ANEXO TÉCNICO

A continuación, se describen los requerimientos técnicos mínimos que comprenden:

1. Nube Privada - Centro de Datos
2. Escritorios Virtuales
3. Equipo de Trabajo
4. Acuerdos de Niveles de Servicio - ANS

1. NUBE PRIVADA – CENTRO DE DATOS

Las especificaciones técnicas mínimas sin limitarse a las mismas comprenden:

1.1 Infraestructura de Datacenter
   a) Plataformas/Productos a Gestionar
   b) Administración Técnica y Gestión
1.2 Conectividad (WAN, LAN, WLAN)
1.3 Mesa de Servicios

1.1 INFRAESTRUCTURA DE DATACENTER

El contratista realizará el aprovisionamiento de la infraestructura y licenciamiento de la nube privada de La Unidad, conforme a las capacidades y demanda requerida. El coste mensual del servicio de la nube privada se realizará basado en la capacidad aprovisionada de las máquinas virtuales es decir total de CPU y Memoria Mensual Utilizado Disponible.

El contratista deberá configurar, administrar y soportar los dos (2) componentes de almacenamiento propiedad de la UGPP, este almacenamiento será utilizado por los diferentes servicios que implemente el contratista, a excepción de la solución de escritorios virtuales, la cual contará con su almacenamiento exclusivo provisto por el contratista. El contratista deberá suministrar los Switch de SAN y el licenciamiento correspondiente, como mínimo 4 puertos disponibles por cada uno.

La estimación de las capacidades a demandar en recursos de memoria, procesamiento y almacenamiento se describe en el documento denominado **LÍNEA BASE DE APLICACIONES.xls**, con su respectiva arquitectura.

Las capacidades iniciales descritas en la **LÍNEA BASE DE APLICACIONES.xls**, puede disminuir y/o aumentar dependiendo del desempeño de cada aplicación.

La Entidad podrá solicitar des aprovisionar y/o aprovisionar nuevas aplicaciones, en tal sentido La línea base tendrá Flexibilidad, teniendo en cuenta que la supervisión

podrá demandar las (n) cantidades en las diferentes líneas de servicio del contrato, de acuerdo con las necesidades tecnológicas que generen las áreas misionales y de apoyo de la entidad comprendiendo que la capacidad de infraestructura y Licenciamiento adicional debe ser provista y cobrada como capacidad adicional.

El contratista es responsable de realizar el soporte técnico y funcional a las plataformas en donde esté alojadas las aplicaciones (Nube privada/pública); para ello debe asumir la atención y solución del Nivel I y II conforme a los requerimientos de la mesa de servicios.

El centro de datos principal provisto para la implementación de la nube privada deberá cumplir con Características TIER III o Nivel IV de ICREA.

El contratista es responsable de la gestión de la red LAN para todo lo relacionado con la conectividad del centro de datos principal y el provisto para el DRP.

El contratista es responsable de asegurar la conectividad WAN (datos/internet) y seguridad perimetral entre los centros de datos (Nube Privada/Pública), donde se alojan las aplicaciones y/o servicios TI de la Entidad; esto según los anchos de banda y especificaciones técnicas mínimas previstas en la sección de conectividad.

El contratista debe realizar la implementación y puesta en marcha de los servicios contratados; teniendo en cuenta los requerimientos de implementación IPv6: Resolución 2710 de 2017 de MinTic, la cual especifica la coexistencia de los protocolos IPv4 e IPv6. La entidad suministra el direccionamiento y renovación cada año. El supervisor durante la ejecución del contrato podrá verificar las configuraciones de las plataformas que se proveen en la nube privada; a fin de constatar el cumplimiento de los requerimientos técnicos y las políticas de seguridad implementadas.

La infraestructura del centro de datos debe contar con esquemas de alta disponibilidad para dar respuesta oportuna ante cualquier interrupción, falla o incidencia a fin de asegurar el Acuerdo de Nivel de Servicio (ANS) de disponibilidad.

El contratista en compañía de la Entidad realizará revisiones técnicas que permitan mejorar las arquitecturas de las aplicaciones alojadas en los centros de datos (nube privada/pública).

El contratista deberá asegurar un espacio dentro del rack de comunicaciones del datacenter principal y el datacenter alterno (colocation) con al menos quince (15) unidades de rack, donde se pueda alojar la infraestructura de los sistemas de almacenamiento de la UGPP, de tal forma que los servicios de nube privada implementados por el contratista tengan conexión directa al almacenamiento de la UGPP. De igual manera los servicios de DRP configurados en el Datacenter alterno deberán hacer uso del sistema de Almacenamiento de la UGPP. Este espacio de alojamiento se debe mantener duranta el plazo de ejecución del contrato y un (1) mes más. Así mismo, el contratista debe asegurar la entrega de al menos 3.5 Kva, garantizar la zona de enfriamiento del almacenamiento de UGPP, con provisiones de 3.5 kva y pdu con energia y conectores a 220 para ser instalados e interconectados

con la solución de procesamiento que vaya a disponer el contratista. La solucion de Switches de fibra para interconectar cada almacenamiento debe ser provista por el contratista y disponer en cada sitio mínimo 4 puertos

El contratista del centro de datos debe garantizar la posibilidad de realizar una Cross Conexión física o lógica, para lograr la conexión entre el centro de datos y otros servicios que puedan ser contratados por La Unidad.

El contratista de centro de datos dado el esquema híbrido de infraestructuras que soportan las aplicaciones de la Entidad; debe implementar conexiones, a nubes públicas a través de VPN.

La plataforma de virtualización empleada por el contratista debe soportar las máquinas actuales de VMware.

El contratista adelantará el proceso de migración del almacenamiento rentado hasta el momento por la UGPP al almacenamiento adquirido por la entidad.

El contratista en su gestión técnica sin limitarse a la misma se obliga a: aprovisionar, administrar, operar, monitorear y brindar el soporte a las plataformas que soportan las aplicaciones de la Entidad, en cada uno de los ambientes (producción, pruebas, desarrollo). En tal sentido le corresponde la:

- Gestión de los sistemas operativos
- Gestión de la plataforma de virtualización
- Gestión de la plataforma de procesamiento
- Gestión de la plataforma de almacenamiento
- Gestión de la plataforma de respaldos y sus servicios asociados
- Gestión de la red LAN de los Centros de Datos
- Gestión de las bases de datos
- Lo correspondiente a la política y estrategia de backup de los servicios alojados en la nube pública
- Gestión de servidores de aplicaciones
- Gestión del soporte técnico funcional de las aplicaciones, realizadas con recursos a demanda por el ítem de mesa de servicios.

El contratista debe asegurar el Plan de Recuperación Tecnológica – DRP, permitiendo asegurar la continuidad de las aplicaciones productivas. En tal sentido, debe elaborar, e implementar un plan de recuperación tecnológica (DRP) para los servicios contratados, contemplando tecnologías que le permitan asegurar un RTO de dos (2) horas y un RPO de quince (15) minutos y en caso de eventos fortuitos operar en un centro de datos alterno en una localización geográfica diferente al datacenter principal.

Las capacidades de recursos requeridos para el DRP serán previamente acordadas por la Entidad.

El contratista es responsable de la estrategia del esquema de replicación asegurando en todo momento el RTO y RPO requerido por la Entidad con porcentajes no Superiores al 30% de las capacidades operativas.

La Entidad debe tener acceso(s) en línea de la plataforma de virtualización, a fin de identificar las máquinas virtuales que se ejecutan en el entorno del centro de datos. Los reportes de la plataforma de virtualización permitirán al Supervisor del contrato aprobar y verificar la capacidad instalada y la utilizada (uso).

El contratista debe asegurar que todo software/licencia esté debidamente licenciado con las políticas del fabricante y tenga soporte vigente durante toda la ejecución del contrato. Así mismo el contratista se obliga atender los requerimientos que La Unidad realice para dar respuesta a entes de control interno o externo en esta materia.

En la implementación de las plataformas tecnológicas se debe asegurar un entorno seguro en la nube privada; esto a nivel de control de perímetro, accesos lógicos, separación de ambientes, segregación de redes, identificación, control y administración de cuentas de usuario privilegiadas.

El contratista en la entrega de todos los servicios objeto del contrato debe cumplir con las políticas, procesos y subprocesos de la Dirección de Gestión de Tecnología para la gestión del servicio, alineado en las buenas prácticas de ITIL y políticas de seguridad de la información de la entidad.

La gestión de las solicitudes se prestará por parte del contratista conforme al modelo de operación de la mesa de TI, descrito en Nivel I y II y para tal fin debe atender y documentar la atención y solución en la herramienta suministrada por la mesa de servicios.

El contratista debe mantener actualizada la base de datos de configuración (CMDB), con cada uno de sus CIs que componen la arquitectura de las aplicaciones. La herramienta empleada es la provista por la mesa de servicios.

El contratista se obliga a realizar el aprovisionamiento de la infraestructura de máquinas virtuales, siendo requerido la atención de cuatro (4) horas hábiles para ambientes productivos y de ocho (8) horas hábiles para ambientes previos (calidad y desarrollo).

El contratista se obliga a comunicar los cambios a realizar en las plataformas con mínimo ocho (8) horas y la aprobación se deberá realizar conforme a lo descrito en el proceso de gestión de cambios.

El contratista se obliga a realizar pruebas de Ethical Hacking/Pentesting, bajo la modalidad de caja blanca, a los activos objeto del servicio con el fin de validar su correcta vigencia frente a las amenazas de seguridad. Se realizará cada semestre previamente planificado y deberá corroborarse con los informes de los tests que deben ser remitidos a la Entidad. El servicio debe cubrir: - Una (1) prueba por semestre.

- Pruebas de caja blanca
- Aproximadamente 15-20 aplicaciones
- Las aplicaciones para evaluar podrán ser externas y/o internas.

Balanceo de Cargas

El contratista debe tener una solución de software y/o hardware que permitan minimizar los tiempos de respuesta y mejorar el desempeño evitando la sobrecarga en la infraestructura que soportan las aplicaciones de la entidad, para mínimo 15 aplicaciones y mínimo usuarios concurrentes es de aprox. 300.

El contratista debe asegurar el balanceo de cargas de tráfico en la red interna y desde o hacia internet de los servicios de tecnología. La solución debe soportar:

- Métodos de balanceo de cargas utilizando mínimo 4 de los siguientes métodos: (Round robin, Sticky sessions, Weighted round robin, Least connections, Least response time).
- Permitir capas de trabajo en capa 4 y 7 (Puertos/sesiones/aplicación).
- El balanceador debe soportar el almacenamiento de datos en caché y compresión de contenido estático y dinámico HTTP / HTTPS.
- Sesiones concurrentes: Conexiones simultáneas en capa 4 soportadas por el servicio.
- El servicio debe soportar el uso de las versiones IPv4 e IPv6 del protocolo de Internet.
- Seguridad: Permitir el filtrado de direcciones IP y permitir/bloquear listas de control de acceso.
- Interfaz de gestión y automatización del balanceador a través de API REST.

Next Generation Firewall - NGFW

La solución de perímetro debe ser de última generación y soportar la tecnología SDWAN, permitiendo integrar la red de datos WAN y LAN de las sedes y demás servicios de tecnología, dado el modelo de datacenter híbrido con la cuenta la entidad (Nube GCP/Nube Privada).

Según el centro de datos las características mínimas del firewall deben cumplir con los siguientes requerimientos mínimos o similares.

Para centro de datos en nube privada:

- Dispositivos físicos en alta disponibilidad.
- Desempeño de protección de amenazas mínimo: 4.0 Gbps
- Conexiones concurrentes: 3.000.000
- Interfaces mínimas: (10) puertos 10/100/1000, (4) puertos 1G SFP, y (4) puertos 1G/10G SFP/SFP+

- Desempeño de inspección SSL: 1.5 Gbps
- El almacenamiento se debe realizar de manera central a través de una herramienta para el almacenamiento de logs
- Capacidades de NGFW, Descrifrado SSL/TLS, VPN (IPSEC y SSL), Protección de Amenazas, Sandbox, Antivirus, IPS/IDS, Antispam Filtrado Web, Filtrado de Archivos, Control de aplicaciones, inspección de contenido en SSL, SD-WAN (con soporte de IPv6 en underlay y overlay), todas soportadas para IPv4 e IPv6
- La solución debe integrarse con la plataforma de SIEM que emplee en el servicio del SOC, para la correlación de eventos de detecciones realizadas.

Toda la solución de seguridad perimetral debe ser configurada con las políticas de seguridad de la información de La Unidad, es responsabilidad del contratista realizar las configuraciones necesarias y permitir la gestión y accesos a las mismas. Sin embargo, el contratista debe proponer, según su experiencia y con base en buenas prácticas, configuraciones a la medida de la Entidad.

Debe permitir la configuración de políticas de seguridad de VPN basado en las características del equipo, por lo menos se deberá recopilar las siguientes características: sistema operativo, dominio de red, versión de parche, software antivirus, software DLP y software de cifrado de disco. De tal forma que si el equipo no cumple cierta condición basado en esas características (Perfilamiento y Postura), no permita el acceso a la VPN o le otorgue acceso de mayores restricciones.

El contratista debe suministrar entornos de trabajo privado a través de VPN (Site to Site o Client to Site), el número actual es de aprox. 10 site to site.

La unidad podrá demandar (n) número de conexiones de usuarios SSL VPN en función a la necesidad y el acceso debe contemplar el doble factor de autenticación, lo cual deberá aprovisionarse a través de una funcionalidad o módulo de la solución, sin que esto implique licenciamiento adicional.

El contratista debe suministrar los (n) entornos de trabajo privado a través de VPN (Site to Site o Client to Site).

La solución de perímetro se debe configurar a partir de políticas de usuarios y/o grupos del Active Directory.

La configuración perimetral debe permitir filtro de contenido permitiendo la restricción de navegación de sitios.

La solución puede ser en cloud y/o local.

En todo caso, deberá tener soporte del fabricante durante el plazo de ejecución del contrato.
La solución debe integrarse con la plataforma de SIEM que emplee en el servicio del SOC, para la correlación de eventos de detecciones realizadas.

En el proceso de implementación y ejecución del servicio, la Oficina de Seguridad de la Información de la Entidad realizará las respectivas recomendaciones que el contratista deberá acoger a fin de proteger la información.

Firewall de Aplicaciones Web - WAF

Según el centro de datos las características mínimas del firewall deben cumplir con los siguientes requerimientos mínimos o similares.

Para centro de datos en nube privada:
- Desempeño: 1.3 Gbps
- Aplicaciones soportadas: 8 sitios
- Capacidades de análisis de anomalías, bots y ataques basados en mecanismos de aprendizaje de máquina.
- Protección de APIs basada en aprendizaje de máquina.
- Protección de antimalware para los archivos subidos a las aplicaciones.
- Protección antidefacement para las páginas de la entidad
- La solución debe incluir funcionalidades nativas de sandboxing

Para centro de datos en nube pública:
Implementación en auto-scaling en caso de ser necesario para agregación de ancho de banda
- Desempeño: 3 Gbps
- Aplicaciones soportadas: 8 sitios
- Capacidades de análisis de anomalías, bots y ataques basados en mecanismos de aprendizaje de máquina.
- Protección de APIs basada en aprendizaje de máquina.
- Protección de antimalware para los archivos subidos a las aplicaciones.
- Protección antidefacement para las páginas de la entidad
- La solución debe incluir funcionalidades nativas de sandboxing
- Integración con soluciones tipo SIEM
- Capacidad de análisis de vulnerabilidades para las aplicaciones protegidas.
- Posibilidad de crear políticas de control de acceso a las aplicaciones o URL basado al menos en:
- Direcciones IP orígenes.
- Blacklist basado en la reputación de la IP en Internet como proxys anónimos, Botnets, Phishing, Spamer.

- Geolocalización, bloquear tráfico de Países.

La solución puede ser en cloud y/o local. En todo caso, deberá tener soporte del fabricante durante el plazo de ejecución del contrato.

La solución debe integrarse con la plataforma de SIEM que se emplee en el servicio del SOC, para la correlación de eventos de detecciones realizadas.

En el proceso de implementación y ejecución del servicio, la Oficina de Seguridad de la Información de la Entidad realizará las respectivas recomendaciones que el contratista deberá acoger a fin de proteger la información.

Contención y Mitigación De Ataques DDOS

El contratista deberá proteger a la entidad de ataques del tipo DoS y DDoS esta solución debe permitir el aseguramiento del acceso desde internet hacia la infraestructura pública de la UGPP, contra ataques especializados de Denegación de Servicio Distribuido.

El sistema debe tener métodos de uso de análisis heurístico y de comportamiento que no requieran suscripciones de firma ni entradas manuales FCAP ni Regex.

La solución debe proteger aplicaciones web, aplicaciones TCP/UDP a nivel de las capas 3, 4 y 7 de OSI

La solución debe ser totalmente compatible con toda la detección y mitigación del protocolo IPv6 en ambas direcciones del tráfico.

Servicio de Detección Centralizada de Malware Avanzado

El Contratista se obliga a implementar una solución para la detección de malware avanzado el cual este aprovisionado con un sistema de detección proactiva y mitigación de amenazas avanzadas que permita la utilización de mecanismos combinados para la detección de virus, virus polimórficos y otras amenazas avanzadas, este componente debe permitir el escaneo de archivo en recursos SMB y NFS, soportar múltiples archivos simultáneos en análisis, soportar como mínimo los siguientes tipos de archivos; .7z, .ace, .apk, .arj, .bat, .bz2, .cab, .cmd, .dll, .doc, .docm, .docx, .dot, .dotm, .dotx, .exe, .gz, .htm, html, .jar, .js, .kgb, .lnk, .lzh, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, url, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip y extensiones definidas por el usuario de forma personalizadas.

Servicio de Endpoint de Antivirus: El Contratista debe implementar una herramienta de antivirus para endpoint, para toda la infraestructura de servidores y estaciones de trabajo de propiedad de la UGPP y arrendadas, a continuación se relacionan algunas características mínimas: ☐ Tener una funcionalidad de detección y Prevención de Intrusos a nivel de host ☐ Proveer alertas de ataques y tener servicio de notificación alertando a administradores sobre eventos críticos, los cuales serán enviados de manera específica o individual vía e-mail. ☐ Funcionalidad de Firewall de escritorio administrable de manera centralizada desde una consola de gestión. ☐ Garantizar la detección, el análisis y solución de virus que se propagan por las aplicaciones de mensajería instantánea y carpetas compartidas. ☐ Analizar y desinfectar los archivos, programas, páginas WEB, mensajes de correo electrónico, o aplicativos WEB que el usuario utilice o descargue de Internet, disquetes, unidades de disco, memorias tipo USB, en tiempo real, así como garantizar el bloqueo de archivos sospechosos. Página 27 de 86 ☐ Opción de iniciar un proceso de búsqueda, detección y erradicación de virus, malware, programas no deseados, que sea iniciado por demanda desde una consola remota de administración. ☐ Análisis por comportamiento para prevenir y detectar ataques y epidemias de la red corporativa. ☐ Permitir la conexión y sincronización con el Directorio Activo para facilitar la instalación, administración y control de los clientes desde una consola. ☐ Generación de Informes: número de virus detectados, versiones de antivirus, Estaciones de trabajo infectadas, y permitir diseño y generación de nuevos informes, exportables a los siguientes formatos: PDF, EXCEL, HTML. ☐ Permitir la instalación o desinstalación del antivirus en las estaciones de trabajo desde la consola de Antivirus. ☐ Módulo de DLP o Prevención de Fuga de Información, con características tales como; descubrimiento y etiquetado automático de archivos en repositorios de información por medio de parámetros configurables, clasificación y etiquetado manual de archivos, monitoreo de archivos nuevos para clasificación y etiquetado por medio de agentes, administración centralizada de los agentes, supervisión de eventos y registros de auditoría para la gestión de incidentes, aplicación de políticas para la restricción de acceso a la información, aplicación de políticas para restringir de carga de archivos adjuntos por correo electrónico o hacia servicios de almacenamiento en la nube.

Copias de Seguridad – Herramienta de Propósito Específico

Es obligación del contratista contar con herramientas de respaldo, actualmente la entidad usa DAtaProtector para realizar las copias de respaldo de la infraestructura e información de la Entidad, de acuerdo con la política establecida por la entidad, así como el suministro de los medios empleados asegurando la integridad de los datos y la generación de los medios de almacenamiento.

Para el proceso de recuperación de las copias de seguridad (backups) el contratista debe emplear la herramienta Data Protector asegurando las restauraciones de las copias históricas, la entidad suministrará el catálogo de backup de esta librería, para poder realizar la restauración de los medios que están en proceso de custodia.

El contratista deberá cumplir con las políticas de backup de la Entidad, así como con la custodia de los medios que se generen y/o entregue. La política actual de Backup corresponde a: Backup Mensual último o primer día del mes con una retención en cinta custodia permanente, los backups Semanales se realizan los sábados o domingos y estos tiene retención de 4 semanas (1 mes), backup incrementales todos los días con excepción el día que se ejecuta el mensual o semanal con retención de 1 semana, para bases de datos transaccionales o archive pueden ejecutarse cada 2, 4 o 6 horas dependiendo de la criticidad de la base de datos estos backup tiene retención de 1 semana.

Los medios de los backups con antigüedad mayor a un (1) mes se deben enviar a custodia externa. La unidad podrá solicitar copias y custodia de respaldo en formato (LTO5 y LTO6 o superior).

El contratista deberá realizar la custodia de los medios de almacenamiento físicos en instalaciones acondicionadas para garantizar la conservación y protección de los datos. En la recolección, el transporte y el almacenamiento de los medios, el contratista debe asegurar un transporte seguro desde el centro de datos hasta las instalaciones externas o sedes de la UGPP.

Los tipos de medios de almacenamiento entregado por La Unidad corresponden a: cintas magnéticas (LTO5, LTO6, LTO7 ó Superior), Disco duro externo, unidades de CD, DVD y memorias USB.

La Entidad entregará aproximadamente 2000 medios para la custodia. En todo caso la entidad podrá solicitar para custodia los (n) medios que se requieran. Se estima que durante el plazo de ejecución del contrato los nuevos medios entregados en custodia sean de aprox. 60 al año.

La frecuencia de recolección de los medios de datos en el centro de datos será diario, semanal y mensual según corresponda a la política de respaldos.

El Contratistas es responsable del transporte garantice la protección de los datos y los medios, así mismo debe llevar inventario de la relación de los medios.

El almacenamiento de los medios se contempla por fuera de las instalaciones físicas /lógicas del datacenter principal y el contratista en el servicio debe contar con instalaciones acondicionadas que cumpla con las siguientes características:

- Ubicación sin riesgos de humedad subterránea o problemas de inundación.
- Estantes metálicos resistentes y anticorrosivos.
- Sistemas de seguridad para el control de acceso del personal, cámaras de video vigilancia y personal de vigilancia las 24 horas del día.
- Sistemas de detección de intrusos, sistema de detección y extinción de incendios.
- Disponer de equipos para atención de desastres como extintores de CO2, solfaclan o multipropósito y extractores de agua de acuerdo con el material a conservar. Evitar el empleo de polvo químico y de agua.
- Sistemas de control ambiental que permiten garantizar la conservación de los medios y la protección de los datos.

El Contratista frente a la recuperación de los medios debe prestar el servicio 7x24, si se presenta un incidente que afecte la disponibilidad de un servicio y requiere ser restaurado a partir de copias de respaldo.

El tiempo de entrega de los medios custodiados debe ser un máximo de cuatro (4) horas continuas. En el transcurso del plazo de ejecución del contrato la Entidad realizará pruebas de restauraciones Trimestrales de forma aleatoria a máximos dos (2) medios que se encuentran en proceso de custodia. Los medios tienen un tamaño aprox. de 3 TB. Lo correspondiente a la política y estrategia de backup de los servicios alojados en la nube pública hacen parte del contrato actual de la UGPP con su proveedor de nube publica.

Gestión de Vulnerabilidades

La gestión de las vulnerabilidades de los activos de la UGPP deberá evaluarse en una plataforma de propósito específico que permita funciones de evaluación de ataques externos, postura de seguridad en la nube pública, escaneo de vulnerabilidades web y evaluación de riesgo de TI.

Debe tener capacidad de integrarse con sistemas tipo SIEM para incrementar la capacidad de visibilidad de amenazas de la entidad, así como de respuesta a vulnerabilidades. Por defecto debe tener la capacidad de integrarse al menos con las siguientes soluciones: Fortinet, Chronicle, IBM Qradar, LogRhytm, Splunk, Stellar Cyber, Sumo Logic.
Las características del servicio deberán conectarse de manera nativa con el servicio de administración y evaluación de riesgos, con fin de consolidar en un solo punto la información provista por la solución permitiendo análisis de 150 activos:

Herramienta para Gestión del gobierno, riesgo y cumplimiento GRC

El contratista deberá suministrar para la UGPP el licenciamiento de NOVASEC con

vigencia de 19 meses, incluyendo los siguientes módulos:

Licencia Novasec SaaS durante la ejecución del contrato.

Procesos

Módulo Riesgos

Módulo Activos

Módulo Indicadores

Módulo Eventos

Módulo Incidentes

Módulo Cumplimiento

Módulo Normatividad

Módulo Hallazgos

Soporte, actualización y mantenimiento directo con Fabricante

Escaneo de vulnerabilidades

- La solución debe incluir la capacidad integrada en modo activo (escaneo) y pasivo (detección) de descubrimiento para lograr plena visibilidad de vulnerabilidades y dispositivos de red.
- La solución debe ser capaz de realizar pruebas sin agente para la detección de vulnerabilidad local y remota sin la necesidad de un agente del lado del cliente instalado en el dispositivo de destino.
- La solución debe ser capaz de realizar pruebas de agentes para la detección de vulnerabilidad local sin costo adicional.
- La solución debe ser capaz de rastrear los cambios de DHCP al asociar los resultados de escaneo de un sistema dado con algo diferente a la dirección IP.
- La solución debe detectar y clasificar problemas, riesgos y vulnerabilidades. Debe proporcionar información detallada sobre la naturaleza del riesgo y recomendaciones para mitigarlos.
- La solución debe incluir resultados detallados de los resultados del análisis.
- La solución debe ser compatible con CVE y proporcionar al menos 10 años de cobertura de CVE.
- La solución debe proporcionar auditorías de parches para los sistemas operativos y aplicaciones de Microsoft para incluir Windows XP, Windows 7, Windows 2008, Internet Explorer, Microsoft Office, IIS, Exchange y más. La solución debe proporcionar auditorías de parches para todos los principales

sistemas operativos Unix para incluir Mac OS, Linux, Solaris, IBM AIX, HP-UX y más.

- La solución debe proporcionar revisión de parches para la infraestructura de red para incluir Fortinet, Cisco, Palo-Alto, Juniper y más.
- La solución debe proporcionar cobertura para aplicaciones de terceros como Java y Adobe.
- La solución debe incluir la calificación de vulnerabilidad de acuerdo con el estándar aceptado por la industria, es decir, el Sistema de calificación de vulnerabilidad común Versión 3 (CVSS 3).
- La solución debe proporcionar un mecanismo automático de re-priorizar vulnerabilidades basado en la probabilidad de que serán utilizadas en un ataque.
- La solución debe proveer una puntuación que indique el orden de prioridad en la cual las vulnerabilidades deben ser remediadas de acuerdo con la probabilidad de que serán utilizadas en un ataque.
- La solución debe proporcionar información de reputación en procesos encontrados y la amenaza en inteligencia alimentada en busca de malware y botnets durante el análisis
- La solución debe proporcionar información de explotación de fuentes de terceros, como Core, Metasploit y Canvas.
- La solución debe proporcionar información de explotación de malware.
- La solución debe seleccionar de forma inteligente las pruebas a realizar basándose en la información obtenida de los escaneos iniciales para intentar realizar pruebas adicionales basadas en la información obtenida previamente sobre un dispositivo o host dado.
- La solución debe realizar un seguimiento de las fechas para el descubrimiento y la observación de vulnerabilidades que se pueden utilizar para filtrar e informar en filtros basados en el tiempo.
- La solución debe permitir que las pruebas seleccionadas se habiliten o deshabiliten durante los escaneos programados.
- La solución no debe depender de la capacidad del sistema operativo para programar tareas.
- La solución debe admitir el escaneo IPv6, con descubrimiento pasivo de objetivos IPv6.
- La visibilidad continua de los entornos de nube pública a través del descubrimiento automatizado de activos debería estar disponible.
- La solución debe rastrear con precisión los activos y sus vulnerabilidades, incluidos los activos de TI altamente dinámicos como dispositivos móviles, máquinas virtuales e instancias en la nube.

Gestión de Parches

El proceso de actualización de plataformas (gestión de parches) se debe atender conforme a lo establecido en las políticas de operación óo seguridad de la información (Subproceso de Gestión de Vulnerabilidades); en donde se debe contemplar la remediación de vulnerabilidades existentes o que lleguen a surgir de los requerimientos de ciberseguridad definidos por la Entidad, evaluaciones internas o de los entes de control.

Esta gestión, será acordada entre el contratista y la Entidad y se realizará un plan de trabajo semestral, no obstante, el contratista debe gestionar de manera prioritaria los boletines de seguridad de los fabricantes y/o requerimientos de posibles incidencias de seguridad críticas en las plataformas.

Gestión de Network Operations Center (NOC)

La operación del NOC es 7X24, el contratista debe apoyar esta gestión con personal y herramientas de propósito específico, que le permitan realizar el monitoreo de las plataformas de la nube privada/pública, para que de manera proactiva pueda gestionar fallas, errores o alertas que se puedan presentar en tiempo real con el desempeño de las plataformas que soportan las aplicaciones.

El contratista en el alcance de esta gestión debe contemplar la gestión de eventos que reporten las (n) plataformas de los ambientes productivos, que soportan las aplicaciones y/o servicios de la Entidad.

Las alertas o eventos de las herramientas del NOC deberán ser compatibles y permitir la integración nativa y/o personalizada con las plataformas de seguridad de la entidad. En todo caso el contratista deberá permitir el acceso a las mismas al equipo técnico de la Entidad.

a) Plataformas/Productos a Gestionar

Las consideraciones respecto al licenciamiento y gestión técnica de las plataformas se consideran las siguientes:

Licenciamiento

La Entidad es responsable del licenciamiento de los productos: SCO, SAP – Sysbase, IBM Filenet – IBM Cloud Pak, Openshift, Open IAM, Suite Mywebmetdos Software AG,Sede Electrónica Esigna, Adobe Creative, Arcgis,Storm, SPSS, WEBMETHODS, KOFAX, DEXON, AUTOCAD, VISION EMPRESARIAL – BSC, KACTUS AP/ HR, SMART Hyperautomation, Google Workspace y los servicios que la Entidad aprovisiona en la nube pública – GCP -Google Cloud Platafform).

El contratista es responsable del licenciamiento de sistema operativo, base de datos, servidor de aplicaciones (middleware) y servicios de File Server, Directorio Activo, DHCP y SMTP, de todas las máquinas virtuales que se aprovisionan en la nube privada. El contratista debe tener en cuenta que el licenciamiento mensual requerido para base de datos ORACLE es hasta 48 CPU y SQLSERVER es hasta 300 CPU.

El contratista frente a la obligación de licenciamiento del datacenter, deberá emitir certificado mes a mes, en donde se relacione la cantidad, número de producto y/o parte y fecha de soporte vigente con el fabricante. En cumplimiento, a la política de licenciamiento de software TI-PIT-004 Política Específica de Licenciamiento de Software que será compartida con los oferentes. Durante el plazo de ejecución del contrato el contratista debe mantener soporte de fábrica vigente para todas las plataformas que soporte la nube privada, a fin de mitigar riesgos de indisponibilidad y/o obsolescencia tecnológica.

A continuación, se relacionan los (n) productos que contemplan las arquitecturas de las aplicaciones:

Sistemas Operativos
- Windows Server
- Linux
- Unix (SCO - OpenServer Enterprise System - Suministrado por la Entidad)
- Windows Server (64 Bits) (Active Directory, DHC, DNS, FTP)
- Redhat Linux (64 Bits)
- Centos (64 Bits)
- SUSE (64 Bits)
- Windows10 para máquinas virtuales de producto Robotización (KRYON – Suite
- MyWebMethods)

Servidores de Aplicaciones
- Apache
- Tomcat
- Jboss
- Glassfish
- IIS
- Drupal
- Websphere Aplication – IBM WAS
- WildFly
- Docker
- Apache Kafka

Contenedores
Openshift - IBM CloudPak

Bases de Datos:

- Sql Server / MS Integration Server /Reporting Services
- Oracle
- MySQL - Maria DB
- Informix
- PostgreSQL
- DB2
- ASE - SYBASE
- IQ

Google Cloud Platafform – GCP (Servicios):

- Compute Engine
- Cloud SQL
- Networking
- Cloud Storage
- Kubernetes Engine - GKE
- Artifact Registry
- Cloud Logging
- Source Repository
- Cloud Build
- Cloud Pub/Sub
- Cloud Monitoring

b) Administración Técnica y de Gestión

El contratista es responsable del soporte, operación y monitoreo de las aplicaciones y/o servicios de la Entidad, independiente del centro de datos (nube privada/pública) donde se alojen, esto dado el modelo híbrido en la arquitectura que las soportan.

La Entidad para los productos de: Software AG, SAP /ASE/IQ Sybase, IBM SPSS, KOFAX y GCP - Google Cloud Platform; existen contratos de Nivel III para administrar y operar la capa del producto. En tal sentido, el alcance que le corresponde al contratista de la nube privada es realizar la gestión de los sistemas operativos, base de datos y servidores de aplicaciones (no incluye contenedores/Kubernetes en nube publica) que emplean estos productos.

En todo caso, el contratista de la nube realizará la administración de los sistemas operativos, base de datos, servidores de aplicaciones (middleware) y servicios de File Server, Directorio Activo, DHCP y SMTP, para todas las aplicaciones o servicios de la Entidad.

La información de las aplicaciones a soportar en nube privada o pública, se describen en el documento de LÍNEA DE APLICACIONES.xls, con sus versiones y capacidades aprovisionadas.

Dentro de las actividades para gestionar las plataformas el contratista sin limitarse a las mismas se obliga a:

- Gestionar, administrar, operar y dar soporte a la infraestructura de los sistemas de información y/o aplicaciones.
- Aplicar las políticas de seguridad definidas por la entidad y/o buenas prácticas para mitigar riesgos de vulnerabilidades en los servicios instanciados.
- Velar por un óptimo aprovechamiento de los recursos costo/beneficio, mediante una arquitectura tecnológica, orientada a la estabilidad, sostenibilidad, agilidad y adaptabilidad a la demanda.
- Realizar la instalación y configuración de aplicaciones y plataforma, de forma integral, coordinado con el equipo de tecnología de La Unidad.
- Realizar la gestión de usuarios y control de acceso a las aplicaciones, en los casos que aplique.
- Realizar el escalamiento y seguimiento a equipos internos de TI y/o fabricantes (para los casos que aplique).
- Monitorizar y realizar reportes periódicos de desempeño de los servicios y gestión relativos a toda la plataforma.
- Revisar, mejorar y mantener la base de conocimiento, relativa a este servicio.
- Identificación, atención, corrección y/o gestión de los eventos que se detecten y/o reporten en la plataforma y/o aplicaciones.
- Analizar y dar reporte semanal, así como seguimiento preventivo a alertas de monitoreo para prevenir incidentes o indisponibilidades en los servicios de la nube.
- Brindar atención de eventos en tiempo real, preventiva y correctiva.
- El contratista debe disponer de personal técnico 7X24 para atender las ventanas de mantenimiento planificadas o de emergencia que se generen del proceso de gestión de cambios.
- Realizar backup internos y externos de acuerdo con las políticas de respaldo de La Unidad.
- Asegurar el respaldo y recuperación a través de las herramientas provistas.
- Validar las mejores prácticas para cada uno de los componentes que hagan parte de las aplicaciones o servicios que se requieran implementar.

Respecto, a la gestión de sistemas operativos y bases de datos en cualquier ambiente de nube privada tendrá en cuenta las siguientes actividades:

En las actividades el contratista deberá realizar las siguientes actividades en la gestión:

- Atención de requerimientos, alarmas, eventos, incidentes y problemas
- Procesos de reinicio, encendido y apagado de las máquinas/instancias/bases de datos.
- Procesos de configuración y control de partes en procesos de instalación/desinstalación y mantenimiento de las plataformas
- Administración integral de los componentes con revisión de procesos, servicios y sucesos.
- Automatización de las tareas administrativas, directivas y procedimientos.
- Administración de sistemas de archivos y unidades.

- Administración de conjuntos de volúmenes y matrices de RAID / ó componentes de las bases de datos o aplicación según su arquitectura.
- Administración de las funciones de red de TCP/IP.
- Configuración de tareas programadas de bases de datos, sistemas operativos o construcción de shell-script.
- Informes de estado de las Bases de datos: presentación de reportes periódicos (reportes quincenales y mensuales) que se realizan para informar el estado, incidencias y problemas o cambios que se presenten durante un período de tiempo.
- Ejecutar procesos en las bases de datos: es la actividad de ejecución integral de dichos procesos de acuerdo con los requerimientos realizados por la UGPP, los cuales deben ser registrados en bitácoras de operación diaria, semanal y mensual, así mismos procedimientos de respaldo, recuperación y reinicio de procesos.
- .
- Monitoreo de rendimiento, crecimiento, alertas, etc., de cada una de las instancias, catálogos y base de datos: en esta actividad se busca medir el desempeño de las instancias y/o bases de datos, la adecuación de su capacidad, su crecimiento en cuando a disco, disponibilidad, incidentes, alertas, etc., con el fin de tomar medidas preventivas o correctivas según los resultados del análisis, para ello el contratista deberá disponer de herramientas de monitoreo que le permitan de manera eficiente y eficaz recolectar dicha información.
- Monitoreo permanente y gestión de los procesos recurrentes que corren sobre los servidores de bases de datos,, que se ejecuten correctamente y que el resultado de la ejecución sea el esperado, en caso de falla, el contratista debe determinar cuál fue la causa de la falla e informar oportunamente a la Entidad acerca del problema.
- Realizar las configuraciones de activación de auditoría que le sean requeridas en aras de evidenciar las acciones efectuadas por los usuarios de la Entidad y así garantizar la seguridad de la información y la generación de reportes.
- Realizar la revisión, gestión y depuración de logs, para evitar inconvenientes que afecten la prestación del servicio.
- Escalamiento de incidencias e instalación de actualizaciones y/o parches que libere el fabricante: En esta actividad se le asignará a cada incidencia una instancia superior de acuerdo al grado de complejidad evitando indisponibilidad en la prestación del servicio y se deberá presentar el plan de aplicación correspondiente.
- Creación, instalación, asignación y configuración de recursos, objetos y usuarios en los motores de bases de datos que requiera la entidad.
- Apoyar la definición y realizar la implementación de las políticas de "Backups" con las que cuenta la UGPP, el contratista ejecutará el proceso de Backups de la información de la base de datos y enviará a custodia las copias de estos Backups, el sitio de custodia no puede estar localizado físicamente en el datacenter, utilizar herramientas especializadas que permitan crear y asegurar los Backups.
- Formular las recomendaciones y mejoras para la optimización de las instancias y/o bases de datos con base en el resultado del monitoreo permanente de estos servicios, las recomendaciones y mejoras deberán ser descritas en el informe quincenal y/o mensual y paralelo a ello se deberá presentar un plan de trabajo.

- Migración motores de base de datos, instancias y/o bases de datos: si la UGPP requiere realizar la migración con todos sus componentes a otro servidor que igualmente cumpla con todas las especificaciones técnicas exigidas.

  Adicional, a las anteriores actividades operativas en las bases de datos, el contratista realizará lo siguiente;

- Definición y control de tamaños y ubicación de almacenamiento de datos.
- Subir y bajar las instancias y/o base de datos cuando sea necesario.
- Ejecutar restauraciones de las instancias y/o base de datos cuando sea requerido.
- Ejecutar mantenimientos preventivos y correctivos sobre las instancias y/o bases de datos.
- Administración de perfiles, roles y usuarios: Creación, modificación, eliminación y bloqueos de perfiles, roles y usuarios en las instancias y/o bases de datos de la UGPP.
- Ejecución de procesos bajo demanda: el CONTRATISTA ejecutará en las instancias y/o bases de datos procesos bajo demanda, es decir, procesos que no son recurrentes y que requieren su ejecución en fecha y hora no programada.
- Administración del comportamiento de las bases de datos: el CONTRATISTA deberá gestionar una bitácora integral de control de incidentes, mantenimientos preventivos y correctivos, fallas, alarmas, backups, incidentes, etc.
- Entrega de informes: el CONTRATISTA será responsable de elaborar y entregar a la UGPP informes quincenales y mensuales, acerca del estado del servicio de administración de Bases de Datos.

Adicionalmente, a las anteriormente señaladas el contratista, sin limitarse a la gestión técnica se obliga a realizar las siguientes actividades propias de la arquitectura técnica que soporta el Gestor de Identidades **OPEN IAM**:

- Realizar monitoreo constante de la plataforma que permita asegurar la disponibilidad y continuidad en el servicio
- Realizar mantenimiento preventivo y correctivo de cada uno de los ambientes de los sistemas a nivel de infraestructura con el de asegurar su funcionalidad.
- Configurar y gestionar el acceso de los usuarios a las plataformas, así como a sus diferentes componentes.
- Gestionar e instalar software proporcionado por la entidad asegurando la ejecución de las tareas necesarias para la actualización o instalación del software necesario.
- Asegurar el entorno ante posibles fallas, intrusiones o vulnerabilidades que puedan llegar a presentarse en los diferentes componentes.
- Creación de reportes e informes sobre el uso de la plataforma, licencias, datos, etc.
- Supervisión de la plataforma, asegurarse de conocer la plataforma como está configurada y distribuida, para detectar oportunamente los puntos de fallo y aportar posibles soluciones.
- Verificación y análisis de sucesos de auditoría entendiendo los diversos sucesos de auditoría que se generan para a partir de estos aportar ideas que permitan mitigar y/o corregir errores que puedan llegar a presentarse.

- Gestionar los diferentes recursos con los que se cuentan en el ambiente para detectar posibles fallos.
- Gestionar, mantener, verificar y asegurar el adecuado uso del almacenamiento asegurando que este se encuentre disponible y proponiendo, mitigando y/o aportando ideas para corregir errores que puedan llegar a presentarse.
- Gestionar, mantener, verificar y asegurar el adecuado uso de las bases de datos asegurando que este se encuentre disponible y proponiendo, mitigando y/o aportando ideas para corregir errores que puedan llegar a presentarse.
- Realizar las configuraciones de los productos disponibles o licenciados por la Entidad, asegurando que se puedan emplear las funcionalidades provistas de fábrica.

Para la plataforma correspondiente al gestor documental Cloud Pak, el contratista realizará labores de administración para los componentes de OpenShift y base de datos DB2. Se obliga a realizar las siguientes actividades propias de la arquitectura técnica:

- Realizar monitoreo constante de la plataforma que permita asegurar la disponibilidad y continuidad en el servicio
- Realizar mantenimiento preventivo y correctivo de cada uno de los ambientes de los sistemas a nivel de infraestructura con el de asegurar su funcionalidad.
- Configurar y gestionar el acceso de los usuarios a las plataformas, así como a sus diferentes componentes.
- Gestionar e instalar software proporcionado por la entidad asegurando la ejecución de las tareas necesarias para la actualización o instalación del software necesario.
- Asegurar el entorno ante posibles fallas, intrusiones o vulnerabilidades que puedan llegar a presentarse en los diferentes componentes.
- Creación de reportes e informes sobre el uso de la plataforma, licencias, datos, etc.
- Supervisión de la plataforma, asegurarse de conocer la plataforma como está configurada y distribuida, para detectar oportunamente los puntos de fallo y aportar posibles soluciones.
- Verificación y análisis de sucesos de auditoría entendiendo los diversos sucesos de auditoría que se generan para a partir de estos aportar ideas que permitan mitigar y/o corregir errores que puedan llegar a presentarse.
- Gestionar los diferentes recursos con los que se cuentan en el ambiente para detectar posibles fallos.
- Gestionar, mantener, verificar y asegurar el adecuado uso del almacenamiento asegurando que este se encuentre disponible y proponiendo, mitigando y/o aportando ideas para corregir errores que puedan llegar a presentarse.
- Gestionar, mantener, verificar y asegurar el adecuado uso de las bases de datos asegurando que este se encuentre disponible y proponiendo, mitigando y/o aportando ideas para corregir errores que puedan llegar a presentarse.
- Realizar las configuraciones de los productos disponibles o licenciados por la Entidad, asegurando que se puedan emplear las funcionalidades provistas de fábrica.

1.2 CONECTIVIDAD (WAN/LAN/WLAN)

El contratista debe implementar las redes WAN, WLAN SDWAN, permitiendo una arquitectura de red que optimice el enrutamiento de forma más eficiente para que el tráfico del centro (s) de datos y sedes de la Entidad y Gestión de LAN, de acuerdo con los requerimientos técnicos mínimos descritos.

- La implementación de la conectividad a través de canales de datos/internet en las sedes y/o datacenter de la Entidad de acuerdo con los anchos de banda requeridos.
- El factor de reuso no debe existir es decir debe ser 1:1,
- Implementar SDWAN sobre las sedes Marriot, Calle13..
- Los canales de datos/internet pueden ser solicitados por la Entidad para cualquier centro de datos de la Entidad (nube privada/nube pública). En la implementación él debe ser redundante (backup).
- Los canales de datos suministrados deben tener redundancia en su última milla.
- El contratista debe cumplir con las políticas, procesos y subprocesos de la Dirección de Gestión de Tecnología para la gestión del servicio, alineado en las buenas prácticas de ITIL y políticas de seguridad de la información de la entidad.
- El servicio de NOC monitoreo de y gestión de incidentes de las plataformas debe ser 7x24x365.
- El contratista debe brindar el respectivo soporte de las soluciones implementadas.
- El contratista debe disponer de personal técnico 7X24X365 para atender las ventanas de mantenimiento planificadas o de emergencia que se generen del proceso de gestión de cambios.
- Las herramientas implementadas deben contar con soporte técnico de fabricante en un esquema 7 x 24 incluyendo actualizaciones de firmware, acceso al portal de soporte y recursos técnicos asociados.
- El contratista debe escalar y atender las fallas críticas que se puedan generar en los servicios de la entidad, gestionando de manera proactiva las aplicaciones.
- Toda solución implementada debe estar licenciada y debe contar con soporte de fábrica por el tiempo del plazo de ejecución del contrato.
- La Unidad podrá realizar revisiones /evaluaciones de las configuraciones de las plataformas que provee, a fin de constatar el cumplimiento de los requerimientos técnicos.
- El contratista deberá realizar la implementación y puesta en marcha de todos los servicios descritos en el presente anexo, teniendo en cuenta los requerimientos de implementación IPv6: Resolución 2710 de 2017 de MinTic, la cual especifica la coexistencia de los protocolos IPv4 e IPv6. Por ende, los dispositivos de la red deben soportar la operación en Dual Stack.
- Los canales de comunicación WAN deben tener redundancia física y lógica, el contratista debe aprovisionar los enlaces de datos dedicados en cada sede de La Unidad, distribuido con la capacidad del ancho de banda contratado.
- El enrutamiento del tráfico de datos e internet debe configurarse con políticas de QoS.
- ,

.

El Qos en el servicio se deberá configurar de acuerdo con las prioridades de los servicios definidos por La Unidad.

El contratista deberá realizar la implementación, puesta en marcha y gestión de todos los servicios descritos en el presente anexo, incluyendo los elementos necesarios para la interconexión entre switches y equipos de enrutamiento y/o otros (Fibra Óptica). El contratista es responsable de llevar a cabo la implementación, puesta en marcha, administración y gestión de la (WAN/LAN/WLAN).

El contratista debe realizar la gestión, administración y monitoreo de la red de datos, siendo el responsable de documentar y realizar el diseño técnico de la arquitectura de red de datos que se implementará.

Es responsabilidad del contratista en el monitoreo de la red de datos de forma integral en la que se incluyen todos los componentes de (WAN/LAN/WLAN).

Los equipos activos de red suministrados deben contar con soporte y garantía vigente, tener compatibilidad IPV6 nativo o dual- stack, posibilidad de soportar conexión entre redes nativas IPV4 a redes nativas IPV6 y viceversa.

Las conexiones de los switches deben realizarse en medio físico de fibra óptica y sus respectivos módulos SFP.

La infraestructura de última milla debe ser exclusiva para La Unidad, es decir no compartida con otros clientes.

El suministro de los equipos activos de red durante el plazo de ejecución del contrato debe mantener soporte de fábrica vigente para todas las plataformas que soporte la nube privada, a fin de mitigar riesgos de indisponibilidad y/o obsolescencia tecnológica.

El contratista realizará la gestión de los centros de cableado de manera integral, La Unidad entregará el inventario completo de los racks de comunicaciones en cada una de las sedes/pisos con sus respectivas conexiones hasta el Patch Panel.

El contratista en la gestión del cableado debe realizar mantenimiento preventivo y correctivo al mismo. (Incluye suministro de repuestos de los Patch Cord y conectores RJ45).

El montaje, configuración de los equipos activos de red que se suministren son responsabilidad exclusiva del servicio.

La puesta en marcha del servicio debe contemplar todos los elementos necesarios para la instalación y configuración de las conexiones de la WAN/LAN/WLAN.

Los switches implementados deben ser compatibles y permitir integración con el firewall de seguridad perimetral del centro de datos principal.

La infraestructura de los equipos activos de red implementados debe tener soporte de fábrica local en el territorio nacional.

Todos los switches deben tener la capacidad de ser administrados de manera centralizada.

El contratista debe aprovisionar los equipos activos de red tipo acceso, distribución y Core y demás elementos /módulos requeridos para la interconectividad de la red LAN.

El dimensionamiento del número de equipos activos de red se basa en el número de puertos de voz/datos instalados en cada una de las sedes de La Unidad:

Ubicación	**Centro de Cableado**	**No. Puertos Voz/Datos**
Marriot Piso8	1	744
Marriot Piso2	1	432
Marriot Piso6	1	144
Calle 13	1	300
Multiplaza	1	24
PAVs	3	72
Total	**8**	**1.716**

Los equipos activos de red switch incluyen la instalación, configuración y puesta en funcionamiento debe cumplir con las siguientes características mínimas, que deben soportar:

- Switch de 48 ó 24 puertos POE+ con conector RJ-45 10/100/1000 Mbps, con almenos 2 puertos basados es 10G/GE SFP+.
-
- Interfaz de red soportada: 10/100/1000 Mbps.
- Velocidad de datos requerida: 10/100/1000 Mbps.
- Coexistencia y compatibilidad IPv4 e IPv6 y funcionamiento en dual-stack
- Capacidad para apilamiento físico o lógico.
- Acceso vía SSH-SSL.
- Montaje en Racks.
- Interfaz de administración basada en web.
-
- Capacidad de apilamiento con interconectividad totalmente redundante en la pila.

En la implementación de la WLAN (WIFI) y LAN, el contratista es responsable de realizar la respectiva implementación y administración por el plazo de ejecución del

contrato. La implementación del servicio Wifi debe estar centralizada permitiendo que los usuarios internos y externos, este último tengan acceso al servicio según los requerimientos del Decreto Número 728 de 2017 del 05 de mayo de 2017. – Zonas de acceso público a Internet inalámbrico.

Se requiere que el contratista administre y gestione el servicio de WIFI de manera centralizada en Cloud (fabricante) o controladora física/virtual.

La infraestructura de los equipos Access Point a implementar debe soportar:

- Frecuencia de 2.4G: 3dBi y 5G: 3dBiInterfaces: 2 de 10/100/1000 RJ45
- Compatibilidad con estándar 802.11 b/g/n/ac;

- Transmisión y recepción simultánea.
- Manejo de anchos de banda Traffic Shaping
  Protocolos y normas de seguridad: WEP, WPA, WPA2-PSK, WPA2-Enterprise with 802.1X.

La solución implementada de Wifi debe ser monomarca.

La solución debe tener anclajes o base para que los AP(s) puedan ser ubicados de manera firme en cualquier tipo de superficies.

La solución implementada debe operar de manera óptima en entornos con alta interferencia.

La gestión técnica del servicio debe contemplar el monitoreo de los servicios del presente anexo y debe contemplar la implementación de una herramienta centralizada que permita:

- Monitoreo del servicio a través del protocolo SNMP v3, el servicio debe contar características confidencialidad, integridad y autenticación de usuario, el mismo debe soportar protocolos de autenticación SHA y MD5, protocolos de privacidad DES y AES.
- Registrar estadísticas de desempeño, comportamiento, tendencias de crecimiento de consumo y disponibilidad del alcance de los servicios contratados. .
- El acceso a la herramienta deberá ser permitido a La Unidad para verificar la disponibilidad de los servicios contratados.
- El contratista debe entregar a La Unidad reportes de:
- Disponibilidad.
- Interrupciones de servicio.
- Latencia.
- Ancho de banda.
- Medida de tráfico de entrada y salida.

- Copias de las configuraciones de los equipos.

Plataforma de Gestión Network Access Control (NAC)

El contratista en la implementación de la red de datos debe contemplar una solución NAC para ofrecer visibilidad de qué hay conectado en cada punto de la red, ya sea una conexión inalámbrica o cableada , obteniendo información del dispositivo y de los usuarios asociados, si los hubiere, y desplegando políticas de control de acceso en función de esta información, garantizando a la vez el acceso de los dispositivos reconocidos, y otorgándoles la conectividad mínima e imprescindible en función del rol que desempeñan, mientras se asegura el aislamiento de cualquier dispositivo no permitido, tan pronto como se conecte.

La solución debe contar con soporte del fabricante durante la duración del contrato. De esta manera, a la vez que se garantiza la seguridad de red, se automatiza la segmentación y la contención de amenazas.

La solución NAC debe incluir los siguientes bloques funcionales:

- Visibilidad de red y perfilado de dispositivos conectados.
-
- OnBoarding de nuevos dispositivos sencillo, versátil y potente.
-
- Gestión de invitados y usuarios externos: Fácil y rápido, sin necesidad de involucrar al personal de IT en el alta de nuevos usuarios externos.

Debe de ser capaz de asociar al dispositivo atributos adicionales, como la ubicación, tipo de dispositivo, fabricante, además de los atributos del usuario conectado.

1.3 MESA DE SERVICIOS

El alcance del servicio comprende la gestión requerida para la atención y solución de todas las solicitudes de tecnología en la Entidad; apoyada con el equipo de Nivel I y II (Agentes, Administradores de Plataforma, Soporte Técnico Funcional y Soporte en sitio) y los respectivos gestores de los procesos ITIL conforme a lo definido en el modelo de operación.

La modalidad de atención a los usuarios es remoto y presencial en sede para el equipo de soporte en sitio y el gestor de calidad. Los horarios de atención son de lunes a viernes de 7:00 a.m. a 7:00 p.m. y sábados de 07:00 am a 02:00 pm.

La mesa de servicio debe operar como único punto de contacto, enmarcado en los lineamientos de buenas prácticas ITIL (Information Technology Infrastructure Library), y bajo este servicio se debe asumir la gestión de todos los procesos enmarcados en el marco de referencia ITIL, alineado con los procesos, procedimientos, políticas y lineamientos de la unidad.

Perfiles requeridos:

No	Cantidad	Rol	Experiencia Laboral Mìnima	Certificaciones
1	6	Soporte Técnico - Funcional	Tres (3) años en el ROL de soporte, administración, configuración de Aplicaciones o sistemas de información.	ITIL Foundation V3 o superior.
2	18	Agentes de Mesa de Servicios / Técnicos de Soporte en Sitio	Tres (3) años en el ROL de Técnico de soporte técnico a hardware y software (Ofimática)	ITIL Foundation V3 o superior.
3	1	Coordinador de (Nivel I y II)	Cinco (5) años como Líder y/o Coordinador de Infraestructura y/o mesa de servicios.	Certificación ITIL Foundation V3 o superior.
4	5	Gestor Procesos ITIL	Cinco (5) de experiencia	ITIL Foundation V3 o superior.

			ejerciendo el ROL de Gestor de Procesos de ITIL	

Dentro de los dos (2) primeros meses de ejecución contractual el contratista establecerá el modelo de la operación de la mesa de servicios basado en el marco de referencia de ITIL y los requerimientos descritos en la presente contratación, este será acordado y aprobado por La UGPP. El dimensionamiento del equipo de trabajo se realiza tomando como base las estadísticas de solicitudes del último trimestre que suministrará reportado por el contratista actual.

La UGPP realizará la entrega de manuales e información para el entrenamiento y capacitación del soporte técnico funcional de las aplicaciones y/o servicios de la Entidad a soportar al personal nuevo empleado por el contratista.

En el catálogo de servicios, el número de aplicaciones/servicios corresponden aprox. a treinta (30) aplicaciones, sin limitarse a la cantidad de las mismas.

El contratista se obliga a prestar el servicio de mesa apoyado en herramientas que le permitan realizar el control remoto a los equipos y realizar la gestión de los procesos de ITIL alineado en el macroproceso de Gestión de Tecnología, así mismo deberá allegar las respectivas Hojas de vida solicitadas para los perfiles requeridos.

El equipo de la mesa de servicios debe atender todas las solicitudes de tecnología de los equipos tecnológicos (propio/arriendo) a servicio de la UGPP, entre ellos Pc de Escritorio, Workstation, portátiles, impresoras, video beams, video proyectores, equipos de videoconferencia, escáner, televisores, smart tv, pantallas, switch, access point (AP), lectores de código de barras, entre otros, así como la instalación, configuración del software de sistema operativo, ofimática, aplicaciones y/o servicios descritos en la **LINEA BASE DE APLICACIONES.XLS.**

La Unidad realizará la respectiva capacitación y documentación de las aplicaciones y/o servicio a soportar.

Si se requiere por parte de La Unidad ampliar el equipo de trabajo el contratista asignará el personal requerido y se ajustará el modelo operativo inicialmente acordado. El equipo de trabajo empleado por el contratista en el desarrollo del contrato es de labor exclusiva en la prestación del servicio de la Entidad, es decir no podrá ser compartido con otros clientes del contratista.

El equipo de trabajo deberá asegurar el cumplimiento de las políticas, procedimientos y demás protocolos establecidos para la prestación de los servicios de tecnología de la entidad.

El contratista deberá presentar los (n) reportes periódicos y estadísticos acordados o a demanda asociados a los servicios de tecnología de la entidad, para seguimiento, planes de mejora y recomendaciones.

Es responsabilidad del contratista identificar oportunidades de mejora de los servicios, asegurando el diseño, elaboración, ejecución, seguimiento y mejora continua de los planes correspondientes.

En la gestión de la mejora continua se solicita al contratista, identificar riesgos asociados a los servicios y asegurar la elaboración, diseño, ejecución, seguimiento y mejora continua de los planes correspondientes, el seguimiento se realizará según lo acordado entre las partes en el modelo de operación.

El contratista debe mantener actualizada la información de los (CIs) de las aplicaciones y/o servicios para apoyar la gestión de la configuración.

El equipo de trabajo debe participar en los comités técnicos y/o reuniones virtual o presencial, con la previa planificación de un (1) día en función de la necesidad de la entidad.

Presentar recomendaciones a la unidad sobre la administración y uso de los servicios de tecnología de la entidad.

El contratista contará con un equipo gestor que tendrá como objetivo realizar las siguientes actividades encaminadas a:

- Controlar la gestión de los incidentes y de las peticiones (solicitudes)
- Generar la documentación y generación de una base de datos de conocimiento
- Realizar la gestión en el manejo de problemas
- Realizar el control y gestión de cambios
- Realizar la Medición de niveles de servicio y operación (ANS/OLA)
- Gestión de activos, administración de equipos
- Gestión de configuración
- Gestión de accesos a las aplicaciones/servicios de la unidad.

En caso de reemplazo del equipo de trabajo el tiempo no debe superar diez (10) días hábiles.

Toda solicitud debe cumplir con el proceso de recepción y registro de llamadas a través de los canales dispuestos para tal fin: (telefónico, chat, correo electrónico y web). La mesa de servicio deberá disponer de una línea telefónica con llamadas entrantes y salientes. El escalamiento de tiquetes en sitio (on site) y soporte de nivel II (soporte especializado), nivel III para el registro de casos a fabricantes y/o administradores de productos y/o herramientas que son soportadas por La Unidad.

La atención y solución técnica de primer nivel se debe realizar a todos los sistemas/aplicaciones de la Unidad, sin limitarse al número de aplicaciones /servicios de IT.

El Service Desk se prestará en instalaciones del contratista.

La mesa de servicios será la encargada de atender todas las solicitudes de gestión de accesos a los servicios/aplicaciones de TI de la UNIDAD

Toda solicitud se gestionará a través de un tiquete.

La UNIDAD asignará el espacio físico para el equipo contratista que estará en sede, este puesto de trabajo lo acompaña una silla, cajonera, punto de red de datos.

El equipo de trabajo del contratista debe disponer del hardware y software requerido con su respectivo licenciamiento, equipo de cómputo con sistema operativo preinstalado con versión soportada por el fabricante y servicio de telefonía móvil y acceso a internet; para los agentes del CALL, se debe proveer de diademas ergonómicas livianas de óptima calidad sonora, audio banda ancha estéreo monoaural, micrófono con reducción de ruido anti-ruido, control volumen, y silencio.

En las instalaciones donde opere la mesa de servicios se debe disponer de una matriz pantalla LCD O LED, que permitan visualizar el estado, en tiempo real de la operación: llamadas en espera, número de soportes libres, ocupados, tiempos de espera, llamadas perdidas y alertas que permitan identificar llamadas que superen los tiempos límites de escalamiento de cada agente y/o soporte en sitio.

El contratista debe realizar la grabación del 100% del total de las llamadas y tendrá una retención de dos (2) meses.

La grabación de las llamadas debe estar disponibles para consulta y entregadas en caso de requerirse.

Se debe contar con un esquema de soporte de reserva para el equipo de trabajo, en caso de ausencia por novedades administrativas (permisos, licencias, renuncias). En todo caso, el contratista debe garantizar que el servicio operará con normalidad sin afectar la atención de los servicios de tecnología.

La unidad podrá solicitar el reemplazo del personal con base en criterios de evaluación técnica semestral acordadas, para ello con el contratista realizará evaluaciones técnicas y de habilidades y destrezas y entregará al supervisor de La Unidad los resultados favorables y desfavorables.

Entre las partes se deberá realizar capacitaciones técnicas periódicas al equipo de trabajo, el temario se acordará y contempla la socialización e interiorización de políticas, procedimientos de la operación de los servicios de tecnología, cambios o actualización de tecnologías entre otros.

Los costos asociados al desarrollo de las capacitaciones serán asumidos por el contratista y el resultado de las capacitaciones y evaluaciones se entregarán a La Unidad. El contratista debe establecer un plan de recuperación tecnológica - DRP, que permita mitigar riesgos en la locación física donde se presta el servicio para

asegurar la continuidad de la operación de la mesa de servicios. Las pruebas del plan de DRP se realizan una (1) vez al año.

Durante la ejecución del servicio es responsabilidad del contratista mantener actualizada la documentación técnica inicial que entregará la unidad.

El equipo de trabajo deberá ser asignado por el contratista desde el inicio de la transición, sus respectivas hojas de vida serán evaluadas de acuerdo con el perfil requerido. Es responsabilidad del contratista mantener actualizado el inventario de los equipos y el software de la entidad y/o los recursos que este provee.

El control del licenciamiento de software instalado en los equipos deberá mantenerse actualizado permanentemente y de manera periódica.

Todos los planes de acción y mejoras en la prestación de los servicios estarán a cargo del contratista y será quien realice el respectivo control y seguimiento para la mejora continua en los servicios de tecnología en la unidad.

Herramienta de Gestión Mesa de Servicios

La solución debe soportar los procesos basados en las prácticas de ITSM:
Las funcionalidades a soportar los procesos de gestión ITIL, sin limitarse a los mismos son:

- Gestión del Portafolio
- Gestión del Catálogo de Servicios
- Gestión de Incidentes
- Gestión de Requerimientos
- Gestión de Problemas
- Gestión de Conocimiento
- Gestión de Niveles de Servicio - ANS
- Gestión de la Configuración (CMDB)
- Gestión de Activos

Debe integrarse a través de WSDL y/o ETL con la herramienta Dexon Software licencia propiedad de La Unidad, para dejar trazabilidad de la gestión de las solicitudes de TI. La autenticación debe realizarse con el Active Directory de la Entidad, asegurando el acceso y comunicación a cada uno de los usuarios de la entidad.

Licencia de cien (100) usuarios resolutores, para funcionarios de la Entidad y Otros prestadores de servicio de tecnología.

La herramienta de gestión de la mesa de servicio debe permitir parametrizar flujos para gestión de requerimientos de desarrollo y/o solicitudes específicas de los sistemas de información, además de generar reportes de manera sencilla en tiempo real. La herramienta debe permitir el registro y asignación automática de los técnicos.

La UGPP cuenta con una herramienta propia y licenciada de ITSM, esta podrá ser utilizada por el contratista o si lo prefiere, el contratista podrá suministrar otra herramienta diferente siempre y cuando cumpla con los requerimientos técnicos antes descritos.

Atención Telefónica

El contratista debe disponer de una línea telefónica con llamadas entrantes y salientes para prestar el servicio.

La telefonía del contratista debe ser integrada con el sistema de telefonía IP ALCATEL, para enrutar las llamadas que se realizan desde las sedes a la mesa de servicio, a través de la línea 5000 (Extensión Telefónica).

La integración que soporta la planta telefónica de la Entidad es SIP / E1.

Grabador de Llamadas

Disponer del dispositivo para grabar el 100% de las llamadas (entrantes y salientes) de la mesa de servicio.

Las grabaciones deben estar disponibles durante los dos (2) últimos meses para su consulta.

Debe registrar los datos de cada llamada recibida como: fecha y hora, identificación del abonado llamante - caller id-, duración de la llamada, actividad de la llamada, menú seleccionado e información relevante en la comunicación telefónica.

Informes de Gestión

El contratista es responsable de realizar la gestión de los procesos de ITIL de la Dirección de Gestión de Tecnología y dentro de sus labores realizará:

Recomendaciones a los procesos descritos en este y otros puntos basados en buenas prácticas de ITIL.

Cambios sugeridos como adopción de buenas prácticas de ITIL y/o mejoramiento continuo de todos los procesos de TI solicitados por la Unidad.

Detallar todos los procesos de TI, de acuerdo con buenas prácticas documentadas en procesos de TI, además de todos aquellas actividades, procedimientos y tareas que haga falta documentar y que La Unidad crea conveniente para la óptima prestación del servicio.

El contratista es el responsable del diseño, generación, documentación y entrega mensual después del primer mes de operación con las métricas del servicio requeridas por la supervisión.

Como también cualquier otro elemento que la Unidad considere relevante para medir la calidad del servicio, el contratista se obliga a generar los respectivos reportes en las herramientas empleadas por el mismo.

El contratista debe remitir junto con las métricas el análisis técnico y de alto nivel de éstas, sera acordadas con la supervisión del contrato.

Priorización

Los criterios de priorización de los tiquetes se registran en función de la necesidad de la atención y los tiempos de solución requerido, teniendo en cuenta la siguiente clasificación:

Prioridad	Descripción	Tiempo solución
Alto	El incidente / petición reportada en la aplicación y/o servicio se requiere para atender un proceso de negocio que implica la gestión en términos legales, indisponibilidad y/o hay usuarios VIP involucrados.	1 hora
Medio	El incidente / petición en la aplicación y/o servicio causa lentitud y/o retraso de un proceso de negocio en alguna de las áreas de la entidad.	2 hora
Bajo	El incidente / petición no genera impacto en la disponibilidad y/o funcionamiento en la aplicación y/o servicio	4 horas

Service Desk /CALL

El contratista es responsable de liderar, coordinar y ejecutar todas las actividades, procesos, procedimientos y tareas para la atención, seguimiento, identificación y cierre de incidentes, problemas, solicitudes, requerimientos y en general cualquier tipo de escalamiento al interior de La Unidad, por parte de cada componente del servicio. Se debe consolidar y realizar seguimiento a los planes de trabajo ejecutados entre las partes. Cada semestre se deben realizar auditorías internas a los procesos de ITIL implementados.

La mesa de servicios realizará seguimiento a la gestión de los eventos del NOC y SOC, a partir de la información suministrada automáticamente y/o telefónicamente suministrada por el servicio de centro de datos y el SOC.

El grupo de soporte técnico del contratista debe garantizar que los tiquetes:

- Se registren, clasifiquen y asignen según su nivel de priorización.
- Se solucionen en los tiempos acordados en los ANS
- Tengan un seguimiento adecuado.
- Cumplan con los esquemas de escalamiento definidos.
- Procedan de acuerdo con la matriz de escalamiento

Niveles de Soporte de las Aplicaciones /Servicios

Nivel	Descripción Soporte
I	Agentes de Call y Soporte en sitio
II	Personal Administrador de plataformas de hardware y software y Soporte Técnico Funcional de las aplicaciones
III	Administrador de Productos y/o Herramientas Soportados por La Unidad y/o Fabricantes de software y/o hardware

Actividades y Responsabilidades del Servicio de Nivel I

Registrar, categorizar, priorizar, solucionar o escalar, hacer seguimiento y cerrar los incidentes y requerimientos reportados por los usuarios a través los diferentes canales de comunicación dispuestos para ello.

El registro y cierre de cada solicitud o requerimiento.

Aplicar los protocolos y listas de chequeo y atender al usuario de acuerdo con estos protocolos y listas.

Capacitar a los usuarios en la atención de las solicitudes, en caso de que aplique. Recibir y atender todas las solicitudes de los usuarios relacionadas con los sistemas y servicios de IT, cumpliendo con los ANS.

Escalar al nivel II o nivel III aquellas solicitudes de los usuarios que no tengan una solución fácil e inmediata en primer nivel, de acuerdo con los protocolos y listas de chequeo establecidas para cada uno de los servicios.

Notificar a los usuarios sobre el avance en la solución de incidentes o requerimientos, tanto colectivos como individuales, según los ANS establecidos.

Verificar con el usuario que su incidente o requerimiento haya sido resuelto, así como la calidad en el cumplimiento del ANS y el nivel de satisfacción frente a la solución.

Cerrar la solicitud de común acuerdo con el usuario las solicitudes de servicio.

El contratista deberá prestar el servicio de nivel I de acuerdo con la modalidad establecida en cada sede, este debe recibir, registrar y hacer seguimiento sobre todos

los eventos, solucionando los que le competen, de acuerdo con su nivel de atención de manera telefónica o virtual por acceso remoto.

Dotar al personal, para dar solución a las solicitudes e incidentes que se escalen en sitio, con un kit de herramientas compuesto, como mínimo, por los siguientes elementos: disco duro externo, quemador externo, equipo de soldadura, juego de destornilladores, multímetro, probadores de continuidad. La dotación debe incluir una aspiradora/sopladora de equipos, módem 3G y equipo celular.

Actividades y Responsabilidades Soporte Nivel II

Es responsabilidad del contratista prestar los servicios de Nivel II para realizar la atención y gestión técnica asegurando la disponibilidad de las aplicaciones de la entidad. El soporte de Nivel II debe enfocarse en dar atención a la gestión de las solicitudes de IT, que se escalen por parte de la mesa de servicios, siempre y cuando no se tenga la información suficiente para atender una solicitud en Nivel I.

La mesa realizará el contacto al equipo de Nivel II de forma remota o en sitio y se debe atender las solicitudes en los horarios definidos por La Unidad.

Toda atención no gestionada en los horarios establecidos y que deban ser escalados al siguiente Nivel deben quedar documentados en la mesa de servicio y/o corresponderá al incumplimiento en la atención de una solicitud.

El soporte de Nivel II debe confirmar con el usuario que el tiquete ha sido resuelto, así como la calidad en el cumplimiento del ANS y el nivel de satisfacción frente a la solución. El soporte de Nivel II debe cerrar de común acuerdo con el usuario las solicitudes de servicio.

El soporte de Nivel II debe entregar los protocolos y las listas de chequeo a Nivel I para la atención de los incidentes y solicitudes o para su documentación al momento de realizar el escalamiento a Nivel II.

Actividades y Responsabilidades Soporte Nivel III

Corresponde a la gestión que realiza el equipo de funcionarios de la DGTI de la Unidad y/o administradores de herramientas ante los fabricantes de productos especializados, tales como Software AG, SAP SYBASE, SPSS y/o equipo de soporte de Google Cloud Platafform entre otros.

Gestión de Procesos - ITIL

El alcance de este proceso debe ser liderado por la gestión de la calidad, asegurando que los procesos y actividades relacionados en el modelo ITIL, esté alineado con los

lineamientos establecidos por Mintic en el marco de referencia de arquitectura empresarial en lo correspondiente al dominio de arquitectura de servicios tecnológicos, así como también los principios definidos para ese dominio los cuales se encuentran en el documento "Modelo de Gestión IT4+" y las políticas de seguridad de la información de la entidad y la DGTI, que se encuentran enmarcadas en el sistema de gestión de calidad SIG:

- Gestión del portafolio y catálogo de servicios
- Gestión de niveles de servicio - ANS
- Gestión de la demanda
- Gestión de la capacidad
- Gestión de la disponibilidad
- Gestión de la continuidad
- Gestión de seguridad de la información
- Gestión de terceros/prestadores de servicio de TI
- Gestión de los cambios
- Gestión de conocimiento
- Gestión del proceso de mejora
- Gestión de activos
- Gestión de configuración
- Gestión de problemas
- Gestión de accesos

Gestión del portafolio de servicios y catálogo de servicios

Las principales actividades a cargo del contratista son:

- Revisar la documentación actual correspondiente y mantenerla actualizada.
- Ajustar el portafolio de servicios tecnológicos y el catálogo de servicios (servicios activos y retirados).
- Definir o revisar la estrategia de actualización.
- Monitorear permanentemente el proceso

Gestión de Incidentes

El objetivo de este proceso es resolver, de la manera más rápida y eficaz posible, cualquier incidente que cause una interrupción en el servicio o reducción en la calidad de un servicio. Los incidentes pueden incluir fallas reportadas por los usuarios, el equipo del servicio o por alguna de las herramientas de monitorización de eventos.

El proceso de gestión de incidentes implementado en el servicio debe asegurar que:

- Los incidentes reportados son registrados y monitoreados.
- Los incidentes son resueltos rápidamente.
- Se minimiza el riesgo y el impacto negativo en la operación de La Unidad.
- Proporciona información para el mejoramiento continuo.

- El contratista deberá ejecutar las siguientes actividades sin limitarse a las mismas:
- Recepción, registro y atención del incidente - Ofrecer una solución inmediata cuando sea posible.
- Verificar usuario y tipo de incidente: determinar si el personal de la mesa de servicios está autorizado a manejar el incidente. Generalmente incluye verificar que el producto que pueda requerir de soporte sea un estándar de La unidad, identificado en el catálogo de servicios y que le corresponde a los ANS.
- identificar, notificar, gestionar y dar tratamiento a los incidentes mayores que se puedan presentar en los servicios.

Recepción Registro y Categorización del Incidente

- Establecer relación con el usuario
- Brindar un soporte inicial
- Tomar la información básica del usuario
- Recolectar toda la información y evidencia de los síntomas del incidente
- Obtener información adicional necesaria básica para apoyar el diagnóstico inicial del incidente.
- Seguir un guion cuando sea necesario. El contratista deberá garantizar que todo incidente recurrente tiene un guion que debe seguir su personal de soporte.
- Clasificar provisionalmente el incidente con la información obtenida hasta el momento. Priorizar el incidente dependiendo del nivel de impacto y urgencia.

Investigación y Diagnóstico

Comienza a documentarse el incidente y los problemas relacionados con el mismo. Se recolectan y registran datos y evidencia adicional requerida para la documentación del diagnóstico del incidente.

Documentar el análisis y posibles soluciones alternas y temporales que, aunque no solucionen el problema, permitan solucionar el incidente o realizar escalamiento. Cuando se reciben varias llamadas relativas a un mismo incidente, se agrupan en un problema.

Clasificar el incidente (categorización): es muy importante que todos los criterios de clasificación y la mayor cantidad posible de información del ticket esté codificada, a fin de poder producir los reportes de manera más efectiva, en miras a detectar y corregir rápidamente los orígenes de las fallas.

Documentar posibles soluciones alternas, temporales que permitan solucionar el incidente o escalamiento, aun cuando se desconozca el problema y/o su solución, esta documentación debe quedar en la base de conocimiento de la herramienta de gestión de servicios que suministre el contratista, permitiendo la búsqueda por parte de otros técnicos para la replicación de las posibles soluciones en casos que el incidente sea recurrente.

Buscar posibles errores conocidos similares.

Resolución del Tiquete

En caso de no poderse solucionar, el tiquete deberá ser escalado al siguiente nivel de soporte, el escalamiento se puede realizar manualmente cuando se conozca cuál especialista es el más indicado dependiendo del tipo de incidencia y/o problema. El escalamiento al siguiente nivel de la mesa de servicios o de personal especializado del contratista también puede ser automático si el problema no es resuelto dentro de un período de tiempo estipulado.

Cierre del Tiquete

Cuando se solucione un tiquete, el agente de la mesa de servicios o el técnico de soporte en sitio que alcanzó la solución, debe registrar el cierre del incidente cumpliendo con los siguientes pasos:

- Verificar la conformidad del usuario con la solución dada.
- Verificar que el incidente haya sido clasificado correctamente, dependiendo de la solución que se haya obtenido
- Verificar que el incidente sea cerrado con síntomas, diagnóstico, causa y solución.
- Verificar que la base de datos de conocimientos de la solución de gestión del servicio sea alimentada con la solución del caso para ser utilizada en la solución de futuros problemas y que queda disponible para consulta por parte de todos los usuarios autorizados.

El usuario puede objetar la solución y puede, conforme a los medios de acceso establecidos, instaurar una inconformidad en el servicio.

Todo incidente debe ser resuelto en la etapa más temprana posible, cuando en una etapa se alcance el tiempo máximo esperado de solución determinado por los ANS, se procede a escalar a la siguiente etapa hasta que se resuelva.

Cada vez que un incidente escale a una siguiente etapa de atención se le deberá informar al usuario afectado de manera automática a través de la herramienta.

Seguimiento

El contratista debe asegurar el diligenciamiento completo de cada incidente. Además, debe proporcionar informes y consultas, con posibilidad de filtros por diferentes variables, acerca de la gestión de la mesa de servicios que están siempre disponibles en línea, para que los administradores verifiquen el cumplimiento y la calidad de los siguientes parámetros:

- Diagnósticos acertados
- Documentación clara, consistente y completa
- Categorización de cierre de acuerdo con la solución
- Escalamiento indicado
- Soluciones claras que resuman el síntoma, causa y los procedimientos de solución

Este mecanismo pretende certificar la calidad de la información contenida en estos registros de incidentes ya que, de la información consignada, dependerá la calidad de los informes y reportes que posteriormente se extraerán para medición y análisis. La calidad del servicio debe ser también evaluada mediante encuestas de satisfacción dirigidas al usuario:

- El modelo de la encuesta se debe diseñar y administrar por parte del contratista y será acordada con La Unidad.
- Debe permitir seleccionar las características de la muestra a encuestar y el tamaño de esta (porcentaje).
- Posteriormente, ejecutar el proceso de forma aleatoria y almacenar los resultados para su publicación.
- La muestra mínima mensual se define en un cinco (5%) del total de incidentes y/o de todos aquellos usuarios que solicitaron el servicio.

Los resultados obtenidos se deberán analizar y permitirán formular planes y acciones de mejora a la prestación del servicio que deben estar incluidos en los informes de gestión presentados a la supervisión del contrato.

Escalamiento

En las labores de escalamiento el contratista deberá apoyarse en la matriz establecida entre las partes para cada servicio de tecnología de la Entidad, este escalamiento deberá ir documentado con el respectivo diagnóstico técnico detallado que permita a cada nivel escalar un proceso de atención y solución más asertivo.

El contratista será responsable de la solución de los incidentes y problemas de los servicios y equipos a su cargo y en caso de no poder solucionar el problema deberá escalar directamente a los contratistas definidos por la dirección de tecnología para su solución. No obstante, la responsabilidad del seguimiento a toda solicitud de tecnología es responsabilidad del contratista del servicio de mesa de servicios.

Suspensión o detención de tiempos

Los criterios para los estados de suspensión o estados donde se realiza detención temporal de los tiempos de atención de los incidentes y solicitudes se definen en el modelo de operación acordado entre las partes.

Reapertura de los servicios

La Unidad define como tiempo establecido de garantía en la atención de un incidente o solicitud de servicio dos (2) días hábiles, a partir la fecha y hora de cierre del tiquete, si durante este tiempo se presenta una inconformidad por parte del usuario final se reabrirá el caso inicialmente reportado y este no se contará como nuevo. Si resultado del análisis se identifica que este no guarda relación con el tiquete inicialmente reportado, o se reporta después del periodo de garantía, será contabilizado como uno nuevo.

Gestión de Problemas

En caso de incidentes de gran impacto y/o incidentes recurrentes o repetitivos, los tiquetes se crearán y categorizarán como un problema y se enviarán para que se gestione su solución por parte de Nivel II. No obstante, por parte de esta gestión se realizará el seguimiento necesario hasta su cierre. En la gestión se debe realizar:

- La identificación proactiva de los problemas
- Categorización y priorización de atención y solicitud de problemas escalados
- Diagnóstico, análisis de causa y resolución de problemas escalados
- Control y seguimiento de problemas y recurrencia
- Validar las soluciones alternativas o temporales para reducir el impacto de un incidente - Evaluación y cierre de problema escalado.
- Revisión de problemas escalados
- Mantener una base de errores conocidos. (KEDB).

El contratista deberá monitorear permanentemente el estado de los problemas escalados con el fin de mitigar riesgos y evitar denegación de servicios. Centrará su atención en mejorar la atención hacia el usuario final analizando los incidentes más recurrentes y los problemas reportados e informando en los comités técnicos las acciones tomadas, y teniendo en cuenta el nivel de criticidad de los servicios y usuarios afectados por el problema.

La mesa de servicios además debe entregar el informe correspondiente, deberá clasificar y/o identificar, entre otros:

- El impacto del problema - Número de usuarios afectados - Nivel de criticidad del usuario.
- Dependencias afectadas.
- Nivel de criticidad del servicio impactado
- Esfuerzo y tiempo requerido para solucionar el problema

El contratista deberá tener el personal requerido, que analice los orígenes y gestione los problemas – estudio de la causa-raíz y deberá presentar a La Unidad los resultados de los problemas e incidentes para todos los servicios, incluyendo las soluciones definitivas y/o temporales al problema.

Gestión de Peticiones/Requerimientos

El contratista en esta gestión le corresponde atender todas las solicitudes de gestión de accesos, gestión de activos de tecnología y demás solicitudes de los servicios de tecnología que demande La Unidad para ello deberá:

Brindar atención en las solicitudes de los servicios de tecnología y recibir servicios estándar para que exista la preaprobación y procesos de calificación de la viabilidad de la petición.

Proporcionar información a los usuarios y clientes sobre la disponibilidad de servicios y el procedimiento para su obtención.

Proveer y entregar los componentes de los servicios solicitados estándar (por ejemplo, accesos, licencias de software y medios de comunicación, entre otros).

Asesorar técnicamente frente a los servicios de tecnología.

Gestionar todo lo relacionado con los accesos lógicos de los servicios de tecnología de La Unidad, de conformidad con lo establecido en la política de acceso lógico y el subproceso de gestión de acceso a los aplicativos y/o servicios de tecnología, atención que se debe realizar con sus debidas autorizaciones.

Gestionar todos los requerimientos relacionados con la preinstalación, instalación, movimiento, adición, cambios y remociones de equipos o elementos arrendados o de propiedad de La Unidad, para ello deberá alinear este tipo de solicitudes con el subproceso de gestión de activos de la configuración.

Prestar soporte técnico a equipos de propiedad/arrendados por La Unidad, se deben incluir estos equipos dentro del registro y control de la CMDB (Configuration Management Database), así como en los reportes de inventario que se obliga a mantener debidamente actualizados.

Atender los requerimientos para prestar acompañamiento y soporte técnico a equipos utilizados, para realizar eventos dentro y fuera de las sedes de La Unidad mediante el desplazamiento de personal técnico en forma temporal y cuando se requiera. Realizar seguimiento a los tiquetes registrados, que cumplan con garantía y calidad. Verificar con el usuario que su tiquete haya sido resuelto, así como la calidad en el cumplimiento del ANS y el nivel de satisfacción frente a la solución del incidente.

Verificar mediante encuesta, el nivel de satisfacción frente a la solución del incidente.

Notificar trimestralmente a La Unidad los resultados de la encuesta de satisfacción y los planes de acción asociados, para el mejoramiento y la gestión realizada con el nivel I y II. Cerrar la solicitud de servicio, previa aprobación del usuario.

Gestión de Niveles de Servicio

El contratista es el responsable de garantizar los niveles de calidad de los servicios de tecnología para ello deberá:

Definir las actividades necesarias para garantizar el cumplimiento - ANS establecidos por La Unidad.

Suministrar los informes solicitados por La Unidad para garantizar los ANS Estar dispuesto a mejorar los servicios que presta con La Unidad.

Gestión de la Demanda

El proceso de gestión de la demanda busca predecir los ciclos de consumo de los servicios de tecnología, adaptando los recursos de tecnología a los picos de mayor exigencia para asegurar que los servicios se cumplan conforme a los ANS pactados, para el logro del objetivo se debe:

- Considerar el impacto de las demandas de tiquetes como producto del incremento de usuarios que hacen uso de los servicios de IT, de acuerdo con las proyecciones de crecimiento en La Unidad.
- Tener como foco el seguimiento a la demanda de los servicios a través de la presentación de informes mensuales en los que se pueda determinar la evolución de los servicios de IT.
- Ser parte activa en el comité operativo para el seguimiento mensual a la demanda.
- Planear entre las partes, los recursos para los servicios de acuerdo con la evolución de la demanda de tal manera que se garantice la capacidad de la infraestructura para la prestación de los servicios.
- Atender eventos no planeados que para efectos del desarrollo de sus servicios sean programados por La Unidad, los cuales se informarán con una anticipación no inferior a un (1) día calendario.
- Realizar análisis, generar estadísticas, proyecciones y presentar informes mensuales relacionados con el comportamiento y uso de las aplicaciones /servicios IT de La Unidad.

Gestión de la Capacidad

La gestión del proceso debe establecer el nivel de las capacidades y monitorear las mismas para cada uno de los diferentes servicios de la DGTI.

Elaborar y mantener actualizado un plan de capacidad, que refleje las necesidades actuales y futuras.

Analizar y monitorear las mediciones de capacidad de los diferentes servicios que le provee la DGTI, entre ellos enlaces de comunicación, equipos, servidores y elementos de configuración (CI).

Generar informes mensuales que reflejen la disponibilidad y la capacidad de los servicios. Brindar asistencia en el manejo y evaluación de los riesgos de incidentes y eventos que puedan impactar la capacidad de los servicios.

Evaluar el impacto de todos los cambios que se ejecuten sobre los servicios de IT. Asegurar la eficacia de las medidas proactivas para mejorar la disponibilidad de los servicios a su cargo.

Proponer y acordar con La Unidad los cambios, mejoras y actualizaciones a la infraestructura para garantizar los niveles de capacidad requeridos en cada una de las áreas.

Mantenimiento de un conjunto de métodos, métricas, técnicas, cálculos y reportes para todas las mediciones de capacidad.

La recolección de mediciones, el análisis y la producción de informes y reportes periódicos y demás informes especiales sobre el servicio y la capacidad de los componentes.

Gestión de la Disponibilidad

Con esta gestión se busca monitorear y garantizar el nivel de disponibilidad de todos los servicios de tecnología, en este proceso se debe incluir:

- El monitoreo de todos los aspectos de disponibilidad, fiabilidad y facilidad de mantenimiento de servicios IT y los componentes de apoyo, con actividades apropiadas, tales como alarmas de umbral, procedimientos de escalamiento, scripts automatizados para la recuperación de información del sistema, medición y observación.
- Mantenimiento de un conjunto de métodos, métricas, técnicas, cálculos y reportes para todas las mediciones de disponibilidad.
- Asistencia a La Unidad con el manejo y evaluación de los riesgos de incidentes que puedan impactar la disponibilidad.
- La recolección de mediciones, el análisis y la producción de informes y reportes periódicos e informes especiales sobre el servicio y la disponibilidad de los componentes solicitados por La Unidad en cualquier momento.
- Elaborar el plan de disponibilidad de los servicios de TI.
- Planificar y pronosticar los futuros niveles de disponibilidad requeridos.
- Identificación y resolución de los incidentes y los problemas asociados con la no disponibilidad de los servicios.

Gestión de la Continuidad

Las principales actividades de la gestión de la continuidad de los servicios de tecnología corresponden a:

- Implementar, verificar y proponer las mejoras a las políticas y el alcance de la gestión de la continuidad de servicios de tecnología de La Unidad.
- Evaluar el impacto en el negocio de una interrupción de los servicios de TI.
- Analizar y prever los riesgos a los que están expuestos los servicios de TI.
- Identificar y establecer las estrategias de contingencia del servicio de TI.
- Adoptar medidas proactivas de prevención del riesgo de tecnología, en caso de que aplique para los servicios a su cargo.
- Diseñar, documentar, mantener actualizado y desarrollar el plan de recuperación tecnológica de los TI, alineados con la política corporativa y los demás prestadores de los servicios de tecnología.
- Planificar las pruebas del plan de recuperación tecnológica mínimo una (1) vez por año. Monitorear el plan de recuperación, así como la implementación de las incidencias resultado de pruebas previas de tal manera que se mitiguen.
- Dar cumplimiento al decreto 2573 de 2014, recogido en el decreto 1078 de 2015, y actualizado con el decreto 1008 de 2018 en el componente tic para la gestión, subcomponente operación de servicios tecnológicos de La Unidad, con lo cual se debe propender por la implementación y ejecución de planes de continuidad de los servicios de TI.
- Dar cumplimiento a toda la normatividad que el gobierno nacional expida sobre la materia.

Gestión de la Seguridad de la Información

Estándar ISO 27001:2013 y las políticas específicas de la oficina de seguridad de la información. Dentro de las actividades establecidas debe realizar:

Apoyo al proceso de mejora continua del proceso.

Participar del rediseño de las políticas, controles y riesgos de los servicios de tecnologías, según las directrices establecidas por la oficina de seguridad de la información de La Unidad.

Implementar los requerimientos de seguridad de la información para el funcionamiento de los equipos y dispositivos tecnológicos de los servicios de La Unidad, con base en lo establecido en las políticas específicas de seguridad de la información de la Unidad. Verificar y realizar seguimiento a la normatividad de seguridad de la información, estándares y buenas prácticas aplicables establecidas por La Unidad.

Analizar los riesgos de seguridad de la información y realizar seguimiento al plan de tratamiento y mitigación.

Realizar seguimiento a las auditorías y evaluaciones de seguridad de los servicios de tecnología en La Unidad.

Presentar conceptos técnicos de seguridad de la información que solicite La Unidad a través del supervisor del contrato, o bien, por solicitudes de la oficina de seguridad de la información de La Unidad.

Participar y acompañar el proceso de concientización, campañas de divulgación y demás elementos necesarios para la divulgación del sistema de gestión de seguridad de la información de La Unidad. Las campañas serán aprobadas por la oficina de seguridad de la información de La Unidad.

Realizar seguimiento a los controles de tecnología, de acuerdo con las directrices establecidas por la oficina de seguridad de la información de La Unidad.

Coadyuvar al proceso desde el ámbito que define gobierno en línea para el sistema de gestión de seguridad de la información en el decreto 1078 de 2015 y con los ajustes implementados con el nuevo modelo de gobierno digital, Decreto 1008 de 2018, con ISO 27001-2 superior, con las normas de regulación colombiana para la seguridad de la información vigente tales como: ley 527 de 1999, ley 1266 de 2008, ley 1273 de 2009, ley 1581 de 2012; decreto 1377 de 2013, ley 23 de 1982, ley 594 de 2000, documento CONPES 3854 de 2016, y con la reglamentación posterior que se expida por parte del Gobierno Nacional. Así mismo, debe cumplir con las directrices establecidas por la Oficina de seguridad de la información de La Unidad.

Gestión de Terceros/Prestadores de TI

La gestión de este proceso se obliga a realizar la gestión, control y seguimiento técnico, para asegurar la disponibilidad de los servicios entre los distintos prestadores de servicio de tecnología de La Unidad, siendo un canal facilitador para la entrega de diagnósticos y escalamiento asertivo; así como del respectivo seguimiento de los ANS. Realizar seguimiento a las solicitudes escaladas a Nivel II y III.

Gestión de Cambios

La gestión de este proceso se obliga y será el responsable de supervisar y monitorear la modificación de los servicios de TI, garantizando que todo el proceso es planificado, instalado, configurado, evaluado, probado y documentado.

En esta gestión, es asegurar que los cambios son registrados y evaluados, autorizados, priorizados, planificados, probados, implementados, documentados y revisados de forma controlada. Los cambios deben ser administrados con el fin de:

Reducir la exposición al riesgo.

Minimizar la gravedad de un impacto en la interrupción o perturbación del servicio. Ser exitoso en el primer intento de cambio que se ejecute eliminando pérdidas de tiempo y de confiabilidad.

El contratista, debe velar por la gestión de cambios que afecten los servicios de tecnología, sean debidamente probados con los administradores de plataforma y funcionarios de la DGTI.

Realizar análisis mensual de los cambios efectuados

Gestión de Activos – Configuración (CMDB)

El contratista debe consolidar y llevar inventario de toda la infraestructura de La Unidad con su respectiva información de los ítems de configuración (IC), independiente del centro de datos (nube privada/pública) y/o sede donde se encuentren alojados los servicios y/o aplicaciones de la entidad.

Realizar la gestión técnica y de escalamiento de la infraestructura de usuario final (Thin Client, NUC, Monitores) propiedad de La Unidad.

Mantener contacto con las demás gestiones, con el fin de mantener actualizada la CMDB.

Gestión de Eventos - (NOC)

El contratista realizará la gestión alineada de acuerdo con las buenas prácticas y herramientas dispuestas en el NOC para tal fin.

Monitorear los servicios de Tecnología y reportar los incidentes que se presenten a la mesa de servicio.

Este proceso debe ser automatizado logrando una gestión proactiva y no reactiva

Gestión del Conocimiento

El contratista gestionará toda la información relevante de los servicios de IT, asegurando que esté disponible para el uso del soporte de nivel I y II, permitiendo en forma relevante reducir los tiempos para el análisis en la atención de solicitudes. Las responsabilidades del contratista asociadas a este componente del servicio son:

El contratista deberá mantener la base de datos de conocimiento actualizada, rediseño de los procesos, así como la interacción de los usuarios a través de un

módulo de preguntas frecuentes (FAQ por sus siglas en inglés) y generación de artículos de interés técnico.

El contratista deberá entregar evidencias de capacitación expedida por el contratista de la solución y actualización bimestral del personal de soporte con mejores prácticas, procedimientos, rutinas de mantenimiento, protocolos de escalamiento y las acciones definidas en los planes de mejora.

Realizar sesión periódica con la DGTI donde se pueda mostrar los últimos documentos publicados, su consulta y la utilidad de estos.

Gestión del Proceso de Mejora - PQRs

El contratista deberá medir la calidad de los procesos para generar acciones de mejora en los servicios de tecnología de La Unidad.

El contratista debe evaluar los servicios de TI de La Unidad y los resultados de las mejoras propuestas se acordarán entre los prestadores de servicio de la DGTI.

El contratista deberá entregar los reportes de gestión del servicio y estadísticas relacionadas con las actividades de cada Nivel de Soporte con su correspondiente medición de ANS.

Gestión de ANS (Tablero de gestión)

El contratista debe integrar bajo un único cuadro de mando, toda la información que permita la visualización en línea de todos los aspectos relacionados con la operación tecnológica, este será acordado entre las partes.

En las instalaciones de la DGTI el contratista se obliga a disponer de una matriz pantalla LCD O LED, que permitan visualizar el estado, en tiempo real de la información mencionada en el punto anterior.

Se debe asegurar que los tableros de control implementados:

- Métricas e indicadores claves de desempeño basados en mejores prácticas y en alineación con ITIL.
- Brindar capacidades para consolidar indicadores de la operación de TI.
- Proveer acceso en línea a los indicadores claves para apoyo en la toma de decisiones.
- Integrar vistas consolidadas, las cuales permitan comprender la disponibilidad e indicadores de impacto de los procesos de soporte de los servicios de TI, tales como incidentes frecuentes y cambios recientes en las configuraciones que pudieran afectar la disponibilidad del servicio.

- Con base en la información producida por la solución de gestión de servicios tecnológicos generar estadísticas e índices para distintos períodos de tiempo y permitir realizar análisis, simulaciones y pronósticos en línea.
- Contar con un asistente para la integración y correlación de fuentes de datos externas para las herramientas adicionales propuestas.
- Brindar capacidades "Drill Down" para un análisis profundo de los datos.
- Proporcionar información que permita identificar las causas raíz de los problemas
- Contar con información que permita evaluar la calidad del soporte técnico que se está brindado.

Estadísticas del Servicio

A continuación, se registran algunas estadísticas promedio de las solicitudes/ tiquetes de los servicios de tecnología:

Cantidad promedio mensual

AÑO	2023		2024									
Tipo/Mes	**Noviembre**	**Diciembre**	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**
Incidentes	3047	3082	2310	3304	2872	3419	3197	2399	2413	3176	3423	3397
Peticiones	2339	2108	2351	2466	2019	2537	2416	2228	1770	1529	1716	1932
Peticiones Accesos	674	523	765	780	574	772	696	578	634	437	346	491
Peticiones Activos	16	25	19	41	15	12	18	15	27	27	35	27
Total	6076	5738	5445	6591	5480	6740	6327	5220	4844	5169	5520	5847

Cantidad promedio mensual de casos atendidos por sede:

Año	2023		2024									
Sede	**Noviembre**	**Diciembre**	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**
Usuarios Remotos Sin Sede	2508	2377	2104	2463	2221	2717	2590	2216	1298	1226	1912	2063
Marriot	3568	3361	3341	4128	3259	4023	3737	3004	3546	3943	3608	3784
Calle 13	201	190	168	197	178	217	207	177	104	98	153	165
Total general	6076	5738	5445	6591	5480	6740	6327	5220	4844	5169	5520	5847

Cantidad de usuarios y equipos por ubicación:

Ubicación	Número de Usuarios en Sitio	Equipo Escritorio (Workstation propios de UGPP)	Equipo Portátil (Propios de UGPP)	Estación Liviana (Propias de UGPP)
Marriot	665	39	80	550
Calle 13	184	0	0	36
Total	**849**	**39**	**80**	**586**

Volumen promedio de ingreso de solicitudes por canal (llamadas, correo, chat, web, etc.) Y franja horaria.

Ubicación	Canal		
	Correo electrónico	Web	Teléfono
Marriot	1208	229	1966
00_REMOTOS SIN SEDE	328	316	398
Calle 13	28	0	0

(*) la franja horaria es de 07:00 am a 07:00 pm.

Porcentaje de casos con solución promedio mensual de sitio y mesa de ayuda:

Nivel Soporte	Cantidad
Soporte en Sitio	2900
Mesa de Ayuda	650
Nivel 2	1600

2. ESCRITORIOS VIRTUALES

Las especificaciones técnicas mínimas sin limitarse a las mismas comprenden:

- 2.1 Licenciamiento
- 2.2 Infraestructura
- 2.3 Configuración del Servicio
- 2.4 Administración y Soporte de la Plataforma

2.1 LICENCIAMIENTO

Respecto del licenciamiento la solución de escritorios virtuales debe ser implementada con los respectivos productos y cantidades mínimas a soportar corresponden a:

- Escritorio en modalidad VDI DAAS para 1100 usuarios concurrentes.
- Microsoft Windows 11 Enterprise multisesión para 1100 usuarios y RDS para el acceso a los usuarios de las aplicaciones cliente servidor que se virtualizarán.
- Microsoft 365 Apps for Enterprise para 1200 Usuarios
- Microsoft Project Plan 3 hasta 100 usuarios.

En todo caso, los servicios prestados en modelo de escritorio virtual deberán estar correctamente licenciados bajo el esquema de Windows 11 Enterprise multisesión y los servicios prestados en modelo de escritorio virtual compartido o publicación de aplicaciones deberán incluir el licenciamiento Windows server y la licencia RDS respectiva para el acceso.

Es responsabilidad del contratista mantener vigente el soporte de las licencias de los productos señalados, en aras de asegurar el soporte de fábrica y el derecho a las actualizaciones de los productos objeto y alcance contractual.

Todas las suscripciones adquiridas deben quedar a nombre de la entidad, así como la configuración bajo el dominio ugpp.gov.co

2.2 INFRAESTRUCTURA

Los requisitos a nivel de infraestructura comprenden la provisión de los recursos de (VCPU, RAM y DD) que deben ser habilitados por perfil de escritorio virtual, conforme a las siguientes capacidades:

Perfil	**Tipo Imagen**	**Usuarios**	**Recursos asignados por usuario virtualizado**			**Sistema Operativo**
			vCPU	**RAM (MB)**	**DD**	
Ofimático Perfil Standard	Pooled	700	4	8	60 GB	Windows 11
Escritorio Ofimático Perfil Avanzado	Pooled	400	8	16	60 GB	Windows 11

Perfil	Tipo Imagen	Usuarios	Recursos Asignados Para Todos los Usuarios			Sistema Operativo
			vCPU	RAM	DD	
Servidor Aplicaciones VirtualApps	Compartida	Por Demanda	80	320	1000 GB	Windows Server 2019

El contratista debe ejecutar todas las actividades de migración de datos de usuario, instalación, configuración e implementación de la solución de los escritorios, habilitando cada uno de los productos descritos en el componente de licenciamiento.

La Unidad suministrará el (los) certificado digital mediante entidad certificadora para que el contratista configure el acceso externo a las plataformas.

El contratista debe contar con herramientas de monitoreo y de gestión en tiempo real, de todos los componentes de la solución implementada, tales como registro de eventos de fallas, alertas y auditoría a nivel de todos los servicios que la componen, experiencia de usuario, tiempos de inicio de sesión, tiempos de inicio de aplicaciones virtualizadas, infraestructura de servidores, almacenamiento y tráfico.

Los registros de monitoreo deben estar disponibles para ser consultados por el SIEM que disponga la entidad y el tiempo de retención de los mismos deben permanecer mínimo noventa (90) días.

El contratista debe documentar el plan de recuperación de desastres (DRP), permitiendo la continuidad del servicio en caso de una falla de disponibilidad en la zona principal. Este esquema de redundancia deberá soportar el 20% de la operación de La Unidad en caso de requerir operar en centro alterno, garantizando asimismo la disponibilidad de los perfiles y data de los usuarios.

El contratista debe asegurar un Backup de todos los componentes de la solución de escritorios virtuales, data usuario y demás objeto y alcance contractual; garantizando el respaldo diario en dado caso de pérdida de estos. De conformidad a la política de Backups de la Entidad. Las políticas de Backups corresponde a: Backup Mensual ultimo o primer día del mes con una retención permanente, los Backups Semanales se realizan los sábados o domingos y estos tiene retención de 4 semanas (1 mes), Backups incrementales todos los días con excepción el día que se ejecuta el mensual o semanal con retención de 1 semana, para bases de datos transaccionales o archive pueden ejecutarse cada 2, 4 o 6 horas dependiendo de la criticidad de la base de datos estos Backups tiene retención de 1 semana.

Estas copias de respaldo conr etencion de mas de 1(un) mes deberán ser almacenadas en una zona diferente a la zona principal donde será desplegada la solución.

.

El contratista deberá implementar el aseguramiento (Hardening) de cada uno de los componentes de la solución y deberá realizar pruebas de vulnerabilidad cada seis (6) meses sobre todos los componentes de la plataforma en las cuales La Unidad podrá participar de las mismas.

El contratista de la solución deberá garantizar durante el plazo de ejecución del contrato que implementará y propondrá de manera proactiva nuevas funcionalidades de la plataforma que hagan sentido para La Unidad a medida que el fabricante VDI libere dichas funcionalidades.

El contratista deberá mantener actualizados los componentes de sistemas operativos y agentes virtuales que residan en su infraestructura. Para cada actualización de agente virtual o sistema operativo se debe realizar el respectivo proceso de pruebas que garantice la compatibilidad y correcta interacción con el ambiente de aplicaciones de La Unidad.

El contratista deberá implementar todos los roles/servicios necesarios para el correcto funcionamiento de la plataforma. Estos roles hacen referencia a DHCP, File Server, Servicio de aprovisionamiento de imágenes, FSLogix, Directorio Activo - Ready On line entre otros. Se requiere la configuración de FSLogix.

2.3 CONFIGURACIÓN DEL SERVICIO

El servicio de los escritorios virtuales debe estar disponible **Lunes a viernes de 7:00 a.m. a 7:00 p.m. y sábados de 07 am a 02 pm**. En caso, de requerirse la prestación del servicio en horarios adicionales a los aquí contemplados, el contratista sin costo alguno habilitará el servicio previa notificación de la supervisión.

Los horarios adicionales corresponden a los dos (2) últimos días de cierre de mes o períodos de compensación, este último en aproximadamente ciento sesenta (160) horas al año, lo anterior para sus respectivas estimaciones del modelo de negocio. De igual manera, las conexiones de usuario por fuera de jornada laboral son aproximadamente de 100 usuarios.

La arquitectura que diseñe el contratista debe proveer y garantizar un modelo de seguridad integral de perímetro (firewall entre otros), basado en las mejores prácticas existentes que permita la protección de la infraestructura frente a posibles ataques internos y externos.

La solución debe integrarse al esquema actual de comunicaciones de la red de La Unidad y deben garantizar la implementación en alta disponibilidad.

La comunicación desde la infraestructura de escritorios y el centro de datos de la nube privada de La Unidad debe tener una capacidad de al menos 200 Mbps (interconexión Cifrada). La conectividad debe integrar al SD-WAN o por MPLS en la topología de red WAN. Así mismo, se debe asegurar la conectividad entre la infraestructura de escritorios y la nube pública de GCP donde se alojan las aplicaciones de la entidad.

La solución debe permitir entre otras cosas:

- Compatible y con Agilidad en despliegue
- Despliegues Híbridos de aplicaciones y Escritorios (Linux, Windows)
- Agilidad en clientes
- Optimización de red
- Administración simplificada
- Agilidad en publicación de aplicaciones
- Autenticación Doble factor Incluida
- Modelos de licenciamiento claro y completo unificado para el TCO (Costo Total de Propiedad)
- Accesos HTML5, Cliente escritorio (Linux, Windows, Mac), Quiosco.

La solución deberá permitir crear escritorios virtuales personalizados para cada usuario, brindado acceso a las aplicaciones y datos necesarios para realizar sus tareas de manera eficiente.

La solución deberá tener compatibilidad Multiplataforma: Utilización de programas y escritorios compartidos y exclusivos de Windows y Linux a través de una sola plataforma integrada de distribución, implementada en el lugar o accesible como un servicio.

La solución deberá contemplar seguridad Avanzada: Como cifrado de datos, autenticación de múltiples factores dentro de un mismo licenciamiento, controles de acceso granulares.

La plataforma deberá facilitar la gestión centralizada de los escritorios virtuales.

El contratista debe contemplar servicios de especialistas autorizados por el fabricante de virtualización y Nube para el acompañamiento del análisis, diseño y QA de la solución implementada..

La memoria técnica de la solución implementada con cada uno de sus productos debe ser documentada y entregada a la Unidad.

El contratista debe realizar la transferencia de conocimiento de la instalación, configuración y operación de la solución al equipo de la Dirección de Gestión de Tecnología asignado para tal fin.

La solución debe permitir la misma experiencia de Windows independiente del dispositivo final, esto quiere decir que la solución debe estar en la capacidad de detectar el tipo de Endpoint y ajustarse a las capacidades de este.

La solución debe tener mecanismos para acceder al ambiente virtual, ingresando un correo electrónico para usuarios internos y externos de forma segura, garantizando conexiones seguras al entorno, así como una capa de protección MFA, 2FA. A fin de asegurar el balanceo de cargas y asegurar la puerta de acceso para la autenticación de los usuarios la solución debe garantizar mecanismos de alta disponibilidad en sus componentes balanceadores, túneles o lo que a sus veces garantice el requerimiento.

La solución se debe poder integrar un Directorio Activo de Microsoft de La Unidad para la gestión de políticas de acceso del usuario basado en grupos de seguridad.

La solución deberá incorporar características que permitan simplificar y centralizar la administración de imágenes de escritorios y servidores virtuales.

La solución debe implementar entregar aplicaciones de tipo cliente-servidor, de escritorio y web independientemente del sistema operativo cliente.

La solución debe garantizar la alta disponibilidad de los escritorios o aplicaciones virtualizadas sin importar la ubicación u origen de los servicios distribuidos en diferentes servidores en el centro de datos.

La solución deberá soportar funcionalidades de clipboard nativas (Copiar y Pegar) las cuales se podrán activar por perfiles de usuario, de acuerdo con los permisos establecido en la Matriz de Perfiles y Accesos a los sistemas. El detalle de esta

La publicación de aplicaciones virtuales (aplicaciones alojadas y ejecutadas en un servidor o servidores) en diferentes versiones de sistemas operativos, permitiendo el acceso seguro de estas aplicaciones en cualquier tipo de dispositivo incluyendo, a iOS, Android, Mac Windows y Linux.

La solución deberá proporcionar un control de acceso basado en roles los cuales sean personalizados con permisos configurables y que se integre con el directorio activo. Se debe implementar un esquema de doble factor de autenticación

La solución debe incluir la funcionalidad de autenticación, autorización y accounting para todos los usuarios a través de la validación de credenciales contra Bases de datos externas integradas.

La solución debe permitir la aplicación de políticas de control de los escritorios y usuarios tales como: políticas de control de puertos, borrado seguro, control de acceso basado en escenarios, consumos de anchos de banda en impresión y de aplicaciones multimedia.

La solución deberá contar con una herramienta de monitoreo y análisis avanzado, que permita generar reportes, análisis de tendencias y alertas personalizadas. De igual forma, deberá integrar una característica que proporcione un modelo de acceso

basado en roles que permita al equipo de soporte técnico diagnosticar y resolver inconvenientes fácilmente.

La solución deberá incorporar una característica de auditoria la cual permita monitorear y dar seguimiento a las actividades de administración en la infraestructura de aplicaciones y escritorios virtuales. La solución deberá permitir ver estos registros con filtros y generar La estructura de logs debe contar con los siguientes parámetros:

- Identificación de usuarios
- Tipo de evento
- Fecha y hora
- Indicación de éxito o fallo. (Verificar que la indicación de éxito o fallo se incluya en las entradas del registro de cualquier tipo de acción).
- Origen del evento
- Identidad o nombre de los datos, componentes del sistema o recursos afectados"

La solución deberá incorporar una característica que permita tener acceso a la información histórica sobre tendencias de sesiones, fallos de conexión, fallos de máquinas, rendimiento de los inicios de sesión y evaluación de carga.

La solución debe ser capaz de ofrecer una única arquitectura unificada para administrar: Virtualización de Aplicaciones, Virtualización de escritorios on-Premises, virtualización en nubes públicas y modelos híbridos.

La solución deberá entregar comunicaciones de voz claras y video nítido en alta definición para herramientas colaborativas, entre ellas Skype for Business, Google Meet, Teams, dentro de un escritorio o aplicación virtual en dispositivos Windows, Mac y Linux. La solución debe incluir un cliente HTML 5 que haga sencillo el acceso a los escritorios y aplicaciones virtuales desde cualquier dispositivo incluyendo aquellos en los que no es posible instalar un cliente local.

La solución debe ser funcional en los equipos de usuario final que serán provistos por el adjudicatario en modalidad de arriendo

La solución debe permitir aplicaciones Windows para dispositivos móviles (incluyendo Smartphone y tabletas táctiles), mientras que se mejora el rendimiento sobre redes de telefonía móvil para afrontar la variabilidad y pérdida de paquetes en estas conexiones, soportando la descompresión de gráficos y multimedia con aceleración de hardware en tablets y smartphones.

La solución deberá permitir el acceso seguro a los escritorios y aplicaciones desde cualquier lugar sin exponer a la red corporativa. Toda la información de misión crítica deberá permanecer protegida en el centro de datos a menos que pueda ser auditada, controlada y asegurada a través de políticas. Solo las actualizaciones de la pantalla, clic del ratón y pulsaciones del teclado (no los datos) viajarán a través de la conexión

remota, manteniendo los datos de las aplicaciones seguros de los hackers y la red corporativa protegida de dispositivos no administrados.

La solución deberá permitir un método para llevar un mejor control del acceso y el uso de los recursos de red, las aplicaciones y escritorios virtuales. Este método permitirá controlar que recursos de red acceden los usuarios según el escenario de acceso de cada uno, y qué tareas pueden ejecutar los usuarios con esos recursos una vez acceden a ellos (ejemplo: imprimir, copiar/pegar, mapeo de unidades).

La solución deberá permitir administrar los parámetros de personalización de los usuarios en entornos de virtualización (aplicaciones o escritorios), con el fin de acelerar el proceso de inicio de sesión de usuarios.

La solución permitirá visibilidad en profundidad del funcionamiento del protocolo de entrega de escritorios y aplicaciones virtuales, asegurando que los administradores tengan toda la información para solucionar problemas y mejorar la experiencia de los usuarios en la infraestructura.

La solución debe incluir un Gateway para la publicación segura de los servicios de virtualización, que permita un acceso remoto sin necesidad de una conexión VPN. Así mismo, se debe garantizar la optimización y visibilidad de las conexiones que se ejecutan hacia los escritorios y aplicaciones virtuales.

La solución debe incluir características de Autenticación de doble factor.

El contratista definirá en conjunto con La Unidad el total de los perfiles de usuarios, con las características mínimas de consumo requeridas.

El contratista debe incluir para cada uno de los perfiles, un esquema de producción, mantenimiento y desarrollo para garantizar una liberación de versión a cero riesgos.

La solución deberá brindar soporte para aplicaciones de 32 y 64 bit en sistemas operativos Windows.

La solución debe contar con una herramienta que permita hacer el análisis correspondiente para virtualizar o migrar aplicaciones a partir de sus instaladores. La solución deberá incluir una funcionalidad que mitigue la carga administrativa asociada a la gestión de múltiples controladores de impresión locales y de red, a través de servicios de impresión centralizados y universales y que además optimicen el rendimiento de la impresión a través de conexiones locales, remotas y móviles.

En caso de una desconexión del dispositivo, por motivos de corte de la comunicación, la solución deberá permitir al usuario tanto la reconexión automática cuando la comunicación se restablezca como la posibilidad de continuar su trabajo desde el mismo lugar previo a la desconexión sin duplicar la sesión.

La solución debe proveer Integración y soporte a periféricos locales, de acuerdo con las listas de compatibilidades existentes de los fabricantes, de forma transparente

para el usuario teniendo en cuenta los privilegios otorgados al usuario. Los usuarios deberán poder insertar un dispositivo USB localmente y usarlos desde su escritorio y aplicaciones virtuales como si estuvieran en su máquina local, esto previamente aprobado y configurado a través de las políticas de seguridad de la información.

La solución debe incluir soporte para que la sesión de escritorio virtual del usuario pueda verse en múltiples monitores a la vez que estén conectados al dispositivo cliente final. La configuración para múltiples monitores o con monitores de diferentes tamaños y resoluciones.

La solución debe de brindar la capacidad de apagar y encender los escritorios en base a necesidad de UGPP en base a carga o utilización de cada usuarios y escritorio. Esta capacidad debe de funcionar de forma automática según la parametrización previamente configurada en consenso con UGPP.

La solución deberá incluir una herramienta que permita monitorear y optimizar el uso del procesador y la memoria en las cargas virtuales, mejorando su performance y garantizando que las diferentes tareas de ejecución de los usuarios no resulten en bloqueo total de máquinas virtuales.

La solución deberá estar en la capacidad de utilizar memoria RAM como caché de escritura de las máquinas virtuales, para reducir el impacto en lectura a disco y no depender del performance del almacenamiento utilizado en la solución.

2.4 ADMINISTRACIÓN Y SOPORTE DE LA PLATAFORMA

El contratista debe realizar la administración de la solución, luego de ser implementada, por el tiempo del plazo de ejecución del contrato. El servicio de monitoreo, administración y soporte a la plataforma se debe dar en modalidad 7X24.

La administración y el soporte que se brinde es remoto, sin embargo, en caso de que la supervisión requiera la asistencia del equipo deberá el contratista atender dicha solicitud. En la gestión del servicio la administración comprende todo lo relacionado a la gestión de todo el servicio objeto descrito en los componentes de licenciamiento e infraestructura requerido por La Unidad (Productos de Virtualización y Infraestructura, MsOffice y/o demás requeridos en la arquitectura de la solución de escritorios virtuales)

En las actividades de VDI la gestión deberá realizar (licenciamiento, configuraciones, cambios o ajustes, paso a producción de imágenes, cambios en políticas de Software de VDI, crear perfiles, eliminar perfiles, asignación de aplicaciones, creación de Delivery Groups, actualización de imágenes, actualizaciones de seguridad) y todas aquellas actividades que permitan mantener la plataforma de de VDI operativa para La Unidad.

En las actividades de la infraestructura que Soporta los VDI la gestión técnica es integral y se deberá soportar cada uno de los componentes habilitados para la

prestación del servicio objeto y alcance contractual, incluidos los servicios de licenciamiento que se configuran en cada escritorio virtual.

Es parte de la gestión de la administración y soporte brindar los niveles de escalamiento establecidos, en el modelo de prestación de la mesa de servicio de la entidad y, en caso tal, gestionar los casos de soporte de usuario final con los agentes y/o soporte en sitio ó directamente con el fabricante de la solución para dar atención a los incidentes y/o requerimientos de los usuarios finales.

El soporte para la atención y resolución de incidentes y/o requerimientos relacionados con el servicio de virtualización de escritorios y aplicaciones, el contratista debe interactuar y operar bajo la herramienta de mesa de servicios que La Unidad disponga para tal fin.

Generar informe mensual del servicio que incluya los casos gestionados, cumplimiento de ANS y mejoras o mejoras que se aplicaron a la plataforma.

3. EQUIPO DE TRABAJO MINIMO

Los horarios del equipo de trabajo para la prestación del servicio son de lunes a viernes de 7:00 a.m. a 7:00 p.m. y sábados de 7:00 am a 2:00 pm.

Durante la ejecución y vigencia del contrato el contratista se obliga a suministrar y mantener el equipo de trabajo descrito, cada especialista no puede ejercer más de un rol y deben tener dedicación completa para atender los requerimientos de la Entidad.

Rol	**Experiencia Laboral Mínima**	**Certificaciones**
Gerente de Proyecto	Cinco años (5) como Gerente de Proyectos de Tecnología	Curso en gestion de proyectos PMP (Project Management Professional), ITIL Foundation V3 o superior
Gestor de Calidad y Aseguramiento del Servicio	Cuatro (4) años como Auditor o Coordinador de Calidad de Procesos de ITIL	ITIL Foundation V3 o superior y Auditor ISO en cualquiera de las siguientes normas: ISO 9001 o ISO 20000 o ISO 27001 ó superior

Arquitecto de Tecnologías	Cinco (5) años de experiencia en el ROL de Arquitecto de Tecnología	Cursos de Arquitectura GCP – Google Cloud Platafform
Administrador de Seguridad Perimetral	Cinco (5) años de experiencia en el ROL de Administrador de Seguridad Perimetral	CISM o CCSA o CCSE o JNCIA o CCNA o CISSP o CCIE Security
Administrador de Redes	Cinco (5) años en el rol de Administrador de redes de comunicaciones	Amplio Conocimiento en Redes cisco . Itil foundation V4
Administrador de Sistemas Operativos LINUX	Cinco (5) años de experiencia en el ROL Sistemas Operativos LINUX y/o Unix	Cursos en Linux.
Administrador de Sistemas Operativos WINDOWS	Cinco (5) años de experiencia en el ROL de Administrador de Sistemas Operativos LINUX y Unix y Windows Server	Cursos en plataformas Windows.
Administrador de Servidores de Aplicaciones	Cinco (5) años de experiencia en el ROL, de Administrador Servidores de Aplicaciones	Cursos de: Apache y Glassfish
Administrador de Base de Datos	Cinco (5) años de experiencia en el ROL de administración de base de datos	Certificaciones de SQL Server y Oracle

Administrador de Almacenamiento y Backups	Cinco (5) años de experiencia en el ROL de Administrador de Sistemas de Backups y/o Almacenamiento	
Administrador de Plataforma Open IAM	Cinco (5) años de experiencia en administración o implementación de soluciones Open IAM	Cursos en linux/Windows.
Administrador de VMware	Cinco (5) años de experiencia en el ROL, en VMware	Curso de Administración en VMware.
Administrador de Plataforma IBM Filenet - CloudPak	Cinco (5) años de experiencia en administración técnica de la plataforma IBM FileNet, IBM BAW, CPE, Records y Navigator y Workplace XT	Curso de IBM FileNet P8 System Implementatio n and Administration ; IBM Content Navigator; Con conocimientos en Cloud pak for Business Automation y Kubernetes and Red Hat OpenShift Container Platform **NOTA**: para este rol se aceptarán cursos en los temas ya descritos, sin que estos sean certificaciones

Administrador de Plataforma CloudPak	Cinco (5) años de experiencia en administración técnica de OpenShift	Conocimientos en Administración OpenShift
Arquitecto de Solución VDI	Experiencia especifica mínimo de cinco (5) años en el rol de Arquitecto en implementación de VDI	Certificación en diseño o implementación de la solución de VDI ofertada
Administrador VDI	Experiencia especifica mínimo de tres (3) años en el rol de Administrador de VDI	Certificación en administración o implementación de la solución de VDI ofertada
DBA (Database Administrator)	Experiencia especifica mínimo de cinco (5) años en el rol de DB2	Certificación en DB2

4. ACUERDOS DE NIVELES DE SERVICIO

Los Acuerdos de Niveles de Servicio se evaluarán mensualmente y los resultados serán incluidos en los informes que serán generados y entregados los cinco (5)

primeros días hábiles del mes siguiente a la prestación del servicio por parte del contratista, donde se indique explícitamente los resultados para cada indicador.

La medición de los ANS se soportará en los reportes generales y detallados que se configuren en la herramienta de mesa de servicios de tecnología y monitoreo. El detalle de la medición para cada indicador se definirá durante los primeros dos (2) meses de ejecución contractual y se denominará Protocolo de Medición de ANS.

El período de medición que aplicará en este acuerdo es de un mes calendario iniciando a las 00:00 horas del 1er día calendario del mes en análisis y finalizando a las 23:59 horas del último día calendario del mismo mes.

Para cada uno de los incidentes asociados a los tiempos de indisponibilidad, se 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.

Toda afectación a los ANS deberá contar con una acción correctiva, con su respectivo plan de trabajo.

EL CONTRATISTA es responsable por el monitoreo de los niveles de servicio y, por tanto, será responsable por entregar los soportes (logs de equipos, registros de la herramienta de gestión) que den muestra del cumplimiento de los ANS. En este sentido, para los tiempos en los que no haya soportes de la prestación de servicios, se entenderá como tiempo de no prestación del servicio. El detalle de la medición para cada indicador se definirá con la entidad y se denominará Protocolo de Medición de ANS.

Excepciones:

El CONTRATISTA responsable de los ANS podrá presentar evidencias objetivas que demuestren que no ha lugar a penalización por incumplimiento de ANS y estas serán evaluadas por el supervisor del contrato en una conciliación previa a la facturación.

Ventanas de mantenimiento programadas.

En cuanto a los indicadores de disponibilidad, estos excluirán los tiempos acordados para ventanas de mantenimientos preventivos programados por el contratista y/o la UGPP. En caso de presentarse fallas debidas a causas naturales, fuerza mayor o daños de terceros no habrá penalización.

INDICADORES

ANS DE "CIERRE BRECHAS DE SEGURIDAD"

META: Mayor o igual al 95.00% de Vulnerabilidades a atender en el periodo

CALCULO = 100% – %Vulnerabilidades a cargo, no resueltas

%No Cierre = (No Resueltas / Planificadas) * 100, para el periodo

%Descuento al ValorBase Facturable del Ítem de Servicio = %NoCierre

Aplicación del Descuento: Cuando el ANS no logre la META

Descuento **Máximo** = 10%

ValorNeto_aFacturar = Valor Base - %NoCierre (si aplica y sin exceder 10%)

ANS DE "DISPONIBILIDAD NUBE PRIVADA POR PLATAFORMA "

META: Mayor o igual al 99.96% en los horarios establecidos **por UGPP**

CALCULO = 100% – %Indisponibilidad

%Indisponibilidad X plataforma = (Down Time / TimePrometido) * 100 en cada Plataforma

%Descuento al ValorBase Facturable del Ítem de Servicio = Suma de

%Indisponibilidades X plataforma

Aplicación del Descuento: Cuando el ANS no logre la META

Descuento **Máximo** = 10%

ValorNeto_aFacturar = Valor Base - %Descuento (si aplica y sin exceder 10%)

Plataformas: Se aplicarán descuentos por las indisponibilidades de cada Plataforma

(Sistema Operativo, Base de Datos, Almacenamiento, Servidores de Aplicación,

Directorio activo, Servidores de Archivos, FTP, Firewall entre otros)

ANS DE "CONECTIVIDAD WAN "

META: Mayor o igual al 99.96% en los horarios establecidos **por UGPP**

CALCULO = 100% – %Indisponibilidad

%Indisponibilidad x Canal = (DownTime / TimePrometido) * 100 en cada Componente

%Descuento al ValorBase Facturable del Ítem de Servicio = Suma de

%Indisponibilidad**es** xComponente

Aplicación del Descuento: Cuando el ANS no logre la META

Descuento **Máximo** = 10%

ValorNeto_aFacturar = Valor Base - %Descuento (si aplica y sin exceder 10%)

Componente: Se aplicarán descuentos por las indisponibilidades de cada componente (Enlaces de Datos, Internet)

ANS DE "CONECTIVIDAD LAN - WLAN"

META: Mayor o igual al 99.96%

CALCULO = 100% – %Indisponibilidad

%Indisponibilidad xPlataforma = (CasosdeFalla / Cantidad del Componente) * 100 en cada Componente

%Descuento al ValorBase Facturable del Ítem de Servicio = Suma de

%Indisponibilidades xComponente

Aplicación del Descuento: Cuando el ANS no logre la META

Descuento **Máximo** = 10%

ValorNeto_aFacturar = Valor Base - %Descuento (si aplica y sin exceder 10%)

Componente: Se aplicarán descuentos por las indisponibilidades de cada Plataforma (Switches, Access Point, Puntos de Red)

ANS DE "ESCALAMIENTO OPORTUNO"

% de Incidentes y Solicitudes que cumplen con el adecuado escalamiento a otros niveles por parte de la mesa de servicio.

META: Mayor o igual al 95,00%

CALCULO = 100% – %InCumplidos

%InCumplidos = (NumerosCasosDevueltos / Total de Casos) * 100

%Descuento al ValorBase Facturable del Ítem de Servicio = %InCumplidos

Aplicación del Descuento: Cuando el ANS no logre la META

Descuento **Máximo** = 10%

ValorNeto_a Facturar = Valor Base - %Descuento (si aplica y sin exceder 10%)

ANS DE "SOLUCIÓN OPORTUNA"

% de Incidentes y Solicitudes a su cargo que cumplen tiempos definidos (1, 2 o 4 horas según prioridad) para resolver una vez escalados

META: Mayor o igual al 95,00%

CALCULO = 100% – %InCumplidos

%InCumplidos = (CasosNoCumplenTiempos / Total de Casos) * 100

%Descuento al ValorBase Facturable del Ítem de Servicio = %InCumplidos

Aplicación del Descuento: Cuando el ANS no logre la META

Descuento **Máximo** = 10%

ValorNeto_aFacturar = Valor Base - %Descuento (si aplica y sin exceder 10%)

ANS DE "CONTINGENCIA EXITOSA"

Cuando haya pruebas del DPR, el % de Componentes (Aplicaciones, Servicios y Mesa de

Ayuda) que logren los RTOs y RPO establecidos

META: Mayor o igual al 95,00%

CALCULO = 100% – %InCumplidos

%InCumplidos = (CasosNoCumplenRTO / Total de Casos) * 100

%Descuento al ValorBase Facturable del Ítem de Servicio = %InCumplidos

Aplicación del Descuento: Cuando el ANS no logre la META

Descuento **Máximo** = 10%

ValorNeto_aFacturar = Valor Base - %Descuento (si aplica y sin exceder 10%)

ANS DE "ACCESO Y DISPONIBILIDAD EN ESCRITORIOS VIRTUALES"

Meta = Mayor o igual al 99,95% en el Período

Cálculo = 100% – %Indisponibilidad

% Indisponibilidad = (IncidentesMayores / Usuarios Virtualizados) * 100

% Descuento al ValorBase Facturable del Ítem de Servicio = %Indisponibilidad

Aplicación del Descuento= Cuando el ANS no logre la META

Descuento Máximo = 10%

Valor Neto a Facturar = Valor Base - %Indisponibilidad (si aplica y sin exceder 10%)