traslado, instalación, reinstalación y puesta en funcionamiento de equipos tecnológicos cuando sea requerido por el ICBF.
- Registrar en la herramienta de gestión de servicios la totalidad de las actividades

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

realizadas, incluyendo diagnóstico, acciones ejecutadas, evidencias y solución implementada.

- Realizar acompañamiento técnico en las jornadas de despliegue tecnológico, renovación de equipos, migraciones, actualizaciones masivas y demás actividades programadas por la supervisión.
- Verificar el correcto funcionamiento de los equipos intervenidos y obtener la conformidad del usuario antes del cierre de cada requerimiento.
- Gestionar oportunamente el escalamiento de incidentes o requerimientos que requieran intervención especializada de otros grupos técnicos o proveedores.
- Ejecutar actividades de soporte relacionadas con servicios de directorio activo, correo electrónico, herramientas colaborativas, soluciones de impresión y demás plataformas utilizadas por el ICBF.
- Apoyar la gestión de garantías de equipos tecnológicos, efectuando diagnósticos, cuando corresponda.
- Garantizar la confidencialidad, integridad y disponibilidad de la información a la que tenga acceso durante la ejecución de las actividades de soporte.
- Participar en reuniones de seguimiento, mesas técnicas, auditorías y demás actividades convocadas por la supervisión del contrato relacionadas con la ejecución del servicio.
- Mantener personal técnico con las competencias, certificaciones y experiencia necesarias para la adecuada prestación del servicio.
- Brindar soporte presencial en la sede principal y en las sedes regionales o centros zonales que determine el ICBF, de acuerdo con el esquema de cobertura definido contractualmente.
- Apoyar las actividades de inventario tecnológico, validación física de activos, conciliación con la CMDB y actualización de información cuando sea requerido por la supervisión.
- Elaborar y mantener actualizada la documentación técnica, procedimientos, instructivos y guías operativas asociadas a las actividades de soporte en sitio.
- Entregar mensualmente los informes de gestión y los soportes asociados, incluyendo evidencias de cumplimiento de ANS, estadísticas de atención, indicadores de desempeño, análisis de tendencias y planes de mejora.
- Transferir el conocimiento y entregar la documentación del servicio al finalizar el contrato Fase de Transición de Salida, garantizando la continuidad operativa y la adecuada gestión de la información.

7.2.2 **Relacionadas con el equipo de trabajo**

- Proveer el personal requerido de acuerdo con los roles establecidos en el capítulo de Gobernabilidad de la ficha de condiciones Técnicas y en el Anexo 01 - Personal mínimo requerido. El personal debe ser de dedicación exclusiva para el desarrollo del contrato siempre que la disponibilidad del perfil sea de tiempo completo de

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

conformidad con el Anexo mencionado anteriormente. Dentro de los cinco (5) días calendario siguientes a la suscripción del contrato deberá presentar las hojas de vida junto con sus soportes de todo el personal requerido para aprobación y validación del supervisor. Una vez validadas y aprobadas las hojas de vida el Contratista deberá presentar, en un plazo no mayor a cinco (5) días calendarios, los respectivos contratos de vinculación del personal con el que desarrollará el presente Contrato.

- Prestar los servicios con personal calificado y especializado que cumpla con los perfiles y experiencia exigidos por el ICBF como se indica en **Anexo 01 - Personal mínimo requerido** en cada uno de los servicios y gestiones.
- Garantizar la operación de los servicios 7X24X365 durante la ejecución del contrato con el personal mínimo relacionado en el Anexo 01 - Personal mínimo requerido, en cada uno de los servicios y gestiones, y el personal analista y de apoyo capacitado y calificado para la prestación de los servicios.
- Desarrollar un proceso de empalme y transferencia de conocimiento de mínimo una semana para el caso de retiros permanentes.
- Presentar un plan de transferencia de conocimiento cruzado entre los recursos humanos del contratista asignados al proyecto, que relacione el recurso de contingencia en cada caso e incluya las actividades de capacitación mensuales y material de entrenamiento a utilizar para garantizar la transferencia de conocimiento entre pares.
- En el caso de retiros temporales asociados a incapacidades o vacaciones, el contratista deberá presentar el plan de acción con los recursos de contingencia sin causar traumatismos ni afectación del servicio.
- Presentar quincenalmente el cronograma de disponibilidad del personal del Contratista asignado al proyecto y el recurso de contingencia en cada caso.
- Presentar notificación con ocho (8) días de anticipación, cuando se planee retirar o reemplazar a cualquier miembro del equipo, explicando el motivo del retiro y el plan de trabajo para reemplazarlo.
- En caso de retiros, ya sea por iniciativa del proveedor o del ICBF, aplicarán los ANS asociados al recurso humano.
- Diseñar, entregar y aplicar los formatos, procesos y procedimientos para la prestación del servicio con el detalle que el ICBF lo exija.
- Designar personal especializado que se encuentre disponible de forma permanente (7X24X365) para responder a las alertas y/o incidentes generados en la plataforma tecnológica.
- Disponer de un especialista por servicio y por gestoría, el cual estará en constante comunicación con el líder del respectivo servicio o gestoría designado por el ICBF.
- Garantizar que la incorporación y/o sustitución de cualquiera de los especialistas, sea informada con ocho (8) días de antelación al ICBF y que se dé cumplimiento a lo requerido en el Anexo 01 - Personal mínimo requerido.
- Cumplir con la disponibilidad de todos los recursos de personal asignados por parte del Contratista a este contrato, de forma permanente, sin que las posibles incidencias relacionadas afecten al ICBF. En este sentido, será responsabilidad

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

exclusiva del Contratista que no exista ningún periodo de carencia entre la baja de un recurso de cualquier perfil y la reposición de este. La incorporación, sustitución, compensatorios o baja de cualquier especialista designado por El Contratista, debe ser informado al ICBF con ocho (8) días de antelación.

- Informar al ICBF los compensatorios de los especialistas quincenalmente y relacionar el recurso de contingencia en cada caso.
- Responder por la formación de su personal, en cuanto a la realización de todos los cursos que se consideren necesarios e imprescindibles, incluyendo los de actualización, para la correcta prestación del servicio.
- El personal que preste el servicio por parte del contratista deberá estar debidamente identificado con carné y/o chaleco en un lugar visible durante su presencia en las instalaciones de la Entidad y suministrar un trato respetuoso y formal a los usuarios acatando fielmente los protocolos de atención y prestación del servicio, establecidos por el ICBF.
- El personal del contratista podrá prestar el servicio de forma remota, excepto para el perfil de Gerente, Coordinador de Operaciones y Coordinador de Calidad quienes deberán estar disponibles en sitio, para este caso, el ICBF dispondrá del puesto de trabajo y conectividad.
- El Contratista deberá tener disponibilidad de los profesionales en caso de requerirse por el supervisor del contrato y conforme a lo establecido en el porcentaje de dedicación de los meses requeridos del Anexo 01 - Personal mínimo requerido., sin costos adicionales para la Entidad.
- En cualquier momento durante de la ejecución del contrato, el supervisor podrá solicitar el cambio de cualquier miembro del equipo de trabajo del Contratista cuando se presenten deficiencias técnicas, profesionales o de actitud en la prestación del servicio o labor a su cargo, de acuerdo con los requerimientos, exigencias y necesidades del ICBF. En este caso el Contratista deberá reemplazar el profesional en un término de 20 días hábiles contados a partir de la solicitud del supervisor. En todo caso, se aplicarán los ANS determinados en el Anexo 02 - Acuerdos de Niveles de Servicio si el servicio prestado al ICBF se ve afectado de alguna manera causado por la rotación del personal del Contratista. En caso de que el contratista efectúe un cambio de algún miembro del equipo de trabajo, deberá informar al supervisor del contrato de manera inmediata del retiro del personal, momento a partir del cual tendrá el término de 20 días hábiles para efectuar el respectivo reemplazo.
- Una vez inicie la ejecución del contrato el Contratista deberá hacer la presentación al supervisor del personal con su respectiva hoja de vida, diplomas de estudio y certificaciones. En caso de que las certificaciones de experiencia del personal mínimo sean expedidas por el oferente o contratista deberá adjuntar evidencia de vinculación laboral y certificado de ingresos y retenciones del personal presentado cuyas fechas coincidan con las certificaciones aportadas. El anterior procedimiento aplica para el reemplazo de personal por iniciativa del contratista o del ICBF.
- En caso de que se realicen cambios en el personal que presta el servicio y las certificaciones de experiencia y/o conocimientos dejasen de estar vigentes por

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

razones como: el fabricante ya no expide la certificación o porque el activo objeto de la certificación entró en desuso, entre otros, el supervisor podrá aprobar nuevas certificaciones que sean equivalentes o superiores a las solicitadas en el Anexo 01 - Personal mínimo requerido.

- Durante la ejecución del contrato, el contratista podrá presentar personal de apoyo si considera que lo requiere el servicio, en cuyo caso no será exigible el cumplimiento de perfil y no generará costos adicionales para la Entidad.
- Presentar dentro de la primera semana a partir de la firma del acta de inicio del contrato del contrato, el organigrama y las hojas de vida del personal mínimo obligatorio conforme a la “Matriz de roles y perfiles de servicios”. Dicho personal deberá incluir los soportes y certificaciones de vinculación al contrato, cumpliendo con los requisitos de formación y experiencia especificados en la matriz mencionada.
- Presentar dentro de la segunda semana a partir de la firma del acta de inicio del contrato, el organigrama y las hojas de vida del personal adicional que conformará el equipo de operación TIC. Es necesario que cada perfil se relacione directamente con las funciones a desempeñar. El organigrama deberá estar alineado con el modelo de operación por servicio y los roles establecidos en la “Matriz de roles y perfiles de servicios”. El ICBF revisará las hojas de vida y aprobará al personal si su perfil cumple con las condiciones y actividades requeridas por el servicio
- El supervisor podrá solicitar actualizaciones de los soportes de la información relacionada en las hojas de vida de los profesionales, técnicos y tecnólogos en sus diferentes roles y gestiones durante la ejecución del contrato, para verificar las competencias y calidad del personal del Contratista.
- El Contratista será responsable de la relación laboral y prestaciones sociales del recurso humano asignado al proyecto y en consecuencia no existirá relación laboral, ni prestaciones sociales a cargo del ICBF.
- El servicio de transporte del personal del Contratista, en los eventos que se requieran según la operación, incluidos diurnos, nocturnos y festivos, y cualquier gasto que se derive de la operación del servicio, será asumido en su totalidad por el Contratista.
- Los computadores, teléfonos móviles/planes voz y datos (para cada personal del Contratista) y herramientas de soporte serán suministrados por el contratista.
- Es responsabilidad del Contratista adoptar los procedimientos, técnicas de operación y conocimientos de la infraestructura que opera en el ICBF.
- Asegurar que el personal del contratista conoce y entiende las necesidades del ICBF, incluidas en el marco contractual y asegurar la satisfacción del ICBF mediante los diferentes controles de calidad aplicados.
- El Contratista deberá considerar a todos los terceros, aliados y socios de negocio del Contratista, que participen en la prestación de servicios objeto del presente documento, como personal del Contratista, por lo cual el Contratista será el único responsable de las acciones que realicen estos terceros.
- En ningún caso el contratista podrá otorgar acceso a los activos de información del

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

ICBF a personal que no tenga la autorización expresa de ingreso a las instalaciones de la entidad, a los activos de información ni esté presentado y aceptado oficialmente por la supervisión del contrato.

7.2.3 **Relacionadas con el inventario**

- Notificar, justificar y proponer de manera inmediata al ICBF cualquier cambio que considere necesario realizar sobre cualquiera de los servicios que le fueron dados en administración para optimizar su operación y someterlo a la aprobación del Comité de Control de Cambios si fuese necesario.
- Mantener actualizado el inventario de la infraestructura administrada incluyendo la topología de estos, la cual deberá ser reportada al ICBF, adicionalmente se debe contar con los mapas de servicio debidamente actualizados.

7.2.4 **Relacionadas con herramientas**

- Gestionar en la herramienta de mesa de servicio que disponga el ICBF los tickets asignados referentes a incidentes, requerimientos y controles de cambios de los diferentes servicios a cargo del Contratista. Esta gestión de tickets consiste en la consulta, documentación de trámite, solución y cierre de los mismos.
- Facilitar al ICBF el acceso a todas las herramientas y consolas de gestión y administración de los servicios, con acceso en modo de lectura, mediante la creación de las cuentas a que haya lugar o la habilitación de los privilegios sobre las cuentas de Directorio Activo que el ICBF designe, configurándolas adecuadamente para tal tipo de acceso.
- Suministrar, administrar o configurar en caso de ser necesario, las herramientas de Gestión para los servicios contratados, así como las herramientas de monitoreo y diagnóstico que permitan gestionar, registrar, monitorear, controlar, alertar y generar reportes de cada servicio requerido con el fin garantizar la óptima prestación de estos.

7.2.5 **Obligaciones de ITIL**

7.2.5.1.1 Coordinación de Calidad

- Liderar el ciclo de vida (análisis, implementación, seguimiento y cierre) de las acciones preventivas, correctivas y de mejora Estas deben estar alineadas estrictamente con el Sistema de Gestión de Calidad (SGC) del ICBF, así como de las recomendaciones técnicas emitidas por la supervisión del contrato. Cada acción debe formalizarse en un Plan de Acción que incluya: análisis de viabilidad, cronograma, responsables y evidencias de impacto medible que demuestren la optimización del servicio y el impacto positivo medible en la prestación del servicio

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

y faciliten la toma de decisiones estratégicas. Documentando y presentando mensualmente un portafolio de experiencias exitosas y mejoras implementadas, que demuestren con datos cuantitativos el incremento en la eficiencia o ahorro de recursos para la entidad.

- Apoyar a la supervisión del contrato en la atención de auditorías internas relacionadas con la gestión de los servicios a cargo del contratista y aportar la documentación que en el marco de estas auditorías sean solicitadas por la supervisión del contrato.
- Liderar Analizar, implementar y realizar seguimiento sistemático, en conjunto con el personal especialista el ciclo de vida de las mejoras del servicio, integrando tanto las propuestas proactivas del contratista para la optimización de recursos y costos, como las recomendaciones técnicas y operativas emitidas por la supervisión. Para ambos casos, el contratista deberá:
    - Formalizar: Elaborar Planes de Acción que incluyan análisis de viabilidad, impacto en la disponibilidad/seguridad, cronograma y criterios de aceptación.
    - Ejecutar: Implementar las actividades aprobadas en conjunto con el personal especialista.
    - Evidenciar: Realizar un seguimiento sistemático que documente el cumplimiento y el impacto real (eficiencia) obtenido en la prestación de los servicios.
- Elaborar, presentar para aprobación de la supervisión y ejecutar un Cronograma Mensual de Mantenimiento para la infraestructura y servicios. Este debe incluir: a) Ficha técnica de actividades a realizar; b) Fecha y Ventanas de mantenimiento aprobadas; c) responsables, d) Informe de cumplimiento con indicadores de efectividad de los mantenimientos realizados
- Demostrar que selecciona y evalúa sus proveedores de bienes y servicios, relacionados directamente con la prestación del servicio contratado, haciendo cumplir las normas legales vigentes, así como las normas y especificaciones técnicas relacionadas y que les hace extensivas las obligaciones del eje de seguridad de la información que correspondan.
- Definir, documentar y reportar mensualmente un Mapa de Indicadores de Gestión (KPIs) que permita medir de forma cuantitativa la calidad del servicio. El contratista deberá presentar la ficha técnica de cada indicador (fórmula, fuente de datos y meta) para aprobación del ICBF. Los indicadores deben cubrir como mínimo: a) Mantenimiento; b) Calidad; c) Nivel de Servicio; d) Operación; y e) Gestión de Servicio
- Establecer, documentar y socializar una política y objetivos de calidad específicos para el proyecto, los cuales deberán ser entregados para aprobación del ICBF dentro del primer mes de ejecución. Dichos objetivos deben ser coherentes con el Sistema Integrado de Gestión (SIG) institucional y servir de base para la medición de los indicadores de gestión del contrato
- Refinar y formalizar la matriz de entregables (Anexo 05) y la matriz de obligaciones,

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

sus entregables, su periodicidad, sus respectivos criterios de aceptación, dentro del primer mes de ejecución contado a partir del acta de inicio

- Realizar revisión de la documentación entregada por los especialistas de los servicios incluidos en el contrato con el fin de garantizar la calidad y completitud conforme a las obligaciones del contrato.
- El contratista debe analizar y estandarizar procesos, formatos y controles de calidad para asegurar la calidad y cumplimiento de las obligaciones contractuales previa aprobación del líder de calidad del ICBF, quien se encargará de verificar con el supervisor del contrato si estos cambios aseguran la calidad y el cumplimiento antes mencionado. Estos cambios se producirán y se ejecutarán una vez el supervisor y el líder de calidad den su aprobación y se realice la respectiva divulgación al interior de la entidad.
- Documentar de manera detallada —como estrategia de transferencia de conocimiento— los procedimientos, instructivos e instrumentos técnicos requeridos para la gestión de cambios y optimización de los servicios. Esta documentación debe cubrir desde el protocolo de solicitud y evaluación del cambio hasta la actualización de manuales finales, garantizando la trazabilidad de la mejora. Todos los documentos deberán ser entregados formalmente y contar con la aprobación previa del ICBF para su implementación y archivo definitivo.
- Las demás dentro del marco de buenas prácticas de ITIL.

7.2.5.2 Gestoría Documental

- Entregar al inicio de la etapa de transición de entrada el Plan de Gestión Documental del proyecto. El Contratista deberá revisar, gestionar y asegurar la vigencia de toda la documentación técnica y administrativa conforme al Listado Maestro de Documentos (LMD) del ICBF y las políticas de administración vigentes. Esto incluye las actividades de planificación, creación, etiquetado y organización jerárquica, garantizando la verificación de formatos y la actualización permanente de los registros según las directrices de la Entidad
- Implementar y mantener instrumentos de control (matrices y checklist) que garanticen la trazabilidad integral de la documentación (actas, informes, planes y correspondencia entrante/saliente). El Contratista será responsable de elaborar, gestionar aprobaciones y custodiar estos registros, asegurando el seguimiento de radicados, tiempos de respuesta, responsables, fechas clave y la ubicación exacta (ruta) en el repositorio oficial. Se debe garantizar la suscripción de actas por las partes autorizadas y la disponibilidad inmediata para procesos de supervisión y auditoría.
- Realizar, administrar, mantener actualizado el repositorio de información, garantizando la disponibilidad permanente, integridad y acceso irrestricto de la supervisión a la documentación a través del repositorio oficial, bajo estrictos protocolos de ciberseguridad y seguridad de la información. El Contratista debe administrar un sistema de control de accesos basado en una matriz de permisos por

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

perfiles (ver, modificar, eliminar) y mantener un registro de auditoría de todos los cambios realizados en la configuración de dichos permisos, asegurando el control de versiones en todo momento.

- Implementar y administrar un Ecosistema Digital de Información que garantice la integridad, legibilidad y preservación histórica de toda la documentación técnica y administrativa (digital y física). El contratista deberá asegurar:
    - Seguridad y Disponibilidad: Acceso permanente en tiempo real para la Supervisión, control estricto de versiones (cambios, autores y fechas) y un Plan de Continuidad y Backup con respaldos periódicos.
    - Integridad: Asegurar que los archivos digitales sean legibles, se encuentren indexados y cuenten con protocolos de seguridad que garanticen su preservación e integridad histórica.
    - Gestión de Cambios: Documentar y validar cualquier ajuste en los procesos documentales, dimensionando impactos en la disponibilidad y definiendo protocolos de reversibilidad, Matriz Documental: Mantener un inventario detallado y actualizado mensualmente de toda la documentación producida en la ejecución del contrato, el cual servirá como instrumento de control para la trazabilidad de los entregables.
    - Estándares Archivísticos: Cumplimiento de las Tablas de Retención Documental (TRD), el Listado Maestro de Documentos (LMD), el Plan de Gestión Documental, las normas archivísticas vigentes y la indexación técnica inmediata de productos finales en el repositorio oficial. En caso de que las TRD se encuentren desactualizadas, la gestión documental deberá alinearse con las mejores prácticas y estándares archivísticos aplicables.
- Contratista deberá estructurar y mantener actualizada una matriz de seguimiento integral que consolide la gestión de los informes mensuales (nivel ejecutivo, por servicio, gestoría, mesa de servicio, soporte en sitio y demás), la cual será el instrumento para verificar el cumplimiento de los siguientes hitos:
    - Entrega Inicial: El Contratista debe radicar los informes ante el ICBF dentro de los primeros cinco (5) días hábiles de cada mes, registrando en la matriz la fecha exacta de envío y el soporte de recepción.
    - Gestión de Subsanación: Ante observaciones del ICBF, el Contratista deberá realizar las correcciones solicitadas en los plazos definidos en el Anexo 02 (ANS). La matriz deberá registrar las fechas de devolución y de reenvío para efectos de auditoría de tiempos de respuesta.
    - Cierre y Aprobación: La matriz debe reflejar las fechas de firma y aprobación final. El ciclo completo (entrega, revisión y subsanación) en ningún caso podrá exceder el décimo (10°) día hábil del mes calendario.
- Régimen de Penalidades: El incumplimiento de los plazos aquí descritos, la extemporaneidad en la entrega o la presentación de informes sin los estándares de calidad y contenido pactados activará las penalizaciones establecidas en el Anexo 02 - Acuerdo de Niveles de Servicio.
- El Contratista, a través de su Gestoría Documental, será responsable de definir,

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

estructurar y validar el contenido mínimo de los informes mensuales de gestión, garantizando la homogeneidad de la información entre los diferentes servicios. Esta obligación incluye:

- A. Definición de Estructura Técnica: El Gestor deberá diseñar y mantener actualizada la plantilla oficial de informes, la cual debe integrar como mínimo:
  - Resumen Ejecutivo: Consolidado de hitos y cumplimiento general del mes.
  - Estado de Ejecución: Análisis de actividades realizadas, ejecutadas, planeadas, suspendidas e incumplidas y causas de incumplimiento.
  - Gestión de ANS: Reporte detallado de Acuerdos de Niveles de Servicio con análisis de causas de incumplimiento si aplica.
  - Operación Técnica: Control de cambios, niveles de utilización (con análisis de crecimiento mensual), gestión de incidentes y análisis de errores/causa raíz.
  - Gestión de Riesgos y Alertas: Identificación de situaciones críticas detectadas en el periodo.
  - Plan de Trabajo: Cronograma de actividades proyectadas para el mes siguiente
  - Plan Mejora: Recomendaciones estratégicas y seguimiento a acciones correctivas previas.
  - Matriz de entregables y Obligaciones: Reporte de estado de cumplimiento de los productos y compromisos contractuales
  - Sugerencias y recomendaciones estratégicas para consideración del ICBF
- B. Aseguramiento de la Calidad (QA): Previo a la entrega al ICBF, la Gestoría Documental, en conjunto con la coordinación de Calidad, realizar una auditoría de contenido para asegurar que los informes sean coherentes, no presenten errores de forma y cuenten con el análisis técnico requerido en el literal A, ausencia de errores de forma y suficiencia del análisis requerido.
- C. Custodia y Repositorio: El Gestor deberá garantizar la indexación y cargue de los informes finales aprobados en el repositorio documental oficial designado, asegurando su trazabilidad e integridad histórica

- Elaborar y mantener actualizada en últimas versiones en medio físico y/o digital toda la documentación relacionada con el presente contrato incluyendo: actas, informes, planes de gestión, planes de mejoramiento relacionadas con el objeto del contrato conforme al plan de gestión documental. Mantener actualizadas los formatos correspondientes a las matrices de seguimiento de obligaciones y entregables (discriminadas por servicio y consolidadas). Asimismo, el Contratista deberá administrar una bitácora de incidentes documentales que registre la descripción, tiempos de respuesta, medios de reporte y estado de gestión de cualquier evento que afecte la custodia de la información. El detalle y los medios de entrega de estos insumos serán pactados con el ICBF, garantizando su disponibilidad permanente para la supervisión

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Ejecutar un Plan de Transferencia de Conocimiento técnico y administrativo sobre la gestión documental del proyecto, que garantice la entrega formal de manuales de usuario, matrices de control, estructuras de archivo y protocolos de administración de la plataforma. Esta labor incluye la realización de jornadas de capacitación y la entrega de un acta de cierre documental detallada, aprobada por la supervisión del ICBF, que certifique que la Entidad cuenta con la información y autonomía necesarias para dar continuidad a la gestión.
- Garantizar la reserva y confidencialidad de la información mediante la suscripción de acuerdos formales por parte de todo el personal asignado. El Contratista deberá atender las mesas técnicas y comités solicitados por el ICBF, brindando asesoría para la optimización de recursos y la disponibilidad de la infraestructura documental. Toda la ejecución de la gestoría deberá regirse por los lineamientos del ICBF y las buenas prácticas de ITIL, asegurando un registro trazable de todas las consultas y respuestas emitidas.
- Gestionar la correspondencia entrante y saliente que se genera durante la ejecución del contrato, manteniendo una matriz de comunicaciones del proyecto
- Las demás dentro del marco de buenas prácticas de ITIL.

7.2.5.3 Gestoría de la Capacidad

- Presentar mensualmente, en el informe de capacidad, la información de la utilización real del sistema comparada con las previsiones del Plan de Capacidad.
- Estimar y proyectar la capacidad de almacenamiento de datos métricos a mediano y largo plazo para obtener tendencias históricas e iniciativas de planificación de la capacidad.
- Proponer recomendaciones y acciones de mejora sobre los servicios, basado en las nuevas tendencias tecnológicas, planes de capacidad y consulta a expertos realizadas.
- Desarrollar un plan de capacidad para todos los servicios objeto del presente contrato como mínimo dos (2) veces al año, donde se evalúe el planteamiento de la suficiencia de la infraestructura del ICBF, así como la proyección y pertinencia de realizar nuevas adquisiciones o mejoras, en el cual se deben definir las actividades principales que se deben llevar a cabo para realizar una correcta gestión de la capacidad, dentro de las cuales se destacan: planear la capacidad, monitorear la infraestructura y realizar ajustes para optimizar los recursos y las buenas prácticas ITIL.
- Proponer y medir mensualmente los KPI ITIL (Gestión de Capacidad) del plan de capacidad desarrollado al inicio del contrato.
- Realizar ajustes al plan de capacidad cada tres (3) meses según los KPI medidos en los meses anteriores.
- Crear casos en la herramienta de gestión de las alertas por capacidad detectadas por el NOC al responsable del servicio.
- Implementar, actualizar y alimentar una herramienta de visualización para realizar

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

seguimientos a las alertas por capacidad detectadas por NOC.
- Las demás dentro del marco de buenas prácticas de ITIL.

7.2.5.4 **Gestoría de la Continuidad**

- Desarrollar un plan de continuidad para todos los servicios objeto del presente contrato como mínimo dos (2) veces al año, que incluya por lo menos: análisis BIA, diseño de contingencias por servicio, análisis de requisitos por contingencia, planes de recuperación, asignación de responsabilidades, plan de comunicación y socialización y pruebas del plan de continuidad.
- Revisar, validar, aprobar y actualizar semestralmente los Planes de Contingencia asociados a los servicios de la Dirección de Tecnología de la Información, incorporando nuevos escenarios de prueba y estrategias que permitan evaluar la efectividad, la capacidad de respuesta y los tiempos de recuperación ante posibles incidentes o interrupciones del servicio
- Identificar y clasificar la criticidad de las aplicaciones y bases de datos institucionales, y definir, documentar e implementar un plan de contingencia de aprovisionamiento específico para cada una, de acuerdo con su nivel de impacto en la operación y los tiempos objetivos de recuperación (RTO) y punto objetivo de recuperación (RPO) establecidos por la Entidad.
- Elaborar, documentar e implementar un Plan de Recuperación ante Desastres (DRP) para las aplicaciones SIM, Cuéntame, Kactus, ADA, Portal Institucional, y demás aplicaciones que se identifiquen como críticas para el negocio, con base en los resultados del Plan de Continuidad del Negocio y el Análisis de Impacto al Negocio (BIA), asegurando la definición del RTO (Tiempo Objetivo de Recuperación) y el RPO (Punto Objetivo de Recuperación) para cada aplicación. Así mismo, ejecutar y documentar pruebas semestrales del DRP, evaluando la efectividad de los procedimientos de recuperación, los tiempos de restablecimiento y las lecciones aprendidas, con el fin de realizar los ajustes y mejoras correspondientes.
- Identificar, evaluar, documentar y actualizar periódicamente los riesgos que afectan la continuidad de los servicios tecnológicos del Instituto, considerando amenazas internas y externas, vulnerabilidades técnicas, operativas y de infraestructura. Priorizar dichos riesgos según su probabilidad de ocurrencia e impacto potencial, definir controles existentes y estrategias de mitigación, e incorporarlos formalmente en la Gestión de Riesgos, garantizando su seguimiento y revisión continua.
- Actualizar el Plan de Continuidad y sus planes de contingencia cuando las modificaciones de la infraestructura modifiquen parcial o totalmente el plan.
- Revisar y ajustar la documentación existente en la entidad relacionada con la gestión de continuidad, identificando oportunidades de mejora y proponiendo los cambios necesarios alineados con las mejores prácticas
- Establecer y reportar mensualmente al ICBF un tablero de indicadores de gestión de continuidad que incluya, como mínimo: cumplimiento del RTO y RPO pactado

por cada servicios y aplicaciones porcentaje de pruebas de continuidad y DRP ejecutadas frente a las planificadas, tiempo de elaboración y entrega de informes post-incidente y post-prueba, y número de hallazgos abiertos frente a cerrados de las pruebas realizadas.

- Elaborar, documentar, socializar y mantener actualizado un Protocolo de Gestión de Crisis, que incluya como mínimo: criterios de activación y declaratoria de crisis, matriz de escalamiento por niveles de severidad e impacto, conformación y roles del Comité de Crisis (incluyendo participación del ICBF), canales y protocolos de comunicación interna y externa durante la contingencia, y mecanismo de desactivación y retorno a la operación normal. Este protocolo deberá ser probado como mínimo una (1) vez al año mediante un ejercicio de simulacro.
- Identificar los servicios, aplicaciones o componentes de infraestructura que dependan de proveedores externos (nube, telecomunicaciones, centros de datos, entre otros), y solicitar, validar y mantener actualizada la evidencia de los planes de continuidad y/o recuperación ante desastres de dichos terceros, verificando su alineación con los RTO/RPO definidos por el ICBF. Cualquier riesgo o brecha identificada en la continuidad de un tercero deberá reportarse al ICBF junto con el plan de mitigación correspondiente.
- Diseñar y ejecutar, con periodicidad mínima semestral, un programa de capacitación y sensibilización dirigido a los roles y responsables definidos en los planes de continuidad, contingencia y DRP, con el fin de garantizar su adecuada preparación para la activación y ejecución de dichos planes. Se deberá dejar evidencia de la asistencia, contenidos abordados y resultados de evaluación, si aplica.
- Las demás dentro del marco de buenas prácticas de ITIL v4 en la práctica de Gestión de la Continuidad de Servicios de TI, y ISO/IEC 22301 (Gestión de Continuidad de Negocio)

7.2.5.5 Gestoría de la Disponibilidad

- Desarrollar un plan de disponibilidad para todos los servicios objeto del presente contrato el cual debe ser entregado al terminar el primer mes desde el inicio el contrato, y ser actualizado de manera semestral, en el cual se deben definir las actividades principales a llevar a cabo para realizar una correcta gestión de la disponibilidad, junto con información detallada sobre iniciativas orientadas al mejoramiento del servicio y/o a hacer que los componentes estén disponibles. Buscando optimizar los recursos y las buenas prácticas ITIL.
- Realizar el seguimiento mensual al plan de disponibilidad, y presentar los resultados en el informe mensual de la gestoría de disponibilidad.
- Proponer y medir mensualmente los KPI ITIL (Gestión de la disponibilidad) del plan de disponibilidad desarrollado al iniciar el contrato, se debe realizar el ajuste al plan de acuerdo con los KPI medidos en los tres (3) meses siguientes al inicio del contrato y cada tres (3) meses hasta terminar el contrato.
- Implementar, actualizar y alimentar una herramienta de visualización para realizar

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

seguimientos a las alertas por disponibilidad detectadas por NOC.

- Crear casos en la herramienta de gestión de las alertas por disponibilidad detectadas por el NOC al responsable del servicio.
- Elaborar plan de mejora de la disponibilidad del servicio tomando en cuenta las necesidades actuales y futuras.
- Las demás dentro del marco de buenas prácticas de ITIL.

7.2.5.6 Gestoría de Seguridad de TI

- Realizar el cruce y la actualización de los usuarios en cada uno de los servicios versus Directorio Activo cada quince (15) días calendario. El Contratista debe garantizar que los usuarios desactivados, eliminados e inactivos no tengan ningún tipo de acceso a los servicios del ICBF.
- Realizar un plan de trabajo, ejecución y seguimiento para la implementación de las políticas, controles y recomendaciones que genere el Sistema de Gestión de Seguridad de la Información (SGSI) del ICBF, y realizar su verificación y efectividad en lo pertinente a la infraestructura tecnológica.
- Garantizar la protección y seguridad de los datos, programas, aplicaciones, bases de datos, infraestructura e información del ICBF velando por cumplir con los tres pilares de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).
- Realizar y documentar en conjunto con el ICBF los procedimientos para llevar a cabo la instalación de aplicativos y bases de datos o cualquier otro software en los equipos al servicio del ICBF.
- Realizar el acompañamiento al ICBF para la creación y/o revisión, implementación y divulgación de las políticas de seguridad de la información.
- Cumplir y dar a conocer a sus colaboradores las políticas, procedimientos, normas y responsabilidades en materia de seguridad definidas por el ICBF.
- El futuro oferente tendrá la responsabilidad de aplicar las mejores prácticas de configuración sobre las plataformas administradas y suministradas asegurándose de que el ICBF cuente con la implementación de estas mejores prácticas de seguridad sobre los servicios contratados.
- Documentar los procedimientos e instructivos críticos que se llevan a cabo para ejecutar la administración y gestión del servicio de seguridad, de manera articulada con los procedimientos del SIGE del ICBF.
- Dar un uso ético y protección a los accesos, contraseñas, información y recursos informáticos proporcionados por el ICBF, guardando estricta confidencialidad de la información sensible que pudiera llegar a manejar durante el desarrollo del presente contrato. Esto derivara en la firma de un acuerdo de confidencialidad.
- Notificar al ICBF, a través del Eje de Seguridad de la información (Gestor de Incidentes de Seguridad) y el líder de Seguridad Informática, cualquier incidente ocurrido sobre la infraestructura tecnológica.
- Realizar acciones de respuesta a incidentes o eventos de seguridad de la

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

información o cibersegruidad, en coordinación con el ICBF a través del Gestor de Incidentes de Seguridad del Eje de Seguridad de la información y el Líder de Seguridad Informática. Para ello, deberá generar mejoras al procedimiento de gestión de incidentes y un plan de respuesta que conlleve a su solución

- Analizar y documentar eventos de seguridad los cuales no clasifican como incidente de seguridad al no afectar la confidencialidad disponibilidad e integridad de la información y presentar un informe mensual consolidado de estos.
- Gestionar y proponer escenarios de pruebas para las actualizaciones de fabricantes que al ser implementadas generen algún tipo de impacto en la funcionalidad de las aplicaciones, herramientas desarrolladas por el ICBF o la infraestructura de la entidad y en caso de no ser aplicables plantear e implementar soluciones alternas.
- Cumplir y dar a conocer a sus colaboradores o personal contratado como recurso humano las políticas, procedimientos, normas y responsabilidades en materia de seguridad definidas por el ICBF.
- Presentar y documentar recomendaciones que propendan por la calidad y seguridad de la distribución de la información por los medios y canales electrónicos del ICBF en caso de requerirse.
- Guardar estricta reserva sobre toda la información y documentos que tenga acceso, maneje en desarrollo de su actividad o que llegue a conocer en desarrollo del contrato y que no tenga carácter de pública. En consecuencia, se obliga a no divulgar por ningún medio dicha información o documentos a terceros, sin la previa autorización escrita del ICBF.
- Implementar y documentar el procedimiento para el manejo, actividades y protocolos para la custodia y entrega de las contraseñas de administración. Estos procedimientos de custodia aplican para todos aquellos casos donde el Contratista haga uso de cuentas y contraseñas de administración de las herramientas usadas para el cumplimiento de los servicios incluidos en el alcance de este proceso de selección, ejemplo, el firewall, consolas de antivirus, bases de datos, aplicativos, IPS/IDS, Correo, Proxy, PC y Servidores.
- Definir, realizar seguimiento y verificación de guías que contengan parámetros técnicos de aseguramiento orientado a sistemas operativos, servidores web, aplicaciones, bases de datos y servicios en internet, con el fin de prevenir ataques y definir mecanismos de endurecimiento para preservar la disponibilidad, confidencialidad e integridad de la información de ICBF.
- Realizar acompañamiento en la implementación, mantenimiento y operación del SGSI del ICBF
- Alinear sus procesos al Sistema de Gestión de la Seguridad de la Información SGSI establecido en el ICBF y acatar todas las acciones y recomendaciones que de él se deriven.
- Notificar al ICBF, a través del líder de Seguridad Informática, cualquier incidente ocurrido sobre la infraestructura tecnológica, realizando la debida documentación de gestión del incidente.
- Realizar acciones de respuesta a incidentes o eventos de seguridad de la

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

información o ciberseguridad, en coordinación con el ICBF a través del Líder de Seguridad Informática. Para ello, deberá generar mejoras al procedimiento de gestión de incidentes y un plan de respuesta que conlleve a su solución.

- Gestionar una base de conocimiento con los eventos y resultados de la gestión de seguridad incluyendo todos los eventos de los servicios de seguridad contratados, esta base deberá estar vigente durante toda la vigencia del servicio y ser entregada al ICBF para los fines que la entidad disponga.
- Definir e implementar procedimientos y proponer políticas para ejecución de análisis forenses.
- Ejecutar análisis forenses y presentar los informes correspondientes, por demanda o cuando la Entidad así lo requiera, como parte de las obligaciones contractuales y sin que ello genere costos adicionales para la Entidad.
- Las demás dentro del marco de buenas prácticas.

7.2.5.7 Gestoría de Riesgos

- Elaborar semestralmente y llevar seguimiento mensual al Plan de identificación y gestión de riesgos de los servicios y gestorías, el cual debe incluir la identificación de riesgos, la evaluación del riesgo inherente, los controles existentes y su nivel de efectividad, los correspondientes planes de tratamiento, remediación y planes de contingencia, así como la valoración del riesgo residual en términos de la probabilidad de ocurrencia y del impacto en caso de materialización. Su seguimiento se realizará en la mesa técnica de gestión de riesgos, con presentación en el comité operativo y evaluación en el comité ejecutivo
- La gestión de riesgos deberá realizarse conforme a las mejores prácticas y lineamientos de las normas ISO/IEC 27001:2022 (Sistemas de Gestión de Seguridad de la Información) e ISO/IEC 27005:2022 (Gestión de Riesgos de Seguridad de la Información), en lo relativo a la metodología de identificación, análisis, evaluación y tratamiento de riesgos, así como a la determinación del riesgo residual frente al apetito y tolerancia al riesgo definidos por el ICBF. Esta articulación deberá evidenciarse en la metodología documentada de la matriz de riesgos de seguridad de la información y los lineamientos de la Guía de Riesgos y Peligros de la Entidad
- Presentar dentro de los 15 días posteriores a la fecha de inicio de ejecución del contrato, la matriz de identificación de riesgos del proyecto para cada una de las etapas de transición de entrada, operación y transición de salida.
- Elaborar, dentro de los 30 días siguientes al inicio de ejecución del contrato, un Plan de Trabajo para la implementación de la metodología de gestión de riesgos y la sensibilización de los responsables de los servicios y gestorías objeto del contrato, el cual deberá incluir como mínimo: cronograma de actividades, colaboradores objetivo, mecanismos y canales de sensibilización, contenidos a socializar, y responsables de su ejecución y seguimiento. Este plan deberá actualizarse cuando se presenten cambios relevantes en la metodología, en los servicios contratados o

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

en los responsables designados

- Elaborar semestralmente un Plan de Mejoramiento de la Gestoría de Riesgos, con seguimiento mensual a su ejecución, orientado a fortalecer la madurez, eficiencia y efectividad del proceso de gestión de riesgos (metodología, herramientas, articulación con las demás gestorías y calidad de la información reportada), a partir de los resultados obtenidos en los comités operativos, las lecciones aprendidas y los hallazgos de auditorías o verificaciones realizadas
- Realizar el análisis cuantitativo y cualitativo de los riesgos identificados, aplicando una metodología documentada, con el fin de determinar su valoración de riesgo inherente y de riesgo residual, en términos de probabilidad de ocurrencia e impacto, conforme a las escalas y criterios definidos en la guía de riesgos y peligros del ICBF. Este análisis deberá actualizarse como mínimo con cada actualización mensual de la matriz de riesgos
- Realizar identificación de herramientas o instrumentos de control como parte del tratamiento de riesgos.
- Realizar seguimiento mensual al cumplimiento de los controles existentes y actividades de los planes de tratamiento de riesgos identificados en los servicios y gestorías, de acuerdo con la periodicidad establecida en la matriz de riesgos para cada uno de estos.
- Elaborar y mantener actualizado el análisis de riesgos asociado a la infraestructura tecnológica que soporte la adecuada prestación de los servicios objeto del contrato, con base en el inventario de activos clasificados por criticidad, identificando las amenazas y vulnerabilidades aplicables, e incorporando dicho análisis en la matriz de riesgos del proyecto
- Informar los riesgos de operatividad, seguridad y degradación del servicio identificando puntos críticos y definiendo e implementando acciones previa autorización del ICBF, e incluirlos en el Plan de Riesgos.
- Proponer medidas de control para el tratamiento de riesgos que no generen costos adicionales para la Entidad con el máximo aprovechamiento de los recursos disponibles.
- Reportar, gestionar y documentar las materializaciones de riesgos que se presenten y que afecten la integridad, disponibilidad y/o confidencialidad de los servicios de TI contratados, para lo cual deberán seguir el procedimiento de atención de incidentes de seguridad de la información y la Guía de Gestión de Riesgos y Peligros (Gestión de Riesgos de Seguridad de la Información, Seguridad Digital y Continuidad del Negocio) definidas por el ICBF.
- Las demás dentro del marco de buenas prácticas de ITIL.
- Identificar, documentar y socializar las lecciones aprendidas resultantes de la gestión de cambios, particularmente frente a riesgos significativos o materializados, incluyendo el análisis de causas raíz, impacto generado y efectividad de los controles aplicados, con el propósito de implementar acciones de mejora e incluir en la matriz de riesgos.
- Reportar mensualmente indicadores de gestión que incluyan, como mínimo: número

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

de riesgos identificados vs. tratados, porcentaje de controles implementados frente a los planificados, riesgos materializados en el periodo, y tiempo promedio de cierre de planes de tratamiento, como insumo para el comité operativo

- Identificar y evaluar los riesgos asociados a proveedores, fabricantes o terceros de los cuales dependan los servicios contratados, incluyéndolos en la matriz de riesgos e informando al ICBF cualquier riesgo relevante derivado de dicha dependencia
- Realizar capacitaciones o sensibilizaciones mínimo de manera cuatrimestral en gestión de riesgos dirigidas a los responsables de los servicios y gestorías, dejando evidencia de asistencia y contenidos presentados
- Mantener un histórico versionado de la matriz de riesgos que permita evidenciar su evolución, los cambios en la valoración de cada riesgo y las justificaciones correspondientes, disponible para consulta del ICBF en cualquier momento.

7.2.5.8 Gestoría de Nivel de Servicio

- Garantizar la medición técnica, el monitoreo continuo y el seguimiento analítico de los Acuerdos de Nivel de Servicio (ANS) para la totalidad de los servicios TIC objeto del contrato. Esta gestión deberá realizarse obligatoriamente mediante herramientas de gestión y monitoreo que aseguren la trazabilidad inalterable, veracidad y disponibilidad de los datos. El Contratista será responsable de la entrega oportuna de los informes de cumplimiento mensuales, los cuales servirán como soporte técnico e insumo vinculante para la certificación del servicio y los procesos de pago correspondientes.
- Elaborar y ejecutar un Plan de Trabajo, sujeto a la aprobación previa de la supervisión del contrato, para la implementación, socialización y sensibilización del Modelo de Gestión de ANS. Este plan deberá contener objetivos medibles, detallar el cronograma de hitos operativos, la metodología pedagógica de capacitación y los mecanismos de evaluación que certifiquen la transferencia efectiva de conocimiento a los actores clave definidos por el ICBF. El cumplimiento de esta obligación se acreditará mediante la entrega de soportes verificables, actas de capacitación y la documentación de los procesos socializados
- Apoyar Activamente y asegurar de manera integral la configuración, parametrización y actualización de los ANS en la herramienta de Mesa de Servicios (ITSM) y en las plataformas de monitoreo y seguridad vigentes. En su rol de Gestoría, el Contratista será el responsable técnico de garantizar la alineación absoluta entre las definiciones contractuales y la ejecución en las herramientas. Para ello, presentará un informe mensual técnico que certifique los umbrales de cumplimiento configurados y las reglas de escalamiento aplicadas, adjuntando evidencias inalterables (logs de sistema, registros de configuración o capturas de pantalla) que validen la confiabilidad de la medición para la totalidad de los servicios objeto del contrato.
- El Contratista se compromete a Garantizar el acceso inmediato, irrestricto y sin excusa alguna a la totalidad de las herramientas de gestión, bases de datos,

registros de actividad (logs) y archivos de configuración que soportan la medición de los niveles de servicio. El Contratista, en su calidad de Gestoría, asegura que dichos insumos estarán disponibles en su estado original y sin alteración alguna. El incumplimiento, dilación o cualquier forma de obstrucción a esta obligación será calificado como un incumplimiento grave del contrato, dando lugar a la aplicación de las multas y sanciones previstas en la cláusula penal pecuniaria

- Elaborar, entregar y actualizar mensualmente el Plan de Mejora y Cronograma de Actividades de la gestoría de ANS, evaluando mensualmente la eficacia del plan, mediante indicadores de impacto que comparen el desempeño del servicio antes y después de su implementación. Este documento debe contener objetivos medibles y realistas, detallar mediante un cronograma las actividades, responsables, fechas de ejecución, evidencias de cumplimiento y las rutas de acceso a la evidencia en el repositorio oficial del ICBF, permitiendo la verificación inmediata de los entregables reportados, una vez aprobado por la supervisión del contrato deberá ser de obligatorio cumplimiento.
- Con el objeto de que el ICBF pueda realizar los respectivos seguimientos y definir los no pagos a que haya lugar por el no complimiento de los ANS, se requiere que el Contratista genere y presente dentro de los primeros cinco (5) días hábiles de cada mes, un informe de ANS mensual para cada uno de los servicios, dado que a partir de la verificación de este informe y mediante las herramientas de monitoreo, seguridad y/o gestión se realizarán los seguimientos mensuales. El informe de ANS debe contener las estadísticas de cálculo y especificar el comportamiento de cada ANS discriminado por servicio
- Ejecutar un análisis mensual de la tendencia histórica de los ANS con el fin de identificar desviaciones, riesgos de incumplimiento o degradaciones progresivas en la calidad del servicio. En coordinación técnica con el área de calidad del ICBF, el Contratista deberá formular, implementar y reportar el estado de avance de los planes de acción orientados a la mitigación de riesgos y la optimización del servicio. El resultado de esta gestión se consolidará de manera obligatoria en un 'Capítulo de Mejora Continua' dentro del informe mensual de servicios, cuya ejecución será objeto de verificación y calificación por parte de la supervisión
- Este seguimiento continuo será en tiempo real donde se mostrará el desempeño operativo de los servicios frente a los ANS pactados, utilizando las herramientas de monitoreo definidas. El Contratista deberá alertar de manera inmediata a la supervisión del contrato sobre cualquier desviación o tendencia que ponga en riesgo el cumplimiento de los niveles de servicio
- Para los casos de indisponibilidad originados por incidentes sobre equipos (hardware) de propiedad del ICBF que no cuenten con soporte y garantía o que presenten obsolescencia tecnológica el contratista deberá restablecer el servicio con las habilidades del recurso humano que dispone y con recursos de hardware de propiedad del ICBF, a excepción de aquellos casos en que la Ficha de condiciones técnicas indique el contratista debe proporcionar repuestos. Adicionalmente debe presentar el informe respectivo con el cual se soportará con evidencia técnica la

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

excepción de las penalizaciones por Acuerdos de Nivel de Servicios con la debida evidencia de que la causa del no cumplimiento de cada ANS a excepcionar es ajena a las obligaciones del contratista

- Revisar Trimestralmente si los ANS establecidos no reflejan la calidad de cada uno de los servicios requeridos por el ICBF, estos serán replanteados, validados y aplicados de común acuerdo entre ICBF y el Contratista. Para ello, los ANS y su forma de medición podrán ser revisados cada tres (3) meses o cuando las necesidades del servicio así lo requieran. Cuando se presente una modificación o inclusión de un ANS este tendrá dos (2) meses de estabilización, periodo durante el cual no presentarán penalización.
- Estos ajustes o mejoras a los indicadores de ANS que se identifique que no responden a las necesidades estratégicas u operativas del ICBF, deberá estar sustentada con evidencias sólidas (análisis técnico, histórico de datos y evaluación de impacto) y será sometida a revisión de la supervisión, quien determinará su viabilidad y formalización mediante el instrumento jurídico o técnico que corresponda.
- Ejecutar pruebas de certificación iniciales y periódicas que validen la exactitud y confiabilidad en la medición de los ANS. El Contratista deberá entregar un informe técnico de resultados, debidamente firmado, que demuestre la trazabilidad del dato desde la ocurrencia del evento hasta su visualización en el reporte final. Estas pruebas deberán ser aprobadas por la supervisión del contrato
- Presentar, dentro de los primeros cinco (5) días hábiles de cada mes, el informe detallado de excepciones a los ANS ocurridas en el mes inmediatamente anterior. Este documento debe incluir la justificación técnica de cada evento y las evidencias verificables y solidas que demuestren la ajenidad del contratista. El informe deberá cumplir con los estándares de calidad del proyecto. En caso de no presentarse, entregarse fuera de tiempo o no ser aprobado por la supervisión, se procederá con la aplicación íntegra de los descuentos definidos en el Anexo 02 (ANS).
- Realizar la medición de los ANS por mes calendario, desde las 00:00:00 horas del primer día hasta las 23:59:59 horas del último día del mes en análisis, conforme a la hora legal de la República de Colombia. Esta ventana de tiempo será la base única para el cálculo de disponibilidad, informes mensuales y aplicaciones de descuentos
- Entregar los soportes técnicos originales, extraídos directamente de las herramientas de gestión y monitoreo, que garanticen la trazabilidad, integridad y verificación de la disponibilidad reportada. El Contratista deberá asegurar que estos soportes permitan auditar los tiempos de inicio y fin de cada evento de indisponibilidad para cada servicio objeto del contrato
- Para cada uno de los incidentes asociados a los tiempos de indisponibilidad, el contratista debe entregar la siguiente información: número de caso, fecha y hora de ocurrencia, fecha y hora de solución, descripción del incidente, sus causas y solución. En la descripción de las causas se debe incluir si el incidente se atribuye o no al Contratista, en este último caso se deben presentar evidencias técnicas que

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

demuestren si el evento es atribuible a su gestión o a factores externos; de lo contrario, el evento se contabilizará para el cálculo de descuentos por ANS.

- Liderar mesas de articulación mensual con otras gestorías, especialistas del proveedor, realizando la citación formal con al menos tres (3) días de antelación. El objetivo será proponer y ejecutar mejoras transversales que optimicen el cumplimiento de los ANS globales. El Contratista deberá radicar mensualmente ante la supervisión las actas de compromiso firmadas y el acceso a las grabaciones de las sesiones dentro de los primeros cinco (5) días.
- Elaborar, actualizar y mantener permanentemente la documentación técnica, manuales de procedimiento, instructivos y políticas asociadas a la gestión y medición del servicio. Toda la documentación deberá seguir los estándares de calidad y gestión documental del ICBF, y deberá ser entregada en formatos editables y PDF en el repositorio designado, garantizando su actualización oportuna ante cualquier cambio en la realidad operativa del servicio, en un plazo no mayor a cinco (5) días hábiles de ocurrida la modificación
- Mantener actualizada la gestión documental de la gestoría en el repositorio institucional designado por el ICBF, siguiendo los lineamientos de su sistema de gestión de calidad, el plan documental
- Generar, ejecutar y documentar acciones correctivas cada vez que se presente una afectación al cumplimiento de los ANS. Dichas acciones correctivas deben cumplir con el estándar de la norma ISO 9001 vigente.
- Las demás dentro del marco de buenas prácticas de ITIL.

7.2.5.9 Gestoría de Cambios

- Elaborar y ejecutar el Plan de Trabajo de Implementación y Sensibilización de Procesos y procedimientos.
- Llevar el registro de los controles de cambios para las actividades que afecten los ambientes administrados en la herramienta dispuesta por el ICBF.
- Llevar el inventario general de todos los cambios gestionados durante la ejecución del contrato y presentar los Cambios realizados en el mes anterior. Se debe entregar los cinco (5) primeros días hábiles del mes.
- Generar, documentar, validar, aprobar y asesorar los controles de cambio que se presenten relacionados a los servicios, dimensionando las ventanas de mantenimiento, tiempos de indisponibilidad, planes de contingencia, rollback, identificación y mitigación de los posibles riesgos, de acuerdo con los procedimientos ya establecidos por el comité de control de cambios del ICBF.
- Gestionar en la herramienta de gestión de mesa de servicio que disponga el ICBF los tickets asignados referentes a incidentes, requerimientos y controles de cambios de los diferentes servicios a cargo del Contratista. Esta gestión de tickets consiste en la consulta, documentación de trámite, solución y cierre de los mismos.
- Llevar el registro de los controles de cambios para las actividades que afecten los ambientes administrados.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Documentar, mantener actualizada y entregar al final del contrato o cuando se requiera, en formatos acordados con el ICBF, la base de datos del conocimiento y de configuraciones en cada servidor de base de datos: Gestión de configuración, Gestión de problemas, Gestión de cambios entre otras.
- Tramitar por el gestor de cambio, todo cambio que se ejecute sobre la Infraestructura y servicios de TIC de acuerdo con el procedimiento de Gestión de Cambios.
- Las demás dentro del marco de buenas prácticas de ITIL.

7.2.5.10 Gestoría de Requerimientos

- Generar planes de trabajo para la implementación efectiva de la Gestion de Requerimientos en la institución.
- Gestionar y documentar los requerimientos en la herramienta definida por la institución con su información pertinente y en los tiempos establecidos.
- Realizar el seguimiento a la atención, solución y documentación de los requerimientos registradas en la herramienta de gestión que disponga la institución.
- Realizar el seguimiento al “backlog” de los requerimientos y gestionar con los responsables su atención y solución.
- Realizar seguimiento a los casos reabiertos y coordinar con la Gestión de Calidad para su respectivo tratamiento.
- Definir en conjunto con los demás servicios incluidos en el contrato y con la institución, los criterios de suspensión de los requerimientos y hacer el seguimiento a los mismos para garantizar un servicio oportuno con:

  a) Generar y presentar un (1) informe consolidado de la gestión mensual de requerimientos, incluyendo: estadísticas de los casos registrados en la herramienta de gestión: por servicios, estado y cumplimiento de los ANS de acuerdo con el Anexo 02 - Acuerdos de Niveles de Servicio.

  b) Documentar y presentar a la institución, planes de mejora durante la vigencia del contrato. Realizar la ejecución de los planes y presentar el porcentaje de avance mensual.

  c) Presentar recomendaciones al Supervisor del contrato con el fin de contar con la mejora continua de la gestoría.

  d) Generar mesas de articulación con las demás gestorías y servicios para proponer mejoras conjuntas que permitan hacer seguimiento al desempeño de la Gestoría de Requerimientos.

  e) Mantener actualizada la documentación de la gestoría en el repositorio definido por la institución.

  f) Garantizar la confidencialidad de los datos y la información relativa a las solicitudes gestionadas.

  g) Aplicar las buenas prácticas ITIL de acuerdo con su versión vigente
- Las demás funciones requeridas por la institución y relacionadas con el objeto del contrato.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

7.2.5.11 Gestoría de Incidentes

- Generar planes de trabajo para la implementación efectiva de la Gestión de Incidentes en la institución.
- Gestionar y documentar los incidentes en la herramienta definida por la institución con su información pertinente y en los tiempos establecidos.
- Notificar a la institución de cualquier incidente, anomalía o alerta que afecte la prestación de algún servicio tecnológico, a través de correo electrónico y/o teléfono u otro medio disponible; según la hora de aparición del incidente y actuar proactivamente en la búsqueda y aplicación de la solución, con el objetivo de minimizar el impacto. Todo incidente debe quedar registrado en la herramienta de gestión de la institución.
- Revisar en la base de conocimiento con el fin de aplicar la respectiva retroalimentación del incidente presentado y minimizar el impacto en la disponibilidad de los servicios objeto del contrato. En caso de que el incidente no se encuentre en la base de conocimiento, debe gestionarse a través de la Gestoría de Incidentes conforme al procedimiento de la institución.
- Realizar la gestión con terceros de incidentes que así lo requiera, previa autorización de la institución.
- Restablecer y minimizar impactos en los servicios afectados de cara a los usuarios.
- Seguimiento continuo de errores, fallas, anomalías y alertas con el fin de mejorar la disponibilidad general de los servicios.
- Actualizar la base de conocimiento de incidentes conforme se presenten y solucionen, durante el tiempo de ejecución del contrato.
- Actuar proactivamente en la búsqueda y aplicación de soluciones, con el objetivo de minimizar el impacto de cualquier incidente.
- Identificar y documentar claramente la causa raíz del incidente previo a su escalamiento y determinar cuándo se puede convertir en un problema; frente a lo cual, se deberá escalar a la Gestoría de Problemas junto con la propuesta de tratamiento de la causa raíz, con el fin de mitigar la reiteración del incidente. Generar y presentar informe de gestión mensual donde se evidencie como mínimo: el estado actual de la gestoría, las actividades realizadas, estadísticas del comportamiento de los incidentes, estado de estos y oportunidades de mejora identificadas, etcétera.
- Generar mesas de articulación con las demás gestorías y servicios para proponer mejoras conjuntas, que permitan hacer seguimiento al desempeño de la gestoría.
- Mantener actualizada la documentación de la gestoría en el repositorio definido por la institución.
- Asignar categorías y prioridades a los incidentes para asegurar que se manejen de manera eficiente y según su impacto en la institución con:
    A. Detección y registro de incidentes: identificar y registrar todos los incidentes reportados por los usuarios o detectados por cualquier sistema de monitoreo.
    B. Categorizar y priorizar: asignar categorías y prioridades a los incidentes para asegurar que se manejen de manera eficiente.
    C. Diagnóstico inicial: realizar un diagnóstico preliminar para intentar resolver

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

el incidente en el primer nivel de soporte.

D. Escalar: si el incidente no puede ser resuelto en el primer nivel, escalarlo al equipo o especialista adecuado.
E. Investigación y diagnóstico: llevar a cabo una investigación profunda para identificar la causa raíz del incidente y aplicar una solución adecuada.
F. Resolución y recuperación: implementar la solución y restaurar el servicio a su estado normal de operación.
G. Cierre del incidente: asegurar de que el incidente esté completamente resuelto; documentar todos los pasos tomados y cerrar el registro del incidente.
H. Comunicación: mantener informados a los usuarios y partes interesadas sobre el estado y progreso de sus incidentes.
I. Mejora continua: analizar los incidentes resueltos para identificar tendencias y áreas de mejora en la gestión de incidentes.
J. Aplicar las buenas prácticas ITIL de acuerdo con su versión vigente.

- Las demás funciones requeridas por la institución y relacionadas con el objeto del contrato.

7.2.5.12 Gestoría de Inventarios, CMDB y Garantías

- Identificar, registrar y verificar los elementos de configuración CIs (hardware, software, servicios, documentación, redes) y sus interrelaciones.
- Controlar los CIs desde su adquisición hasta su eliminación o reasignación, con la ayuda de la herramienta de gestión definida por la institución.
- Realizar seguimiento/auditorías periódicas para asegurar que los datos en la CMDB coinciden con la infraestructura física y lógica real, garantizando la integridad de la base de datos.
- Implementar herramientas que escaneen la red para mantener el inventario de la CMDB actualizado y veraz.
- Manejar avanzado las diferentes herramientas ofimáticas.
- Asegurar que los datos de configuración cumplan con las políticas de seguridad de la institución y normativas vigentes.
- Generar tableros de control y reportes que ayuden a la institución a tomar decisiones sobre renovaciones tecnológicas, presupuestos y optimización de recursos.
- Monitorear las entradas y salidas de equipos (cómputo, servidores, licencias, switches, etcétera) en tiempo real; en coordinación con el Grupo de Almacén e Inventarios de la institución
- Realizar el seguimiento desde la adquisición hasta la disposición final; incluyendo la instalación, mantenimiento, actualización y eliminación segura de componentes tecnológicos.
- Coordinar reparaciones, mejoras de hardware y actualizaciones de software para prolongar la vida útil de los elementos tecnológicos.
- Gestionar el retiro seguro de equipos obsoletos, asegurando la eliminación correcta

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

de datos y el cumplimiento de normativas ambientales.

- Administrar el proceso de garantía de los productos/servicios tecnológicos de la institución; desarrollar e implementar políticas y procedimientos de garantía, garantizar el cumplimiento de las leyes y regulaciones pertinentes, y gestionar las reclamaciones y reparaciones en garantía en caso de fallas o daños de manera oportuna.
- Registrar las garantías, realizar un seguimiento de las fechas de caducidad, iniciar reclamos y rastrear las reparaciones o sustituciones que se encuentran bajo garantía.
- Aplicar las buenas prácticas ITIL de acuerdo con su versión vigente.
- Las demás funciones requeridas por la institución y relacionadas con el objeto del contrato.

7.2.5.13 Gestoría de Problemas

- Gestionar, notificar y documentar los problemas en la herramienta definida por la institución con su información pertinente y en los tiempos establecidos.
- Ejecutar y registrar la gestión realizada frente a cualquier problema y cumplir con el escalamiento según lo especificado en su procedimiento.
- Evaluar cualquier problema hasta identificar su causa raíz; proponiendo e implementando soluciones efectivas para minimizar su impacto.
- Realizar seguimiento a las soluciones implementadas con el fin de validar si la solución fue efectiva en la resolución del problema.
- Analizar y evaluar los incidentes postulados por la institución como problema.
- Diligenciar la documentación y presentar medición de resultados de las soluciones implementadas con el fin de finalizar o cerrar los problemas.
- Proponer y ejecutar mejoras al procedimiento de Gestión de Problemas para optimizar los tiempos de resolución de problemas que se presenten en la ejecución del contrato.
- Realizar articulación con la Gestión de Conocimiento, para los problemas solucionados con causa raíz, incluyendo documentación de soluciones implementadas y su respectiva creación en bases de datos de conocimiento.
- Mantener registros detallados de los problemas y sus soluciones y comunicar el estado y progreso a las partes interesadas.
- Aplicar las buenas prácticas ITIL de acuerdo con su versión vigente.
- Las demás funciones requeridas por la institución y relacionadas con el objeto del contrato

7.2.5.14 Gestoría de Portafolio, Catálogo de Servicios y Conocimiento

- Administrar y mantener actualizado el Catálogo de Servicios del ICBF, incluyendo la información funcional, técnica y operativa de los servicios ofrecidos por la Dirección de Tecnologías de la Información.

- Documentar, revisar y actualizar las fichas de servicio que conforman el Catálogo de Servicios, incluyendo como mínimo: nombre del servicio, descripción, alcance, usuarios objetivo, canales de atención, horarios de atención, requisitos, responsables, ANS asociados, restricciones, prerequisitos y procedimientos relacionados.
- Garantizar que el Catálogo de Servicios esté alineado con los servicios contratados, la línea base del servicio, el modelo operativo, los acuerdos de niveles de servicio, los procedimientos de Mesa de Servicio y las mejores prácticas ITIL vigentes.
- Gestionar el ciclo de vida de los servicios dentro del Catálogo, asegurando el registro, modificación, actualización, retiro o suspensión de servicios, previa validación y aprobación del ICBF.
- Coordinar con los líderes de servicio, gestores ITIL, Mesa de Servicio y equipos técnicos la identificación de cambios, ajustes o nuevas necesidades que deban ser incorporadas en el Catálogo de Servicios o en la Base de Conocimiento.
- Administrar y mantener actualizada la Base de Conocimiento, garantizando que contenga artículos, guías, procedimientos, instructivos, preguntas frecuentes, soluciones conocidas, errores conocidos, manuales y demás documentación requerida para apoyar la atención, diagnóstico y solución de incidentes, requerimientos y solicitudes de servicio.
- Asegurar que la Base de Conocimiento sea clara, útil y reutilizable, orientada tanto al personal técnico como a los agentes de Mesa de Servicio y, cuando aplique, a los usuarios finales del ICBF.
- Definir, implementar y mantener un procedimiento para la creación, revisión, aprobación, publicación, actualización y retiro de artículos de conocimiento, garantizando trazabilidad, control de versiones y responsables definidos.
- Identificar oportunidades de generación de conocimiento a partir de incidentes recurrentes, problemas, requerimientos frecuentes, cambios implementados, errores conocidos, solicitudes de usuarios, lecciones aprendidas y actividades de operación.
- Promover el uso de la Base de Conocimiento por parte de la Mesa de Servicio y los equipos técnicos, con el fin de mejorar los tiempos de atención, aumentar la resolución en primer contacto y reducir la recurrencia de incidentes y solicitudes.
- Realizar revisiones periódicas de calidad y vigencia sobre los artículos de conocimiento y fichas del Catálogo, eliminando información obsoleta, duplicada, incompleta o inconsistente.
- Entregar reportes periódicos sobre la gestión del Catálogo y Conocimiento, incluyendo como mínimo: número de artículos creados, actualizados, retirados, consultados, servicios actualizados, brechas identificadas, acciones de mejora y estado de avance de las actividades.
- Apoyar la transferencia de conocimiento durante las etapas de transición de entrada, operación y transición de salida, garantizando la entrega organizada y documentada de la información técnica, funcional y operativa requerida para la continuidad del servicio.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Mantener actualizada la documentación asociada a procedimientos, manuales, instructivos, matrices, formatos y guías operativas, asegurando su disponibilidad para el ICBF y para los equipos responsables de la operación.
- Asegurar la trazabilidad de la información documentada, identificando fecha de creación, fecha de actualización, responsable, versión, estado de aprobación y dependencia o servicio relacionado.
- Participar en las mesas de trabajo, comités o espacios definidos por el ICBF relacionados con la actualización del Catálogo de Servicios, gestión documental, transferencia de conocimiento, mejora continua y operación de servicios .
- Apoyar la mejora continua de los servicios de DTI mediante el análisis de información documentada, tendencias de uso, solicitudes frecuentes, oportunidades de automatización, simplificación de trámites y mejora de la experiencia del usuario.
- Garantizar que la información publicada en el Catálogo y en la Base de Conocimiento cumpla con criterios de claridad, oportunidad, completitud, seguridad, confidencialidad y pertinencia, de acuerdo con los lineamientos definidos por el ICBF.
- Articular la gestión de conocimiento con los procesos de incidentes, requerimientos, problemas, cambios, configuración, disponibilidad, niveles de servicio y continuidad, asegurando que la información generada en dichos procesos sea aprovechada para fortalecer la operación.
- Entregar a la finalización del contrato la totalidad de la documentación, artículos de conocimiento, fichas de servicio, matrices de control, reportes, evidencias y repositorios organizados, garantizando la continuidad operativa y la transferencia adecuada al ICBF o al nuevo operador.

7.2.5.15 Gestoría de Calidad

- El Contratista deberá ejecutar y documentar el proceso integral de monitoreo de llamadas. Esta obligación incluye: (i) la identificación de la totalidad de llamadas entrantes y salientes atendidas en la semana inmediatamente anterior; (ii) la definición de una muestra representativa para auditar conforme a los niveles pactados; (iii) la ejecución de la auditoría técnica bajo los procesos establecidos; y (iv) la consolidación de resultados, incluyendo hallazgos y observaciones detalladas para su entrega semanal. Asimismo, será responsable de la formulación y seguimiento de un plan de mejora en caso de detectarse desviaciones críticas que afecten los Servicios, garantizando la implementación de las acciones correctivas a que haya lugar
- El Gestor deberá administrar y supervisar la integridad documental de los incidentes, requerimientos y problemas. Esta obligación comprende: (i) la determinación de la muestra a auditar según los criterios de representatividad definidos en el Anexo 02 (ANS) para los Niveles I, II; (ii) el análisis técnico de la documentación y de la gestión operativa de los casos; y (iii) la consolidación de hallazgos mediante informes de auditoría que incluyan observaciones detalladas. Asimismo, deberá ejecutar el seguimiento y control permanente sobre los indicadores de calidad del servicio para

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

asegurar el cumplimiento de los estándares pactados y la mejora continua del servicio.

- El Gestor realizará auditorías mensuales aleatorias sobre la documentación técnica del Nivel III, verificando el cumplimiento de:
    - **Transparencia Técnica:** Asegurar que los diagnósticos, soluciones y análisis de causa raíz (RCA) cuenten con el soporte evidenciable en la herramienta ITSM y las bases de conocimiento.
    - **Transferencia de Conocimiento:** Validar que los procedimientos de solución estén estandarizados para garantizar su transferencia efectiva hacia otros niveles de soporte.
- El Gestor de Calidad será responsable de identificar y analizar las encuestas de evaluación de la satisfacción para los Niveles I, II, obligándose a:
    - **Identificación:** Consolidar la totalidad de encuestas resueltas en el periodo de gestión, así mismo clasificando aquellas encuestas con resultados inferiores al umbral de calificación definido en el Anexo 02 (Acuerdo de Niveles de Servicio).
    - **Intervención:** Gestionar de forma proactiva las encuestas negativas mediante el contacto directo con el usuario final para determinar la causa raíz de la insatisfacción.
    - **Resolución:** Coordinar con el área técnica o servicio involucrado la ejecución de una solución inmediata al requerimiento del usuario.
    - **Trazabilidad:** Documentar el resultado de la gestión, la solución brindada y el estado final de satisfacción en los registros oficiales de control.
- El Contratista será responsable de liderar la creación, actualización y mejora continua de los activos de conocimiento de los niveles I, II y III. Esta obligación incluye la gestión integral de procedimientos, políticas, guías, instructivos, plantillas y scripts operativos. Dicha labor deberá realizarse de manera articulada con los líderes de cada servicio, garantizando que toda la documentación técnica y de gestión esté alineada con los estándares de calidad vigentes, las necesidades operativas de la Gestoría y que se encuentre disponible y socializada con el personal asistencial correspondiente.
- El Contratista será responsable de la administración del ciclo completo de Peticiones, Quejas, Reclamos, Sugerencias y Felicitaciones (PQRSF) recibidas a través de los canales oficiales. Esta obligación incluye:
    - (i) la clasificación técnica y el análisis de causa raíz.
    - (ii) el tratamiento y trámite conforme a los términos legales y contractuales vigentes.
    - (iii) la emisión de respuestas de fondo que aseguren la solución efectiva de la solicitud.
- El Gestor deberá garantizar que cada interacción esté debidamente documentada y orientada a la satisfacción final del usuario, en estricto cumplimiento del objeto del contrato
- Elaborar y ejecutar un Plan de Trabajo, sujeto a la aprobación previa de la

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

supervisión del contrato, para la implementación, socialización y sensibilización del Modelo de Gestión de Calidad. Este plan deberá contener objetivos medibles, detallar el cronograma de hitos operativos, la metodología pedagógica de capacitación y los mecanismos de evaluación que certifiquen la transferencia efectiva de conocimiento a los actores clave definidos por el ICBF. El cumplimiento de esta obligación se acreditará mediante la entrega de soportes verificables, actas de capacitación y la documentación de los procesos socializados

- Elaborar, entregar y actualizar mensualmente el Plan de Mejora y Cronograma de Actividades de la gestoría de Calidad. Este documento debe contener objetivos medibles y realistas, detallar mediante un cronograma las actividades, responsables, fechas de ejecución, evidencias de cumplimiento y las rutas de acceso a la evidencia en el repositorio oficial del ICBF, permitiendo la verificación inmediata de los entregables reportados, una vez aprobado por la supervisión del contrato deberá ser de obligatorio cumplimiento.
- Presentar, dentro de los primeros cinco (5) días hábiles de cada mes, un Informe de la Gestoría de calidad, el cual constituirá el soporte técnico vinculante para el seguimiento operativo. El informe deberá contener de manera obligatoria: estadísticas detalladas de desempeño, la metodología y fórmulas de cálculo aplicadas, las fuentes de datos, el análisis del comportamiento histórico.
- Las demás dentro del marco de buenas prácticas de ITIL.

7.2.6 Relacionadas con Seguridad de la Información y CISO (Chief Information Security Officer)

- Mantener monitoreados todos los servicios Principales y redundantes (HA) del servicio de seguridad 7X24X365, durante la duración del contrato.
- Reportar por escrito al ICBF cualquier sugerencia que contribuya a la obtención de mejores resultados.
- Garantizar la protección y seguridad de los datos, programas, aplicaciones, bases de datos, infraestructura e información del ICBF velando por cumplir con los tres pilares de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).
- Realizar y documentar en conjunto con el ICBF los procedimientos para llevar a cabo la instalación de aplicativos y bases de datos o cualquier otro software en los equipos al servicio del ICBF.
- El futuro oferente tendrá la responsabilidad de aplicar las mejores prácticas de configuración sobre las plataformas administradas y suministradas asegurándose de que el ICBF cuente con la implementación de estas mejores prácticas de seguridad sobre los servicios contratados.
- Dar un uso ético y protección a los accesos, contraseñas, información y recursos informáticos proporcionados por el ICBF, guardando estricta confidencialidad de la información sensible que pudiera llegar a manejar durante el desarrollo del presente

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

contrato. Esto derivara en la firma de un acuerdo de confidencialidad.

- Gestionar y proponer escenarios de pruebas para las actualizaciones de fabricantes que al ser implementadas generen algún tipo de impacto en la funcionalidad de las aplicaciones, herramientas desarrolladas por el ICBF o la infraestructura de la entidad y en caso de no ser aplicables plantear e implementar soluciones alternas.
- Presentar y documentar recomendaciones que propendan por la calidad y seguridad de la distribución de la información por los medios y canales electrónicos del ICBF en caso de requerirse.
- Implementar y documentar el procedimiento para el manejo, actividades y protocolos para la custodia y entrega de las contraseñas de administración. Estos procedimientos de custodia aplican para todos aquellos casos donde el Contratista haga uso de cuentas y contraseñas de administración de las herramientas usadas para el cumplimiento de los servicios incluidos en el alcance de este proceso de selección, ejemplo, el firewall, consolas de antivirus, bases de datos, aplicativos, IPS/IDS, Correo, Proxy, PC y Servidores.
- Definir e implementar procedimientos y proponer políticas para ejecución de análisis forenses.
- Ejecutar análisis forenses y presentar informes de estos por demanda o cuando la entidad así lo requiera.
- Reportar por escrito al ICBF cualquier sugerencia que contribuya a la obtención de mejores resultados.
- Implementar y configurar un tablero centralizado de monitoreo y análisis de datos en tiempo real, que traiga información de incidentes, eventos y amenazas de todos los servicios de seguridad perimetral y ciberseguridad.
- Integrar fuentes de información de seguridad, incluyendo SIEM, XDR, EDR, Firewalls, IDS, IPS, y soluciones de seguridad de fin de cliente, para poder visualizar y analizar información en tiempo real.
- Asegurar que el tablero centralizado-automático de monitoreo y análisis de datos en tiempo real, esté actualizado y compatible con las últimas tecnologías y soluciones de seguridad.
- Brindar capacitaciones que contribuyan a proteger los activos digitales del ICBF y a fomentar una cultura de seguridad de la información entre los empleados, generando así, la protección continua contra amenazas cibernéticas. Estas capacitaciones principalmente se deben enfocar y desarrollar en: Concienciación en Seguridad Informática, Gestión de Incidentes de Seguridad, Cumplimiento Normativo, Evaluación y Gestión de Riesgos, Seguridad en la Nube, Técnicas de Ciberseguridad Avanzadas.

7.2.7 Servicio de Aplicaciones

- Planear, documentar y coordinar el despliegue y puesta en producción de la infraestructura para los proyectos de software, de acuerdo con el procedimiento interno del ICBF de puesta en producción de proyectos de software.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Conocer, analizar e interpretar contadores relacionados con las aplicaciones y correlacionarlos con contadores de base de datos, comportamiento de la infraestructura y sistema operativo.
- Proponer, diseñar, administrar, monitorear y configurar esquemas de alta disponibilidad que se requieran para el montaje de Clúster, Network Load Balancing (NLB), balanceo por hardware u otros de similares o mejores características que se determine, utilizando el hardware y el software proporcionado por el ICBF.
- Realizar el despliegue, emitir recomendaciones de mejores prácticas en configuración y optimización y puesta en producción de las aplicaciones que se implementen durante la ejecución del contrato siguiendo para ello el procedimiento interno del ICBF para puesta en producción de proyectos de software.
- Entregar mensualmente, o por solicitud del ICBF, informes sobre los incidentes o mejoras que se efectúen sobre las aplicaciones y las acciones tomadas sobre cada caso.
- Cumplir con las tareas, compromisos y solicitudes en los tiempos establecidos y acordados en los planes de trabajo para la administración del servicio de aplicaciones que se presenten durante la vigencia del contrato.
- Generar, implementar y documentar estándares para la instalación, administración y monitoreo de performance de aplicaciones previa aprobación por parte del ICBF.
- Mantener actualizado el inventario de Aplicaciones de acuerdo con el formato establecido entre el Contratista y el ICBF. Además, generar mapas de servidores de aplicaciones, bases de datos, componentes de software, conexiones lógicas y físicas y mantenerlos actualizados mensualmente.
- Garantizar que los resultados finales de los informes, revisiones del servicio y diagnósticos, que le sean encomendados, cumplan las especificaciones de calidad y plazos que se hayan acordado previamente para cada caso.
- Informar los riesgos de operatividad, seguridad y degradación del servicio identificando puntos críticos y definiendo e implementando acciones previa autorización del ICBF
- Recopilar y guardar la información con las estadísticas de aplicaciones como lo son: concurrencia por usuario, número de usuarios que visitan la aplicación (horas, días y por mes), páginas más solicitadas, cantidad de tráfico, duración de las visitas, origen de la conexión, páginas de entrada y salida, código de respuesta (HTML) y concurrencia de usuarios. Estas estadísticas deben ser visualizadas por la entidad a través de una herramienta suministrada por el contratista, para el caso del Portal Web e intranet debe suministrar la herramienta y licencia vitalicia Google Anlitycs para que por medio de la herramienta señalada se genere estadísticas de consumo de portal e intranet.
- Realizar el apoyo cuando se requiera para implementar, configurar o Instalar los ambientes de prueba o pre productivos de los sistemas de información del ICBF.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

7.2.8 OBLIGACIONES BASES DE DATOS

- Responder por la administración, operación, monitoreo y mantenimiento de la plataforma de base de datos, así como la ejecución de todas las tareas recurrentes, programadas y no programadas para mantener en estado de operación óptima y eficiente las bases de datos del ICBF.
- Realizar un Informe mensual sobre el comportamiento y performance de las bases de datos que incluya como mínimo: informe de bloqueos (deadlock), recomendaciones, comportamiento estadístico de las bases de datos, recomendaciones de mejoras para optimizar las bases de datos, así como también: tablas a particionar, vistas, índices, top 10 de sentencias que consuman más recursos.
- Llevar bitácora de control de las bases de datos y sus componentes del ICBF, incluyendo como mínimo crecimiento mensual, almacenamiento disponible, incidentes, ejecución de backup, tareas automáticas, análisis de errores, optimización de procesos y alertas debe ser un anexo para el informe mensual de gestión.
- Definir Documentar y comunicar las políticas, procedimientos, planes de mantenimiento y estándares de las bases de datos con previa aprobación del ICBF.
- Brindar apoyo técnico y proponer activamente recomendaciones y buenas prácticas tanto de configurar de base de datos como de desarrollo de consultas transact o procedimientos almacenados, tendientes a optimizar el uso de recursos, asegurar la disponibilidad, seguridad, integridad, consistencia, continuidad, operación y buen desempeño de las bases de datos del ICBF.
- Dar respuesta a las consultas técnicas realizadas por el ICBF, asesorando en el mejoramiento y optimización de recursos, con el fin de garantizar la disponibilidad y buen desempeño de las bases de datos en los tiempos definidos por El ICBF.
- Instalar, administrar y soportar bases de datos Oracle 10G o superior, MySQL y MariaDB, administrar y configurar RMAN (Recovery Manager).
- Instalar, Implementar y administrar bases de datos Motor SQL server.
- Administrar, configurar y automatizar tareas de mantenimiento y optimización de los motores de bases de datos a través de las herramientas propias del motor de base de datos o que el Contratista suministre.
- Mantener actualizado el inventario de Base de Datos de acuerdo con los formatos establecidos en conjunto con el ICBF.
- Documentar, mantener actualizada y entregar al final del contrato o cuando se requiera, en formatos acordados con el ICBF, la base de datos del conocimiento y de configuraciones en cada servidor de base de datos: Gestión de configuración, Gestión de problemas, Gestión de cambios entre otras.
- Presentar recomendaciones sobre el diseño, configuración, arquitectura de todos los componentes y servicios de los motores de bases de datos.
- Identificar consultas a optimizar y suministrar recomendaciones y mejores prácticas

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

en la construcción de sentencias SQL.

- Generar y presentar un cronograma de las actividades de mantenimiento de las bases de datos con fechas de ejecución y responsables, el cual debe ser validado por el ICBF.
- Realizar los traslados físicos de las bases de datos, bajo solicitud y aprobación del ICBF, mediante un proceso de control de cambios, previa aprobación del comité de control de cambios.
- Realizar pruebas de carga, estrés y seguridad sobre ambientes de prueba o pre productivos para dimensionar su capacidad y concurrencia de usuarios sobre las bases de datos de los sistemas de información actuales y nuevos proyectos que se implementen durante la duración del contrato. El proveedor debe proporcionar software especializado para realizar estas labores.
- Realizar apoyos cuando se requiera para implementar, configurar e instalar los ambientes de Sistemas de Informacion de ICBF.

7.2.9 OBLIGACIONES DEL SERVICIO BIG-DATA

- Administrar, operar, monitorear, mantener y optimizar la plataforma Big Data y Analítica del ICBF y sus componentes, garantizando su disponibilidad, capacidad, desempeño, continuidad y adecuado funcionamiento durante la ejecución del contrato.
- Administrar, operar y monitorear los procesos de ingesta, integración, orquestación, extracción, transformación y carga de datos – ETL/ELT, verificando su correcta ejecución, gestionando oportunamente las fallas y optimizando los tiempos de procesamiento.
- Administrar, operar y monitorear los componentes Data Lake, Data Warehouse y demás repositorios analíticos que hagan parte de la plataforma, garantizando la disponibilidad, integridad, consistencia, capacidad y adecuado desempeño de la información almacenada.
- Administrar y brindar soporte técnico a los componentes de analítica, inteligencia de negocios y visualización de información, así como apoyar técnicamente la implementación, operación y mantenimiento de modelos analíticos requeridos por el ICBF.
- Monitorear la calidad de los datos administrados y procesados en la plataforma Big Data y Analítica, evaluando como mínimo criterios de completitud, consistencia, unicidad, integridad y duplicidad, identificando hallazgos y gestionando las acciones correctivas y de mejora correspondientes.
- Implementar y mantener los controles de seguridad aplicables a la plataforma Big Data y Analítica, incluyendo la gestión de usuarios, perfiles, privilegios, accesos, vulnerabilidades y trazabilidad de las actividades realizadas sobre los componentes administrados.
- Garantizar la ejecución y verificación de los procesos de respaldo, restauración, recuperación y continuidad aplicables a los componentes Big Data, manteniendo

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

actualizados los procedimientos y evidencias correspondientes.

- Gestionar los incidentes, problemas, requerimientos y cambios asociados al servicio BIG-DATA, conforme con las prácticas y herramientas de gestión definidas por el ICBF, garantizando su registro, seguimiento, documentación y trazabilidad.
- Mantener actualizada la Línea Base del Servicio, el inventario y la documentación técnica y operativa de la plataforma Big Data y Analítica, incluyendo diagramas de arquitectura, configuraciones, procesos ETL/ELT, procedimientos, manuales, bitácoras y control de versiones.
- Optimizar el uso y consumo de los recursos tecnológicos asociados a la plataforma Big Data y Analítica, incluyendo capacidad de procesamiento, almacenamiento, cómputo e infraestructura y servicios en nube, implementando acciones orientadas al aprovechamiento eficiente de la capacidad instalada, la reducción de consumos innecesarios y la mejora del desempeño, sin afectar la disponibilidad, seguridad y continuidad del servicio.
- Elaborar y presentar mensualmente el informe de gestión del servicio BIG-DATA, incluyendo como mínimo el comportamiento de la plataforma, disponibilidad, capacidad, utilización, desempeño, ejecución de procesos ETL/ELT, calidad de los datos, incidentes, respaldos, riesgos, resultados de optimización de recursos, recomendaciones y oportunidades de mejora.
- Identificar, proponer e implementar acciones de automatización y mejora continua sobre los procesos operativos y de procesamiento de datos de la plataforma Big Data y Analítica, orientadas a reducir actividades manuales, optimizar tiempos de procesamiento y fortalecer la eficiencia, estabilidad y desempeño del servicio.
- Incorporar y administrar los nuevos componentes tecnológicos, herramientas, fuentes de información y capacidades analíticas que sean requeridos por el ICBF durante la ejecución del contrato, garantizando su integración con la arquitectura tecnológica institucional y la actualización de la Línea Base y documentación correspondiente.
- Ejecutar y documentar la transferencia de conocimiento asociada a la operación, administración, configuraciones, procesos ETL/ELT, mejoras y cambios implementados en la plataforma Big Data y Analítica, garantizando que el ICBF disponga de la información técnica necesaria para asegurar la continuidad del servicio.

7.2.10 SEGURIDAD INFORMÁTICA

7.2.10.1 Obligaciones Trasversales seguridad informática

7.2.10.1.1 Implementación y Transición

- Entregar la totalidad de la plataforma de seguridad instalada, configurada y en correcto funcionamiento dentro de los quince (15) días siguientes al inicio del contrato, disponiendo los elementos en el datacenter interno y externo del ICBF para adelantar configuración y pruebas durante la etapa de transición.
- Entregar, al momento de la implementación, carta de la fabricante firmada por su Representante Legal certificando que la plataforma y/o servicios cuentan con las

mejores prácticas de configuración y estándares de seguridad.

- Entregar en la etapa de transición un documento firmado por el representante legal que soporte, frente a datasheet, el cumplimiento de todos los requerimientos técnicos mínimos, relacionando página y numeral exactos donde se evidencia cada ítem.
- Soportar los servicios con plataformas que dispongan de todas las interfaces de red necesarias (cables, fibras, conectores) y totalmente compatibles con IPv6, acreditado mediante carta de fabricante.
- Presentar el plan de trabajo detallando etapas, resultados esperados, estrategias, técnicas y herramientas para la ejecución del contrato, previa aprobación del ICBF.

7.2.10.1.2 Operación, administración y soporte

- Velar por la seguridad informática del ICBF en todas sus sedes mediante suministro, instalación, configuración, administración, soporte y monitoreo de las soluciones, dispositivos y herramientas requeridos en la ficha técnica.
- Brindar soporte de segundo nivel sobre todas las soluciones de seguridad instaladas y/o configuradas en la infraestructura del ICBF.
- Entregar evidencia de que los equipos y servicios cuentan con soporte y garantía directa del fabricante en modalidad 7x24x365, y que el licenciamiento cumple la ley de derechos de autor y propiedad intelectual.
- Planear y desarrollar actividades mensuales que garanticen la máxima cobertura de actualizaciones de seguridad de sistemas operativos sobre servidores y equipos de cómputo.

7.2.10.1.3 Monitoreo, disponibilidad y ANS

- Mantener monitoreados todos los servicios principales y redundantes (HA) de seguridad en modalidad 7x24x365 durante toda la vigencia del contrato.
- Realizar actividades mensuales de estudio de tráfico en redes LAN, WAN, Internet y DMZ con análisis de protocolos, presentando informe de hallazgos, planes de acción y ejecución de correcciones.

7.2.10.1.4 Detección, respuesta y gestión de incidentes

- Identificar, diagnosticar, solucionar y reportar problemas e incidentes de seguridad sobre la infraestructura tecnológica del ICBF o la provista por el contratista.

7.2.10.1.5 Integración (SIEM/SOAR/SOC)

- Garantizar que todos los servicios de seguridad informática puedan integrarse con el SIEM/SOAR y sean monitoreados por el SOC en tiempo real.

7.2.10.1.6 Reportería, documentación y trazabilidad

- Mantener actualizada la documentación (hoja de vida del servicio) de todas las

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

actividades, cambios, instalaciones, configuraciones y labores de administración, proponiendo mejoras traducidas en planes de acción.
- Retener y almacenar los logs de la infraestructura de seguridad (perimetral y SOC) con retención en línea mínima de seis (6) meses y fuera de línea mínima de doce (12) meses, en formatos que permitan lectura con herramientas alternas.
- Presentar informe mensual con estado, avances, estadísticas, cumplimiento de ANS y toda la información de la gestión de seguridad informática, definido y aprobado en conjunto con el ICBF.
- Suministrar topologías del servicio y documentación técnica con el máximo detalle, contemplando las capas del modelo OSI, almacenando los datos en contenedores cifrados y controlados que garanticen integridad, continuidad y disponibilidad.
- Reportar por escrito al ICBF cualquier sugerencia que contribuya a la obtención de mejores resultados.

7.2.10.1.7 Pruebas, auditoría y mejora continua

- Atender pruebas de validación aleatorias solicitadas por la Entidad en cualquier momento para constatar el estado y funcionamiento de cualquiera de los servicios de seguridad contratados.
- Validar semestralmente las configuraciones de todos los servicios de seguridad para certificar el seguimiento de las mejores prácticas recomendadas por cada fabricante.
- Disponer de personal certificado y vigente durante toda la ejecución del contrato, de uso exclusivo del proyecto ICBF, para la operación de los servicios de seguridad.

7.2.10.2 SERVICIO DE SEGURIDAD PERIMETRAL (NGFW / IPS-IDS / PROXY / VPN)

7.2.10.2.1 Implementación y transición

- Suministrar, instalar y configurar los firewalls de nueva generación (NGFW) entregados como servicio, con appliances nuevos de clase Enterprise en HA en ambas ubicaciones.
- Presentar plan de migración controlada de políticas, reglas y objetos que incluya inventario, matriz de equivalencia, identificación de reglas obsoletas/duplicadas/inseguras, plan de pruebas, plan de reversa, ventanas de cambio y aprobaciones del ICBF.
- Elaborar planes para la migración de servidores y aplicaciones web a la DMZ, de común acuerdo y bajo aprobación del ICBF, contemplados en la etapa de transición.
- Ejecutar las labores técnicas de migración de servidores y aplicaciones web a la DMZ y realizar la configuración y soporte para mantener la DMZ en operación.
- Acreditar el rendimiento mínimo requerido: firewall ≥145 Gbps, IPS/IDS ≥30 Gbps, control de aplicaciones ≥35 Gbps, inspección SSL/TLS ≥20 Gbps, VPN IPsec AES-256 ≥20 Gbps y 3.000.000 de sesiones concurrentes.
- Implementar y mantener segmentación basada en zonas de confianza,

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

microsegmentación cuando aplique y principios Zero Trust.

- Revisar trimestralmente la totalidad de las políticas del firewall para identificar reglas obsoletas, duplicadas, inseguras o sin uso.
- Implementar análisis automatizado de políticas y evaluación continua de cumplimiento normativo.
- Implementar como mínimo treinta (30) casos de uso personalizados para detección de amenazas perimetrales integrados con el SIEM.

7.2.10.2.2 Configuración, aseguramiento y hardening

- Documentar y aplicar las políticas y reglas de seguridad del firewall asociadas a la infraestructura, con revisión, mantenimiento y actualización periódica de la base de reglas.
- Configurar los módulos de IPS/IDS, control de aplicaciones, protección contra malware e inspección de contenido SSL conforme a las mejores prácticas del fabricante.
- Suministrar, configurar y operar un proxy transparente en alta disponibilidad para el acceso a Internet de acuerdo con las categorías de la política de navegación del ICBF.
- Habilitar y sintonizar las capacidades de IA/ML del NGFW para la identificación y control de aplicaciones independientemente del puerto y protocolo.

7.2.10.2.3 Operación, administración y soporte

- Otorgar, administrar, gestionar y brindar soporte a los accesos mediante conexiones VPN client-to-site y site-to-site.
- Mantener la VPN SSL con capacidad mínima de 12.000 usuarios concurrentes con autenticación multifactor durante toda la vigencia.

7.2.10.2.4 Monitoreo, disponibilidad y ANS

- Configurar la herramienta de monitoreo para medir la disponibilidad del servicio de firewall en cada periodo de operación, permitiendo al ICBF determinar la aplicación del ANS asociado.
- Garantizar la alta disponibilidad del servicio de firewalls del Datacenter Principal Externo y de la Sede Dirección General, permitiendo pruebas de continuidad y conmutación.

7.2.10.2.5 Pruebas, auditoría y mejora continua

- Establecer un programa semestral de pruebas de continuidad sobre los firewalls en HA (conmutación primario-esclavo y HA geográfico entre datacenter principal y secundario), presentando mensualmente el seguimiento, avance y evidencias de ejecución.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

7.2.10.3 SERVICIO DE PROTECCIÓN CONTRA AMENAZAS PERSISTENTES AVANZADAS (SANDBOXING / APT)

7.2.10.3.1 Implementación y transición

- Suministrar, instalar y configurar la solución de seguridad contra amenazas persistentes avanzadas (sandboxing) entregada como servicio, en alta disponibilidad.

7.2.10.3.2 Configuración, aseguramiento y hardening

- Configurar las políticas de análisis de archivos y URL sospechosas, retención de muestras y acciones de contención automatizadas conforme a las mejores prácticas del fabricante.
- Realizar detonación automática y manual de archivos sospechosos, URL, scripts, documentos y objetos potencialmente maliciosos.
- Compartir automáticamente indicadores de compromiso (IOC) con las plataformas SIEM, SOAR, NGFW, WAF y EDR/XDR.
- Mantener repositorio histórico de amenazas analizadas, indicadores identificados y acciones ejecutadas.

7.2.10.3.3 Monitoreo, disponibilidad y ANS

- Configurar la herramienta de monitoreo para medir la disponibilidad del servicio de protección contra APT en cada periodo de operación, permitiendo determinar la aplicación del ANS.

7.2.10.3.4 Integración (SIEM/SOAR/SOC)

- Integrar la solución de sandboxing con el NGFW, el correo y el SIEM/SOAR para el intercambio de indicadores y la contención automatizada de amenazas detectadas.

7.2.10.3.5 Reportería, documentación y trazabilidad

- Presentar informe mensual o por demanda (dentro de las 24 horas siguientes a la solicitud) sobre las amenazas avanzadas detectadas y contenidas, con su respectivo análisis.

7.2.10.4 SERVICIO DE SEGURIDAD EN APLICACIONES WEB (WAF)

- Suministrar, instalar y configurar los firewalls de aplicaciones (WAF) necesarios para la seguridad de las aplicaciones web del ICBF, entregados como servicio.
- Configurar las políticas de protección del WAF (OWASP Top 10, mitigación de bots, protección de APIs e inspección de tráfico cifrado) conforme a las mejores prácticas

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

del fabricante.

- Configurar las herramientas de monitoreo para medir la disponibilidad del servicio de seguridad en aplicaciones web en cada periodo de operación, permitiendo determinar la aplicación del ANS.
- Presentar informe mensual o por demanda (dentro de las 24 horas siguientes a la solicitud) con el estado y eventos relevantes de la seguridad en aplicaciones web, con su respectivo análisis.
- Entregar evidencia de instalación y operación de una herramienta para análisis de vulnerabilidades sobre las aplicaciones web protegidas, de forma que se identifiquen y remedien hallazgos.
- Implementar protección específica contra OWASP Top 10, OWASP API Top 10 y amenazas emergentes.
- Ejecutar pruebas periódicas de validación de protección sobre las aplicaciones publicadas.
- Implementar perfiles de aprendizaje, protección de APIs, mitigación de bots y protección contra ataques automatizados.

7.2.10.5 SERVICIO DE SEGURIDAD EN BASES DE DATOS (DAM)

7.2.10.5.1 Implementación y transición

- Suministrar, instalar y configurar la herramienta tecnológica necesaria para brindar seguridad a todas las bases de datos del ICBF, aplicando las mejores prácticas.

7.2.10.5.2 Configuración, aseguramiento y hardening

- Configurar las políticas de auditoría, enmascaramiento y alertamiento de actividad sobre las bases de datos, con detección de accesos privilegiados indebidos, conforme a las mejores prácticas del fabricante.
- Monitorear actividades privilegiadas sobre bases de datos.
- Identificar comportamientos anómalos de usuarios y cuentas privilegiadas.
- Integrar los eventos generados con el SIEM/SOAR para generar alertas y automatizar acciones de respuesta.

7.2.10.5.3 Monitoreo, disponibilidad y ANS

- Configurar las herramientas de monitoreo para medir la disponibilidad del servicio de seguridad en bases de datos en cada periodo de operación, permitiendo determinar la aplicación del ANS.

7.2.10.5.4 Reportería, documentación y trazabilidad

- Presentar informe mensual o por demanda (dentro de las 24 horas siguientes a la solicitud) con el estado y eventos relevantes de la seguridad en bases de datos, con su respectivo análisis.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

7.2.10.6 SERVICIO DE SEGURIDAD EN CORREO ELECTRÓNICO (SEG / ANTI-SPAM / DLP)

7.2.10.6.1 Implementación y transición

- Suministrar, instalar y configurar las plataformas de Anti-spam que soportan el servicio de seguridad en correo electrónico, garantizando la seguridad del servicio.
- Suministrar, instalar, configurar, administrar y monitorear los módulos de DLP de correo electrónico siguiendo las mejores prácticas del fabricante.
- Implementar mecanismos de autenticación SPF, DKIM y DMARC.
- Realizar simulaciones periódicas de campañas de phishing definidas por el ICBF.
- Integrar los eventos del servicio con SIEM, SOAR y SOC para investigación y respuesta.

7.2.10.6.2 Configuración, aseguramiento y hardening

- Configurar las políticas anti-spam, anti-phishing, protección antimalware y reglas DLP de correo alineadas con la política de tratamiento de datos personales (Ley 1581 de 2012) y los lineamientos del ICBF.

7.2.10.6.3 Monitoreo, disponibilidad y ANS

- Configurar las herramientas de monitoreo para medir la disponibilidad del servicio de seguridad en correo electrónico en cada periodo de operación, permitiendo determinar la aplicación del ANS.

7.2.10.6.4 Reportería, documentación y trazabilidad

- Presentar informe mensual del estado de configuración y eventos relevantes del módulo DLP de correo (Top 10 de detecciones y acciones realizadas por cada detección).
- Presentar informe mensual o por demanda (dentro de las 24 horas siguientes a la solicitud) con el estado y eventos relevantes del servicio de correo, con su respectivo análisis.

7.2.10.7 SERVICIO DE PROTECCIÓN CONTRA DENEGACIÓN DE SERVICIO DISTRIBUIDO (ANTI-DDoS)

7.2.10.7.1 Implementación y transición

- Suministrar un servicio en alta disponibilidad para controlar los ataques de denegación de servicio distribuido dirigidos contra la infraestructura web y de seguridad perimetral del ICBF.

7.2.10.7.2 Configuración, aseguramiento y hardening

- Configurar los umbrales, perfiles de tráfico y políticas de mitigación (volumétrica, de

protocolo y de capa de aplicación) conforme a las mejores prácticas del fabricante.
- Ejecutar pruebas controladas de efectividad de mitigación DDoS.
- Mantener procedimientos documentados de respuesta ante ataques volumétricos, protocolarios y de capa de aplicación.
- Integrar los eventos de mitigación con el SOC para monitoreo centralizado.

7.2.10.7.3 Monitoreo, disponibilidad y ANS

- Configurar las herramientas de monitoreo para medir la disponibilidad del servicio de protección contra DDoS en cada periodo de operación, permitiendo determinar la aplicación del ANS.

7.2.10.7.4 Reportería, documentación y trazabilidad

- Presentar informe mensual o por demanda (dentro de las 24 horas siguientes a la solicitud) con los eventos de ataque, mitigaciones ejecutadas y su respectivo análisis.

7.2.10.8 SERVICIO DE GESTIÓN DE EVENTOS Y CORRELACIÓN (SIEM) — HISTÓRICO, LOGS Y REPORTES

7.2.10.8.1 Implementación y transición

- Suministrar, licenciar, configurar, gestionar y monitorear la plataforma de propósito específico SIEM/SOAR, soportada con datasheet del fabricante.

7.2.10.8.2 Configuración, aseguramiento y hardening

- Garantizar la compatibilidad e interoperabilidad entre todos los dispositivos de seguridad informática y el SIEM/SOAR.
- Mantener actualizadas las definiciones de ataques, vulnerabilidades y categorización de eventos en el correlacionador, con servicio de suscripción vigente durante todo el contrato.

7.2.10.8.3 Operación, administración y soporte

- Proporcionar el mantenimiento de hardware y las actualizaciones de software (parches y upgrades de versión) de la plataforma por la duración del contrato.
- Proporcionar soporte técnico del fabricante con atención mínima 8x5 por la duración del contrato.
- Garantizar en toda circunstancia la posibilidad de escalamiento del servicio con el fabricante para la solución oportuna de incidentes de la infraestructura como servicio.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

7.2.10.8.4 Reportería, documentación y trazabilidad

- Presentar informe técnico de los servicios en monitoreo considerando el alcance de aplicaciones e infraestructura (on-premise, híbrida y cloud).
- Proporcionar entrenamiento sobre la infraestructura implementada a nivel de administrador y usuario final.
- Suministrar, licenciar, configurar, gestionar y monitorear la plataforma de propósito específico de SIEM y SOAR, soportadas con datasheet del fabricante.
- Presentar informe técnico de los servicios en monitoreo teniendo en cuenta el alcance aplicaciones e infraestructura. (On-premise – infraestructura Hibrida - Cloud)
- Garantizar compatibilidad e interoperabilidad entre todos los dispositivos de seguridad informática y el SIEM (SOAR)
- Efectuar automatización entre los diferentes componentes de seguridad del servicio (SIEM SOAR – FIREWALLS) Para llevar a cabo contención automatizada de amenazas aplicando las mejores prácticas del fabricante.
- Realizar configuración y casuística del componente SOAR con el fin de contar con automatización aplicando las mejores prácticas del fabricante.
- Presentar informe mensual de estado de la configuración, casuística y eventos relevantes a la automatización para la contención de amenazas.
- Presentar el plan de trabajo, especificando etapas, resultados esperados, estrategias para asegurar el logro de los productos en los tiempos establecidos y describir las técnicas y herramientas que utilizará en la ejecución del contrato, previa aprobación del ICBF.
- Garantizar el servicio de monitoreo de la gestión integrada de seguridad compuesto por:
    - Gestión de Bitácoras y Correlación de Eventos de Seguridad en tiempo real
    - Gestión de eventos en tiempo real
    - Gestión de Configuraciones en tiempo real
- Administrar y monitorear componentes principales y segundarios (HA) 7X24X365 la gestión integrada de seguridad del ICBF.
- Proporcionar el mantenimiento de hardware y actualizaciones de software (parches y upgrades de versión) por la duración del contrato.
- Proporcionar Soporte técnico del fabricante con atención mínimo 8x5 por la duración del contrato.
- Mantener actualizadas las definiciones de ataques, vulnerabilidades y categorización de eventos en el correlacionador de eventos durante la vigencia del contrato y contar con un servicio de suscripción para la actualización de contenidos de seguridad.
- Garantizar en toda circunstancia la posibilidad de escalamiento del servicio con el fabricante para una oportuna solución de incidentes relacionados con la infraestructura como servicio implementado.
- Proporcionar entrenamiento sobre la infraestructura implementada para la prestación del servicio a nivel administrador y usuario final.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Presentar un informe mensualmente o por demanda (el tiempo de generación y entrega de este no deberá exceder 4 horas) de la Entidad, este informe deberá contener como mínimo los siguientes ítems y será entregado desde el servicio de SOC con su respectivo análisis:
    - Reporte de Incidentes de Seguridad.
    - Reporte de Actividades Sospechosas de Usuarios / Equipos / Aplicaciones.
    - Reporte de Integridad de Archivos.
    - Reporte de Cambios de Configuraciones.
    - Reporte de Cambios no Autorizados en los Registros de Windows.
    - Reporte de Violaciones de Políticas en Bases de Datos.
    - Reporte de Violaciones de Políticas de Control de Acceso.

7.2.10.9 Servicio de SOC (Security Operation Center)

- Noventa (90) casos de uso personalizados para la plataforma SIEM, construidos específicamente para el ICBF, considerando los activos tecnológicos, aplicaciones, servicios, usuarios, entornos híbridos, cargas en nube, infraestructura crítica, fuentes de eventos y requerimientos de monitoreo definidos por la Entidad.
- Ciento veinte (120) playbooks y/o casos de uso personalizados de automatización y orquestación para la plataforma SOAR, orientados a la detección, investigación, contención, escalamiento, análisis y respuesta ante incidentes de seguridad informática.
- Los casos de uso SIEM y playbooks SOAR exigidos corresponderán exclusivamente a desarrollos, parametrizaciones y personalizaciones realizadas para el ICBF, por lo que no se aceptarán como cumplimiento de este requisito los contenidos, plantillas, reglas, casos de uso, automatizaciones, conectores, paquetes, dashboards o playbooks suministrados por defecto por el fabricante o incluidos de fábrica dentro de la solución.
- Cada caso de uso y playbook deberá entregarse debidamente documentado, incluyendo como mínimo objetivo, descripción funcional, lógica de correlación, fuentes de eventos involucradas, técnicas MITRE ATT&CK asociadas, criticidad, criterios de activación, acciones automáticas, responsables, flujo de escalamiento, evidencias de validación y procedimientos de mejora continua.
- El contratista deberá ejecutar pruebas funcionales, pruebas de escritorio (Tabletop Exercises), simulaciones controladas, validaciones operativas y ejercicios de verificación sobre la totalidad de los casos de uso personalizados SIEM y playbooks SOAR implementados, con el fin de garantizar su correcto funcionamiento y efectividad.
- Como evidencia de las actividades de validación, el contratista deberá realizar sesiones técnicas formales con participación del supervisor y/o personal designado por el ICBF, generando para cada sesión el acta correspondiente, listas de asistencia, conclusiones, compromisos, resultados obtenidos y evidencias técnicas

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

que soporten la ejecución de las pruebas realizadas.

- Durante la ejecución contractual, el contratista deberá efectuar actividades periódicas de afinamiento (Tuning), optimización y mejora de los casos de uso SIEM y playbooks SOAR, orientadas a reducir falsos positivos, falsos negativos, tiempos de respuesta, ruido operacional y mejorar los indicadores de detección y contención de amenazas.
- El contratista deberá presentar mensualmente un informe técnico especializado donde se evidencie el estado de los casos de uso SIEM y playbooks SOAR implementados, incluyendo cobertura, efectividad, incidentes detectados, automatizaciones ejecutadas, oportunidades de mejora, casos ajustados, resultados de pruebas realizadas y plan de trabajo para el siguiente periodo.
- El ICBF podrá solicitar durante la vigencia contractual la creación, modificación, ajuste o retiro de casos de uso SIEM y playbooks SOAR derivados de nuevas amenazas, cambios tecnológicos, nuevos servicios, hallazgos de auditoría, incidentes de seguridad, requerimientos operativos o necesidades de la Entidad, sin que ello genere costos adicionales para el ICBF dentro del alcance contratado.
- Todos los casos de uso SIEM y playbooks SOAR desarrollados, parametrizados o ajustados durante la ejecución contractual deberán quedar documentados, transferidos y disponibles para el ICBF al finalizar el contrato, incluyendo configuraciones, reglas, flujos de automatización, matrices de correlación, bases de conocimiento, lecciones aprendidas y documentación técnica asociada.
- Implementar y mantener como mínimo noventa (90) casos de uso personalizados para la plataforma SIEM, desarrollados específicamente para el entorno tecnológico, riesgos y procesos del ICBF.
- Implementar y mantener como mínimo ciento veinte (120) playbooks personalizados para la plataforma SOAR orientados a detección, investigación, contención, respuesta y automatización.
- Los casos de uso y playbooks exigidos deberán corresponder exclusivamente a desarrollos, configuraciones o personalizaciones realizadas para el ICBF, por lo que no se aceptarán contenidos, plantillas, reglas, dashboards o automatizaciones suministradas por defecto por el fabricante.
- Ejecutar pruebas funcionales, simulaciones controladas y pruebas de escritorio sobre la totalidad de los casos de uso y playbooks implementados.
- Realizar sesiones técnicas periódicas de validación con el ICBF, dejando evidencia mediante actas, listas de asistencia, resultados obtenidos, hallazgos, oportunidades de mejora y compromisos.
- Ejecutar actividades permanentes de afinamiento (Tuning) para reducir falsos positivos, falsos negativos y mejorar la efectividad operacional de la plataforma.
- Incorporar matrices de cobertura MITRE ATT&CK para medir el nivel de cobertura de detección y respuesta del SOC.
- Garantizar la integración nativa y bidireccional entre la solución de Antivirus, NGAV, EDR o XDR con la que cuente el ICBF y las plataformas SIEM, SOAR y SOC implementadas para la prestación del servicio, asegurando la recolección,

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

normalización, correlación y análisis en tiempo real de la totalidad de la telemetría, eventos, alertas, incidentes, Indicadores de Compromiso (IOC), Indicadores de Ataque (IOA), actividades sospechosas, comportamientos anómalos, acciones de contención y demás registros generados por la solución de protección de endpoints.
- Presentar mensualmente indicadores de cobertura, efectividad de detección, tiempo medio de detección (MTTD), tiempo medio de respuesta (MTTR), incidentes gestionados, automatizaciones ejecutadas y evolución de madurez del SOC.
- Garantizar la integracio de SIEM y SOAR con la solución de Antivirus con la que cuente la entidad. Debe correacionar telemetria de la solución de antivirus de manera obligatoria.
- Implementar automatizaciones orientadas a la contención de amenazas mediante aislamiento de dispositivos, bloqueo de procesos, cuarentena de archivos, bloqueo de indicadores de compromiso y demás acciones soportadas por la plataforma de antivirus.

Ciberinteligencia y Threat Intelligence
- Implementar y operar un servicio de ciberinteligencia orientado a la identificación, análisis, correlación y seguimiento de amenazas, vulnerabilidades, campañas maliciosas, actores de amenaza (Threat Actors), indicadores de compromiso (IOC), indicadores de ataque (IOA) y tácticas, técnicas y procedimientos (TTP) que puedan afectar al ICBF.
- Consumir y gestionar fuentes de inteligencia de amenazas comerciales, gubernamentales, abiertas (OSINT) y proporcionadas por fabricantes, garantizando su integración con las plataformas SIEM, SOAR, EDR/XDR, NGFW, WAF, DAM y demás soluciones de seguridad implementadas.
- Correlacionar de forma obligatoria los indicadores de compromiso (IOC), indicadores de ataque (IOA), direcciones IP maliciosas, dominios, URL, hashes, firmas y demás artefactos de inteligencia de amenazas dentro de la plataforma SIEM con el fin de fortalecer las capacidades de detección temprana.
- Implementar mecanismos automatizados para el enriquecimiento de alertas e incidentes mediante fuentes de Threat Intelligence, permitiendo contextualizar amenazas, determinar criticidad y priorizar actividades de respuesta.
- Mantener actualizada una base centralizada de inteligencia de amenazas integrada con las capacidades de monitoreo, correlación, investigación y respuesta del SOC.

Threat Hunting
- Ejecutar actividades mensuales de Threat Hunting proactivo sobre la infraestructura tecnológica del ICBF, orientadas a identificar amenazas avanzadas, persistencia, movimientos laterales, actividad maliciosa no detectada por mecanismos tradicionales, abuso de privilegios y comportamientos anómalos.
- Implementar y mantener como mínimo veinte (20) casos de uso personalizados de Threat Hunting basados en MITRE ATT&CK, ajustados al entorno tecnológico, riesgos y amenazas relevantes para el ICBF.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Documentar cada ejercicio de Threat Hunting mediante informes técnicos que incluyan hipótesis investigadas, metodología utilizada, hallazgos identificados, indicadores descubiertos, acciones realizadas y recomendaciones de mejora.
- Alertamiento Estratégico
- Emitir alertas tempranas sobre amenazas emergentes, campañas de ransomware, vulnerabilidades críticas explotadas activamente, campañas de phishing dirigidas, ataques contra entidades gubernamentales, grupos de amenaza persistente avanzada (APT) y cualquier situación que pueda representar un riesgo para la operación del ICBF.
- Informar oportunamente al ICBF sobre vulnerabilidades incluidas en catálogos de vulnerabilidades explotadas activamente (Known Exploited Vulnerabilities - KEV), indicando posibles impactos, activos potencialmente afectados y recomendaciones de mitigación.
- Informes de Ciberinteligencia
- Presentar un boletín mensual de ciberinteligencia que incluya como mínimo:
- Amenazas relevantes del período.
- Campañas activas identificadas a nivel nacional e internacional.
- IOC e IOA de relevancia para el ICBF.
- Actores de amenaza con impacto potencial en entidades gubernamentales.
- Vulnerabilidades críticas publicadas.
- Riesgos emergentes.
- Recomendaciones técnicas y operativas de mitigación.
- Presentar informes extraordinarios de ciberinteligencia cuando se identifiquen amenazas críticas que puedan afectar directa o indirectamente los servicios, plataformas, activos o información del ICBF.

7.2.10.10 SERVICIO DE ADMINISTRACIÓN DE ANTIVIRUS

- Configurar, mantener, monitorear, gestionar, soportar y actualizar las plataformas de las soluciones de antivirus que el ICBF tenga a disposición.
- Garantizar el despliegue y actualización del Antivirus que se tenga en producción, e informar mensualmente el estado general de actualización y amenazas detectadas por el mismo.
- Documentar y aplicar sobre el servicio de antivirus del ICBF las políticas y reglas de seguridad asociadas a la infraestructura tecnológica. Además, realizará la revisión, mantenimiento y actualización de políticas y de la plataforma de antivirus de común acuerdo y con la autorización del líder del servicio de seguridad informática del ICBF.
- Configurar las herramientas de monitoreo para medir la disponibilidad del servicio de antivirus del ICBF durante cada periodo de operación con el fin de que el ICBF pueda determinar la aplicación o no del ANS asociado.
- Configurar, administrar y monitorear todos los módulos del antivirus del ICBF: control de aplicaciones, firewall, entre otros, bajo las mejores prácticas del fabricante. Adicional, de todas las características recomendadas por el especialista

para el correcto funcionamiento del servicio. Esto debe aplicar para todas las plataformas de antivirus con las que cuente la Entidad.

- Presentar informe mensual de cobertura de servicios de antivirus del ICBF el cual deberá al menos 99.8% del parque computacional del ICBF incluyendo (servidores / desktops / laptops). En caso de que ICBF cuente con (servidores / desktops / laptops) con sistema operativo fuera de soporte por el fabricante del sistema operativo (4 versiones anteriores a la versión vigente S.O) se deberán contemplar métodos alternativos para garantizar la protección de dichos equipos.
- Presentar informe mensual de gestión de (IOC) con temas relevantes a la IOC "conjunto de datos sobre un objeto o una actividad que indica acceso no autorizado al equipo o red."
- Presentar un informe mensualmente o por demanda estos deberán ser entregados dentro de las 24 horas siguientes a la solicitud por parte de la Entidad, este informe deberá contener como mínimo los siguientes ítems y será entregado desde la gestión de antivirus con su respectivo análisis:
    - Top 10 de malware.
    - Top 10 de usuarios con malware.
    - Equipos actualizados por regional
    - Servidores actualizados.
    - Top 10 ataques.
- Mantener un inventario actualizado de equipos protegidos identificando activos sin agente, agentes desactualizados, agentes inactivos y equipos fuera de cumplimiento.
- Ejecutar actividades permanentes para garantizar la cobertura y actualización de la totalidad de los activos definidos por el ICBF.
- Implementar mecanismos de seguimiento para identificar equipos que permanezcan más de un (1) mes sin reportar telemetría a la consola centralizada
- Monitorear y gestionar permanentemente eventos, alertas, incidentes, indicadores de compromiso (IOC), indicadores de ataque (IOA), actividades sospechosas y comportamientos anómalos detectados por la solución.
- Realizar análisis técnico de malware, ransomware, ataques sin archivos (Fileless Malware), amenazas persistentes avanzadas (APT) y demás eventos relevantes detectados por la solución.
- Identificar amenazas activas mediante capacidades de Threat Intelligence, Threat Hunting y Behavioral Analytics cuando estas se encuentren disponibles en la solución licenciada.
- Garantizar la integración de la solución de protección de endpoints con las plataformas SIEM, SOAR y SOC del ICBF para permitir el monitoreo centralizado y la respuesta coordinada ante incidentes.
- Garantizar el envío en tiempo real de eventos, alertas, telemetría, IOC, IOA y hallazgos de seguridad hacia la plataforma de correlación de eventos.
- Validar semestralmente la configuración de la solución implementada frente a las mejores prácticas y recomendaciones del fabricante.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Ejecutar actividades periódicas de afinamiento (Tuning) para reducir falsas alertas, falsos positivos y falsos negativos.
- Mantener actualizadas las firmas, motores de detección, modelos de inteligencia artificial, indicadores de compromiso y bases de conocimiento proporcionadas por el fabricante.

7.2.10.11 SERVICIO DE DETECCIÓN Y GESTIÓN DE VULNERABILIDADES (VA / ETHICAL HACKING / PENTEST / VIRTUAL PATCHING)

- Configurar, mantener, monitorear, gestionar, soportar y actualizar la herramienta de análisis de vulnerabilidades que el ICBF o el futuro proveedor tengan a disposición.
- Configurar, mantener, monitorear, gestionar, soportar y actualizar la herramienta de análisis de vulnerabilidades que el ICBF o el futuro proveedor tengan a disposición.
- Realizar análisis de vulnerabilidades internos y externos sobre la infraestructura tecnológica del ICBF, incluyendo servidores físicos y virtuales, estaciones de trabajo, dispositivos de red, dispositivos de seguridad, aplicaciones web, bases de datos, servicios expuestos a Internet, ambientes híbridos y servicios en nube.
- Ejecutar escaneos periódicos de vulnerabilidades autenticados y no autenticados, garantizando una cobertura integral de los activos tecnológicos definidos por el ICBF.
- Realizar actividades de Ethical Hacking y pruebas de penetración controladas sobre los activos priorizados por el ICBF, de acuerdo con un plan de trabajo previamente aprobado por la Entidad.
- Identificar, clasificar y priorizar las vulnerabilidades detectadas con base en estándares reconocidos internacionalmente como CVSS, OWASP, CWE, MITRE ATT&CK y CISA Known Exploited Vulnerabilities (KEV) o los que los sustituyan.
- Presentar informes ejecutivos y técnicos de cada ejercicio de análisis de vulnerabilidades, Ethical Hacking o Pentest realizado, incluyendo hallazgos, nivel de criticidad, evidencia técnica, impacto potencial, probabilidad de explotación y recomendaciones de mitigación.
- Realizar seguimiento continuo a la remediación de vulnerabilidades identificadas y reportadas, verificando su cierre efectivo y generando indicadores de gestión y cumplimiento.
- Ejecutar actividades de validación posterior a la remediación mediante rescaneos o pruebas de comprobación, con el fin de verificar la eliminación o mitigación efectiva de las vulnerabilidades identificadas.
- Implementar controles de Virtual Patching cuando no sea técnicamente viable realizar la corrección inmediata de una vulnerabilidad, documentando las medidas implementadas, el riesgo residual y el plan de remediación definitivo.
- Mantener integrada la plataforma de gestión de vulnerabilidades con las herramientas SIEM, SOAR, EDR/XDR, monitoreo, gestión de activos y demás

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

soluciones de seguridad que conformen la arquitectura tecnológica del ICBF.

- Implementar, configurar y mantener como mínimo treinta (30) casos de uso personalizados para la identificación, correlación, seguimiento y priorización de vulnerabilidades dentro de la plataforma SIEM, alineados con los riesgos, activos críticos y necesidades operativas del ICBF.
- Implementar, configurar y mantener como mínimo veinte (20) playbooks personalizados en la plataforma SOAR orientados a la automatización de actividades de detección, clasificación, notificación, seguimiento, escalamiento y validación de vulnerabilidades.
- Los casos de uso y playbooks exigidos deberán corresponder a desarrollos, configuraciones o personalizaciones realizadas específicamente para el ICBF, por lo que no serán aceptados como cumplimiento contractual aquellos casos de uso, reglas, automatizaciones, dashboards, plantillas o contenidos suministrados de forma predeterminada por el fabricante.
- Ejecutar pruebas funcionales, simulaciones controladas y pruebas de escritorio sobre la totalidad de los casos de uso y playbooks personalizados implementados, con el fin de validar su correcto funcionamiento y efectividad operativa.
- Realizar sesiones técnicas periódicas con participación del personal designado por el ICBF para la revisión, validación, optimización y mejora de los casos de uso y playbooks implementados, dejando como evidencia las respectivas actas de reunión, listas de asistencia, resultados obtenidos, compromisos y soportes técnicos.
- Generar y mantener actualizado un inventario de vulnerabilidades identificadas, indicando estado, nivel de criticidad, fecha de detección, responsable de remediación, fecha compromiso y fecha efectiva de cierre.
- Presentar mensualmente un informe consolidado del servicio que incluya como mínimo vulnerabilidades identificadas, vulnerabilidades remediadas, vulnerabilidades pendientes, tendencias, indicadores de exposición, activos afectados, avances en remediación, actividades de Virtual Patching realizadas y recomendaciones de mejora continua.
- Proveer asesoría técnica especializada al ICBF para la definición de estrategias de mitigación, priorización basada en riesgo y fortalecimiento continuo de la postura de ciberseguridad institucional.
- Mantener una base de conocimiento actualizada sobre vulnerabilidades críticas, amenazas emergentes, campañas activas de explotación y recomendaciones de seguridad aplicables al entorno tecnológico del ICBF.
- Garantizar la transferencia de conocimiento al personal designado por el ICBF sobre la operación de la solución, interpretación de resultados, priorización de vulnerabilidades, metodologías de Pentest, Virtual Patching y mejores prácticas de gestión continua de vulnerabilidades.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

7.2.11 SERVICIO DE RESPALDOS

- Administrar la(s) herramienta(s) de respaldo con la(s) que cuenta el ICBF.
- Prestar el servicio de Backups de acuerdo con las políticas y el dimensionamiento que requiera el ICBF durante la ejecución del contrato.
- Cumplir a cabalidad con lo definido por el ICBF respecto a la gestión de copias de seguridad y a la gestión para la restauración de copias de seguridad vigentes, junto a sus eventuales cambios que puedan presentarse durante el desarrollo del contrato.
- Realizar el monitoreo 7X24X365 de las soluciones de respaldo y el registro de incidencias presentadas, tales como fallos en la ejecución de una tarea de respaldo.
- Desarrollar las actividades relacionadas con respaldo (Backups) y restauración (restore) dejando registradas las acciones realizadas en la herramienta de gestión suministrada por el ICBF.
- Realizar, en coordinación con el servicio de administración de aplicaciones, el levantamiento de aplicativos y bases de datos a nivel nacional, para determinar con los diferentes responsables la pertinencia de la creación, modificación o eliminación de las políticas de respaldo asociadas a estas.
- Realización de copias de seguridad exitosas de todas las aplicaciones, bases de datos, correo electrónico, repositorios del ICBF y plataforma de virtualización, así como la verificación y certificación de la correcta realización de estas con la(s) herramienta(s) de respaldo con la(s) que cuenta la Entidad de acuerdo con las políticas de Backups vigentes en el ICBF.
- Atender las solicitudes respectivas a las políticas de Backups de la Entidad (inclusión, modificación, retiro), especificadas a través del procedimiento descrito para tal fin y de acuerdo con los tiempos allí descritos.
- Revisar mensualmente las Políticas de Backups configuradas verificando Retención, Configuración, Ejecución, Rotación y las que solicite el supervisor del contrato.
- Coordinar internamente con el ICBF y la empresa encargada de la custodia externa de los medios, los tiempos de respuesta para la restauración de copias de seguridad en casos de contingencia como: daños de equipos, desastres naturales, robos, ataques malintencionados, siniestros, fortuitos o en los casos en que el ICBF lo requiera.
- Recibir medios magnéticos (CD provenientes de las regionales y cintas de las tareas de respaldo centralizado), y remitirlos a la empresa de custodia externa de medios
- Suministrar las cintas requeridas (1800TB de almacenamiento en cintas anuales) para realizar tareas de Backups, las cuales deberán ser proporcionadas de manera granular previa solicitud del supervisor del contrato, de tipo LTO8 o en la máxima referencia en uso por la Entidad.
- Mantener actualizada, en documentación previamente concertada con el ICBF, la información correspondiente como mínimo de:
    - Inventario de medios
    - Políticas de Backups

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Información respaldada
- Reporte Consumo de almacenamiento (Cintas y Discos)

- Realizar por lo menos una (1) vez por semestre, tareas de mantenimiento preventivo sobre las soluciones de Backups con las que cuenta el ICBF, registrando las actividades realizadas en una bitácora y se presentarán en el informe del respectivo mes.
- Realizar actividades de restauración de pruebas, tanto a nivel de base de datos como de aplicación de los Backups realizados, basado en un cronograma presentado anualmente y aprobado por la Dirección de Información y Tecnología del ICBF.
- Prestar el servicio de Backups con las herramientas con la(s) herramienta(s) de respaldo con la(s) que cuenta la Entidad, para realizar las copias de seguridad de todas las aplicaciones, sistemas operativos de servidor, bases de datos, correo electrónico, repositorios de información y plataforma de virtualización.
- Proveer y mantener vigente durante la ejecución del contrato el servicio de custodia de medios que cuente con: almacenamiento, transporte de medios magnéticos, bóvedas especiales, personal capacitado en la manipulación de información y estrictas medidas de seguridad, que permitan garantizar la conservación y seguridad de la información.
- Informar al líder del servicio del ICBF sobre extravío, hurto o deterioro de los medios dentro de las 24 horas de ocurrido el suceso. En estos casos el Contratista deberá asumir los costos de reposición respectivos.
- El contratista será responsable de realizar la migración de los respaldos desde la plataforma Networker hacia la nueva plataforma Veeam Backup & Replication, asegurando que los procesos de copia y retención en cinta se ejecuten en la librería IBM TS4300.

7.2.12 MICROSOFT 365 - AD

- El Contratista será responsable de la administración, gestión operativa, soporte y monitoreo continuo de la infraestructura híbrida de identidad, colaboración y seguridad del ICBF, la cual integra servicios On Premise y On Line que conforman el ecosistema de Microsoft 365. Dicha infraestructura incluye, entre otros, Active Directory, DNS, Certificate Authority, Microsoft Entra Connect, Exchange On Premise, Exchange Online, Microsoft Teams, SharePoint Online, Microsoft Defender for Identity, Microsoft Purview y Microsoft Defender for Office 365, garantizando su operación segura, estable y alineada con los lineamientos institucionales.
- Administrar, operar, soportar, mantener, controlar y monitorear Microsoft 365 (Online) y componentes Onpremises relacionados, incluido Active Directory (AD), DNS y sincronización híbrida (AD – Entra ID).
- Administrar licenciamiento (asignación, optimización, auditoría) conforme políticas ICBF. Reporte de consumo y recomendación mensual.
- Preparar evidencias técnicas y acompañar escalamiento a Microsoft u otros,

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

documentando comunicaciones y resoluciones. Notificar al Líder de Servicio al escalar.

- Garantizar disponibilidad del servicio ≥ 95% mensual (excluyendo mantenimientos programados).
- Administrar cuentas (crear, modificar, deshabilitar, eliminar), políticas de contraseñas, MFA, y controles de mínimo privilegio. Implementar y documentar cambios mediante GPO y políticas.
- Gestionar todas las solicitudes en la herramienta ITSM definida por ICBF, cumpliendo ANS. Registrar diagnóstico, acciones, evidencias y cierre.
- Operar y mantener sincronización híbrida (AD Connect), garantizar integridad y resolución de conflictos. Monitoreo y verificación diaria de replicación y estado de controladores de dominio.
- Proveer solución controlada para envíos de correos externos bajo demanda sin afectar reputación del dominio ICBF; generar reportes por envío (entregados, rechazados, errores detallados, aperturas y cliente/navegador). Integración previa autorización del ICBF.
- Implementar y gestionar política de backup y recuperación para Exchange, OneDrive, SharePoint, Teams y componentes Onpremises.
- Proponer mejoras (plan, beneficios, riesgo), y capacitar al personal designado por ICBF cuando se active nuevas funcionalidades o servicios.
- Mantener documentación técnica actualizada (configuraciones, diagramas, evidencias) y facilitar auditorías. Entregar reportes operativos mensuales y documentación requerida en auditorías.
- Administrar, operar, soportar y monitorear las capacidades de Microsoft Purview implementadas por ICBF, incluyendo etiquetas de sensibilidad, políticas de retención, clasificación de información y controles de protección de datos, garantizando su correcta operación y alineación con los lineamientos institucionales.
- Administrar, monitorear y optimizar las políticas de Prevención de Pérdida de Datos (DLP) implementadas en Exchange Online, SharePoint Online, OneDrive y Microsoft Teams. Analizar alertas, gestionar excepciones autorizadas, investigar eventos y proponer ajustes para minimizar riesgos de fuga o exposición de información institucional.

7.2.13 REDES LAN

- Administrar, operar y monitorear los equipos activos de la red LAN de las Sede Dirección General, Datacenter principal, Sede Metrópolis y Archivo Documental Sede anexa de la Dirección General, sedes Regionales, Centros Zonales, Caivas, Casas de Justicia, Unidad local, CESPA y SRPA (servicio de responsabilidad penal de adolescentes), Casas atrapasueños, CDI (Centros de Desarrollo Infantil) del ICBF.
- Mantener actualizados los inventarios de la infraestructura de la red LAN en los centros de cableado y centro de cómputo de la Sede Dirección General, Datacenter

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

principal, Sede Metrópolis y Archivo Documental Sede anexa de la Dirección General, sedes Regionales, Centros Zonales, Caivas, Casas de Justicia, Unidad local, CESPA y SRPA (servicio de responsabilidad penal de adolescentes), Casas atrapasueños, CDI (Centros de Desarrollo Infantil) del ICBF

- Desarrollar actividades periódicas de análisis de tráfico en redes LAN. Dichas actividades se desarrollarán trimestralmente y como resultado de ellas, el Contratista presentará un informe detallando el análisis de protocolos realizado, porcentaje de utilización de ancho de banda por protocolo, hallazgos de seguridad y hallazgos relacionados con configuraciones de switching en las redes y sus respectivos planes de acción para corregir problemas y mejorar las condiciones o configuraciones actuales.
- Mantener actualizada la documentación de la topología de las redes LAN de los centros de cableado y centro de cómputo de la Dirección General, datacenter principal y Sedes Anexas, incluyendo diagramas y planos, en medio magnético y notificar los cambios vía correo electrónico a la persona encargada en el ICBF.
- Realizar el escalamiento de incidentes de los problemas de hardware o software al fabricante o proveedor de los equipos de red administrados.
- Realizar respaldo periódico de las configuraciones de switches y demás equipos activos de red.
- Realizar análisis de capacidad y crecimiento de la red LAN, identificando riesgos de saturación y recomendaciones de ampliación.
- Actualizar matrices de direccionamiento IP, VLAN, puertos utilizados y asignación de equipos.
- Mantener organizado y etiquetado los cables de datos de los racks que se encuentran en los cuartos de cableado y centro de cómputo de la sede de la Dirección General, DIT y Datacenter Principal.
- Realizar el mantenimiento correctivo y preventivo a los equipos de la red LAN instalados en la Sede Dirección General, Datacenter principal, Sede Metrópolis y Archivo Documental Sede anexa de la Dirección General, sedes Regionales, Centros Zonales, Caivas, Casas de Justicia, Unidad local, CESPA y SRPA (servicio de responsabilidad penal de adolescentes), Casas atrapasueños, CDI (Centros de Desarrollo Infantil) del ICBF. que se encuentra fuera de soporte por proveedor y se deberá realizar una (1) vez al año durante el periodo del contrato.

7.2.14 REDES WLAN

- Administrar, configurar, monitorear y dar soporte de la red inalámbrica (WLAN) para las Sede Dirección General, Datacenter principal, Sede Metrópolis y Archivo Documental Sede anexa de la Dirección General, sedes Regionales, Centros Zonales, Caivas, Casas de Justicia, Unidad local, CESPA y SRPA (servicio de responsabilidad penal de adolescentes), Casas atrapasueños, CDI (Centros de Desarrollo Infantil) del ICBF
- Mantener actualizados los inventarios de la infraestructura de la red WLAN en las

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

sedes Sede Dirección General, Datacenter principal, Sede Metrópolis y Archivo Documental Sede anexa de la Dirección General, sedes Regionales, Centros Zonales, Caivas, Casas de Justicia, Unidad local, CESPA y SRPA (servicio de responsabilidad penal de adolescentes), Casas atrapasueños, CDI (Centros de Desarrollo Infantil) del ICBF.

- Entregar un informe de zonas de cobertura trimestral como mínimo o cuando el ICBF lo requiera.
- Llevar control y actualización del inventario de Access Points de acuerdo con el formato establecido por el ICBF.
- Configurar y dar soporte al portal cautivo para ingreso de visitantes a la red WLAN del ICBF de acuerdo con las políticas establecidas por el ICBF.
- Realizar el escalamiento de incidentes de los problemas de hardware o software.
- Implementar y administrar mecanismos de autenticación y seguridad (WPA2/WPA3 Enterprise, 802.1X, Radius, certificados digitales).
- Realizar estudios de cobertura (site survey) cuando se implementen nuevas sedes o se evidencien problemas de conectividad.

7.2.15 SERVICIOS DE NUBE

- Administrar, operar, monitorear y soportar de manera continua los servicios de Microsoft Azure contratados por el ICBF, garantizando su disponibilidad, desempeño, estabilidad, capacidad, seguridad y correcta operación en los ambientes de Producción, Pruebas y Desarrollo.
- Gestionar el soporte técnico especializado de los servicios de Microsoft Azure, incluyendo la atención, seguimiento y escalamiento ante Microsoft de incidentes, requerimientos, problemas, fallas y eventos que afecten la infraestructura, los servicios en la nube o los entornos híbridos de la Entidad.
- Administrar, mantener y optimizar la arquitectura Cloud del ICBF, incluyendo la Landing Zone de Azure, suscripciones, grupos de administración, grupos de recursos, redes, almacenamiento, bases de datos, máquinas virtuales, servicios PaaS, componentes de integración y demás recursos que hagan parte del entorno tecnológico administrado.
- Administrar y mantener la integración entre los servicios de Microsoft Azure y la infraestructura On-Premise del ICBF, incluyendo la gestión de entornos híbridos, sincronización de servicios, conectividad, interoperabilidad y operación de los recursos tecnológicos que interactúen con la plataforma.
- Administrar los servicios de identidad, control de acceso y gobierno de recursos de Microsoft Azure, incluyendo usuarios, grupos, roles, permisos, RBAC, identidades administradas, políticas de acceso, segregación de funciones y demás mecanismos de control que permitan garantizar la seguridad y gobernabilidad de la plataforma.
- Implementar, administrar y mantener los mecanismos de gobierno de Azure mediante Azure Policy, Management Groups, Landing Zone, etiquetas (Tags), estándares de configuración, clasificación de recursos, organización de

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

suscripciones y demás controles requeridos para asegurar la adecuada administración, trazabilidad y cumplimiento de los lineamientos definidos por el ICBF.

- Ejecutar actividades de mantenimiento, actualización, optimización, migración, reorganización, consolidación, transformación o traslado de recursos y servicios de Microsoft Azure que sean requeridas o autorizadas por el ICBF, garantizando la continuidad operativa, la minimización de riesgos y la documentación correspondiente de los cambios realizados.
- Administrar, configurar y operar los servicios de continuidad del negocio, respaldo, recuperación y recuperación ante desastres implementados sobre Microsoft Azure, garantizando la ejecución de copias de seguridad, recuperación de información y protección de recursos críticos conforme a los lineamientos establecidos por el ICBF.
- Administrar, mantener y optimizar Microsoft Azure Arc, así como los servicios asociados para la gestión centralizada de servidores y recursos híbridos, incluyendo la administración de configuraciones, inventario, extensiones, actualizaciones, parches de seguridad y demás funcionalidades habilitadas por la Entidad.
- Administrar y optimizar los servicios de monitoreo, observabilidad, registros, diagnóstico y alertamiento de Microsoft Azure, incluyendo herramientas como Azure Monitor, Log Analytics Workspace, Application Insights y demás servicios equivalentes, garantizando la supervisión permanente de la plataforma y la atención oportuna de eventos operativos y de seguridad.
- Administrar y operar Microsoft Defender for Cloud, Microsoft Defender for Servers y demás servicios de seguridad habilitados por el ICBF, realizando el monitoreo, análisis, gestión y seguimiento de alertas, vulnerabilidades, recomendaciones, hallazgos, controles de cumplimiento, Secure Score y actividades de remediación que se requieran dentro del alcance del servicio.
- Realizar el control y seguimiento del consumo de los servicios de Microsoft Azure, manteniendo actualizado el inventario de recursos, la documentación técnica y de arquitectura, así como generando informes periódicos y recomendaciones orientadas a la optimización del servicio, el fortalecimiento de la seguridad, la mejora continua y la eficiencia en el uso de los recursos contratados.
- Gestionar todas las solicitudes de Incidentes, Requerimientos, Problemas y Cambios a través de los mecanismos definidos por el ICBF, garantizando el cumplimiento de los Acuerdos de Nivel de Servicio (ANS), el acceso a la información requerida para supervisión y auditoría, la participación en mesas técnicas cuando sea requerido y la ejecución de todas las actividades conforme a las mejores prácticas del fabricante, los lineamientos de arquitectura, seguridad y gobierno definidos por el ICBF y la normatividad vigente aplicable.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

7.2.16 ADMINISTRACIÓN CENTRO DE CÓMPUTO

- Administrar y monitorear 7X24X365 la operación de la infraestructura del Centro de Cómputo de la Sede de la Dirección General y del Centro de Datos Principal. Referirse a la ficha de condiciones técnicas con su respectivo anexo de Acuerdos de Nivel de Servicio, para mayor claridad en los tiempos de respuesta.
- Llevar el registro continuo durante la ejecución del contrato de fallas, problemas, soluciones, acciones desarrolladas, respaldos, recuperaciones, trabajos realizados y en general todos los detalles de la operación en la herramienta de gestión Help People donde se registran los incidentes, requerimientos, problemas y cambios. Adicionalmente el contratista debe generar la CMDB (Configuration Management Database o Base de Datos de Gestión de la Configuración) y promover el uso de la CMDB en las operaciones diarias para asegurar que se mantenga actualizada y precisa, para ello debe poner en práctica procesos de gestión asociados a ITIL como son gestión de cambios y gestión de incidentes y problemas.
- Realizar descubrimiento automático y/o manual de inventario de activos TI de la herramienta de gestión y monitoreo provista por el ICBF.
- Entregar información actualizada de los equipos que administra para la alimentación de la CMDB del ICBF cuando este la requiera, la CMDB será administrada por el Contratista de Mesa de Servicios.
- Diseñar, documentar y mantener actualizados los procesos, procedimientos, lineamientos e instructivos del servicio y la administración de Centro de Cómputo de la sede de la Dirección General.
- Proveer los suministros y consumibles requeridos para una correcta operación del Centro de Cómputo de la Sede de la Dirección General, previa autorización del supervisor del contrato, en los equipos: UPS de 30 KVA, UPS de 270 KVA, aires acondicionados, sistema de control de incendios, sistema de control de ambiente y piso técnico, asegurando la prestación del servicio y llevando un registro actualizado de la utilización de los suministros y consumibles. Se debe incluir cambio de baterías cuando sea requerido, así como la respectiva disposición de las baterías de residuo, antes de la etapa de transición de salida.
- Gestionar las condiciones ambientales y técnicas necesarias para el funcionamiento adecuado del centro de cómputo de la sede de la Dirección General entregadas por el ICBF, en caso de daño en algún componente este deberá ser arreglado o reemplazado (incluyendo instalación y materiales) en forma inmediata por el Contratista con el fin de normalizar la operación.
- En caso de presentarse un proveedor diferente a los involucrados en el contrato, como por ejemplo un proveedor de conectividad que requiera el ingreso al centro de cómputo, el contratista debe realizar el acompañamiento al personal técnico que adelante trabajos (cualquier actividad) en el Centro de Cómputo del ICBF durante el desarrollo de su labor, previa comunicación del ICBF al Contratista.
- Realizar la gestión, administración y monitoreo para el correcto funcionamiento de los sistemas que componen el Centro de Cómputo tales como:

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Aires acondicionados.
- Sistema de puesta a tierra.
- Sistema de detección de incendios.
- Sistema eléctrico regulado UPS 30 KVA
- Control de seguridad física (seguridad perimetral, sistemas de vigilancia, sistemas de control de accesos).
- Circuito cerrado de televisión (CCTV).

Nota: El ICBF entregará al Contratista los elementos mencionados con su respectivo inventario. Para este inventario por favor referirse a la Ficha de Condiciones Técnicas y al Anexo técnico de la línea base.

- Realizar mantenimiento preventivo y/o correctivo incluyendo partes, repuestos e instalación de los siguientes equipos que se encuentran en el centro de cómputo de la sede de Dirección General:
  - Sistema Control de Incendios.
  - Transformador de aislamiento.
  - Aires Acondicionados
  - Sistema de control de acceso biométrico
  - Sistema eléctrico regulado y no regulado (tableros eléctricos) incluyendo sus componentes.
  - Sistema eléctrico regulado UPS 30 KVA y 270 KVA.
- Mantener actualizada la información de los elementos que componen el Centro de Cómputo de la sede de la Dirección General, los cuales incluyen entre otros:
  - Mapas e inventario de racks y/o equipos al servicio de ICBF alojados en ellos.
  - Mapas distribución sistema contra incendio.
  - Diagramas unifilares de tableros, puesta a tierra y sistemas eléctricos.
  - Inventario de equipos con marca, modelo y referencia, incluyendo:
  - Sistema contra incendio.
  - Aires acondicionados y climatización.
  - Trasformador de aislamiento
  - Gestión de alarmas.
  - Control de seguridad (seguridad perimetral, sistemas de vigilancia, sistemas de control de accesos).
  - Sistema eléctrico regulado UPS 30 KVA y 270 KVA
  - Topología del Data Center Principal y Centro de Cómputo
- Implementar los niveles de seguridad física necesarios como son circuito cerrado de TV y monitoreo IP, para proteger todos los equipos que se encuentran en el centro de cómputo de la sede de Dirección General. Estas medidas de seguridad también aplican en el evento que el ICBF incorporen nuevos equipos propiedad de la Entidad o equipos de terceros para proyectos o pilotos, éstos se reportarán con debida antelación al Contratista para que sean incorporados en su esquema de seguridad. El inventario inicial, junto con la línea base que establece el anexo técnico línea base, se le entregará al contratista en la etapa de transición de entrada y la

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

entidad junto con el contratista detallará dicho inventario para el efecto de cumplir las actividades contractuales.
- Realizar la inspección del control de incendio y en caso de requerirse, realizar la recarga del sistema FM200.

7.2.17 Administrador de la herramienta ITSM y Power BI

- Monitorear permanentemente la disponibilidad operativa de la plataforma ITSM y reportar de forma inmediata al fabricante y a la supervisión cualquier falla o degradación del servicio
- Parametrizar y actualizar en la herramienta los flujos de asignación automática, árboles de decisión, plantillas de correo electrónico y flujos de aprobación requeridos para la operación diaria.
- Administrar y ejecutar los procesos de creación, modificación, suspensión y desactivación de cuentas de usuario dentro de la plataforma ITSM
- Garantizar que los formularios, campos de captura de datos y flujos de información parametrizados cumplan rigurosamente con la política de Protección de Datos Personales del ICBF y la normativa legal colombiana vigente
- Escalar y tramitar ante el fabricante de la herramienta los incidentes o fallas de compatibilidad visual o funcional que surjan tras la aplicación de parches o actualizaciones del sistema
- Desarrollar y mantener automatizadas las conexiones de datos necesarias para alimentar los tableros analíticos e indicadores de gestión en Microsoft Power BI
- Control el ciclo de vida del catálogo, ejecutando la creación de nuevos servicios, la actualización de los vigentes o el retiro de los obsoletos, previa autorización de la supervisión del ICBF
- Vincular de forma unívoca cada servicio o trámite configurado en el catálogo con su respectiva matriz de tiempos de respuesta y solución (ANS) en la plataforma
- Configurar las matrices de Acuerdos de Niveles de Servicio (SLA) en el sistema, habilitando y probando las alertas tempranas visuales y notificaciones automáticas
- Alimentar y actualizar el módulo de la Base de Conocimiento, asegurando la correcta categorización de soluciones conocidas y artículos de ayuda vinculados al catálogo de servicios
- Generar, consolidar y mantener actualizado el backlog de requerimientos técnicos, mejoras funcionales, nuevas parametrizaciones y reportes solicitados por las diferentes dependencias del ICBF para la herramienta ITSM
- Apoyar la gestión de procesos ITSM, tales como Gestión de Incidentes, Requerimientos, Cambios, Activos, Configuración (CMDB), aportando información técnica confiable desde la plataforma administrada
- Diseñar, desarrollar y mantener tableros de control (dashboards) en Power BI, orientados al seguimiento de indicadores de gestión de TI, tales como disponibilidad de servicios, cumplimiento de SLA, estado de parches, inventario, seguridad y operación.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- integrar información proveniente de SCCM, herramientas ITSM y otras fuentes de datos autorizadas en Power BI, garantizando la calidad, consistencia y actualización de la información presentada.
- Implementar y configurar Gestión Integral de Tableros de Control (Dashboards): El Contratista deberá realizar el diseño, configuración, despliegue y transferencia de los tableros de control solicitados por el ICBF, garantizando su alineación con la arquitectura de datos de la Entidad. Esta obligación se desglosa en los siguientes componentes:
- Implementación y Publicación: Diseñar y configurar los tableros utilizando exclusivamente las herramientas, licenciamiento y servicios tecnológicos vigentes en el ICBF. El despliegue se realizará en los entornos (producción/pruebas), plataformas (Power BI, Tableau, etc.) y dispositivos institucionales que la Entidad designe, asegurando la optimización para diferentes formatos de visualización.
- Transferencia de Propiedad y Administración: Una vez aprobado el tablero por la supervisión, el Contratista deberá realizar la transferencia total de la administración y la propiedad intelectual de los desarrollos al ICBF. Esto incluye la entrega de un Anexo Técnico detallado que contenga:
    - Arquitectura de la solución y fuentes de datos conectadas.
    - Documentación lógica de todas las métricas, indicadores y medidas, independientemente del lenguaje de programación o motor de cálculo utilizado (DAX, SQL, Python, R, entre otros).
    - Diccionario de datos (dimensiones y hechos).
    - Parametrización de permisos y niveles de seguridad.

- Aseguramiento y Soporte Técnico: Garantizar la disponibilidad, integridad y correcta actualización de los datos visualizados en los tableros desarrollados. El Contratista deberá brindar soporte técnico correctivo y evolutivo durante toda la vigencia del contrato, resolviendo incidencias de visualización, errores en los cálculos o ajustes por cambios en las fuentes de origen en los tiempos de respuesta definidos en los Niveles de Servicio (SLA).

7.2.18 Administrador SystemCenter y Herramientas de Gestión y monitoreo, Intune y AZURE ARC:

- Configurar en la herramienta de monitoreo los niveles de servicio establecidos, habilitando y probando las alertas tempranas visuales, umbrales de rendimiento y notificaciones automáticas previas a la indisponibilidad de los servicios.

- Generar la documentación necesaria a fin de verificar los ANS establecidos en el anexo 02.

- Garantizar la gestión y el monitoreo de la Infraestructura desde el primer día de la operación mediante la herramienta propiedad del ICBF.

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Administrar, configurar, operar y mantener las capacidades de Microsoft Intune disponibles para el ICBF, orientadas a la gestión centralizada de dispositivos, cumplimiento de políticas, administración de aplicaciones, perfiles de configuración, líneas base de seguridad, enrolamiento, inventario, control de acceso condicional y gobierno de endpoints corporativos, conforme a los lineamientos definidos por la Entidad.
- Definir, implementar, ajustar y monitorear políticas de cumplimiento y configuración sobre dispositivos administrados mediante Microsoft Intune, incluyendo equipos Windows, dispositivos móviles y demás endpoints que el ICBF determine, garantizando su alineación con las políticas institucionales de seguridad, protección de la información, administración de identidades y gestión de activos tecnológicos.
- Gestionar el ciclo de vida de los dispositivos administrados por Intune, incluyendo enrolamiento, asignación de perfiles, despliegue de aplicaciones, scripts, configuraciones, actualización de políticas, retiro, baja o cambio de estado de los equipos, asegurando la trazabilidad y actualización de la información en los repositorios, inventarios o CMDB definidos por el ICBF.
- Administrar, operar y mantener las capacidades de Azure Arc disponibles para el ICBF, con el fin de habilitar la gestión, gobierno, inventario, monitoreo, actualización, etiquetado, cumplimiento y seguridad de servidores, máquinas virtuales, recursos híbridos, multinube u on-premise que sean incorporados por la Entidad bajo este modelo de administración.
- Implementar y mantener actualizados los agentes, conectores, extensiones y configuraciones requeridas para la integración de servidores y recursos tecnológicos con Azure Arc, garantizando su correcta visualización, administración, monitoreo y cumplimiento desde las herramientas habilitadas por el ICBF.
- Apoyar la definición, implementación y seguimiento de políticas de gobierno, seguridad, cumplimiento, actualización y monitoreo sobre los recursos incorporados a Azure Arc, incluyendo inventario, etiquetas, estado de conectividad, cumplimiento de configuraciones, administración de actualizaciones, alertas y reportes asociados.
- Integrar la información generada por System Center, Intune, Azure Arc, Azure Operations Management Suite y demás herramientas de gestión y monitoreo disponibles, con los procesos de gestión de configuración, inventario, incidentes, problemas, cambios, capacidad, disponibilidad, seguridad y continuidad definidos por el ICBF.
- Implementar y operar los todos módulos System Center y Azure Operations Management Suite que estén disponibles en el ICBF para el monitoreo y control de la infraestructura el ICBF. El ICBF podrá solicitar la implementación y/o modificación, técnica, funcional y operativa de cualquiera de los módulos de la suite System Center y Azure Operations Management Suite. Toda implementación, modificación y/o configuración, bases de datos que estén sobre System Center y Azure Operations Management Suite, será total propiedad del ICBF, las mismas deben alinearse a los procedimientos y lineamientos que el ICBF disponga para tal fin, debe cumplir con las buenas prácticas del fabricante y al final del contrato deben ser entregadas debidamente

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

documentadas.

- Definir, administrar y monitorear las políticas de actualización de parches para servidores, computadoras de usuarios finales y otros dispositivos actualizables como tabletas y móviles según sea el caso, por medio de WSUS o cualquier otra herramienta disponible para mantener actualizada la seguridad de los sistemas operativos.
- Garantizar el debido funcionamiento de WSUS integrado con SystemCenter durante toda la ejecución del contrato.
- Presentar informe mensual de herramientas de gestión y monitoreo donde se incluya el estado y gestión de estas.
- Realizar y/o Actualizar toda la documentación que el ICBF requiera respecto al servicio de Herramientas de Gestión y Monitoreo, la documentación debe estar alojada en los repositorios que el ICBF designe para tal fin.
- Usar la Suite System Center para cumplir los requerimientos del presente documento a nivel de herramientas, en caso de necesitar algún módulo de System Center o Azure Operations Management Suite no implementado, El Contratista podrá implementar y operar el mismo en pro del beneficio y utilización de herramientas propias del ICBF.
- Implementar, mejorar, optimizar o actualizar los servicios de los distintos módulos de SystemCenter y Azure Operations Management Suite con el fin de realizar la gestión de Administración, Gestión y Monitoreo acordes a las necesidades del ICBF y su infraestructura tecnológica.
- Utilizar System Center y Azure Operations Management Suite para resolver cualquiera de los requerimientos del presente anexo técnico, siempre y cuando la herramienta lo realice de forma nativa o con los módulos certificados por fabricante para este fin (Configurations y Management Packs), en caso de que el módulo o la funcionalidad no esté implementada El Contratista deberá implementarla, administrarla y gestionarla, con el personal idóneo y aprobado por el ICBF; Antes y durante la implementación de cualquier modulo debe realizar las integraciones pertinentes con otros servicios y/o contratos dentro del marco del presente anexo técnico, toda implementación y/o acción debe quedar debidamente documentada.
- Suministrar las herramientas adicionales que considere necesario para el cumplimiento del presente previo concepto-consulta técnica del fabricante o su documentación publicada, de las herramientas que están como propiedad del ICBF donde se evidencie el no cumplimiento del requerimiento específico, esto en caso de que la Suite System Center o Azure Operations Management Suite o las herramientas antes expuestas no cumplan algún requerimiento del presente capitulo.
- Suministrar toda la infraestructura con su respectivo licenciamiento, Bases de Datos, Sistemas Operativos, recursos físicos o lógicos necesarios para el funcionamiento de las herramientas que sean de propiedad del contratista, o que use en el marco de la ejecución de este contrato. En caso de suministrar herramientas de monitoreo y gestión adicionales estas deben ser de dedicación exclusiva del ICBF durante la ejecución del Contrato.
- Mantener, Administrar y Operar las herramientas de gestión que están actualmente implementadas en el ICBF.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Suministrar Herramienta(s) en caso de que las herramientas del ICBF de forma comprobada técnicamente no cumplan algún requerimiento que se solicite.
- Permitir la generación de notificaciones de eventos y alarmas en tiempo real para la creación automática de tickets para la herramienta de gestión de mesa de servicio del ICBF y que éstas también lleguen al personal designado por el ICBF.
- Programar y realizar transferencias de conocimiento con la duración que se necesite en lo que concierne a la operación, dirigidas al personal que el ICBF designe, donde se incluya: herramientas de gestión, monitoreo y diagnóstico provistas por El Contratista y las demás herramientas que se utilicen durante el desarrollo del proyecto. Las transferencias de conocimiento deben realizarse de manera periódica cuando existan actualizaciones sobre las herramientas o cambios en el personal designado por el ICBF.
- Gestionar la administración y monitoreo de todos los Ítems solicitados en el capítulo de herramientas de gestión y monitoreo del presente documento, a través de las herramientas propias del ICBF y/o suministradas por El Contratista en caso de ser necesario, permitiendo generar esquemas de monitoreo personalizables y accesibles.
- Gestionar el monitoreo para todos los EndPoints productivos, activos o de contingencia que el ICBF designe, a través de las herramientas propias del ICBF o suministradas por El Contratista en caso de ser necesario, permitiendo generar esquemas de monitoreo personalizables y accesibles.
- Parametrizar y monitorear todos los elementos activos, pasivos y de contingencia que se encuentren operativos en la infraestructura del ICBF dentro de la Herramienta provista por la Entidad o la dispuesta por el contratista.
- Gestionar el adecuado descubrimiento automático de hardware y software de los Endpoints que el ICBF designe, de tal manera que se almacene y actualice de manera automática el inventario en la base de datos centralizada (CMDB) que este activa en el momento para ICBF, deberá contener detalles de cada ítem o elemento de configuración de la infraestructura tecnológica y debe permitir la relación entre ellas y las incidencias, problemas, cambios y otros datos del servicio de TI, garantizando así, contar con la información actualizada.
- Realizar despliegue de Aplicaciones, Configuraciones, Scripts, Componentes de Software a través de SystemCenter según lo requiera el ICBF.
- Activar, administrar, gestionar, monitorear y soportar el licenciamiento de todos los Equipos Servidores del ICBF productivos, activos o de contingencia, usando las herramientas entregadas por ICBF (System Center, Servidor KMS para Licenciamiento Microsoft, servidor de licencias AutoCAD, servidor de licencias SPSS, otros) y utilizar los medios necesarios para administrar el licenciamiento que se adquiera o que no esté cubierto por las herramientas entregadas por ICBF.
- Mantener control de la línea base de Licenciamiento y el número de máquinas reportadas por las herramientas (maquinas activas
- y de laboratorio), para así trabajar en conjunto con el ICBF en la correcta gestión y control del licenciamiento que el ICBF tiene adquirido.
- Ejecutar una aplicación que permita trimestralmente identificar en los servidores y equipos de usuario final de los colaboradores del ICBF si tienen herramientas SQL

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

server instaladas, con su respectiva versión-edición y entregar un informe detallado de los servidores y equipos que se detecten con dichas herramientas.
- En caso de que la Entidad requiera cambiar la plataforma de monitoreo, contratista deberá realizar la migración de todos los elementos de configuración.
- El contratista deberá presentar el contrato de adquisición del licenciamiento de la herramienta alterna usada por el en caso de requerirse y deberá estar acorde con las normativas de derechos de autor aplicables.

7.2.19 SERVIDORES Y ALMACENAMIENTO

- Instalar y configurar adecuadamente el software de Sistema Operativo y de aplicaciones de acuerdo con los requerimientos del ICBF y las mejores prácticas del fabricante.
- Generar un plan con el fin de que los logs de seguridad de los servidores queden en un repositorio centralizado el cual pueda ser indexado por una herramienta para la búsqueda de soluciones a incidentes presentados o consultados por el especialista del Contratista.
- Verificar las bitácoras de errores, problemas y logs para búsqueda de causas de incidentes ocurridos y/o para prevenir su ocurrencia.
- Instalar, configurar, administrar y monitorear nuevo hardware y software para servidores que entren en operación durante el contrato, cuando el ICBF así lo requiera.
- Realizar la instalación, configuración, administración y monitoreo a nivel de servidores, servicios DHCP, DNS, FTP Server, Terminal Server, File Server, FailOver Clúster, políticas GPO.
- Generar un plan y realizar la aplicación de actualizaciones a firmware, fixes y parches de sistemas operativos en servidores de producción el cual debe someterse a una fase de prueba en máquinas dedicadas para ello, las cuales son suministradas por el ICBF.
- Realizar la marcación de los servidores físicos de acuerdo con los lineamientos dados por el ICBF.
- Administrar, monitorear y mantener durante la ejecución del contrato los espacios en disco, realizando depuración y/o generando la notificación al ICBF a que haya lugar para prevenir incidentes.
- Generar y entregar al líder de servicio vía correo electrónico informe trimestral con la lista de servidores sin utilizar en un período igual o mayor a 3 meses.
- Configurar en todos los servidores objeto de monitoreo los agentes necesarios para la notificación en la herramienta de gestión que se encuentre en operación en el ICBF para la apertura de tickets.
- Notificar al líder del servicio del ICBF cualquier incidente que afecte la prestación del servicio, a través de correo electrónico y/o telefónicamente o por otro medio disponible según la hora de aparición del incidente, y actuar proactivamente en la búsqueda y aplicación de la solución.
- Proponer cambios en caso de requerirse, documentar y mantener actualizados los procesos, procedimientos, lineamientos e instructivos del servicio de Servidores.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Analizar, diseñar, proponer y ejecutar las configuraciones y arreglos de servidores necesarios para dotar de alta disponibilidad la plataforma de clusterización de servidores.
- Instalar, configurar, administrar, monitorear y/o brindar apoyo a los proveedores sobre el nuevo hardware de servidores y software que entre en operación durante el contrato cuando el ICBF lo requiera.
- Analizar, diseñar, proponer y ejecutar las configuraciones necesarias previa verificación del ICBF de nuevos sistemas que optimicen procedimientos.
- Generar los mapas lógicos de interconexión de servidores de aplicaciones y base de datos y mantenerlos actualizados.
- Dar respuesta a las consultas técnicas realizadas por el ICBF por el medio definido en acta de comité técnico y el tiempo establecido en ella, asesorando en el mejoramiento, estructura y ampliación de los servidores, con el fin de incluir nuevos servicios tanto para el cliente externo (servicios en Internet) como para el cliente interno, y respondiendo a las necesidades de crecimiento del ICBF en servicios y aplicaciones.
- Documentar cada ticket en la herramienta que disponga el ICBF (llamada de servicio, incidente o problema) relacionado con fallos en los servidores. Dar apoyo en el diagnóstico de las causas de estos, independientemente del ambiente del servidor (Piloto, Desarrollo, Pruebas, Producción) y presentar el informe respectivo.
- Mantener actualizado el listado de servidores, sus componentes y software instalado y suministrar la información al contratista de mesa de servicio con el fin de mantener la CMDB actualizada. Además, mantendrá actualizadas las hojas de vidas de los servidores en un formato diseñado para ello en conjunto y presentarlas al ICBF cuando este lo requiera.
- Llevar a cabo el análisis, diagnóstico y corrección de fallos y problemas técnicos presentados en hardware y en sistemas operativos y/o hacer seguimiento al proveedor o fabricante en el evento de que alguna solución requiera de tal escalamiento y presentar los informes correspondientes en un tiempo no superior a las 24 Horas siguientes al incidente.
- Cuando se presente una falla en los servidores y no sea posible la solución remota, El Contratista deberá desplazarse a los Datacenter y dar soporte en sitio.
- Permitir el acceso a ficheros compartidos por la red de área local.
- Mantener la disponibilidad de las soluciones de almacenamiento y File Server del ICBF.
- Mantener y presentar carpetas gestionando el acceso y permisos a los colaboradores del ICBF.
- Entregar en calidad de servicio y durante toda la etapa de operación una infraestructura tipo hiperconvergente en alta disponibilidad que incluya su licenciamiento, soporte técnico y garantía hasta la vigencia del contrato, que cumpla como mínimo la siguiente capacidad de cómputo establecidos en el numeral **6.9.13**.

7.2.20 SERVICIO DE TELEFONÍA

- Instalar y configurar adecuadamente el software de Sistema Operativo y de aplicaciones

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

de acuerdo con los requerimientos del ICBF y las mejores prácticas del fabricante.

- Generar un plan con el fin de que los logs de seguridad de los servidores queden en un repositorio centralizado y vinculado al SIEM el cual pueda ser indexado por una herramienta para la búsqueda de soluciones a incidentes presentados, correlación de eventos o consultados por el especialista de El Contratista. El análisis de éstos debe ser responsabilidad del SOC.
- Verificar las bitácoras de errores, problemas y logs para búsqueda de causas de incidentes ocurridos y/o para prevenir su ocurrencia.
- Instalar, configurar, administrar y monitorear nuevo hardware y software para servidores de telefonía que entren en operación durante el contrato, cuando el ICBF así lo requiera.
- Realizar la marcación de los servidores de telefonía físicos de acuerdo con los lineamientos dados por el ICBF.
- Configurar en todos los servidores de telefonía objeto de monitoreo los agentes necesarios para la notificación en la herramienta de gestión que se encuentre en operación en el ICBF para la apertura de tickets.
- Gestionar actualizaciones y parches de la plataforma de telefonía Gestionar la configuración de teléfonos IP y softphones
- Realizar el monitoreo proactivo de las troncales SIP asociadas al servicio, garantizando su disponibilidad, estabilidad y correcto funcionamiento bajo un esquema de atención continua 7x24x365Realizar escalamiento de incidentes con fabricantes y operadores de telecomunicaciones.
- Notificar al líder del servicio del ICBF cualquier incidente que afecte la prestación del servicio, a través de correo electrónico y/o telefónicamente o por otro medio disponible según la hora de aparición del incidente, y actuar proactivamente en la búsqueda y aplicación de la solución.

7.2.21 SISTEMA DE CORRIENTE REGULADA

- Realizar el mantenimiento preventivo de las UPS de acuerdo con el cronograma establecido, verificando el correcto funcionamiento de los equipos y sus componentes.
- Ejecutar las actividades de mantenimiento correctivo requeridas para atender fallas o anomalías detectadas en las UPS, garantizando la pronta recuperación de la operación.
- Inspeccionar y verificar el estado de las baterías, conexiones eléctricas, módulos de potencia, sistemas de ventilación y demás componentes asociados a las UPS.
- Realizar pruebas funcionales y de autonomía de los equipos, con el fin de validar su capacidad de respaldo y continuidad del servicio ante interrupciones del suministro eléctrico.
- Presentar informes técnicos de mantenimiento que incluyan las actividades ejecutadas, hallazgos, recomendaciones, repuestos utilizados y estado general de los equipos intervenidos.
- Atender oportunamente las solicitudes y requerimientos de soporte técnico, cumpliendo los tiempos de respuesta y solución definidos por la entidad.
- Suministrar e instalar los repuestos y elementos necesarios para la reparación de las

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

UPS cuando se requiera, garantizando que sean compatibles y cumplan con las especificaciones técnicas del fabricante.
- Cumplir con las normas de seguridad industrial, salud en el trabajo y normatividad eléctrica vigente, durante la ejecución de las actividades de mantenimiento.
- Mantener actualizada la documentación e historial de mantenimiento de las UPS, registrando las intervenciones realizadas, novedades identificadas y acciones ejecutadas para asegurar la trazabilidad de los equipos.

7.3 Obligaciones del Sistema Integrado de Gestión

7.3.1 Obligaciones del Eje de Calidad

- Asegurar que el personal requerido para la prestación del servicio cuente con el perfil de: Educación (formal: primaria, secundaria, pregrado, posgrado), formación (cursos específicos de la actividad a desarrollar como diplomados, seminarios, talleres entre otros) o experiencia para garantizar la óptima prestación del servicio.
- Socializar con el equipo de trabajo que realiza las actividades definidas en el contrato, la información básica del ICBF (Misión, Visión, Normatividad interna vigente, Objetivos Estratégicos, Políticas y Sistema Integrado de Gestión SIGE) así como dar a conocer los diferentes documentos (lineamientos técnicos, manuales operativos, procedimientos, guías, formatos, entre otros) necesarios para la operación de los servicios contratados.
- Identificar y gestionar acciones de mejora que fortalezcan de manera adecuada la prestación de servicio.
- Contar con información documentada para la recepción, tratamiento y respuesta a las peticiones, quejas, reclamos y sugerencias (PQRS), en el marco de la ejecución del objeto contractual.
- Contar con un registro de los documentos utilizados para la operación del servicio, incluyendo de ser necesario, el control de los cambios realizados.

7.4 Obligaciones del Eje de Seguridad de la Información

- Certificar el cumplimiento, seguimiento y revisión de los asuntos correspondientes a seguridad de la información enmarcado en la normativa interna del ICBF vigente en virtud de la ejecución del objeto del contrato.
- Suscribir un documento de compromiso de confidencialidad el cual deberá ser entregado al supervisor del contrato una vez se firme el contrato.
- Informar al supervisor, en el momento que ocurran incidentes de seguridad o se materialice un riesgo de seguridad de la información que afecten la disponibilidad, integridad y/o confidencialidad de la información del ICBF, en el marco de la ejecución del contrato.
- Certificar el cumplimiento de la cadena de Suministro TIC, de acuerdo con establecido en la Política de la Seguridad de la Información del ICBF.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Prever el plan de recuperación y contingencia del servicio contratado ante los eventos que puedan afectar el cumplimiento de la ejecución de este.
- Certificar el cumplimiento de la cadena de Suministro TIC, de acuerdo con establecido en la Política de la Seguridad de la Información del ICBF.
- Cumplir con lo establecido en la G22.GT “Guía para el Uso de dispositivos personales -BYOD”- cuando se requiera conexión de equipos que no son propiedad de ICBF a la red institucional
- Identificar, documentar y evaluar los riesgos de seguridad de la información relacionados con los procesos, sistemas y servicios que estén dentro del alcance del objeto contractual, conforme a las mejores prácticas internacionales, tales como las establecidas en la norma ISO/IEC 27001:2022 o su equivalente y alineadas con la Política de Seguridad de la información definidas con el operador de servicios de tecnología

7.5 Obligaciones del Eje de Seguridad y Salud en el Trabajo

- Certificar que cuenta con un representante de seguridad y salud en el trabajo, que cumpla con el perfil establecido en la Resolución 312 de 2019, o a la norma que adicione, modifique o sustituya y garantice el cumplimiento de obligaciones contractuales establecidas en el marco de la ejecución del contrato o convenio y la normatividad vigente.
- Presentar la identificación de peligros, valoración de riesgos y determinación de controles, documentados, en el marco de la Seguridad y Salud en el Trabajo durante la ejecución del contrato o convenio.
- Realizar la inducción al equipo de trabajo que se empleará durante la ejecución del contrato o convenio en materia de Seguridad y Salud en el Trabajo.
- Suministrar a los colaboradores vinculados para la ejecución del contrato o convenio los elementos de protección personal requerido para la realización de sus actividades.
- Presentar el concepto médico ocupacional favorable de los colaboradores vinculados para la ejecución del contrato o convenio.
- Informar al ICBF los Accidentes de Trabajo y enfermedad Laboral – ATEL del personal a cargo del operador/contratista, reportados a la ARL y EPS, durante el plazo de ejecución del contrato o convenio.
- Designar un brigadista para que haga parte activa del Plan de Emergencias y Contingencias del ICBF, así como garantizar la socialización de este Plan a los colaboradores vinculados por el contratista que prestan sus servicios en las sedes del ICBF.

7.6 Obligaciones del Eje de Gestión Ambiental

- Adoptar las medidas necesarias para el ahorro y uso eficiente de agua, energía,

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

papel, y manejo de residuos que se generen durante la ejecución del contrato, de acuerdo con la Política Ambiental de la Entidad.

- Utilizar productos, empaques y materiales amigables con el medio ambiente.
- Adoptar las medidas necesarias para el almacenamiento y manejo adecuado de los productos químicos utilizados durante la ejecución del contrato; de acuerdo con la normatividad vigente.
- Adoptar las medidas necesarias para el manejo adecuado y la disposición final de los residuos especiales y/o peligrosos que se generen durante la ejecución del contrato.

8. LUGAR DE EJECUCIÓN DEL CONTRATO

El lugar de ejecución del contrato será a nivel nacional, teniendo en cuenta que los servicios se prestarán en la Sede de la Dirección General y la sede donde esté ubicada la Dirección de Tecnologías de la Información, el Centro de Cómputo, las Sedes Regionales (ubicadas en las ciudades capitales de cada departamento), el lugar donde esté ubicado el Datacenter Externo y/o principal, de acuerdo con el alcance de los servicios descritos en la Ficha de Condiciones Técnicas y este documento.
El Contratista deberá garantizar la presencia física de los especialistas encargados de los servicios objeto de este contrato cuando la operación lo requiera, ya sea en las instalaciones de la Sede de la Dirección General o en los Datacenter de la Entidad.

Nota: En caso de que las sedes se trasladen o cambien sus ubicaciones físicas, el Contratista deberá continuar prestando los servicios de operación global en las nuevas ubicaciones informadas por el ICBF. Para aquellos lugares diferentes a Bogotá y sus alrededores el servicio podrá ser prestado de forma remota, previa aprobación de la supervisión del contrato.

9. PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será por 12 meses, previo cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato.

10. FORMA DE PAGO DEL VALOR DEL CONTRATO

El valor del contrato a suscribir será por el valor resultante de la adjudicación, incluidos todos los costos directos e indirectos asociados a la prestación del servicio, incluido el IVA y demás impuestos de ley.

Parágrafo 1 – Servicios Efectivamente Prestados: Los pagos se efectuarán únicamente por los servicios efectivamente prestados y conciliados mensualmente, previa entrega y

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

aprobación de los informes y productos mensuales establecidos en las obligaciones y en el anexo técnico, y sujeto a la conformidad del ICBF. En caso de que el servicio requerido no sea prestado a la Entidad, el contratista no incluirá dicho servicio en la respectiva factura.

Parágrafo 2 – Descuentos por ANS: Adicionalmente, a partir del mes (inclusive) sobre los servicios efectivamente prestados mensualmente, se efectuará el descuento por acuerdos de niveles de servicio (si aplica, de acuerdo con la conciliación del servicio), con lo establecido en el anexo técnico y anexo de ANS. Los pagos se realizarán previa certificación de la supervisión a los cuales se les efectuará los descuentos por acuerdos de niveles de servicio.

Se pagará al contratista así:

- Durante la etapa de transición de entrada no se reconocerán pagos al contratista por dicha labor.

- Durante la etapa de Operación, el ICBF realizará pagos mensuales al Contratista por los servicios efectivamente prestados. El valor por pagar mensualmente corresponderá al valor ofertado por el contratista para cada servicio descrito en el Anexo 03 - Línea Base de Servicios TI, luego de haber aplicado los ANS descritos en el Anexo 02 – Acuerdos de Niveles de Servicio o cuando a ello hubiere lugar. Y en el caso de evidenciar servicio no prestado se afectará el pago mensual del servicio afectado.

- Se aclara que, una vez finalizadas las implementaciones, se iniciará con la medición de los ANS, sin penalización durante un (1) mes considerándolo este tiempo de estabilización del servicio. Y en el mes subsiguiente se aplicarán las respectivas penalizaciones, las cuales se verán reflejadas como descuentos en la facturación. Lo anterior, con el fin que el servicio entregado cumpla con lo requerido por la entidad, con las características de calidad y oportunidad.

- Los entregables o productos requeridos por la entidad, vinculados a las actividades de gestorías y considerados servicios transversales de la operación, serán catalogados como servicios no prestados en caso de que no hayan sido suministrados en su totalidad. La omisión o cumplimiento parcial en la prestación de estos servicios afectará el ítem correspondiente a la gestión de proyecto en la propuesta económica, conforme a los términos y condiciones establecidas en el contrato.

- El contratista deberá presentar la factura de los servicios efectivamente prestados post aprobación de los informes mensuales de gestión (por servicio del respectivo periodo facturado) y el informe de ANS aprobado por el ICBF.

- El Contratista deberá discriminar de manera separada en la facturación los ítems adquiridos con cargo a la Bolsa de Consumibles para Mantenimientos Correctivos y

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Repuestos, Partes y Accesorios, como requisito para su validación, aprobación y pago por parte del ICBF.

- Para los mantenimientos preventivos se pagará mensualmente conforme a los servicios efectivamente suministrados al ICBF, de acuerdo con el valor unitario ofertado y previa aprobación por parte del supervisor del contrato, incluidos descuentos por no cumplimiento conforme a lo establecido en el "Anexo_02 Acuerdo de Niveles de Servicio", o por servicios no prestados en cuanto a mantenimientos preventivos.

- La no presentación a tiempo de la factura generará penalizaciones. Sin embargo, la fecha máxima de radicación de facturas se establecerá dependiendo de los cronogramas definidos por la Dirección Financiera del ICBF. En aquellos casos que la radicación sea posterior, para el cierre de vigencias se podrá pagar o constituir como una cuenta por pagar, siempre y cuando las disposiciones financieras de la entidad lo permitan.

- Los pagos se realizarán previa certificación de recibo a satisfacción por parte del supervisor y presentación de la factura correspondiente con sus respectivos soportes: certificación del revisor fiscal o representante legal, según corresponda, cumplimiento en el pago de los aportes parafiscales y de seguridad social de sus empleados, certificación bancaria. Lo anterior, con lo establecido en el artículo 50 de la Ley 789 de 2002 y artículo 23 de la Ley 1150 de 2007.

- El contratista deberá presentar la factura de los servicios efectivamente prestados dentro de los primeros diez (10) días hábiles de cada mes. Teniendo en cuenta la implementación de facturación electrónica, el contratista debe remitir las facturas al buzón siifnacion.facturaelectronica@minhacienda.gov.co, indicando en el asunto los siguientes datos: PCI;#CONTRATO;CORREO SUPERVISOR. Se deberá adjuntar únicamente la factura electrónica en representación gráfica y el archivo XML de la factura. En las notas de la factura se debe incluir el siguiente texto: #$PCI;CONTRATONo.;CORREOSUPERVISOR#$. Las facturas se revisarán, aprobarán o rechazarán por el supervisor del contrato, directamente en la plataforma SIIF Nación del Ministerio de Hacienda. Si al realizar la verificación de una factura esta no cuenta con la información completa para su aprobación, será rechazada y se solicitarán las correcciones a la misma. La factura corregida debe ser enviada nuevamente al buzón de SIIF Nación. Los documentos adicionales a la factura deberán ser remitidos directamente al correo que el supervisor del contrato disponga para el efecto.
- El pago se realizará dentro de los treinta (30) días hábiles siguientes a la radicación de la factura y la certificación de cumplimiento, previa aprobación del PAC (Programa Anual Mensualizado de Caja).

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

- Si la(s) factura(s) no ha(n) sido correctamente elaborada(s), o no se acompañan los documentos requeridos para el pago, el término para este solo empezará a contarse desde la fecha en que se presenten debidamente corregidas, o desde que se haya aportado el último de los documentos solicitados. Las demoras que se presenten por estos conceptos serán de responsabilidad del contratista y no tendrá por ello, derecho al pago de intereses o compensación de ninguna naturaleza.

- Todos los pagos se realizarán conforme al PAC del Instituto Colombiano de Bienestar Familiar y la obligación de pago de EL ICBF se contará a partir de la fecha en que se reciba la factura o cuenta de cobro con los documentos exigidos, y correcta situación que sabe y acepta EL CONTRATISTA. Las retenciones y descuentos de Ley a que haya lugar estarán a cargo de EL CONTRATISTA.

11. TIPIFICACIÓN, VALORACIÓN Y ASIGNACIÓN DE LOS RIESGOS PREVISIBLES

Con el fin de conocer los riesgos que afectarían el contrato que se pretende adelantar, tanto en aspectos favorables como adversos; y con el fin de contribuir a asegurar los fines que el estado persigue con la contratación, el ICBF ha preparado el **Anexo 04 - Matriz de tipificación, valoración y asignación de riesgos,** el cual permite dilucidar aspectos que deben ser considerados en la adecuada estructuración de ofertas y planes de contingencia y continuidad del proyecto.

De este modo, corresponderá al contratista seleccionado la asunción del riesgo previsible propio de este tipo de contratación, asumiendo su costo, siempre que el mismo no se encuentre expresamente a cargo del ICBF en el **Anexo 04 - Matriz de tipificación, valoración y asignación de riesgos**

Los riesgos que podrían afectar el **normal** desarrollo de las actividades previstas en esta contratación se analizan en el **Anexo 04 - Matriz de tipificación, valoración y asignación de riesgos.**

12. ANEXOS

Anexo 01 –Personal mínimo requerido.
Anexo 02 – Acuerdos de Niveles de Servicio.
Anexo 03 – Línea Base de Servicios TI.
Anexo 04 – Matriz de tipificación, valoración y asignación de riesgos.
Anexo 05 – Entregables
Anexo 06 - Catalogo de Servicios
Anexo 07 - Sedes Soporte en Sitio
Anexo 08 - Listado de Consumibles para Mantenimientos Correctivos y Repuestos, Partes y Accesorios
Anexo 09 - Anexo 09 – UPS Nuevas y Mantenimientos Preventivos

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012

Anexo 10 – Histórico Consumo Bolsa 2025

13. ACEPTACIÓN CUMPLIMIENTO DE REQUERIMIENTOS TÉCNICOS

Señor proveedor o contratista potencial: Al remitir cotización y/o propuesta, usted está aceptando que la misma cumple con la totalidad de los requerimientos incluidos en el presente documento y que incluye la totalidad de costos y gastos, directos e indirectos, así como los impuestos, asociados a la ejecución del contrato. Así mismo, que, en caso de resultar adjudicatario del proceso de selección correspondiente, podrá prestar el servicio y/o entregar el bien, con las condiciones técnicas descritas en el presente documento.

14. APROBACIONES ICBF

Aprobaciones	Nombre	Cargo	Firma
Aprobó:	Luis Fernando Lozano Mier	DIRECTOR TÉCNICO	

Reviso:

Luz Adriana Rodriguez Diaz Profesional Especializado DTI
Jairo Enrique Baez – Contratista DTI

Elaboro:

John Adolfo Lizcano – Profesional Especializado DTI -Responsable del servicio Soporte en Sitio
Wilson Libardo Salas – Profesional Especializado DTI- Responsable de la Gestoría de Incidentes, Gestoría de Solicitudes, Gestoría de Inventario y CMDB.
Andrea Victoria Paez – Profesional Especializado DTI
Omar Uriel Ramos Ariza – Técnico Administrativo
Michel Giovanni Calderon– Contratista DTI
Marlon Guillermo Perez – Contratista DTI
Sandra Margoth Rozo – Contratista DTI
Angie Tatiana Castañeda – Contratista DTI
Eder Leonardo Castellanos – Contratista DTI
Helda Patrica Correa Muñuz – Contratista DTI
Julian Camilo Melendez – Contratista DTI
Cesar Julio Sanchez – Contratista DTI
Reinel Albeiro Vega – Contratista DTI
Teresa Quilindo Sarasti – Contratista DTI
Maura Rocio Ruiz – Contratista DTI

LOS DATOS PROPORCIONADOS SERÁN TRATADOS DE ACUERDO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL ICBF Y A LA LEY 1581 DE 2012