

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

ANEXO TÉCNICO - ESPECIFICACIONES TECNICAS DEL OBJETO CONTRACTUAL:

Objeto: PRESTACIÓN DE SERVICIOS PARA LA OPERACIÓN, ADMINISTRACIÓN, MONITOREO, SEGURIDAD, CONTINUIDAD, SOPORTE Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA, DE TELECOMUNICACIONES, DE INFORMACIÓN Y DEL SOFTWARE BASE DEL DATA CENTER DE LA CORPORACIÓN AUTÓNOMA REGIONAL DEL ATLÁNTICO – C.R.A.

A. ITEMS A CONTRATAR

1. Presentar a la supervisión del contrato, dentro de los tres (3) días hábiles siguientes a la orden de inicio, para su revisión y aprobación, las hojas de vida y demás documentos soporte del equipo mínimo de profesionales requerido y ofertado, quienes deberán contar con residencia verificable en la ciudad de Barranquilla durante la ejecución contractual, de conformidad con los perfiles, requisitos y condiciones establecidos en el pliego de condiciones:

El proponente deberá garantizar que durante la ejecución del contrato y dos (2) meses más, esté disponible el equipo de trabajo calificado que garantice la correcta ejecución del objeto contractual exigido, esto es, Expertos certificados con disponibilidad inmediata en sitio que se encargaran de ejecutar los servicios complementarios de instalación, configuración, soporte especializado y garantía de los mismo, profesionales con los que debe contar la Empresa para este Proyecto (Habilitante)

Los proponentes deberán adjuntar con su propuesta las hojas de vida y los respectivos soportes que acrediten los requisitos de formación académica, certificaciones y experiencia mínimos requeridos, así como carta de aval mencionada más abajo, del **EQUIPO DE TRABAJO MÍNIMO HABILITANTE**, con residencia verificable en la ciudad de Barranquilla durante el termino de ejecución del objeto contractual, que está conformado por los siguientes perfiles:

ROL	FORMACIÓN	EXPERIENCIA
Profesional Especializado 1: Director o coordinador de Servicios.	Profesional en Ingeniería de Sistemas. Con especialización en redes de computadores y/o Telecomunicaciones, Electrónica o carreras afines.	Experiencia General: Mínimo de 15 años de experiencia general certificada. Experiencia Específica: Acreditar experiencia mínima de diez (10) años como director coordinador de Servicios o director de Proyectos, desempeñando funciones de dirección, coordinación y supervisión de servicios administrados de tecnologías de la información (TI), liderando la operación, soporte y continuidad de los servicios, así como el cumplimiento de los Acuerdos de Niveles de Servicio (SLA).
Profesional Especializado 2 en sitio 7x4 para soluciones	Profesional en Ingeniería de Sistemas.	Experiencia General: Mínimo de 15 años de experiencia general certificada.



**OFICINA ASESORA DE CIENCIA,
TECNOLOGÍA E INNOVACIÓN**

ANEXO TÉCNICO



ROL	FORMACIÓN	EXPERIENCIA
Dell y Soluciones Fortinet Coordinador de Servicios de administración y manejo de software base para data center y seguridad en redes de computadores.	Con especialización en redes de computadores y/o Telecomunicaciones. El profesional deberá contar con certificaciones técnicas vigentes en redes y seguridad, cumpliendo con las siguientes certificaciones en redes: • Cisco CCNA o Cisco CCNP • CompTIA Network+ • Dell EMC en networking, servidores, storage • O certificación equivalente	Experiencia Específica: Deberá acreditar al menos 10 años de experiencia específica, debidamente certificada, en administración, mantenimiento y soporte de infraestructura de red de alto desempeño, incluyendo, switches Core, routers, redes backbone y configuración avanzada de redes LAN en entornos de Datacenter. Adicionalmente, deberá demostrar experiencia en la administración, configuración y gestión de dispositivos de seguridad perimetral, especialmente firewalls de la marca Fortinet. • En participación de 2 contratos cuyo objeto sea instalación y/o configuración del producto Firewall - FortiGate. • En la participación de contratos 2 cuyo objeto sea instalación y/o configuración del producto HYPERSIVOR, VMWARE Y VCENTER
Profesional Especializado 3: DBA - en sitio 7x4 para soporte y soluciones en Bases de Datos. Coordinador de Servicios para servidores de Bases de Datos, PostgreSQL, MySQL y Oracle Database.	Profesional en Ingeniería de Sistemas.	Experiencia General: Mínimo de 15 años de experiencia general certificada. Experiencia Específica: Experto como mínimo de 10 años de experiencia en la instalación y/o configuración y/o afinamiento y/o migración de Bases de Datos Oracle, y/o administración, soporte y optimización de bases de datos Oracle en ambientes de producción. Experiencia Específica en la participación de 2 contratos cuyo objeto sea instalación y/o configuración y/o afinamiento y/o migración de Bases de Datos Oracle.
Profesional 4: Redes y WAF en sitio 7x4 Para soluciones y soporte en la administración y manejo de software base para para redes, seguridad de redes y WAF.	Profesional en Ingeniería de Sistemas, y/o Ingeniero Telemático y/o Telecomunicaciones, Electrónica o carreras afines.	Experiencia General: Mínimo de 5 años de experiencia general certificada. Experiencia Específica: Experto como mínimo de 2 años de experiencia como en administración, soporte y optimización de redes de computadores y/o configuración e implementación de Firewalls de Aplicaciones Web (WAF) De igual forma, como mínimo de 1 año de experiencia específica en la administración, configuración e implementación de Firewalls de Aplicaciones Web (WAF).
Profesional 5 -		Experiencia General:

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

ROL	FORMACIÓN	EXPERIENCIA
Kaspersky en sitio 7x4 para soluciones, Datacenter y Hardware: Coordinador de Servicios Mesa de Ayuda. Experto de Soluciones Kaspersky, Copias de Seguridad y Respaldo. Especialista en Infraestructura Tecnológica e Integraciones y mantenimiento de Data Center.	Profesional en Ingeniería de Sistemas y/o Telecomunicaciones, Electrónica o carreras afines. Certificado en: • Contar con certificación técnica vigente emitida por el fabricante sobre el producto Antivirus Kaspersky. • Contar con certificación técnica vigente emitida por el fabricante sobre el producto Acronis.	Mínimo de 10 años de experiencia general certificada. Experiencia Específica: Experto como mínimo de 5 años de experiencia en administración de consolas y soporte de soluciones basadas en Kaspersky Antivirus y plataformas de copias de seguridad Cloud.
Profesional 6: Profesional en Sistemas – Telefonía IP / PBX	Profesional en Ingeniería de Sistemas y/o Telecomunicaciones, Electrónica o carreras afines y/o tecnólogo en sistemas y a afines. Con experiencia específica en el diseño, implementación, migración y soporte de plataformas de telefonía IP/PBX de código abierto, incluyendo configuración de troncales SIP, IVR, colas, grupos de timbrado, grabación, reportes operativos y medidas básicas de seguridad de voz. Deberá acreditar formación o certificación específica en tecnologías de VoIP o PBX IP, y experiencia en integración con redes de datos y con operadores de telefonía, acorde con el componente de soporte de plataforma de telefonía IP definido en el Anexo Técnico.	Experiencia General: Mínimo de 3 años de experiencia general certificada. Experiencia Específica: Experto como mínimo de 2 años de experiencia como en administración, soporte y optimización de bases de datos Oracle en ambientes de producción
Profesional 7 Auxiliar en Redes y Gestión de Sistemas Informáticos.	Profesional en ingeniería Telemática o Técnico y/o Tecnólogo en Gestión de Sistemas Informáticos y/o ingeniería Telemática.	Experiencia Específica: Deberá acreditar al menos un (1) año de experiencia específica, debidamente certificada, en administración, mantenimiento y soporte de infraestructura de red de alto desempeño, incluyendo, switches Core, routers, redes backbone y configuración avanzada de redes LAN en entornos de Datacenter. Adicionalmente contar con certificación en Ethical Hacking, expedida por una entidad certificadora de reconocimiento nacional o internacional, que acredite competencias en la identificación, evaluación y explotación

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

ROL	FORMACIÓN	EXPERIENCIA
		controlada de vulnerabilidades de seguridad informática.
Profesional 8 Técnico y/o Tecnólogo: Auxiliar DBA de Soporte del administración y manejo de software base, información y telemática.	Profesional o Técnico y/o Tecnólogo en sistemas o afines.	Experiencia Específica: Como mínimo de 3 años de experiencia en la instalación y/o configuración y/o afinamiento y/o migración de Bases de Datos Oracle, y/o administración, soporte y optimización de bases de datos Oracle en ambientes de producción.

El equipo de trabajo deberá garantizar la atención de incidentes de ciberseguridad bajo un esquema de disponibilidad **7x24**, tanto de manera remota como presencial en sitio, de acuerdo con la naturaleza, criticidad y complejidad de cada incidente. Asimismo, cuando se requiera atención presencial, esta deberá prestarse dentro de los tiempos de respuesta establecidos en el Anexo Técnico.

Para tal efecto, el proponente deberá demostrar que cuenta con la capacidad operativa para prestar atención presencial en la ciudad de Barranquilla o su área metropolitana, mediante un equipo de profesionales con disponibilidad local que permita cumplir los niveles de servicio y los tiempos de atención exigidos durante la ejecución del contrato.

El proponente deberá acreditar con su propuesta el equipo mínimo de trabajo para habilitarse, incluyendo las respectivas hojas de vida, las certificaciones laborales y formación académica (diplomas y/o actas de grado y matrícula profesional) por cada profesional.

NOTA: En caso de que el oferente sea persona jurídica, deberá acreditar la vinculación del personal que reúna la experiencia general y específica descrita en el ítem anterior.

Para la acreditación de la experiencia no se tendrá en cuenta la experiencia traslapada (experiencias realizadas en el mismo periodo de tiempo) del personal descrito en el presente numeral.

Los profesionales del equipo mínimo habilitante propuesto deberán avalar mediante la suscripción de una carta de compromiso personal debidamente firmada que se comprometan a trabajar en la ejecución del contrato en caso de salir favorecidos con la adjudicación del contrato y certificar y manifestar expresamente que su hoja de vida es presentada única y exclusivamente por el proponente que lo presenta, además, que no ha participado en la preparación o elaboración del presente proceso de selección.

- Documentos requeridos para el equipo de trabajo mínimo habilitante

Para acreditar el perfil y la experiencia de los profesionales ofertados se deberá presentar la siguiente documentación:

- Copia del documento de identificación.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

- Copia de la tarjeta o matricula profesional.
- Certificado de vigencia de la matricula profesional expedido por la autoridad competente.
- Copia del título de pregrado o acta de grado.
- Certificaciones de experiencia que contengan la siguiente información: - Nombre de la empresa Contratante (Dirección y Teléfono). - Nombre del profesional y documento de identificación. - Número del contrato (si tiene). - Objeto del contrato - Cargo si aplica. - Actividades del contrato. - Fecha de iniciación indicando día, mes y año - Fecha de terminación indicando día, mes y año - Nombre y firma del funcionario o persona que expide la certificación.

- Consideraciones frente a la experiencia:

- 1) Las experiencias reportadas podrán estar vigentes, caso en el cual se contabilizarán hasta la fecha de expedición de la certificación.
- 2) Cuando las certificaciones de experiencia aportadas no contengan la información suficiente que acredite el requisito requerido en los términos de referencia, el proponente deberá anexar a la propuesta copia del contrato, copia del acta de cierre, copia del acta de liquidación, o los documentos soporte que sean del caso. No obstante, estos documentos no servirán para subsanar la omisión de aportar la certificación de experiencia, toda vez que sólo tienen un valor complementario a ella.

El personal que designe el contratista no tendrá ningún vínculo laboral con la entidad contratante, por tal razón el contratista se encargará de todas las prestaciones laborales que conlleve este proceso.

Una vez la entidad contratante apruebe el personal mínimo propuesto, que ocurrirá cuando se suscriba el contrato con el proponente que resulte adjudicatario y se firme el acta de inicio, éste sólo podrá ser cambiado durante la ejecución del proyecto con la aprobación del supervisor del contrato, de conformidad con lo establecido en la Obligación específica, por un funcionario de igual o superior perfil.

La entidad contratante no dispondrá de personal adicional, ni suministrará personal que colabore con actividades de tipo operativo, todas esas actividades deben ser previstas y asumidas por el proveedor.

El proponente deberá proponer un único profesional por cada perfil y allegar los respectivos documentos.

2. Prestar servicios para la implementación, administración, operación, configuración, monitoreo, mantenimiento y soporte de la solución tecnológica FortiAnalyzer Cloud, incluyendo las funcionalidades de inteligencia artificial (IA) y Attack Surface Rating, garantizando la disponibilidad y operación del servicio para el análisis de hasta diez (10) GB diarios de información y una retención de datos durante la vigencia contractual y/o hasta el 31 de diciembre de 2026:

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Alcance Técnico:

El contratista deberá prestar el servicio integral para la implementación, configuración, administración, operación, monitoreo, mantenimiento y soporte especializado de la plataforma FortiAnalyzer Cloud, como servicio SaaS con su respectivo licenciamiento, por parte del contratista, del FortiAnalyzer Cloud para integrarse al Firewall Fortigate FG 100F de la C.R.A., garantizando su correcta integración con la infraestructura de seguridad Fortinet de la Entidad y la disponibilidad del servicio durante toda la ejecución del contrato.

El servicio comprende la configuración inicial de la plataforma, la integración con los dispositivos Fortinet definidos por la Entidad, la administración de la recepción y procesamiento de registros (logs), la configuración y optimización de eventos, alertas, reportes, paneles de monitoreo (Dashboards), perfiles de acceso y políticas de retención de información.

Asimismo, comprende la administración y operación de las funcionalidades de Inteligencia Artificial (IA) y Attack Surface Rating (ASR) disponibles en la solución, con el fin de fortalecer la detección de amenazas, el análisis del comportamiento de la infraestructura tecnológica y la identificación de riesgos de exposición de los activos administrados.

Durante toda la vigencia contractual el contratista deberá garantizar la operación continua de la plataforma para el procesamiento de hasta diez (10) GB diarios de registros (logs), así como la conservación de la información durante la vigencia del contrato y/o hasta el 31 de diciembre de 2026, de conformidad con las capacidades licenciadas por la Entidad.

El servicio incluye la administración permanente de la plataforma, el monitoreo de su estado operativo, la atención de incidentes relacionados con FortiAnalyzer Cloud, la ejecución de ajustes de configuración autorizados por la supervisión del contrato, la aplicación de buenas prácticas de administración recomendadas por el fabricante y la verificación periódica de la correcta recepción de registros provenientes de los dispositivos Fortinet administrados.

Actividades mínimas:

Administración FortiAnalyzer Cloud:

- Implementar y configurar la plataforma FortiAnalyzer Cloud
- Integración del Firewall con FortiAnalyzer Cloud.
- Integrar los dispositivos Fortinet definidos por la C.R.A.
- Configurar la recepción, almacenamiento y administración de registros (logs).
- Configurar políticas de retención de información.
- Configurar eventos, alertas, paneles de monitoreo e informes automáticos.
- Administrar usuarios, perfiles y permisos de acceso.
- Administrar las funcionalidades de Inteligencia Artificial (IA) y Attack Surface Rating (ASR).
- Monitorear permanentemente el estado de la plataforma y la recepción de registros.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

- Ejecutar ajustes, optimizaciones y afinamiento de configuraciones cuando sean requeridos.
- Atender incidentes y requerimientos relacionados con la operación de FortiAnalyzer Cloud.
- Realizar respaldos de la configuración antes de modificaciones relevantes y conservar las versiones vigentes.
- Mantener actualizada la documentación técnica de la solución durante la ejecución del contrato.

Inteligencia Artificial:

Configuración y operación de las funcionalidades de Inteligencia Artificial disponibles en FortiAnalyzer Cloud, incluyendo:

- Detección automática de anomalías.
- Identificación de comportamientos atípicos.
- Priorización inteligente de eventos.
- Recomendaciones automáticas de mitigación.
- Análisis asistido por IA.

Attack Surface Rating:

Configuración y operación del módulo ASR incluyendo:

- Evaluación de exposición.
- Identificación de activos expuestos.
- Análisis de riesgo.
- Identificación de vulnerabilidades visibles.
- Recomendaciones de fortalecimiento.

Entregables:

El contratista deberá entregar como mínimo:

• Entregable	• Periodicidad
• Documento de implementación y configuración inicial de FortiAnalyzer Cloud, incluyendo arquitectura, dispositivos integrados, configuración aplicada y validación de funcionamiento.	• Una (1) vez, dentro de los diez (10) días siguientes al inicio del contrato.
• Informe mensual de administración y operación de la plataforma, incluyendo disponibilidad del servicio, volumen de registros procesados, eventos relevantes, incidentes atendidos, configuraciones realizadas y estado de las funcionalidades de IA y Attack Surface Rating.	• Mensual.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

• Entregable	• Periodicidad
• Reporte de alertas y eventos críticos generados por la plataforma, con el análisis correspondiente y las recomendaciones de mejora cuando aplique.	• Mensual.
• Evidencias de las configuraciones implementadas y de los cambios autorizados durante la ejecución del contrato.	• Cada vez que se realicen cambios.
• Respaldo actualizado de la configuración de la plataforma FortiAnalyzer Cloud.	• Mensual y previo a cambios mayores.
• Informe final de operación, que incluya el estado de la plataforma, configuración vigente, dispositivos integrados, estadísticas de operación, incidentes relevantes, recomendaciones técnicas y transferencia de conocimiento.	• Al finalizar el contrato.

Criterios de aceptación:

- La obligación se entenderá cumplida cuando:
 - La plataforma FortiAnalyzer Cloud permanezca operativa durante la ejecución del contrato.
 - Se garantice el procesamiento de hasta diez (10) GB diarios de registros conforme a la capacidad licenciada.
 - Los dispositivos Fortinet definidos por la C.R.A. se encuentren integrados y reportando información correctamente.
 - Las funcionalidades de Inteligencia Artificial (IA) y Attack Surface Rating se encuentren habilitadas y operativas, cuando hagan parte del licenciamiento contratado.
 - Se entreguen oportunamente los informes y evidencias definidos en el presente anexo.
 - Los cambios realizados cuenten con la aprobación del supervisor cuando corresponda.
 - La documentación técnica permanezca actualizada durante toda la ejecución contractual.
3. Realizar un (1) mantenimiento Preventivo de Datacenter el cual consistirá en Limpieza técnica especializada de equipos y servidores, de acuerdo con el inventario definido en el Anexo Técnico; organización física de racks; mantenimiento del cableado estructurado; revisión de la infraestructura eléctrica; revisión del sistema de climatización; optimización del flujo térmico; revisión de la seguridad física; mantenimiento general preventivo de una UPS de 10 KVA marca Powercom; suministro de baterías selladas libres de mantenimiento de 12 V – 7.5 Ah para la UPS; e instalación de 40 baterías en la UPS.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Mantenimiento de Datacenter:

a. Mantenimiento preventivo de Datacenter

Nombre del servicio	Mantenimiento preventivo y soporte especializado de la infraestructura física y tecnológica del Datacenter de la CRA.
Alcance del Servicio	Prestación del servicio de mantenimiento preventivo programado sobre la infraestructura física y tecnológica del Datacenter de la CRA, incluyendo como mínimo servidores, soluciones de almacenamiento, racks, cableado asociado, UPS, tableros eléctricos asociados, climatización de sala y demás componentes definidos en el Inventario Técnico Oficial o en el inventario que la CRA entregue para la ejecución del contrato. El servicio tendrá como finalidad preservar las condiciones de operación, seguridad, orden, limpieza, continuidad y funcionamiento general de la infraestructura intervenida mediante actividades programadas de inspección, limpieza técnica, revisión de estado, pruebas de funcionamiento, ajuste, verificación operativa, documentación y entrega de evidencias. El mantenimiento preventivo se ejecutará a todo costo únicamente respecto de las actividades incluidas en el alcance y de los suministros o elementos expresamente incorporados dentro de la oferta económica como parte del componente, incluyendo los casos específicos previamente identificados por la entidad, como las baterías de la UPS y su instalación. No forman parte del alcance económico del servicio los repuestos, partes averiadas, consumibles, herramientas adicionales, accesorios o suministros no incorporados expresamente en la oferta para el mantenimiento preventivo. Toda intervención deberá coordinarse con la CRA para evitar afectación a los servicios críticos, por lo cual las ventanas de mantenimiento, pruebas e intervenciones que impliquen riesgo operativo deberán ser previamente autorizadas por la supervisión del contrato.
Unidad de facturación del producto / servicio	Servicio Global
Cantidad	1

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

EQUIPOS:

MARCA	MODELO	CANTIDAD MMTOS	ACTIVIDADES
FORTIGATE – SEDE 1:	FIREWALL FG 100F	1	Limpieza del polvo y la suciedad del interior, actualizaciones de firmware y controladores, verificación de componentes internos, como ventiladores, discos duros y tarjetas de expansión para identificar signos de desgaste o daño, ejecución de pruebas de diagnóstico para verificar la salud del hardware con reportes entregables, reemplazo de baterías, y uso herramientas de monitoreo para supervisar el rendimiento, la temperatura y las alertas con reportes de estado.
DELL	SERVIDOR EMC R520	1	Limpieza del polvo y la suciedad del interior, actualizaciones de firmware y controladores, verificación de componentes internos, como ventiladores, discos duros y tarjetas de expansión para identificar signos de desgaste o daño, ejecución de pruebas de diagnóstico para verificar la salud del hardware con reportes entregables, reemplazo de baterías, y uso herramientas de monitoreo para supervisar el rendimiento, la temperatura y las alertas con reportes de estado.
DELL	SERVIDOR EMC R740	1	Limpieza del polvo y la suciedad del interior, actualizaciones de firmware y controladores, verificación de componentes internos, como ventiladores, discos duros y tarjetas de expansión para identificar signos de desgaste o daño, ejecución de pruebas de diagnóstico para verificar la salud del hardware con reportes entregables, reemplazo de baterías, y uso herramientas de monitoreo para supervisar el rendimiento, la temperatura y las alertas con reportes de estado.
DELL	SERVIDOR EMC R520	1	Limpieza del polvo y la suciedad del interior, actualizaciones de firmware y controladores, verificación de

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

MARCA	MODELO	CANTIDAD MMTOS	ACTIVIDADES
			componentes internos, como ventiladores, discos duros y tarjetas de expansión para identificar signos de desgaste o daño, ejecución de pruebas de diagnóstico para verificar la salud del hardware con reportes entregables, reemplazo de baterías, y uso herramientas de monitoreo para supervisar el rendimiento, la temperatura y las alertas con reportes de estado.
DELL	STORAGE COMPELLENT EMC 3020	1	Limpieza del polvo y la suciedad del interior, actualizaciones de firmware y controladores, verificación de componentes internos, como ventiladores, discos duros y tarjetas de expansión para identificar signos de desgaste o daño, ejecución de pruebas de diagnóstico para verificar la salud del hardware con reportes entregables, reemplazo de baterías, y uso herramientas de monitoreo para supervisar el rendimiento, la temperatura y las alertas con reportes de estado. Revisión y reconfiguración de discos duros.
DELL	STORAGE POWER VAULT MD3600i	1	Limpieza del polvo y la suciedad del interior, actualizaciones de firmware y controladores, verificación de componentes internos, como ventiladores, discos duros y tarjetas de expansión para identificar signos de desgaste o daño, ejecución de pruebas de diagnóstico para verificar la salud del hardware con reportes entregables, reemplazo de baterías, y uso herramientas de monitoreo para supervisar el rendimiento, la temperatura y las alertas con reportes de estado. Revisión y reconfiguración de discos duros.
DELL	SWITCH EMC N1124T-ON	1	Limpieza del polvo y la suciedad del interior, actualizaciones de firmware y controladores, verificación de componentes internos para identificar

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

MARCA	MODELO	CANTIDAD MMTOS	ACTIVIDADES
			signos de desgaste o daño, ejecución de pruebas de diagnóstico para verificar la salud del hardware con reportes entregables, y uso herramientas de monitoreo para supervisar el rendimiento, la temperatura y las alertas con reportes de estado.
DELL	SWITCH EMC N1148T-ON	1	Limpieza del polvo y la suciedad del interior, actualizaciones de firmware y controladores, verificación de componentes internos para identificar signos de desgaste o daño, ejecución de pruebas de diagnóstico para verificar la salud del hardware con reportes entregables, y uso herramientas de monitoreo para supervisar el rendimiento, la temperatura y las alertas con reportes de estado.
DELL	SWITCH EMC S4128F	1	Limpieza del polvo y la suciedad del interior, actualizaciones de firmware y controladores, verificación de componentes internos para identificar signos de desgaste o daño, ejecución de pruebas de diagnóstico para verificar la salud del hardware con reportes entregables, y uso herramientas de monitoreo para supervisar el rendimiento, la temperatura y las alertas con reportes de estado.
DELL	SWITCH EMC S4112F	1	Limpieza del polvo y la suciedad del interior, actualizaciones de firmware y controladores, verificación de componentes internos para identificar signos de desgaste o daño, ejecución de pruebas de diagnóstico para verificar la salud del hardware con reportes entregables, y uso herramientas de monitoreo para supervisar el rendimiento, la temperatura y las alertas con reportes de estado.
DELL	SWITCH EMC S4112F	1	Limpieza del polvo y la suciedad del interior, actualizaciones de firmware y controladores, verificación de componentes internos para identificar

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

MARCA	MODELO	CANTIDAD MMTOS	ACTIVIDADES
			signos de desgaste o daño, ejecución de pruebas de diagnóstico para verificar la salud del hardware con reportes entregables, y uso herramientas de monitoreo para supervisar el rendimiento, la temperatura y las alertas con reportes de estado.
DELL	SWITCH EMC N2048P	1	Limpieza del polvo y la suciedad del interior, actualizaciones de firmware y controladores, verificación de componentes internos para identificar signos de desgaste o daño, ejecución de pruebas de diagnóstico para verificar la salud del hardware con reportes entregables, y uso herramientas de monitoreo para supervisar el rendimiento, la temperatura y las alertas con reportes de estado.
HP	SWITCH V1910	1	Limpieza del polvo y la suciedad del interior, actualizaciones de firmware y controladores, verificación de componentes internos para identificar signos de desgaste o daño, ejecución de pruebas de diagnóstico para verificar la salud del hardware con reportes entregables, y uso herramientas de monitoreo para supervisar el rendimiento, la temperatura y las alertas con reportes de estado.
HP	SWITCH V1910	1	Limpieza del polvo y la suciedad del interior, actualizaciones de firmware y controladores, verificación de componentes internos para identificar signos de desgaste o daño, ejecución de pruebas de diagnóstico para verificar la salud del hardware con reportes entregables, y uso herramientas de monitoreo para supervisar el rendimiento, la temperatura y las alertas con reportes de estado.
HP	SWITCH V1910	1	Limpieza del polvo y la suciedad del interior, actualizaciones de firmware y controladores, verificación de componentes internos para identificar

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

MARCA	MODELO	CANTIDAD MMTOS	ACTIVIDADES
			signos de desgaste o daño, ejecución de pruebas de diagnóstico para verificar la salud del hardware con reportes entregables, y uso herramientas de monitoreo para supervisar el rendimiento, la temperatura y las alertas con reportes de estado.
3COM	SWITCH V2928 DE 24 PUERTOS	1	Limpieza del polvo y la suciedad del interior, actualizaciones de firmware y controladores, verificación de componentes internos para identificar signos de desgaste o daño, ejecución de pruebas de diagnóstico para verificar la salud del hardware con reportes entregables, y uso herramientas de monitoreo para supervisar el rendimiento, la temperatura y las alertas con reportes de estado.
POWERCOM	UPS ON LINE DE 10KVA POWERCOM- BIFASICA	1	Revisión general del estado del equipo, limpieza general, ajuste mecánico de componentes y partes, ajuste de los terminales de conexión eléctrica, revisión del proceso de control : Tarjeta drivers, tarjeta de cargador, tarjeta de Inversor, tarjeta de control y sensores; revisión y verificación de los procesos de medición y señalización: Tarjeta de medición y señalización, Pantalla LCD, Indicadores luminosos; revisión y comprobación de potencia: Transformadores y amortiguadores, Módulos HEAD SLINK con dispositivos electrónicos, relés, filtros y condensadores, ventiladores y refrigeradores; revisión de los bancos de baterías: Terminales de conexión, voltaje, corriente, pruebas de descarga controlada; inicio de la comprobación del equipo y ajuste de los parámetros de funcionamiento: Voltaje de la fuente de alimentación, voltaje de entrada y salida, corriente de entrada y salida, pruebas en vacío, pruebas con carga, pruebas para verificar bancos de baterías, revisión, limpieza y prueba de transformadores de

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

MARCA	MODELO	CANTIDAD MMTOS	ACTIVIDADES
			aislamiento, limpieza general del entorno de la UPS, sustitución de componentes de acuerdo a las recomendaciones técnicas del fabricante, calibración del dispositivo de monitoreo, pruebas del UPS con el tablero de transferencia automática, revisión, limpieza y prueba de los transformadores de aislamiento, prueba del funcionamiento de la UPS con carga, con entrada automática de batería. INCLUYE EL CAMBIO DE BATERÍAS.
MANTENIMIENTO CORRECTIVO			
Mantenimiento correctivo:		Servicio Global Integral	Atención técnica especializada bajo demanda para diagnóstico de fallas, revisión funcional, aislamiento de causa, ajuste, calibración, reconfiguración menor, corrección operativa, reinstalación menor cuando aplique, pruebas de funcionamiento, estabilización del servicio y verificación de restablecimiento sobre los componentes de la infraestructura física y tecnológica del Datacenter cubiertos por el alcance del servicio. INCLUYE EL SUMINISTRO DE 40 PARA UPS SELLADAS LIBRES DE MANTENIMIENTO DE 12V-7.5A/H. NO INCLUYE EN NINGÚN CASO SUMINISTRO O CAMBIO DE REPUESTOS, PARTES, CONSUMIBLES, ACCESORIOS O MATERIALES.

DESCRIPCIÓN DEL REQUERIMIENTO:

Característica Requerida	Descripción del requerimiento
Características técnicas	El proveedor deberá ejecutar por una sola vez las actividades programadas de mantenimiento preventivo sobre los componentes definidos por la CRA, incluyendo inspección visual y funcional, limpieza técnica especializada, verificación de estado, revisión de

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Característica Requerida	Descripción del requerimiento
	conexiones, ajuste básico, pruebas operativas y validación general de condiciones de funcionamiento. • El proveedor deberá realizar actividades de organización física de racks, revisión del cableado asociado, validación de etiquetado cuando aplique, identificación de condiciones de desorden o riesgo y recomendaciones para mejorar la gestión física de la infraestructura. • El proveedor deberá efectuar revisión de la infraestructura eléctrica asociada al Datacenter dentro del alcance definido, incluyendo verificación general de tableros relacionados, puntos de alimentación visibles, condiciones de conexión y estado funcional de los elementos intervenidos, sin que ello implique rediseño eléctrico ni ejecución de obras civiles o eléctricas mayores. • El proveedor deberá revisar el funcionamiento general de la climatización de sala y las condiciones térmicas observables del entorno intervenido, así como emitir recomendaciones de mejora cuando identifique condiciones que puedan afectar la operación de los equipos. • El proveedor deberá ejecutar mantenimiento preventivo de la UPS incluida en el alcance, así como el suministro e instalación de las baterías expresamente previstas en la oferta económica, con sus respectivas pruebas y puesta en servicio. • El proveedor deberá documentar la intervención preventiva mediante informe técnico, registro de actividades ejecutadas, hallazgos, recomendaciones, evidencias técnicas y, cuando aplique, evidencias fotográficas o actas de trabajo suscritas con la CRA, y diligenciar los formatos definidos por ésta. • Cuando en desarrollo del mantenimiento preventivo se identifiquen fallas, desgaste, daño, obsolescencia o necesidad de sustitución de partes no incluidas expresamente en la oferta, el proveedor deberá emitir diagnóstico y recomendación técnica, sin que su suministro quede comprendido dentro del valor del servicio. • El mantenimiento correctivo que sea requerido por la CRA deberá ejecutarse cuando aplique, con la trazabilidad del servicio, descripción de la actividad realizada y evidencia técnica de cierre.
Servicio/soporte	• El mantenimiento preventivo deberá ejecutarse conforme a un cronograma acordado con la CRA durante el inicio del contrato, definiendo componentes a intervenir, ventanas autorizadas, responsables, evidencias esperadas y criterios de aceptación de cada actividad programada. • Toda solicitud correctiva deberá quedar soportada en ticket, acta, correo de autorización o mecanismo formal definido por la CRA,

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Característica Requerida	Descripción del requerimiento
	indicando activo afectado, situación reportada, diagnóstico, actividad ejecutada, tiempo consumido, resultado y estado final del caso. - La atención correctiva se prestará de forma remota o en sitio, según la naturaleza técnica del caso, y deberá sujetarse a la tabla unificada de ANS del Anexo Técnico o al mecanismo de prioridades que defina la CRA para la ejecución del contrato. - El proveedor deberá entregar informe consolidado con el avance del cronograma preventivo, actividades ejecutadas hallazgos, riesgos identificados, recomendaciones técnicas, pendientes y evidencias de intervención.
Sitio de las pruebas	Local en las instalaciones de la CRA.

4. Prestar de servicios especializados para la integración del nuevo host de las estaciones de monitoreo de la CRA a la infraestructura del centro de datos, incluyendo la configuración de controles de acceso, seguridad de la información, servicios tecnológicos y mecanismos de respaldo para su correcta operación y protección.

ANEXO TÉCNICO:

Obligación No. 3

Integración del Host de las Estaciones de Monitoreo a la Infraestructura del Data Center

Alcance Técnico:

El contratista deberá prestar los servicios especializados para la integración del nuevo host destinado al almacenamiento y procesamiento de la información proveniente de las estaciones de monitoreo de la C.R.A. a la infraestructura tecnológica del Data Center institucional, garantizando su incorporación segura, estable y operativa dentro de la arquitectura tecnológica de la Entidad.

El servicio comprende todas las actividades técnicas necesarias para la puesta en operación del host dentro del entorno institucional, incluyendo la configuración de conectividad, direccionamiento IP, integración a la infraestructura de red, incorporación al dominio institucional cuando aplique, sincronización de servicios de infraestructura, configuración de almacenamiento, habilitación de servicios tecnológicos requeridos y validación de la interoperabilidad con la infraestructura existente.

Asimismo, el contratista deberá implementar los controles de acceso y las configuraciones de seguridad de la información requeridas para proteger el servidor y la información almacenada, aplicando las políticas institucionales de autenticación, autorización, administración de privilegios, endurecimiento (hardening) del sistema operativo,

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

sincronización de tiempo, registros de auditoría y demás controles de seguridad definidos por la C.R.A.

Integración del agente y cliente respectivo del antivirus Kaspersky de la entidad para el servidor.

Como parte de la integración, el contratista deberá configurar los mecanismos de respaldo de la información, incorporando el servidor a la plataforma institucional de copias de seguridad, definiendo las políticas de respaldo, retención y recuperación aprobadas por la Entidad y verificando mediante pruebas que la información pueda recuperarse satisfactoriamente.

Igualmente, deberá realizar las pruebas técnicas de conectividad, disponibilidad, rendimiento y funcionamiento de los servicios implementados, verificando la correcta comunicación entre el host y los demás componentes de la infraestructura tecnológica del Data Center antes de su puesta en operación.

El servicio comprende el acompañamiento técnico durante la estabilización de la plataforma y la atención de los ajustes que resulten necesarios para garantizar la correcta integración del host dentro de la infraestructura institucional.

No hace parte del alcance el suministro del servidor, licencias de software, sistemas operativos, plataformas de monitoreo ambiental, desarrollo de aplicaciones o administración funcional de las estaciones de monitoreo.

Actividades mínimas:

El contratista deberá ejecutar como mínimo las siguientes actividades:

- Verificación de los requisitos técnicos del servidor objeto de integración.
- Integración del host a la infraestructura del Data Center.
- Configuración de red, direccionamiento IP, VLAN y servicios de conectividad.
- Incorporación al dominio institucional, cuando aplique.
- Configuración de servicios tecnológicos requeridos para su operación.
- Implementación de controles de acceso y perfiles de seguridad.
- Aplicación de medidas de hardening del sistema operativo conforme a las políticas de la Entidad.
- Configuración de registros de auditoría y sincronización de tiempo.
- Integración del servidor a la plataforma institucional de respaldo.
- Configuración de políticas de respaldo y recuperación.
- Ejecución de pruebas de respaldo y restauración.
- Verificación de conectividad, disponibilidad y funcionamiento.
- Corrección de inconsistencias identificadas durante la implementación.
- Documentación de la configuración realizada.
- Acompañamiento durante la estabilización del servicio.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Entregable	Oportunidad
Documento de diseño e integración del host a la infraestructura del Data Center, incluyendo arquitectura lógica, direccionamiento IP, servicios habilitados y controles de seguridad implementados.	Una (1) vez.
Evidencias de la configuración de red, controles de acceso, seguridad de la información y servicios tecnológicos implementados.	Una (1) vez.
Evidencia de incorporación del servidor a la plataforma institucional de copias de seguridad, incluyendo configuración de políticas de respaldo y resultados de las pruebas de restauración.	Una (1) vez.
Acta de pruebas funcionales y de aceptación de la integración del host, con los resultados de las validaciones de conectividad, disponibilidad y funcionamiento.	Una (1) vez.
Documento de configuración final y memoria técnica de la implementación, incluyendo recomendaciones para su operación y administración.	Al finalizar la implementación.

5. Prestar el servicio como SaaS para la implementación y operación del Firewall para Aplicaciones Web (WAF) del portal web institucional, incluyendo su configuración, administración, afinamiento, monitoreo permanente y gestión de incidentes, así como la implementación de controles de seguridad para la protección de aplicaciones web, el fortalecimiento del servidor, la configuración segura de SSL/TLS y los mecanismos de protección frente a ataques DDoS y bots, garantizando la disponibilidad, integridad y seguridad del portal institucional.

ANEXO TÉCNICO:

Obligación No. 4

Implementación y Operación del Firewall para Aplicaciones Web (WAF) bajo la modalidad SaaS

Alcance Técnico:

El contratista deberá prestar el servicio bajo la modalidad Software como Servicio (SaaS) para la implementación, configuración, administración, operación, monitoreo y soporte de un Firewall para Aplicaciones Web (Web Application Firewall – WAF) destinado a la protección del portal web institucional de la C.R.A., garantizando la disponibilidad, integridad, confidencialidad y continuidad del servicio.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

El servicio comprende la implementación inicial de la solución WAF, su integración con el portal web institucional y la infraestructura tecnológica asociada, así como la configuración y optimización permanente de las políticas de seguridad necesarias para la protección de las aplicaciones web frente a amenazas de capa de aplicación (OWASP Top 10 y amenazas equivalentes), accesos no autorizados, ataques automatizados, explotación de vulnerabilidades conocidas y demás riesgos que puedan comprometer la disponibilidad o seguridad del portal.

El contratista deberá realizar el diagnóstico inicial de seguridad del portal web para establecer la línea base de configuración de la solución, implementar y ajustar las políticas de inspección, protección y filtrado del tráfico HTTP/HTTPS, configurar certificados y protocolos seguros SSL/TLS conforme a las buenas prácticas vigentes, fortalecer (hardening) la configuración del servidor web cuando sea procedente y compatible con la arquitectura definida por la Entidad, y aplicar las configuraciones necesarias para reducir la superficie de exposición del servicio.

Asimismo, el servicio comprende la habilitación y administración de mecanismos de protección frente a ataques de denegación de servicio distribuido (DDoS), ataques automatizados (Bot Management), intentos de explotación de vulnerabilidades, inyecciones de código, ataques de fuerza bruta, manipulación de sesiones, ataques de tipo Cross-Site Scripting (XSS), SQL Injection y demás amenazas propias de aplicaciones web

Durante toda la vigencia contractual el contratista deberá efectuar el monitoreo permanente del servicio, el análisis de eventos y alertas de seguridad, la atención inicial de incidentes relacionados con el WAF, el ajuste y afinamiento continuo de las reglas de protección para minimizar falsos positivos y falsos negativos, garantizando el adecuado funcionamiento del portal institucional sin afectar la disponibilidad del servicio.

El contratista deberá mantener actualizada la configuración de la solución, aplicar las mejores prácticas de seguridad recomendadas por el fabricante, conservar respaldos de la configuración y documentar las modificaciones relevantes efectuadas durante la ejecución del contrato.

No hacen parte del alcance el desarrollo o modificación del código fuente del portal web, la corrección de vulnerabilidades propias de la aplicación, el suministro de infraestructura adicional, el desarrollo de software o la prestación de servicios de pruebas de penetración (Pentesting), Ethical Hacking o análisis de vulnerabilidades diferentes a los expresamente contemplados en el contrato.

Actividades mínimas:

El contratista deberá ejecutar, como mínimo, las siguientes actividades:

- Implementar y poner en operación la solución WAF bajo modalidad SaaS.
- Integrar la solución con el portal web institucional.
- Realizar el diagnóstico inicial de seguridad de la aplicación web.
- Configurar y optimizar las políticas de protección para aplicaciones web.
- Configurar reglas de inspección y filtrado del tráfico HTTP y HTTPS.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

- Configurar y administrar certificados y protocolos SSL/TLS conforme a las buenas prácticas de seguridad.
- Implementar controles de protección contra ataques de denegación de servicio distribuido (DDoS).
- Implementar mecanismos de gestión y mitigación de tráfico automatizado (Bot Management).
- Fortalecer (hardening) la configuración del servidor web cuando corresponda al alcance del servicio.
- Monitorear permanentemente el estado operativo del WAF y los eventos de seguridad generados.
- Ajustar y afinar las reglas de seguridad para optimizar la detección y reducir falsos positivos.
- Atender y gestionar los incidentes relacionados con la operación del WAF.
- Realizar respaldos de la configuración antes de cambios relevantes.
- Documentar las configuraciones implementadas y los cambios efectuados durante la ejecución del contrato.

Entregable	Oportunidad
Documento de implementación de la solución WAF, incluyendo arquitectura, configuración inicial, políticas de seguridad implementadas y validación de funcionamiento.	Dentro de los primeros quince (15) días calendario contados a partir del acta de inicio.
Informe de diagnóstico inicial de seguridad del portal web, con identificación de riesgos, configuraciones aplicadas y recomendaciones técnicas.	Una (1) vez, al finalizar la implementación inicial.
Informe mensual de operación del servicio, incluyendo disponibilidad del WAF, eventos relevantes, incidentes atendidos, ajustes realizados, estadísticas de tráfico, ataques mitigados, estado de SSL/TLS, protección DDoS y Bot Management, así como recomendaciones de mejora.	Mensual.
Evidencias de las configuraciones implementadas, afinamiento de reglas y cambios autorizados durante la ejecución contractual.	Cada vez que se realicen cambios relevantes.
Respaldo actualizado de la configuración de la solución WAF.	Mensual y previo a cambios mayores.
Informe final del servicio, incluyendo configuración vigente, políticas implementadas, estadísticas consolidadas de	Al finalizar el contrato.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Entregable	Oportunidad
operación, incidentes gestionados, recomendaciones técnicas y documentación para la continuidad del servicio.	

Criterios de aceptación:

La obligación se entenderá cumplida cuando:

- La solución WAF se encuentre implementada e integrada con el portal web institucional.
 - Las políticas de protección de aplicaciones web se encuentren configuradas y operativas.
 - Los mecanismos de protección SSL/TLS, DDoS y Bot Management estén habilitados y funcionando conforme al diseño aprobado.
 - El servicio permanezca disponible durante la vigencia contractual conforme a los niveles de servicio establecidos.
 - Los incidentes relacionados con la solución sean atendidos dentro de los tiempos definidos en los ANS.
 - Se entreguen oportunamente los informes, respaldos y evidencias definidos en el presente anexo.
 - Las configuraciones implementadas y los cambios efectuados cuenten con la aprobación del supervisor cuando corresponda.
 - El supervisor del contrato emita el recibido a satisfacción de los entregables.
6. Prestar los servicios especializados para la migración, actualización y administración de las bases de datos de la Entidad, incluyendo la planeación, configuración, implementación, validación y puesta en operación de los servidores de bases de datos sobre una plataforma con sistema operativo actualizado, garantizando la alta disponibilidad, continuidad del servicio e integridad de la información. El servicio incluye la administración especializada de bases de datos (DBA), con actividades de soporte, configuración, optimización, afinamiento (tuning), monitoreo, mantenimiento y verificación periódica de la ejecución de las copias de seguridad.

ANEXO TÉCNICO:

Obligación No. 6

Migración, Actualización y Administración Especializada de Bases de Datos (DBA)

Alcance Técnico:

El contratista deberá prestar los servicios especializados para la planeación, migración, actualización, implementación, administración y puesta en operación de los servidores de bases de datos de la C.R.A., garantizando la continuidad del servicio, la alta disponibilidad de la plataforma, la integridad de la información y la correcta operación de las bases de datos institucionales.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

El servicio comprende la evaluación de la infraestructura existente, la definición de la estrategia de migración, la instalación y configuración de los nuevos servidores de bases de datos sobre un sistema operativo actualizado, la migración de las instancias, bases de datos, usuarios, configuraciones y demás componentes requeridos, así como la validación funcional y técnica de la plataforma antes de su entrada en operación.

El contratista deberá ejecutar las actividades de migración minimizando la indisponibilidad de los servicios institucionales y garantizando la preservación de la integridad, consistencia y disponibilidad de la información durante todo el proceso.

Como parte del servicio, el contratista prestará la administración especializada de bases de datos (DBA), incluyendo la administración de las instancias de bases de datos definidas por la C.R.A., la configuración de parámetros de operación, optimización del desempeño (tuning), monitoreo de disponibilidad y rendimiento, mantenimiento preventivo y correctivo lógico, análisis de capacidad, soporte técnico especializado y atención de incidentes relacionados con la plataforma de bases de datos.

Asimismo, deberá verificar periódicamente la correcta ejecución de las copias de seguridad de las bases de datos administradas, validar la integridad de los respaldos y realizar pruebas de restauración cuando sean autorizadas por la supervisión del contrato, con el fin de garantizar la recuperación de la información en caso de contingencia.

El servicio comprende la actualización de parámetros de configuración, revisión de registros (logs), administración de usuarios y privilegios, monitoreo de consumo de recursos, implementación de buenas prácticas recomendadas por el fabricante y documentación de las actividades ejecutadas.

No hacen parte del alcance el suministro de licencias de motores de bases de datos, adquisición de infraestructura física, desarrollo o modificación de aplicaciones, ajustes funcionales a los sistemas de información, migración de aplicaciones diferentes a las bases de datos, ni la administración de plataformas que no sean definidas por la C.R.A. dentro del alcance contractual.

a. Soporte especializado Oracle

Nombre del servicio	Soporte especializado Oracle
Alcance del Servicio	Prestación de soporte técnico especializado sobre la plataforma Oracle Database on premise de la CRA, para la atención de incidentes, problemas, requerimientos técnicos especializados, actividades preventivas, correctivas, de aseguramiento, ajuste, recuperación operativa y optimización que resulten necesarias para contribuir a la continuidad, estabilidad y correcto funcionamiento del servicio de base de datos institucional. El servicio cubre, como mínimo, tres (3) instancias Oracle en

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN ANEXO TÉCNICO	
---	---	--

	ambiente de producción y deberá prestarse sobre la infraestructura local de la CRA, incluyendo acompañamiento técnico sobre los componentes de base de datos y aquellos elementos de su entorno inmediato que sean estrictamente necesarios para el diagnóstico o la solución del caso, sin que ello implique administración integral de plataformas ajenas a este numeral. La plataforma soportada corresponde a Oracle Database en esquema on premise, de la cual dependen, entre otros, el sistema integrado de gestión financiera PCT, el software de gestión de personal y nómina Humano y la solución documental DocuNet, esta última en estado de legado con conservación de información histórica.
--	--

DESCRIPCIÓN DEL REQUERIMIENTO

Característica Requerida	Descripción del requerimiento
Características Técnicas	• El proveedor deberá prestar soporte especializado sobre Oracle Database instalado on premise, incluyendo diagnóstico, análisis, corrección de fallas, ajuste de parámetros, revisión de rendimiento, verificación de integridad, apoyo en actividades de recuperación operativa y demás intervenciones requeridas para mantener la operación de las bases de datos institucionales cubiertas por el servicio. • El proveedor deberá atender requerimientos asociados a administración técnica de las instancias cubiertas, incluyendo revisión de logs, jobs, tablespaces, sesiones, bloqueos, usuarios, privilegios, actividades de soporte sobre respaldos lógicos y demás tareas equivalentes dentro del alcance autorizado por la CRA. • El proveedor deberá realizar análisis técnico y emitir recomendaciones para mantener la estabilidad, disponibilidad y seguridad operativa de la plataforma, incluyendo revisión de configuraciones, parámetros relevantes, capacidad, riesgos de obsolescencia, hallazgos operativos y acciones de mejora. • Cuando se requieran actividades de reconfiguración, ajuste técnico del entorno Oracle, recuperación operativa o puesta a punto sobre infraestructura definida por la CRA, estas podrán ejecutarse dentro del servicio de soporte contratado, siempre que

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Característica Requerida	Descripción del requerimiento
	correspondan al alcance de soporte especializado del componente y cuenten con autorización previa de la entidad. • No se entenderán incluidas dentro del alcance ordinario de este numeral las migraciones mayores, rediseños de arquitectura, implementaciones de nuevas instancias, actualizaciones mayores de versión, reinstalaciones completas por cambio estructural de plataforma o proyectos de transformación tecnológica, salvo que se prevean expresamente en el contrato o mediante el mecanismo formal de modificación contractual. • El proveedor deberá documentar las actividades ejecutadas, hallazgos, cambios aplicados, incidencias identificadas, acciones correctivas, riesgos y recomendaciones, dejando soporte en la herramienta de trazabilidad definida por la CRA o en el mecanismo acordado entre las partes para este componente. • El proveedor deberá advertir oportunamente a la CRA sobre condiciones técnicas que puedan afectar la continuidad del servicio, incluyendo obsolescencia de versión, ausencia de soporte del fabricante, limitaciones de compatibilidad, riesgos de seguridad, dependencia de infraestructura subyacente y demás situaciones que exijan tratamiento técnico o decisión institucional. • El detalle técnico de la versión exacta, parámetros de instalación, dependencias específicas, arquitectura y configuraciones particulares podrá manejarse mediante apéndice técnico controlado o en visita técnica bajo acuerdo de confidencialidad, cuando así lo defina la CRA.
Servicio/soporte	• Toda actividad ejecutada deberá registrarse en la herramienta de trazabilidad definida por la CRA, indicando fecha, solicitud o incidente asociado, descripción de la labor realizada, tiempo consumido, profesional que intervino, evidencias técnicas y validación del responsable designado por la entidad. • La atención deberá brindarse por canales remotos y, cuando la criticidad del caso o la naturaleza técnica de la intervención lo requieran, mediante atención presencial en sitio. Los tiempos de respuesta y atención aplicables a este componente deberán sujetarse a la tabla unificada de ANS del Anexo Técnico o al instrumento que la sustituya. • El proveedor deberá disponer de personal con experiencia comprobable en administración y soporte de Oracle Database y deberá escalar internamente los casos que requieran nivel

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Característica Requerida	Descripción del requerimiento
	experto, garantizando continuidad en la atención hasta su cierre técnico o hasta la emisión de recomendación formal a la CRA cuando se trate de una limitación estructural no solucionable dentro del alcance contractual.

Actividades mínimas:

El contratista deberá ejecutar, como mínimo, las siguientes actividades:

- Elaborar el plan de migración de las bases de datos.
- Evaluar la infraestructura actual y validar los requisitos técnicos del nuevo servidor.
- Instalar y configurar el sistema operativo del nuevo servidor conforme a las políticas de la Entidad.
- Instalar, configurar y poner en operación el motor o motores de bases de datos definidos por la C.R.A.
- Migrar las bases de datos, instancias, usuarios, permisos y configuraciones requeridas.
- Validar la integridad, consistencia y disponibilidad de la información posterior a la migración.
- Ejecutar pruebas funcionales y de rendimiento antes de la puesta en producción.
- Implementar configuraciones orientadas a garantizar la alta disponibilidad y continuidad del servicio, cuando aplique.
- Administrar las bases de datos mediante servicios especializados DBA.
- Configurar y optimizar parámetros de operación y desempeño (tuning).
- Monitorear permanentemente la disponibilidad, capacidad, rendimiento y utilización de recursos.
- Atender incidentes y requerimientos relacionados con las bases de datos.
- Ejecutar actividades de mantenimiento lógico de las bases de datos.
- Administrar usuarios, perfiles y privilegios de acceso cuando sean autorizados por la C.R.A.
- Verificar periódicamente la correcta ejecución de las copias de seguridad y documentar su resultado.
- Realizar pruebas de restauración cuando sean programadas o autorizadas por la Entidad.
- Mantener actualizada la documentación técnica de la plataforma administrada.

Entregable	Oportunidad
Plan de migración de bases de datos, incluyendo cronograma, estrategia de migración, riesgos, plan de contingencia y procedimiento de reversión.	Dentro de los primeros quince (15) días calendario contados a partir del acta de inicio.
Documento de implementación de la nueva plataforma, incluyendo configuración del sistema operativo, motor de	Una (1) vez, al finalizar la migración.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Entregable	Oportunidad
base de datos, parámetros de configuración y evidencias de la migración.	
Informe mensual de verificación de copias de seguridad, indicando el resultado de la ejecución de los respaldos, incidencias detectadas y acciones correctivas implementadas, cuando aplique.	Mensual.

7. Integrar, configurar y administrar el canal de respaldo de Internet dentro de la infraestructura tecnológica de la entidad, implementando mecanismos de balanceo de carga y/o alta disponibilidad (failover), con el fin de garantizar la continuidad, disponibilidad y resiliencia de los servicios de conectividad institucionales.

ANEXO TÉCNICO

Obligación No. 7

Integración, Configuración y Administración del Canal de Respaldo de Internet

Alcance Técnico:

El contratista deberá prestar los servicios especializados para la integración, configuración, administración y puesta en operación del canal de Internet de respaldo contratado por la C.R.A., incorporándolo a la infraestructura tecnológica institucional con el fin de garantizar la continuidad, disponibilidad y resiliencia de los servicios de conectividad.

El servicio comprende la integración del nuevo enlace de Internet con la infraestructura de comunicaciones existente, incluyendo el firewall institucional, equipos de borde, dispositivos de red y demás componentes necesarios para su correcta operación, de conformidad con la arquitectura tecnológica de la Entidad.

El contratista deberá configurar y optimizar los mecanismos de balanceo de carga (Load Balancing) y/o alta disponibilidad (Failover), según la arquitectura definida por la C.R.A., garantizando la conmutación automática o controlada entre el canal principal y el canal de respaldo ante eventos de indisponibilidad o degradación del servicio, minimizando la afectación de la operación institucional.

El servicio comprende la configuración de rutas, políticas de enrutamiento, monitoreo del estado de los enlaces, pruebas de conmutación, validación de la estabilidad del servicio, ajuste de parámetros de operación y optimización del desempeño de la conectividad institucional.

Asimismo, el contratista deberá realizar el monitoreo del funcionamiento del canal de respaldo, atender incidentes relacionados con la configuración implementada y efectuar los ajustes técnicos necesarios para mantener la correcta operación de la solución durante la vigencia contractual.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

No hacen parte del alcance el suministro del servicio de Internet, la contratación del proveedor de conectividad, la provisión de direcciones IP públicas, la adquisición de equipos de comunicaciones, el mantenimiento de la infraestructura del proveedor de Internet ni la atención de fallas atribuibles al operador del servicio.

Actividades mínimas:

El contratista deberá ejecutar, como mínimo, las siguientes actividades:

- Verificar las características técnicas del canal de Internet de respaldo suministrado por la C.R.A.
- Integrar el canal de respaldo a la infraestructura de red institucional.
- Configurar el firewall institucional para la operación del enlace de respaldo.
- Configurar las políticas de enrutamiento requeridas para la operación de ambos enlaces.
- Implementar mecanismos de balanceo de carga (Load Balancing) y/o alta disponibilidad (Failover), conforme a la arquitectura aprobada por la C.R.A.
- Configurar los mecanismos de monitoreo del estado de los enlaces de conectividad.
- Ejecutar pruebas de conmutación entre el enlace principal y el enlace de respaldo, verificando la continuidad de los servicios institucionales.
- Ajustar la configuración de la solución para optimizar el desempeño y la estabilidad de la conectividad.
- Atender incidentes relacionados con la configuración implementada.
- Documentar la configuración realizada y mantener actualizada la información técnica de la solución.

Entregable	Oportunidad
Documento de diseño e integración del canal de respaldo, incluyendo la arquitectura implementada, esquema de conectividad, configuración de balanceo de carga y/o failover, políticas de enrutamiento y topología lógica.	Dentro de los primeros quince (15) días calendario contados a partir del acta de inicio o de la disponibilidad del canal por parte de la C.R.A.
Acta de pruebas de funcionamiento, con evidencia de las pruebas de balanceo de carga y/o conmutación automática (Failover), validando la continuidad de los servicios institucionales.	Una (1) vez, posterior a la implementación.
Informe mensual de operación, incluyendo disponibilidad del enlace de respaldo, incidentes atendidos, ajustes realizados y recomendaciones técnicas para optimizar la conectividad institucional.	Mensual.
Documento técnico final con la configuración vigente, diagramas actualizados, procedimientos	Al finalizar el contrato.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Entregable	Oportunidad
de operación y recomendaciones para la administración de la solución implementada.	

8. Ejecutar, administrar, operar, monitorear y gestionar el servicio de copias de seguridad, respaldo y recuperación de la información de hasta trescientos (300) buzones de correo institucional de Office 365, con capacidad de hasta un (1) TB por buzón, garantizando el cumplimiento de los planes de respaldo programados, la disponibilidad de las copias de seguridad y la recuperación de la información conforme a los niveles de servicio e indicadores de desempeño establecidos por la Entidad.

ANEXO TÉCNICO

Obligación No. 8

Servicio SaaS de Copias de Seguridad, Respaldo y Recuperación de Información de Microsoft Office 365

Alcance Técnico:

El contratista deberá prestar, a todo costo, el servicio administrado bajo la modalidad Software como Servicio (SaaS) para la ejecución, administración, operación, monitoreo y gestión de las copias de seguridad, respaldo y recuperación de la información de hasta trescientos (300) buzones de correo institucional de Microsoft Office 365, mediante la plataforma Acronis Cyber Protect Cloud, incluyendo la protección de los servicios Exchange Online, OneDrive y demás componentes autorizados por la Entidad.

El servicio deberá garantizar la ejecución automática de los planes de respaldo programados, la disponibilidad permanente de las copias de seguridad, la integridad de la información respaldada y la capacidad de recuperación de la información conforme a los Acuerdos de Nivel de Servicio (ANS) e indicadores de desempeño establecidos por la C.R.A.

La solución deberá permitir la protección de buzones con una capacidad de hasta un (1) TB por usuario, incluyendo el respaldo de correos electrónicos, calendarios, contactos, tareas, carpetas, archivos almacenados en OneDrive y demás elementos soportados por la plataforma contratada.

El contratista será responsable de la configuración inicial de la plataforma, la incorporación de las cuentas institucionales objeto del servicio, la definición y administración de las políticas de respaldo, la programación de las tareas automáticas, el monitoreo permanente de su ejecución, la atención de fallas, la corrección de errores de respaldo, la ejecución de restauraciones solicitadas por la Entidad y la generación de informes periódicos sobre el estado del servicio.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Asimismo, deberá mantener la plataforma permanentemente actualizada, administrar las licencias suministradas para el servicio, verificar diariamente la ejecución de los respaldos programados, atender oportunamente las alertas e incidentes generados por la plataforma y realizar los ajustes necesarios para mantener el porcentaje de éxito de las copias de seguridad conforme a los indicadores definidos en el contrato.

No hacen parte del alcance el suministro de licencias Microsoft 365, la administración funcional de los buzones de correo, la recuperación de información eliminada por fuera de los periodos de retención definidos por la plataforma, la migración de correo electrónico entre plataformas ni el suministro de infraestructura física.

Actividades mínimas:

El contratista deberá ejecutar, como mínimo, las siguientes actividades:

- Configurar e implementar la plataforma Acronis Cyber Protect Cloud para Microsoft 365.
- Incorporar hasta trescientos (300) buzones institucionales al servicio de respaldo.
- Configurar las políticas de respaldo conforme a los lineamientos definidos por la C.R.A.
- Configurar la protección de Exchange Online y OneDrive.
- Programar la ejecución automática de las copias de seguridad.
- Monitorear diariamente la ejecución de los respaldos.
- Verificar el éxito de cada tarea programada.
- Atender y corregir fallas o errores presentados durante la ejecución de los respaldos.
- Ejecutar restauraciones parciales o completas de buzones o archivos cuando sean autorizadas por la Entidad.
- Monitorear la capacidad de almacenamiento utilizada y su crecimiento.
- Administrar usuarios, permisos y configuraciones de la plataforma.
- Gestionar las licencias asociadas al servicio.
- Generar reportes periódicos de operación, disponibilidad y cumplimiento de los respaldos.
- Mantener actualizada la documentación técnica de la plataforma durante la ejecución del contrato.

Entregable	Oportunidad
Documento de implementación del servicio, incluyendo configuración de la plataforma, cuentas protegidas, políticas de respaldo, frecuencia de ejecución y parámetros de recuperación.	Dentro de los diez (10) días hábiles siguientes al acta de inicio.
Inventario actualizado de los buzones y servicios protegidos por la plataforma.	Inicial y cuando se presenten modificaciones.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Entregable	Oportunidad
Informe mensual de operación del servicio, indicando número de buzones protegidos, respaldos ejecutados, porcentaje de éxito, fallas presentadas, incidentes atendidos, restauraciones realizadas, consumo de almacenamiento y recomendaciones.	Mensual.
Reporte de ejecución de copias de seguridad con evidencia del cumplimiento de los planes de respaldo programados.	Mensual.
Evidencias de las restauraciones realizadas, indicando fecha, usuario, elementos recuperados, tiempo de recuperación y resultado de la operación.	Cada vez que se ejecute una restauración.
Informe final del servicio, consolidando estadísticas de respaldo, recuperación, disponibilidad, incidentes, capacidad utilizada, configuraciones implementadas y recomendaciones para la continuidad del servicio.	Al finalizar el contrato.

Exclusiones

El servicio **no incluye**:

- Suministro de licencias de Microsoft 365.
- Administración funcional de Exchange Online o OneDrive.
- Migración de buzones entre plataformas de correo.
- Recuperación de información eliminada fuera del período de retención soportado por la solución.
- Desarrollo de herramientas o integraciones no soportadas por la plataforma Acronis.
- Protección de servicios o aplicaciones diferentes a los expresamente definidos por la C.R.A.
- Suministro de infraestructura física o almacenamiento local.

Recomendación técnica:

El contratista será responsable de verificar diariamente la ejecución de las tareas programadas y de adoptar las acciones correctivas necesarias para garantizar el cumplimiento del indicador de ejecución de copias de seguridad establecido por la Entidad, no siendo suficiente la sola configuración de la plataforma.

9. Prestar el servicio de configuración, administración, operación, monitoreo y gestión de los planes de copias de seguridad, respaldo, recuperación y continuidad de la

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

información, incluyendo los servicios de Backup, Disaster Recovery (DR) y Disaster Recovery as a Service (DRaaS), para hasta treinta (30) máquinas virtuales con una capacidad de almacenamiento de veinte (20) TB por mes, garantizando la ejecución de los respaldos programados, la disponibilidad e integridad de las copias de seguridad y la recuperación de la información de conformidad con los niveles de servicio e indicadores de desempeño establecidos por la Entidad.

ANEXO TÉCNICO

Obligación No. 9

Servicio SaaS de Copias de Seguridad, Recuperación y Continuidad de Máquinas Virtuales mediante Acronis Cyber Cloud

Alcance Técnico:

El contratista deberá prestar, a todo costo, el servicio administrado bajo la modalidad Software como Servicio (SaaS) para la configuración, administración, operación, monitoreo y gestión de las copias de seguridad, respaldo, recuperación y continuidad de la infraestructura virtual de la C.R.A., mediante la plataforma Acronis Cyber Protect Cloud, incluyendo las funcionalidades de Backup, Disaster Recovery (DR) y Disaster Recovery as a Service (DRaaS).

El servicio comprenderá la protección de hasta treinta (30) máquinas virtuales, con una capacidad de almacenamiento de hasta veinte (20) TB por mes, garantizando la ejecución de los planes de respaldo programados, la disponibilidad de las copias de seguridad, la recuperación de la información y la continuidad operativa de los servicios críticos, de conformidad con los Acuerdos de Nivel de Servicio (ANS) e indicadores de desempeño establecidos por la C.R.A.

El contratista será responsable de la configuración inicial de la plataforma, la incorporación de las máquinas virtuales al esquema de protección, la definición y administración de las políticas de respaldo y retención, la programación de las tareas automáticas de copia de seguridad, el monitoreo permanente de su ejecución, la verificación diaria del cumplimiento de los respaldos programados y la atención de fallas o incidentes relacionados con el servicio.

Asimismo, deberá configurar y mantener los mecanismos de recuperación ante desastres (DR) y de recuperación como servicio (DRaaS), incluyendo la definición de planes de recuperación, la preparación de los ambientes de contingencia, la ejecución de pruebas de recuperación cuando sean programadas por la Entidad y la validación de la capacidad de restauración de las máquinas virtuales protegidas.

El servicio comprende la administración permanente de la plataforma, la gestión de alertas, el monitoreo de la capacidad de almacenamiento, la optimización de las políticas de respaldo, la verificación periódica de la integridad de las copias de seguridad y la ejecución de restauraciones parciales o completas cuando sean autorizadas por la supervisión del contrato.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

No hacen parte del alcance el suministro de infraestructura física, la adquisición de licencias adicionales no contempladas en el contrato, la administración funcional de las aplicaciones alojadas en las máquinas virtuales, la migración entre plataformas de virtualización distintas a las definidas por la C.R.A. ni la implementación de un sitio alternativo diferente al provisto por la solución contratada.

Servicio de copias de seguridad y restauración de información institucional:

Nombre del servicio	Servicio de copias de seguridad y restauración de información institucional
Alcance del Servicio	El contratista deberá implementar, configurar, operar y soportar un servicio de copias de seguridad y restauración de información institucional desde una plataforma del proveedor o equivalente funcional, incluyendo licenciamiento, almacenamiento en nube, operación del servicio, monitoreo, soporte y ejecución de restauraciones durante la vigencia contractual. La solución deberá cubrir como mínimo el respaldo de hasta 300 cuentas o buzones de Microsoft 365 y hasta 30 máquinas virtuales, con capacidad de almacenamiento en nube de hasta 20 TB, conforme al alcance definido por la CRA y a las prioridades de protección que esta establezca durante la ejecución contractual. El servicio comprende la configuración de políticas de respaldo, programación y ejecución de copias de seguridad, monitoreo de la correcta ejecución de los trabajos, gestión de alertas, verificación básica de integridad de las copias, restauración de información bajo solicitud de la CRA, pruebas periódicas de restauración y emisión de reportes técnicos del servicio.
Unidad de facturación del producto/servicio	Servicio Mes
Cantidad	3

DESCRIPCIÓN DEL REQUERIMIENTO

Característica Requerida	Descripción del requerimiento
Características técnicas	La solución ofertada deberá ser una plataforma empresarial unificada de copias de seguridad y restauración, administrable desde una consola centralizada web, con capacidad de gestionar desde un mismo entorno los respaldos de Microsoft 365 y de máquinas virtuales incluidas en el alcance contractual.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Característica Requerida	Descripción del requerimiento
	• La solución deberá permitir la definición y administración centralizada de políticas de protección, programación de tareas, grupos de respaldo, retención, alertas, bitácoras, tableros y reportes técnicos del servicio. • Para Microsoft 365, la solución deberá soportar respaldo y restauración de cargas de trabajo del ecosistema contratado, con capacidad de restauración granular de elementos específicos y recuperación a nivel de buzón, archivo o componente individual según la carga protegida. • Para ambientes virtualizados, la solución deberá soportar respaldo de máquinas virtuales a nivel de imagen completa y recuperación granular desde el mismo respaldo, sin exigir la reinstalación total del sistema para recuperar archivos o elementos puntuales. • La solución deberá soportar respaldos incrementales y mecanismos de optimización del almacenamiento y del tráfico, incluyendo como mínimo compresión y deduplicación o tecnologías equivalentes de eficiencia de almacenamiento. • La solución deberá garantizar cifrado de la información respaldada en tránsito y en reposo, así como controles de autenticación y autorización para la administración del servicio y el acceso a las copias. • La solución deberá contar con mecanismos de validación de recuperabilidad o verificación de integridad de los respaldos, de manera que permita comprobar que las copias generadas son utilizables para restauración. • La solución deberá contar con capacidades de protección del repositorio de respaldo frente a alteración maliciosa, borrado no autorizado o afectación por ransomware, mediante controles de inmutabilidad, protección del almacenamiento, resguardo equivalente o funcionalidades de seguridad de nivel empresarial. • La solución deberá generar alertamiento automático por fallos, trabajos incompletos, degradación de capacidad, errores de retención o eventos críticos del servicio, y deberá permitir la trazabilidad histórica de ejecuciones y restauraciones. • La solución deberá permitir restauraciones completas y restauraciones granulares bajo demanda, así como pruebas periódicas de restauración para validar la recuperabilidad de la información protegida. • La solución deberá ofrecer escalabilidad para proteger, como mínimo, hasta 300 buzones o cuentas de Microsoft 365 y hasta 30 máquinas virtuales con una capacidad total de

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Característica Requerida	Descripción del requerimiento
	almacenamiento en nube de hasta 20 TB, conforme al alcance previsto por la CRA. • La solución debe ser de fabricante con soporte empresarial y documentación técnica pública, con actualizaciones activas y trazabilidad de versiones. • El oferente debe acreditar que la plataforma propuesta ya se encuentra desplegada y operando comercialmente para las cargas requeridas, y no como desarrollo a la medida o integración artesanal. • La solución deberá corresponder a una plataforma de mercado especializada en respaldo empresarial de cargas híbridas y cloud, con soporte nativo o formalmente integrado para Microsoft 365 y plataformas de virtualización, especialmente VMware, con agentes para máquinas virtuales y Vcenter. • La solución ofertada deberá corresponder a una plataforma integrada de respaldo empresarial, no a la simple combinación de servicios independientes de almacenamiento, scripts, utilitarios de copia o herramientas de respaldo de propósito limitado, y deberá acreditar capacidades nativas de administración centralizada, protección de Microsoft 365, respaldo de máquinas virtuales, restauración granular, validación de respaldos, cifrado y protección del repositorio. • La solución ofertada deberá corresponder a una plataforma empresarial de copias de seguridad y restauración que cuente con un programa formal de seguridad y cumplimiento, y el oferente deberá indicar de manera expresa los estándares internacionales, marcos de referencia y marcos regulatorios con los cuales se encuentra alineada, certificada o soportada la solución propuesta, según aplique, incluyendo como mínimo estándares de la serie ISO/IEC 27000, familia de normas ISO 9000, Controles de Sistema y Organización 2 (SOC 2), IEC 62443-4-1: Ciclo de Vida de Desarrollo de Productos Seguros (SSDLC) y marcos regulatorios de protección de datos y seguridad de la información aplicables a servicios cloud. • El oferente deberá aportar evidencia documental vigente emitida por el fabricante, por un tercero competente o por el portal oficial de confianza y cumplimiento del fabricante, en la que se identifiquen de forma verificable las certificaciones, estándares, atestaciones, marcos de control y consideraciones regulatorias aplicables a la solución propuesta. • No se aceptarán manifestaciones genéricas de cumplimiento sin soporte verificable; la información presentada deberá distinguir claramente entre certificaciones vigentes, alineación con estándares, adopción de marcos de control y soporte para

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Característica Requerida	Descripción del requerimiento
	requerimientos regulatorios, indicando su alcance sobre la solución ofertada o sobre la infraestructura que la soporta.
Servicio/soporte	• Los incidentes, requerimientos, solicitudes de restauración, consultas operativas y demás casos asociados al servicio de copias de seguridad y restauración serán registrados, gestionados y atendidos a través de Kaía o de la herramienta que la CRA defina, garantizando trazabilidad del caso, comunicaciones de avance, evidencias técnicas y cierre formal. • El proveedor deberá disponer de mesa de servicio y soporte técnico para la atención de incidentes y requerimientos asociados al servicio, por los canales definidos para la operación contractual, incluyendo atención remota y, cuando la naturaleza del caso lo requiera y la CRA lo autorice, acompañamiento especializado para restauraciones o validaciones técnicas. • El proveedor deberá garantizar tiempos máximos de primera respuesta según criticidad, como mínimo: alta gravedad una (1) hora, gravedad media cuatro (4) horas y gravedad baja el siguiente día hábil, o el esquema equivalente de prioridades que la CRA adopte formalmente en su tabla de ANS. • Toda solicitud de restauración deberá quedar documentada con identificación del activo o información requerida, fecha y hora de la solicitud, responsable que autoriza, alcance de la restauración, resultado obtenido, evidencias técnicas y fecha de cierre. • Cuando se presenten fallos de respaldo, errores de ejecución, inconsistencias de retención, incidentes de acceso o eventos que afecten la disponibilidad del servicio contratado, el proveedor deberá realizar análisis, corrección, reproceso cuando aplique y documentación del caso, dejando trazabilidad completa en Kaía. • La CRA podrá ejecutar directamente operaciones administrativas y de restauración dentro del alcance de sus permisos, sin perjuicio del deber del proveedor de prestar soporte, acompañamiento y atención cuando la naturaleza del caso lo requiera. • Acceso de la CRA a la plataforma de respaldo ○ La CRA deberá contar durante toda la ejecución contractual con acceso directo a la consola de administración de la solución, sobre el espacio, capacidad y recursos asignados a la entidad para la prestación del servicio. ○ Dicho acceso deberá permitir, como mínimo, la gestión

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Característica Requerida	Descripción del requerimiento
	administrativa y operativa de las copias de seguridad dentro del alcance contratado, incluyendo creación, asignación, modificación, suspensión o retiro de planes de respaldo; asociación o desasociación de activos o cargas protegidas; ejecución manual o programada de copias; consulta de estado de trabajos; monitoreo de alertas; administración de retenciones soportadas por la solución; ejecución de restauraciones; consulta de bitácoras, reportes, consumo y trazabilidad operativa. ○ La CRA deberá contar con credenciales propias e independientes de las del proveedor, con roles de administración sobre su entorno o espacio lógico asignado, sin dependencia exclusiva del contratista para la operación ordinaria del servicio dentro del alcance autorizado. ○ El proveedor deberá garantizar que las facultades administrativas de la CRA se ejerzan sobre los recursos, políticas y datos correspondientes a la entidad dentro del servicio contratado, sin acceso a información, configuraciones o componentes pertenecientes a otros clientes o al entorno compartido del proveedor. ○ La solución deberá permitir que la CRA ejecute de manera autónoma, cuando así lo requiera, operaciones de administración y restauración dentro de los permisos asignados, sin perjuicio del soporte y acompañamiento técnico que deba prestar el proveedor.
Sitio de las pruebas	Local en las instalaciones de la CRA y/o de forma remota, cuando la naturaleza del servicio lo permita y la CRA lo autorice.

Actividades mínimas:

El contratista deberá ejecutar, como mínimo, las siguientes actividades:

- Configurar e implementar la plataforma Acronis Cyber Protect Cloud para la protección de las máquinas virtuales.
- Incorporar hasta treinta (30) máquinas virtuales al servicio de respaldo.
- Configurar las políticas de respaldo, retención y recuperación conforme a los lineamientos de la C.R.A.
- Programar la ejecución automática de las copias de seguridad.
- Monitorear diariamente la ejecución de los respaldos programados.
- Verificar el cumplimiento de los planes de respaldo y gestionar las fallas detectadas.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

- Configurar y administrar los servicios de Disaster Recovery (DR) y Disaster Recovery as a Service (DRaaS).
- Configurar los planes de recuperación de las máquinas virtuales protegidas.
- Ejecutar restauraciones de información y recuperación de máquinas virtuales cuando sean autorizadas por la Entidad.
- Realizar pruebas de recuperación y continuidad cuando sean programadas por la supervisión del contrato.
- Monitorear la capacidad de almacenamiento y el estado de las copias de seguridad.
- Administrar usuarios, permisos y configuraciones de la plataforma.
- Generar reportes periódicos de operación, disponibilidad y cumplimiento del servicio.
- Mantener actualizada la documentación técnica y los planes de recuperación durante la ejecución contractual.

Entregable	Oportunidad
Documento de implementación del servicio, incluyendo la configuración de la plataforma, máquinas virtuales protegidas, políticas de respaldo, retención, recuperación y continuidad.	Dentro de los diez (10) días hábiles siguientes al acta de inicio.
Inventario actualizado de las máquinas virtuales incorporadas al servicio de Backup, DR y DRaaS.	Inicial y cuando se presenten modificaciones.
Informe mensual de operación del servicio, indicando máquinas virtuales protegidas, porcentaje de éxito de los respaldos, capacidad utilizada, incidentes atendidos, restauraciones realizadas, estado de los servicios DR y DRaaS y recomendaciones técnicas.	Mensual.
Reporte mensual de ejecución de los planes de respaldo, con evidencia del cumplimiento de las tareas programadas y de las acciones correctivas implementadas frente a fallas presentadas.	Mensual.
Evidencias de las restauraciones y pruebas de recuperación ejecutadas, indicando fecha, máquina virtual, alcance de la recuperación, tiempo empleado y resultado obtenido.	Cada vez que se realice una restauración o prueba de recuperación.
Informe final del servicio, consolidando estadísticas de respaldo, recuperación, continuidad, disponibilidad, incidentes, configuraciones implementadas y recomendaciones para la operación futura del servicio.	Al finalizar el contrato.

Criterios de aceptación:

La obligación se entenderá cumplida cuando:

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

- La plataforma Acronis Cyber Protect Cloud se encuentre implementada y operativa para las máquinas virtuales definidas por la C.R.A.
- Las treinta (30) máquinas virtuales objeto del contrato se encuentren protegidas conforme a las políticas de respaldo y recuperación establecidas.
- Los planes de respaldo programados se ejecuten con un porcentaje de éxito igual o superior al indicador definido por la Entidad.
- Las copias de seguridad se encuentren disponibles e íntegras para su recuperación durante el período de retención configurado.
- Los servicios de Disaster Recovery (DR) y Disaster Recovery as a Service (DRaaS) permanezcan configurados y operativos.
- Las restauraciones solicitadas por la C.R.A. se ejecuten dentro de los tiempos establecidos en los ANS.
- Se entreguen oportunamente los informes, evidencias y documentación técnica definidos en el presente anexo.
- El supervisor del contrato emita el recibido a satisfacción de los entregables.

Exclusiones:

El servicio no incluye:

- Suministro de infraestructura física o almacenamiento adicional distinto al contemplado en la solución contratada.
- Migración de cargas de trabajo entre plataformas de virtualización no definidas por la C.R.A.
- Recuperación de información no protegida por las políticas de respaldo configuradas.
- Diseño o construcción de un sitio alternativo de contingencia diferente al proporcionado por la solución DRaaS contratada.

10. Prestar servicios de apoyo para implementar, configurar, monitorear, administrar, operar, gestionar, mantenimiento y soporte técnico con ingeniería en sitio, de la solución telemática y de comunicaciones y de LAN extendida entre sede 1 y sede 2 de la C.R.A., con ajuste de cargas de trabajo y de red LAN, extendida LAN y W-LAN., basada en tecnologías de telecomunicaciones y segmentación mediante VLANs, garantizando la conectividad segura y la comunicación entre las 2 sedes.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

ANEXO TÉCNICO

Obligación No. 10

Implementación, Administración y Soporte de la Solución Telemática, LAN Extendida y Comunicaciones entre las Sedes de la C.R.A.

Alcance Técnico:

El contratista deberá prestar los servicios especializados para la implementación, configuración, administración, operación, monitoreo, mantenimiento y soporte técnico de la infraestructura de comunicaciones de la C.R.A., incluyendo la red LAN, LAN Extendida (LAN Extension) y la red inalámbrica (WLAN) que soportan la comunicación entre la sede principal y la sede alterna de la Entidad.

El servicio comprende la integración de la infraestructura de comunicaciones existente, la configuración y optimización de los equipos activos de red definidos por la C.R.A., la implementación y administración de la segmentación lógica mediante VLAN, la configuración de enlaces troncales (trunk), direccionamiento IP, enrutamiento, políticas de comunicación entre segmentos, calidad de servicio (QoS) cuando aplique, y los ajustes necesarios para garantizar la conectividad segura, estable y continua entre ambas sedes.

El contratista deberá realizar el análisis y ajuste de las cargas de trabajo de la infraestructura de red, optimizando el desempeño de la LAN, LAN Extendida y WLAN, verificando el adecuado funcionamiento de los enlaces de comunicación, la disponibilidad de los servicios de red y la correcta operación de la infraestructura de telecomunicaciones asociada.

Como parte del servicio deberá administrar la infraestructura de comunicaciones, realizar el monitoreo permanente del estado operativo de los enlaces y dispositivos administrados, atender incidentes y requerimientos relacionados con la red institucional, ejecutar actividades de mantenimiento preventivo y correctivo sobre las configuraciones autorizadas, documentar los cambios efectuados y brindar soporte técnico especializado con disponibilidad de ingeniería en sitio cuando las actividades no puedan resolverse de manera remota o cuando así lo requiera la supervisión del contrato.

El contratista deberá garantizar que las configuraciones implementadas mantengan la continuidad operativa de los servicios institucionales, minimizando las interrupciones y ejecutando las actividades de mantenimiento dentro de las ventanas autorizadas por la C.R.A.

No hace parte del alcance el suministro de equipos activos de red, cableado estructurado, fibra óptica, licencias de software, ampliaciones de infraestructura física, obra civil, instalación de nuevos puntos de red o la contratación de servicios de telecomunicaciones con terceros.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Actividades mínimas:

El contratista deberá ejecutar, como mínimo, las siguientes actividades:

- Configurar e integrar la infraestructura LAN, LAN Extendida y WLAN entre las sedes de la C.R.A.
- Configurar y administrar VLAN, enlaces troncales (Trunk), direccionamiento IP y segmentación lógica de la red.
- Configurar y optimizar la comunicación entre las sedes mediante la infraestructura de telecomunicaciones existente.
- Ajustar la distribución de cargas de trabajo y optimizar el desempeño de la red.
- Configurar parámetros de calidad de servicio (QoS) cuando sean requeridos por la Entidad.
- Administrar y monitorear los dispositivos activos de red definidos por la C.R.A.
- Verificar permanentemente la disponibilidad de los enlaces y servicios de comunicación.
- Atender incidentes, fallas y requerimientos relacionados con la infraestructura de comunicaciones.
- Ejecutar mantenimiento preventivo y correctivo sobre las configuraciones autorizadas.
- Realizar respaldos de las configuraciones de los equipos antes de efectuar modificaciones.
- Documentar las configuraciones implementadas y los cambios realizados.
- Brindar soporte técnico especializado con ingeniería en sitio cuando sea requerido por la Entidad.
- Ejecutar pruebas de conectividad y funcionamiento posteriores a las configuraciones o cambios realizados.

Entregable	Oportunidad
Documento de implementación y configuración, incluyendo las VLAN, direccionamiento IP, enlaces troncales, políticas de comunicación, diagramas de red actualizados y parámetros configurados.	Una (1) vez, una vez finalizada la implementación.
Respaldo de las configuraciones de los equipos administrados antes y después de cambios relevantes.	Cada vez que se realicen cambios de configuración.
Informe mensual de operación y administración de la infraestructura de comunicaciones, indicando disponibilidad de los enlaces, incidentes atendidos, cambios ejecutados, mantenimientos realizados, utilización de recursos, recomendaciones y estado general de la red.	Mensual.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Entregable	Oportunidad
Informe final del servicio, incluyendo configuración vigente, inventario lógico actualizado, diagramas de red, respaldo de configuraciones, incidentes relevantes y recomendaciones para la operación futura.	Al finalizar el contrato.

Criterios de aceptación:

La obligación se entenderá cumplida cuando:

- La infraestructura LAN, LAN Extendida y WLAN se encuentre configurada y operando de acuerdo con los requerimientos de la C.R.A.
- La comunicación entre la sede principal y la sede alterna funcione correctamente y de forma continua.
- La segmentación mediante VLAN y las configuraciones de red implementadas permitan la operación segura de los servicios institucionales.
- Los ajustes de configuración no afecten la disponibilidad de los servicios institucionales, salvo durante las ventanas de mantenimiento previamente autorizadas.
- Los incidentes y requerimientos sean atendidos dentro de los tiempos establecidos en los ANS del contrato.
- Se entreguen oportunamente los informes, respaldos de configuración, documentación técnica y demás evidencias definidas en el presente anexo.

11. Prestar los servicios especializados para la asesoría, configuración, implementación, integración y puesta en operación de la nueva troncal SIP de la plataforma de telefonía IP de la Entidad, incluyendo la parametrización, pruebas de funcionamiento, interoperabilidad y acompañamiento técnico necesarios para garantizar la comunicación de ciento veinte (120) extensiones de voz sobre IP entre las sedes 1 y 2, asegurando la disponibilidad, continuidad y correcto funcionamiento del servicio de telefonía institucional.

ANEXO TÉCNICO

Obligación No. 11

Implementación, Integración y Puesta en Operación de la Troncal SIP para la Plataforma de Telefonía IP

Alcance Técnico:

El contratista deberá prestar los servicios especializados para la asesoría, configuración, implementación, integración y puesta en operación de la nueva troncal SIP de la plataforma de telefonía IP institucional de la C.R.A., garantizando la interoperabilidad entre la

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN ANEXO TÉCNICO	
---	---	--

infraestructura tecnológica existente y la solución de comunicaciones unificadas que adopte la Entidad.

El servicio comprende la implementación y configuración de la plataforma de telefonía IP, la integración de la troncal SIP suministrada por el operador de telecomunicaciones con el servidor de telefonía institucional, la parametrización de los servicios de voz, la configuración del plan de numeración, extensiones, rutas de llamadas, reglas de marcación, perfiles de usuarios y demás parámetros requeridos para la correcta operación del servicio. Asimismo, el contratista deberá realizar la integración de la plataforma con la infraestructura de red institucional, verificando la correcta operación sobre la red LAN y LAN Extendida entre las sedes 1 y 2, configurando los parámetros necesarios para garantizar la calidad del servicio (QoS), la disponibilidad de las comunicaciones, la continuidad del servicio y el adecuado desempeño de la solución.

El servicio incluye la configuración y habilitación de hasta ciento veinte (120) extensiones IP, la implementación de las funcionalidades básicas de telefonía institucional, la ejecución de pruebas funcionales, pruebas de interoperabilidad, pruebas de llamadas internas y externas, validación del establecimiento y finalización de llamadas, verificación del flujo de audio bidireccional, pruebas de transferencia, conferencias, buzón de voz (cuando aplique) y demás funcionalidades soportadas por la plataforma implementada.

El contratista deberá realizar el acompañamiento técnico durante la estabilización de la solución, atender los incidentes derivados de la implementación, efectuar los ajustes de configuración que resulten necesarios y documentar la configuración definitiva de la plataforma.

No hacen parte del alcance el suministro de la troncal SIP por parte del operador de telecomunicaciones, el suministro de terminales telefónicos IP, licencias adicionales no contempladas en el contrato, ampliaciones del número de extensiones, adecuaciones de cableado estructurado, obras civiles ni la contratación de servicios de telefonía con terceros.

Soporte de la plataforma de telefonía IP.

Nombre del servicio	Soporte de la Plataforma de Telefonía IP
Alcance del Servicio	Prestación del servicio especializado de soporte, regularización técnica, configuración, aseguramiento, actualización y mantenimiento de la plataforma de telefonía IP institucional de la CRA, con base en la solución existente, orientado a su correcta operación, estabilidad, seguridad y continuidad durante la vigencia contractual. El servicio comprende la validación técnica inicial del estado actual de la plataforma PBX basada en Asterisk o tecnología equivalente existente en la CRA, la identificación de brechas operativas o de configuración, la ejecución de ajustes y parametrizaciones autorizadas, la integración o regularización de la troncal SIP y componentes asociados, la configuración funcional requerida y la

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

	estabilización operativa de la solución intervenida. El alcance incluye soporte sobre extensiones, troncales, IVR, funcionalidades básicas de operación, ajustes menores, hardening razonable del servidor y del PBX, actualización y mantenimiento de la plataforma, monitoreo operativo y atención de incidentes atribuibles a la solución intervenida, de acuerdo con los subcomponentes efectivamente contratados. No se entenderán incluidos dentro del alcance ordinario de este numeral el reemplazo integral de la plataforma por una nueva solución, la adquisición de licencias o appliances no previstos, la expansión no presupuestada de funcionalidades de comunicaciones unificadas, la renovación contractual con el operador de telefonía, ni obras o adecuaciones físicas adicionales distintas de las expresamente autorizadas por la CRA.
Unidad de facturación del producto/servicio	Servicio Mes
Cantidad	3

DESCRIPCIÓN DEL REQUERIMIENTO

Característica Requerida	Descripción del requerimiento
Características técnicas	- El proveedor deberá realizar un diagnóstico inicial de la plataforma existente, incluyendo estado general del servidor PBX, configuración de extensiones, troncales, rutas, IVR, parámetros funcionales relevantes, condiciones básicas de seguridad y riesgos identificados, dejando informe o acta de línea base. - Con base en la validación inicial, el proveedor deberá ejecutar las actividades de regularización, configuración, ajuste o puesta a punto que resulten necesarias y que correspondan al alcance contratado, dejando trazabilidad de los cambios efectuados y del punto a partir del cual asume responsabilidad sobre la solución intervenida. - El proveedor deberá administrar y ajustar las extensiones, parámetros operativos, rutas, horarios, IVR, grupos de timbrado, colas y demás configuraciones funcionales básicas requeridas para la operación de la CRA, siempre que no impliquen rediseño mayor de la arquitectura ni adquisición de componentes no contemplados. - El proveedor deberá integrar o regularizar la interoperabilidad con el operador de telefonía mediante troncal SIP o mecanismo equivalente existente, incluyendo validaciones técnicas de conectividad y funcionamiento, autenticación, enrutamiento y

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Característica Requerida	Descripción del requerimiento
	pruebas básicas de llamadas entrantes y salientes. • El proveedor deberá implementar medidas razonables de hardening sobre el servidor y la plataforma PBX intervenida, incluyendo restricciones de acceso administrativo, uso de canales seguros, cuentas auditable, bitácora de cambios y medidas básicas para reducir exposición y uso no autorizado. • El proveedor deberá ejecutar actividades de actualización y mantenimiento de la plataforma dentro de la vigencia contractual, siempre que sean compatibles con la arquitectura existente y no correspondan a migraciones mayores o cambios estructurales no previstos en el alcance contratado. • El proveedor deberá mantener mecanismos de respaldo de la configuración y parámetros críticos de la solución intervenida, así como procedimientos básicos de restauración operativa acordes con el alcance del servicio. • El proveedor deberá entregar documentación técnica y operativa actualizada de la solución efectivamente intervenida, incluyendo inventario funcional de extensiones, troncales, rutas, parámetros relevantes, procedimientos básicos de administración y evidencias de configuración. • La capacitación al personal designado por la CRA deberá enfocarse en la operación básica y administración funcional de la plataforma intervenida, en la medida compatible con el alcance efectivamente ejecutado durante la vigencia contractual.
Servicio/soporte	• El soporte deberá prestarse mediante atención remota y, cuando la naturaleza del caso lo requiera, atención en sitio previamente coordinada con la CRA, para incidentes atribuibles a la plataforma PBX, errores de configuración, ajustes autorizados, restauraciones operativas y actividades de estabilización relacionadas con la solución intervenida. • El soporte cubierto por este numeral se orienta a la atención especializada de la plataforma de telefonía IP y no incluye la gestión de incidentes originados exclusivamente en el operador de telefonía, en fallas eléctricas, en daños de hardware no cubiertos, o en alteraciones efectuadas por terceros sin autorización y sin control de cambios. • Todo incidente, requerimiento o cambio atendido deberá quedar registrado en la herramienta de trazabilidad definida por la CRA o en el mecanismo acordado entre las partes, con identificación del caso, análisis realizado, acciones ejecutadas, evidencias y cierre. • Los tiempos de respuesta y atención aplicables a este componente deberán sujetarse a la tabla unificada de ANS del Anexo Técnico o al instrumento que la sustituya, evitando compromisos implícitos

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Característica Requerida	Descripción del requerimiento
	de disponibilidad irrestricta que no correspondan al valor del componente. El proveedor deberá entregar informe mensual con estado de la plataforma, incidentes atendidos, cambios realizados, hallazgos, recomendaciones y actividades pendientes relacionadas con el servicio.

Actividades mínimas:

El contratista deberá ejecutar, como mínimo, las siguientes actividades:

- Realizar el diagnóstico de la infraestructura de red requerida para la implementación de la telefonía IP.
- Configurar e implementar la plataforma de telefonía IP institucional.
- Integrar la troncal SIP suministrada por el operador con la plataforma de telefonía.
- Configurar el plan de numeración institucional.
- Configurar hasta ciento veinte (120) extensiones IP.
- Configurar rutas de llamadas, reglas de marcación y perfiles de usuario.
- Configurar los parámetros de calidad del servicio (QoS) requeridos para el tráfico de voz sobre IP.
- Integrar la solución con la infraestructura LAN y LAN Extendida entre las sedes de la C.R.A.
- Ejecutar pruebas de interoperabilidad con la troncal SIP.
- Ejecutar pruebas de llamadas internas y externas.
- Validar el correcto funcionamiento de las funcionalidades implementadas.
- Atender incidentes derivados de la implementación y efectuar los ajustes requeridos.
- Documentar la configuración definitiva de la solución.
- Brindar acompañamiento técnico durante el proceso de estabilización.

Criterios de aceptación:

La obligación se entenderá cumplida cuando:

- La plataforma de telefonía IP se encuentre implementada e integrada con la troncal SIP del operador.
- Las ciento veinte (120) extensiones IP se encuentren configuradas y operativas, de acuerdo con el alcance definido por la C.R.A.
- La comunicación entre las sedes 1 y 2 funcione correctamente mediante la infraestructura institucional.
- Las pruebas de interoperabilidad y funcionamiento se ejecuten satisfactoriamente y sean aprobadas por la supervisión del contrato.
- La calidad de las comunicaciones permita la operación normal del servicio de telefonía institucional.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

- Se entregue la documentación técnica, los respaldos de configuración y las evidencias establecidas en el presente anexo.

12. Prestación de servicios especializados para la administración, monitoreo y gestión de la infraestructura tecnológica, redes, servicios digitales y componentes de ciberseguridad institucional:

Servicios especializados para la gestión, monitoreo, análisis, recuperación, continuidad y optimización de los recursos tecnológicos de la CRA, incorporando controles de ciberseguridad, para asegurar la disponibilidad, el rendimiento y la protección de la infraestructura tecnológica y de la información institucional frente a incidentes y amenazas digitales.

- Monitoreo de switches, servidores y firewall, monitoreo de endpoints y tráfico de red, incluye redes Wireless, red cableada y de datacenter, enlaces entre sedes, protección de marca, ajuste de cargas de trabajo y de red LAN y W-LAN.

Nombre del servicio	Monitoreo de switches, servidores y firewall, monitoreo de endpoints y tráfico de red, incluye redes Wireless, ajuste de cargas de trabajo y de red LAN y W-LAN.
Alcance del Servicio	Prestación del servicio especializado de monitoreo, análisis y seguimiento operativo sobre la infraestructura tecnológica de la CRA definida en el Inventario Técnico Oficial incluido en este Anexo, comprendiendo como mínimo los equipos de red LAN, switches core y de borde, firewall perimetral, servidores físicos, plataformas virtualizadas, almacenamiento asociado y acces points de la red inalámbrica. El servicio deberá permitir la observación continua del estado, disponibilidad, desempeño, capacidad, tráfico, eventos relevantes y comportamiento de los activos monitoreados, mediante herramientas especializadas provistas por el contratista o integradas con las herramientas dispuestas por la CRA, generando visibilidad suficiente para la detección temprana de fallas, degradaciones del servicio, cuellos de botella, anomalías de tráfico y eventos que puedan afectar la continuidad o seguridad de la operación institucional.
Unidad de facturación de producto/servicio	Servicio Mes
Cantidad	3

DESCRIPCIÓN DEL REQUERIMIENTO

Característica Requerida	Descripción del requerimiento
--------------------------	-------------------------------

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Características técnicas	• Monitoreo periódico de disponibilidad, salud y rendimiento de switches, servidores, firewall, enlaces, tráfico LAN/WAN/WLAN, servicios expuestos y almacenamiento, sobre la infraestructura priorizada por la CRA. • Elaboración, dentro del primer mes de ejecución, de una línea base técnica de comportamiento de la infraestructura monitoreada, que incluya, según la cobertura efectivamente contratada, servicios, puertos, protocolos, aplicaciones, direcciones IP internas y públicas, utilización de enlaces, consumo de ancho de banda, picos de tráfico, latencia, pérdida de paquetes, interfaces críticas y comportamiento general de la red. • Actualización o contraste de dicha línea base al cierre del contrato, o cuando la CRA lo requiera por cambios significativos en la infraestructura, incidentes relevantes o necesidades de supervisión técnica. • Definición e implementación de umbrales, alertas y reglas de escalamiento para eventos de capacidad, disponibilidad, desempeño y comportamiento anómalo de los activos monitoreados, con notificación al supervisor del contrato. • Emisión de informe mensual técnico y ejecutivo con estado del servicio, activos monitoreados, eventos relevantes, interrupciones, alertas relevantes, hallazgos operativos, recomendaciones y plan de mejora cuando aplique. • Entrega de informe final consolidado con balance general del período, comportamiento de la infraestructura monitoreada, principales incidencias, ajustes efectuados, riesgos identificados y recomendaciones priorizadas para la continuidad del servicio. • Toda actividad de monitoreo deberá contar con trazabilidad y soporte documental suficiente, incluyendo como mínimo reportes de consola o herramienta, tickets asociados cuando aplique, bitácora de cambios, evidencias técnicas y registro de incidentes o alertas relevantes. • Los registros y evidencias derivados del servicio de monitoreo deberán conservarse con controles razonables de acceso, integridad y trazabilidad durante la ejecución contractual y por el período que defina la CRA para efectos de supervisión, auditoría y cierre del contrato, conforme a la naturaleza de la información y al alcance del servicio contratado. • El contratista deberá emitir recomendaciones de ajuste, tratamiento u optimización sobre la infraestructura monitoreada cuando identifique comportamientos anómalos, riesgos de capacidad, indisponibilidades recurrentes o condiciones técnicas que puedan afectar la continuidad, el rendimiento o la seguridad de la información.
---------------------------------	---

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

b. Gestión de vulnerabilidad de la seguridad informática.

Nombre del servicio	Gestión de vulnerabilidad de la seguridad informática
Alcance del Servicio	Prestación del servicio especializado para la identificación, clasificación, priorización, seguimiento y reporte de vulnerabilidades técnicas sobre los activos definidos por la CRA dentro del Inventario Técnico Oficial y aquellos que se incorporen durante la ejecución contractual mediante control de cambios. El servicio deberá incluir la ejecución de una evaluación inicial como línea base sobre los activos priorizados por la CRA, el seguimiento periódico al estado de los hallazgos identificados, la formulación de recomendaciones de tratamiento y, cuando aplique, la validación técnica de las acciones ejecutadas dentro del alcance de los servicios efectivamente contratados o la formalización de la aceptación del riesgo por parte de la CRA. Para efectos de estructuración de la oferta, el proveedor deberá contemplar dentro de su propuesta los recursos técnicos, operativos y de soporte necesarios para la adecuada prestación del servicio, de acuerdo con el alcance contratado, la cobertura definida por la CRA y el universo de activos priorizados durante la ejecución contractual.
Unidad de facturación del producto/servicio	Servicio Mes
Cantidad	3

DESCRIPCIÓN DEL REQUERIMIENTO

Característica Requerida	Descripción del requerimiento
Características técnicas	- El alcance mínimo del análisis deberá incluir los activos críticos definidos por la CRA, componentes de borde y perímetro, firewall, exposición de IP públicas, conmutación y red, switches, controladores y puntos de acceso de red inalámbrica, servidores críticos, plataformas virtualizadas y demás activos priorizados por la entidad dentro del Inventario Técnico Oficial. - Dentro de los primeros cuarenta y cinco (45) días de ejecución contractual, el proveedor deberá realizar una evaluación inicial de vulnerabilidades sobre los activos priorizados por la CRA, con el fin de establecer una línea base del servicio y presentar sus resultados al supervisor del contrato. - El proveedor deberá entregar como mínimo un informe ejecutivo con matriz de riesgo, tendencias, criticidad de hallazgos y principales

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Característica Requerida	Descripción del requerimiento
	vulnerabilidades identificadas, así como un informe técnico detallado por activo evaluado, vulnerabilidad identificada, evidencia, criticidad, exposición, impacto y recomendación de tratamiento. • La priorización de hallazgos deberá considerar, como mínimo, la criticidad del activo, su nivel de exposición, la probabilidad de explotación, el impacto operativo o de seguridad y la existencia de evidencia de explotación, cuando aplique. • El proveedor deberá efectuar seguimiento periódico al estado de los hallazgos identificados, reportando su condición, criticidad, evolución, tratamiento recomendado y estado general de gestión, sin que ello implique por sí mismo la ejecución material de la remediación sobre todos los activos evaluados. • Cuando una vulnerabilidad pueda ser tratada dentro del alcance técnico de los servicios efectivamente contratados y sobre plataformas administradas por el proveedor, este deberá documentar las acciones ejecutadas y dejar la respectiva evidencia técnica. En los demás casos, deberá formular la recomendación de tratamiento correspondiente para decisión y gestión de la CRA. • Cuando una vulnerabilidad no pueda ser corregida de manera inmediata por razones técnicas, operativas, presupuestales o de dependencia con terceros, el proveedor deberá documentar el riesgo residual, la medida compensatoria propuesta, la justificación y la recomendación de tratamiento para análisis y decisión de la CRA. • Toda vulnerabilidad reportada deberá contar con trazabilidad de gestión, incluyendo como mínimo identificación del activo, descripción del hallazgo, nivel de criticidad, evidencia disponible, tratamiento recomendado, estado de seguimiento y, cuando aplique, soporte de cierre o de aceptación del riesgo por parte de la CRA. • Las evidencias de cierre o tratamiento podrán consistir, según aplique, en validación técnica, capturas de configuración, respaldos, comandos ejecutados, registros de sistema, ticket cerrado en la herramienta definida por la CRA o evidencia equivalente verificable por el supervisor del contrato. • Toda aceptación de riesgo deberá quedar formalmente documentada por la CRA, indicando como mínimo el activo afectado, la vulnerabilidad identificada, el nivel de riesgo, la justificación, la medida compensatoria cuando exista y la fecha prevista de revisión. • Los hallazgos de vulnerabilidades deberán incorporarse en el informe mensual del servicio, con indicación de los principales riesgos identificados, el estado general de seguimiento y las recomendaciones priorizadas para su tratamiento. • El proveedor deberá conservar los resultados, evidencias técnicas, bitácoras de evaluación y soportes asociados al servicio con

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Característica Requerida	Descripción del requerimiento
	controles razonables de acceso, integridad y trazabilidad durante la ejecución contractual y por el período que defina la CRA para efectos de supervisión, auditoría y cierre del contrato.
Sitio de las pruebas	Local en las instalaciones de la CRA y/o de forma remota, de acuerdo con la naturaleza del activo, siempre que se garantice autorización previa, trazabilidad de la actividad y protección de la información institucional.

- c. Servicios de gestión, monitoreo, análisis, recuperación, continuidad y optimización de ciberseguridad

Nombre servicio	del	Continuidad del servicio y optimización de Ciberseguridad
Alcance Servicio	del	Prestación del servicio especializado orientado a fortalecer la continuidad operativa y la capacidad de prevención, detección, respuesta, recuperación y mejora frente a incidentes de seguridad de la información que puedan afectar los servicios críticos de la CRA. El servicio deberá articularse con el Inventario Técnico Oficial, con los componentes de monitoreo, gestión de vulnerabilidades, respaldos, recuperación y con los lineamientos institucionales de seguridad de la información y continuidad del negocio definidos por la CRA. El proveedor deberá ejecutar, apoyar y documentar las actividades técnicas y operativas requeridas para contribuir a la continuidad de los servicios críticos definidos por la CRA dentro del alcance contratado, incluyendo la aplicación de procedimientos operativos, la atención y recuperación frente a incidentes, la validación de criterios de recuperación, la generación de evidencias de prueba cuando aplique y la formulación de recomendaciones de mejora derivadas de los resultados obtenidos. Cuando la CRA disponga de planes, procedimientos o lineamientos institucionales de continuidad, respuesta a incidentes o recuperación, el proveedor deberá articular su actuación con dichos instrumentos. En caso de identificarse necesidades de ajuste sobre componentes bajo su alcance, deberá emitir las recomendaciones técnicas correspondientes, sin que ello implique la elaboración integral de documentación institucional por fuera del alcance contratado.
Unidad facturación del producto/servicio	de	Servicio Mes
Cantidad		3

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

DESCRIPCIÓN DEL REQUERIMIENTO

Característica Requerida	Descripción del requerimiento
Características técnicas	- Planificación, ejecución y documentación de actividades operativas orientadas a apoyar la continuidad de los servicios críticos definidos por la CRA, incluyendo dependencias técnicas, rutas de escalamiento, criterios de activación y acciones de recuperación dentro del alcance contratado. - Aplicación y articulación con los lineamientos, planes, procedimientos o instructivos de continuidad, recuperación y respuesta a incidentes que la CRA tenga definidos para los servicios priorizados, sin que ello implique la elaboración integral de documentación institucional por parte del contratista. - Validación operativa de criterios de recuperación sobre los servicios críticos cubiertos por el contrato, incluyendo prerequisites técnicos, secuencia general de restablecimiento, dependencias relevantes y verificación funcional básica posterior a la recuperación, cuando aplique. - Implementación de medidas de fortalecimiento de ciberseguridad orientadas a reducir la superficie de exposición y apoyar la continuidad operativa, incluyendo revisión de configuraciones de seguridad, apoyo en ajustes de firewall, controles de acceso, endurecimiento de configuraciones y articulación con los demás componentes efectivamente contratados. - Atención y gestión operativa de eventos o incidentes que puedan afectar la continuidad de los servicios críticos cubiertos por el contrato, con coordinación con la CRA, aplicación de procedimientos definidos y registro formal de las actuaciones ejecutadas. - Documentación de hallazgos, lecciones aprendidas y recomendaciones de mejora cuando ocurra un incidente relevante o cuando se ejecute una actividad de validación o recuperación sobre servicios críticos, incorporando como mínimo descripción del evento o ejercicio, impacto observado, acciones ejecutadas, resultado obtenido y recomendaciones derivadas. - Ejecución y documentación de actividades de validación o prueba sobre procedimientos de recuperación o continuidad respecto de los servicios críticos cubiertos por el contrato, cuando hayan sido previamente autorizadas por la CRA, de acuerdo con la naturaleza del servicio, la disponibilidad operativa y el alcance efectivamente contratado. - Cada actividad de validación, prueba autorizada o incidente relevante deberá generar registro o informe técnico con alcance, escenario ejecutado cuando aplique, resultados observados, incidencias identificadas y recomendaciones de mejora.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

	- El proveedor deberá entregar reporte mensual de continuidad y ciberseguridad con incidentes atendidos, eventos relevantes, actividades ejecutadas, hallazgos identificados, cambios relevantes y recomendaciones de mejora sobre los componentes cubiertos por el contrato. - Todas las actividades del componente deberán quedar soportadas en tickets, actas, bitácoras, reportes, evidencias técnicas y demás registros verificables, disponibles para supervisión, auditoría y seguimiento contractual.
Sitio de las pruebas	Local en las instalaciones de la CRA y/o de forma remota, según la naturaleza del escenario, siempre que exista autorización de la entidad, trazabilidad del ejercicio y protección adecuada de la información institucional.

13. Servicios de operación y soporte del software base y plataformas del Datacenter.

a. Software base de Datacenter, redes y ciberseguridad

Nombre servicio	del	Mantenimiento y soporte de software base
Alcance Servicio	del	Prestación del servicio de operación, administración, mantenimiento y soporte del software base y de las plataformas críticas de Datacenter definidas por la CRA, con el fin de contribuir a su disponibilidad, estabilidad, seguridad operativa, continuidad e integración con los demás componentes de la infraestructura tecnológica institucional. El servicio aplica, como mínimo, a los sistemas operativos de servidores, plataformas de virtualización en operación, herramientas de software base y plataformas tecnológicas de apoyo a la infraestructura institucional que la CRA identifique en el inventario técnico inicial y en sus controles de cambio, dentro de la cobertura efectivamente contratada. El alcance comprende actividades preventivas, correctivas y de soporte especializado sobre los componentes cubiertos, incluyendo revisión de configuraciones, aplicación controlada de actualizaciones y parches cuando resulten técnica y contractualmente procedentes, ajustes operativos, atención de incidentes, acompañamiento en ventanas de mantenimiento, documentación técnica y recomendaciones de mejora. No se entenderán incluidos dentro del alcance ordinario de este numeral el mantenimiento especializado de hardware, la reposición de partes, la adquisición o renovación de licencias, las actualizaciones mayores de versión, las migraciones de plataforma, la administración

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN ANEXO TÉCNICO	
---	---	--

	integral de herramientas de ciberseguridad que tengan numeral propio, ni los servicios de respaldo empresarial, continuidad, SOC/NOC, soporte nivel 3 y 4 o mantenimiento físico de datacenter ya contemplados en otros componentes del proceso. El detalle de los activos efectivamente cubiertos, sus versiones, criticidad, dependencias y condiciones particulares de operación deberá formalizarse en el inventario técnico inicial y administrarse mediante control de cambios durante la ejecución contractual, sin perjuicio del alcance mínimo aquí definido.
Unidad de facturación del producto/servicio	Servicio Mes
Cantidad	3

DESCRIPCIÓN DEL REQUERIMIENTO

Característica Requerida	Descripción del requerimiento
Características técnicas	• El proveedor deberá realizar la administración y soporte técnico del software base y de las plataformas cubiertas por el servicio, incluyendo sistemas operativos de servidores, hipervisores o plataformas de virtualización en operación y demás componentes de software base definidos por la CRA en el inventario técnico del contrato. • El proveedor deberá ejecutar actividades de mantenimiento preventivo y correctivo sobre los componentes cubiertos, tales como revisión de configuraciones, validación de servicios, ajuste de parámetros, aplicación controlada de parches y correcciones, y estabilización operativa conforme a la criticidad del activo y a las ventanas de mantenimiento aprobadas por la CRA. • El proveedor deberá identificar y atender fallas operativas, errores de configuración, degradaciones de desempeño, eventos relevantes y condiciones de riesgo que afecten la continuidad de los componentes cubiertos, dejando evidencia de la gestión realizada y de las recomendaciones emitidas. • El proveedor deberá apoyar actividades de restauración operativa de configuraciones y servicios cuando se presenten fallas, corrupciones, errores de operación o afectaciones de continuidad, siempre que dichas actividades correspondan al alcance del software base cubierto y a los mecanismos de respaldo disponibles en la CRA o en los demás componentes contratados. • El proveedor deberá mantener documentación técnica actualizada de los componentes cubiertos, incluyendo inventario operativo, configuraciones relevantes, cambios ejecutados, incidencias

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Característica Requerida	Descripción del requerimiento
	recurrentes, dependencias identificadas y recomendaciones técnicas para su adecuada administración. • El proveedor deberá apoyar a la CRA en la identificación de riesgos de obsolescencia, incompatibilidad, expiración de soporte del fabricante o limitaciones de licenciamiento que puedan afectar la operación de las plataformas cubiertas, emitiendo alertas y recomendaciones de tratamiento. • Toda intervención sobre los componentes cubiertos deberá quedar registrada en la herramienta de trazabilidad definida por la CRA, indicando activo afectado, tipo de actividad, justificación, ventana aprobada cuando aplique, evidencias, resultado y responsable de ejecución. • Cuando un caso requiera intervención especializada de fabricante, tercero, licenciamiento adicional, cambio mayor de versión, sustitución de hardware o atención correspondiente a otro numeral del contrato, el proveedor deberá escalarlo oportunamente y dejar registro de la gestión efectuada.
Servicio/soporte	• El servicio deberá prestarse mediante atención remota y, cuando la naturaleza del caso lo requiera, atención presencial previamente coordinada con la CRA, para la gestión de incidentes, problemas, requerimientos técnicos especializados, mantenimientos programados y demás intervenciones autorizadas sobre los componentes cubiertos. • La atención deberá ser brindada por personal con experiencia comprobable en administración de sistemas operativos, software base y plataformas de infraestructura tecnológica afines al alcance contratado, con posibilidad de escalamiento técnico interno o a fabricante cuando el caso lo requiera. • Toda solicitud deberá registrarse y gestionarse a través de la herramienta de trazabilidad definida por la CRA, con clasificación por tipo de caso, servicio o activo afectado, prioridad, severidad, bitácora de acciones, evidencias técnicas y cierre formal. • Los tiempos de respuesta y atención aplicables a este componente deberán sujetarse a la tabla unificada de ANS del Anexo Técnico o al instrumento que la sustituya, evitando reglas paralelas de 30 minutos, 2 horas o 24x7 automático dentro de este numeral. • El soporte cubierto por este numeral corresponde a la operación y mantenimiento del software base y de las plataformas cubiertas, y no implica por sí mismo disponibilidad presencial permanente, administración total de todos los activos del datacenter ni ejecución de proyectos de transformación tecnológica. • El proveedor deberá entregar informe mensual del servicio con actividades ejecutadas, incidentes y requerimientos atendidos,

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Característica Requerida	Descripción del requerimiento
	cambios realizados, hallazgos, riesgos identificados, pendientes y recomendaciones técnicas.

14. Administración, Operación y Soporte de la Plataforma Kaspersky Next EDR Optimum

ANEXO TÉCNICO

Obligaciones Nos. 14, 15 y 16

Alcance Técnico:

El contratista deberá prestar los servicios especializados para la administración, configuración, operación, monitoreo, mantenimiento y soporte técnico de la plataforma institucional **Kaspersky Next EDR Optimum**, garantizando la protección de las estaciones de trabajo, servidores y cuentas de Microsoft Office 365 definidas por la C.R.A., conforme a las licencias disponibles y a las políticas institucionales de seguridad de la información.

El servicio comprende la administración integral de la consola de gestión en la nube, la incorporación, configuración y administración de equipos protegidos, la instalación, actualización, migración y reconfiguración de agentes de seguridad, la administración de las políticas de protección, la supervisión permanente del estado de los equipos protegidos, el monitoreo de eventos de seguridad y la implementación de las configuraciones necesarias para mantener el correcto funcionamiento de la solución.

Asimismo, el contratista deberá implementar y administrar las políticas de ciberseguridad definidas por la C.R.A., configurando las reglas de protección para estaciones de trabajo, servidores y cuentas de Microsoft Office 365, administrando las funcionalidades de prevención, detección y respuesta propias de la plataforma Kaspersky Next EDR Optimum, de conformidad con las mejores prácticas del fabricante y las directrices impartidas por la supervisión del contrato.

Como parte del servicio, el contratista deberá mantener actualizada la plataforma, verificar periódicamente el estado de los agentes instalados, gestionar las alertas e incidentes generados por la solución, optimizar las políticas de seguridad, activar las funcionalidades disponibles conforme al licenciamiento contratado, generar reportes ejecutivos y técnicos, analizar los resultados obtenidos y formular recomendaciones orientadas al fortalecimiento continuo de la postura de ciberseguridad de la Entidad.

El contratista deberá garantizar que la totalidad de los equipos y cuentas objeto del servicio permanezcan protegidos, administrados desde la consola centralizada y con los agentes de seguridad operando correctamente durante toda la vigencia contractual. No hacen parte del alcance el suministro de licencias adicionales, la adquisición de equipos, la atención de incidentes de ciberseguridad distintos de los administrados por

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

la plataforma, los servicios SOC, la ejecución de análisis de vulnerabilidades, Ethical Hacking, Pentesting o actividades de respuesta forense digital.

Actividades mínimas:

El contratista deberá ejecutar como mínimo las siguientes actividades:

Administración de la plataforma:

- Administrar la consola Kaspersky Next EDR Optimum.
- Incorporar y retirar equipos de la consola cuando sea requerido.
- Administrar estaciones de trabajo, servidores y cuentas Microsoft Office 365 protegidas.
- Instalar, actualizar y reconfigurar agentes de seguridad.
- Verificar permanentemente el estado de los agentes instalados.
- Administrar usuarios, grupos y permisos de la plataforma.
- Mantener actualizadas las versiones de los componentes administrados.
- Realizar respaldo de la configuración de la consola cuando se efectúen cambios relevantes.

Administración de políticas de ciberseguridad:

- Configurar y administrar políticas de seguridad.
- Configurar reglas de protección para Endpoints y Servidores.
- Configurar políticas de protección para Microsoft Office 365.
- Administrar exclusiones autorizadas.
- Configurar perfiles de análisis.
- Administrar reglas de cuarentena.
- Configurar políticas de actualización.
- Implementar las políticas de seguridad definidas por la C.R.A.
- Optimizar continuamente las configuraciones de protección.

Operación y monitoreo:

- Monitorear permanentemente el estado de la plataforma.
- Monitorear eventos de seguridad.
- Gestionar alertas generadas por la solución.
- Analizar incidentes detectados por el EDR.
- Verificar el cumplimiento de las políticas implementadas.
- Generar reportes técnicos y ejecutivos.
- Formular recomendaciones para fortalecer la seguridad institucional.
- Ejecutar ajustes autorizados por la supervisión del contrato.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Entregable	Oportunidad
Documento de diagnóstico inicial de la plataforma Kaspersky Next EDR Optimum, incluyendo inventario de equipos protegidos, estado de la consola, políticas existentes, agentes instalados y hallazgos identificados.	Dentro de los diez (10) días hábiles siguientes al acta de inicio.
Documento de configuración y administración de la plataforma, incluyendo políticas implementadas, estructura de grupos, configuración de protección, exclusiones autorizadas y parámetros de operación.	Una (1) vez y cada vez que se presenten cambios relevantes.
Informe mensual de administración de la plataforma, indicando equipos protegidos, estado de agentes, eventos relevantes, incidentes atendidos, políticas modificadas, actualizaciones realizadas y recomendaciones técnicas.	Mensual.
Reporte mensual de protección de Endpoints, Servidores y Microsoft Office 365, incluyendo estadísticas de amenazas detectadas, acciones ejecutadas, equipos sin protección, cumplimiento de actualizaciones y estado general de la plataforma.	Mensual.
Evidencias de instalación, actualización o reconfiguración de agentes cuando se incorporen nuevos equipos o se ejecuten cambios relevantes.	Cada vez que aplique.
Informe final del servicio, incluyendo configuración vigente, inventario actualizado, estado de protección, políticas implementadas, estadísticas consolidadas de operación, incidentes relevantes y recomendaciones para la continuidad del servicio.	Al finalizar el contrato.

15. Servicio integral de seguridad y protección de sitios web institucionales.

Nombre del servicio	Servicio integral de seguridad y protección de sitios web institucionales de la CRA.
Alcance del Servicio	Prestación del servicio especializado para la protección, aseguramiento, monitoreo, soporte y administración de la publicación segura de los sitios y aplicativos webs institucionales de la CRA, con el fin de garantizar su disponibilidad, integridad, continuidad operativa y protección frente a amenazas de seguridad informática asociadas a la exposición de servicios web en Internet.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

El servicio comprende, como mínimo, la implementación, configuración, puesta en operación, administración y soporte de mecanismos de protección tipo Web Application Firewall (WAF) o tecnología equivalente, la gestión de certificados digitales SSL/TLS requeridos para la operación segura de los sitios y aplicativos web institucionales, el monitoreo continuo de disponibilidad y eventos de seguridad, la gestión de alertas, la atención de incidentes asociados a la publicación web y la entrega de reportes técnicos y ejecutivos sobre el estado del servicio. El alcance del servicio aplicará sobre los dominios, subdominios, sitios y aplicativos webs institucionales que defina la CRA dentro del inventario técnico oficial y mediante los mecanismos de control de cambios que se adopten durante la ejecución contractual. El detalle técnico de dichos activos, así como sus configuraciones, tipos de certificados, dependencias y condiciones particulares de publicación, tendrá el tratamiento de información reservada o controlada que defina la CRA. La solución propuesta por el contratista deberá corresponder a una plataforma o servicio gestionado de protección web de nivel empresarial, equivalente o superior en capacidades de seguridad, disponibilidad, trazabilidad y administración a las soluciones reconocidas del mercado para este tipo de servicio. En todo caso, la herramienta o plataforma utilizada deberá cumplir los requerimientos funcionales, técnicos y de seguridad exigidos por la CRA en el presente Anexo, sin que ello implique limitación indebida a una marca o fabricante específico.	
Unidad de facturación del producto/servicio	de Servicio Mes
Cantidad	6

DESCRIPCIÓN DEL REQUERIMIENTO

Característica Requerida	Descripción del requerimiento
Características técnicas	El proveedor deberá implementar y operar un esquema de protección de sitios y aplicativos webs que asegure la inspección, filtrado y control del tráfico HTTP/HTTPS dirigido a los activos cubiertos por el servicio, evitando rutas de bypass no autorizadas y garantizando que la publicación externa quede protegida por el mecanismo de seguridad dispuesto para tal fin.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Característica Requerida	Descripción del requerimiento
	• La solución deberá permitir la detección, análisis y bloqueo de amenazas comunes contra aplicaciones web, incluyendo como mínimo intentos de Cross-Site Scripting (XSS), inyección SQL, inclusión de archivos locales o remotos, traversal de directorios, carga maliciosa de archivos, explotación automatizada y demás patrones de ataque equivalentes a los riesgos contemplados en referentes reconocidos para seguridad de aplicaciones web. • La herramienta o servicio utilizado deberá soportar políticas diferenciadas por sitio, aplicativo, URL, servicio o nivel de exposición, y deberá permitir ajustes graduales de seguridad, listas de confianza o exclusión controladas, manejo de excepciones autorizadas, perfiles de protección y mecanismos para reducción de falsos positivos, sin afectar indebidamente la operación institucional. • El contratista deberá garantizar que la solución utilizada permita la generación, conservación y consulta de registros detallados de eventos, accesos, bloqueos, alertas, cambios de configuración y demás actividades relevantes para la operación del servicio, con controles de acceso, integridad, trazabilidad y disponibilidad para verificación por parte de la CRA durante la ejecución contractual y el tiempo de retención que esta defina. • El proveedor deberá garantizar la integración del servicio con los componentes de seguridad perimetral y de monitoreo que la CRA tenga definidos, incluyendo, cuando aplique, firewalls, herramientas de análisis de eventos, plataformas de correlación, mecanismos de notificación y demás componentes de la arquitectura institucional de ciberseguridad. • El servicio deberá incluir la gestión integral de certificados digitales SSL/TLS requeridos por la CRA para los sitios y aplicativos institucionales cubiertos, comprendiendo como mínimo la solicitud, emisión, instalación, configuración, renovación, reemplazo, seguimiento de vigencias y atención de incidentes asociados a dichos certificados, de conformidad con las políticas y necesidades definidas por la Entidad. • Para efectos de estructuración de la oferta y ejecución contractual, la CRA requiere la provisión, gestión, renovación, instalación y soporte de certificados digitales SSL/TLS tipo DV (Domain Validation) para los dominios, subdominios, sitios y aplicativos webs institucionales cubiertos por el presente Anexo. Este

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Característica Requerida	Descripción del requerimiento
	requerimiento aplica como estándar general de la Entidad, en consideración a que los servicios web objeto del contrato corresponden mayoritariamente a aplicativos y portales de uso institucional o de acceso controlado. • El contratista deberá contemplar dentro de su propuesta el suministro y administración de certificados DV para hasta nueve (9) dominios y/o aplicativos webs institucionales definidos por la CRA. En caso de que durante la ejecución la CRA determine justificadamente la necesidad de un certificado de mayor nivel de validación para un activo específico, dicha necesidad deberá ser gestionada mediante control de cambios o por el mecanismo contractual que corresponda, previa sustentación técnica y presupuestal. • El proveedor deberá asegurar que la plataforma o herramienta utilizada disponga de capacidades de monitoreo permanente, generación de alertas, consulta de estado, tableros de seguimiento, reporte de eventos relevantes, revisión de capacidad y análisis de comportamiento del tráfico, de forma que la CRA pueda supervisar de manera efectiva la prestación del servicio. • La CRA deberá contar durante toda la ejecución contractual con acceso de consulta permanente a la consola, tablero, portal o mecanismo equivalente que permita verificar el estado del servicio, la vigencia de los certificados, las alertas generadas, los eventos de seguridad identificados, las reglas activas, las actividades ejecutadas por el proveedor y, cuando técnicamente aplique, las acciones de restauración, reversión o restablecimiento asociadas a la publicación o protección de los activos cubiertos. • El contratista deberá garantizar que las credenciales, perfiles y accesos asociados al servicio se administren bajo principios de mínimo privilegio, trazabilidad y segregación de funciones, y que la CRA conserve en todo momento la posibilidad de supervisar, auditar y validar las actividades realizadas sobre la plataforma o servicio suministrado. • El proveedor deberá ejecutar, con la periodicidad que defina la CRA o como mínimo de forma trimestral, actividades de revisión, validación o prueba controlada de la efectividad del servicio de protección web, documentando resultados, hallazgos, falsos positivos relevantes, acciones de ajuste y recomendaciones de mejora.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Característica Requerida	Descripción del requerimiento
	El contratista deberá entregar informe mensual técnico y ejecutivo del servicio, incluyendo como mínimo estado general de los sitios y aplicativos protegidos, eventos e incidentes relevantes, certificados instalados y próximos a vencer, cambios realizados, alertas atendidas, hallazgos de seguridad, disponibilidad del servicio, riesgos identificados, recomendaciones y plan de mejora cuando aplique.
Servicio/soporte	- El servicio deberá prestarse en modalidad 7x24 para la atención de incidentes, eventos de seguridad, alertas críticas, indisponibilidades, fallas de publicación, problemas asociados a certificados digitales y demás situaciones que afecten la disponibilidad o seguridad de los sitios y aplicativos webs institucionales cubiertos. - Toda solicitud, incidente, requerimiento o evento relacionado con este servicio deberá quedar registrado en la herramienta de trazabilidad definida por la CRA, con su respectiva clasificación, prioridad, descripción del caso, acciones ejecutadas, evidencias, tiempos de atención y cierre formal. - El proveedor deberá atender y gestionar los casos de acuerdo con los niveles de prioridad y tiempos de respuesta definidos por la CRA para servicios críticos de infraestructura y seguridad, sin perjuicio de los ANS particulares que se establezcan en la tabla unificada del contrato. - El contratista deberá brindar acompañamiento técnico a la CRA en actividades de validación de publicación, ajustes de reglas, atención de incidentes, verificación de eventos, revisión de certificados, recuperación operativa y restablecimiento del servicio cuando se presenten fallas o bloqueos que afecten la operación institucional. - Durante la ejecución contractual, el proveedor deberá realizar transferencia de conocimiento al personal designado por la CRA sobre la operación básica del servicio, consulta de tableros, interpretación de alertas, verificación de vigencias, validación de eventos y procedimientos de escalamiento.
Sitio de las pruebas	Local en las instalaciones de la CRA y/o de forma remota, cuando la naturaleza del servicio lo permita y la CRA lo autorice.

16. Soporte Especializado Nivel 3 y Nivel 4 para Datacenter, Redes y Seguridad de la Información (gestión de incidentes, problemas y eventos, escalamiento técnico especializado bajo demanda).

Obligación No. 16

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Operación de la Mesa de Servicios para la Gestión de Incidentes, Requerimientos, Solicitudes y Cambios

Alcance Técnico:

El contratista deberá disponer y mantener durante toda la ejecución del contrato un equipo de profesionales con las competencias técnicas requeridas para atender integralmente los incidentes, requerimientos, solicitudes de servicio y cambios relacionados con la infraestructura tecnológica, telecomunicaciones, ciberseguridad, plataformas, servicios y demás componentes objeto del contrato.

La atención de los servicios deberá realizarse **exclusivamente a través de la Mesa de Servicios institucional Kaía**, utilizando los flujos, categorías, prioridades, niveles de atención y procedimientos definidos por la C.R.A. En situaciones de contingencia que impidan el registro inmediato en la plataforma, el contratista podrá atender los casos mediante canales alternos autorizados por la Entidad (telefónico, correo electrónico o atención en sitio), garantizando la posterior regularización y documentación completa del caso en Kaía.

El contratista será responsable de registrar la totalidad de las actividades ejecutadas durante la atención de cada caso, manteniendo la trazabilidad completa desde la apertura hasta el cierre, incluyendo diagnóstico, análisis de causa, actividades ejecutadas, evidencias técnicas, tiempos de atención, escalamientos realizados, solución implementada y validación del usuario o del supervisor cuando corresponda.

El servicio comprende la recepción, clasificación, priorización, asignación, atención, seguimiento, escalamiento, resolución y cierre de los casos registrados, garantizando el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) establecidos por la C.R.A., así como la disponibilidad del personal técnico necesario para atender eventos críticos, emergencias o contingencias que requieran intervención remota o presencial, incluyendo disponibilidad **7x24** para la atención de incidentes críticos cuando así lo exijan los niveles de servicio definidos en el contrato.

El contratista deberá generar la información necesaria para el seguimiento del servicio, asegurando la disponibilidad de indicadores de gestión, reportes estadísticos, historial de atención, trazabilidad de las actuaciones y evidencia documental que permita verificar el cumplimiento de las obligaciones contractuales.

Actividades mínimas:

El contratista deberá ejecutar, como mínimo, las siguientes actividades:

- Recibir, registrar, clasificar y priorizar los incidentes, requerimientos, solicitudes y cambios.
- Gestionar la atención de los casos mediante la Mesa de Servicios Kaía.
- Asignar los casos al recurso técnico competente según la naturaleza del servicio.
- Atender los incidentes dentro de los tiempos de respuesta y solución establecidos en los ANS.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

- Ejecutar actividades de diagnóstico, análisis y solución de los casos reportados.
- Escalar oportunamente los casos que requieran intervención especializada.
- Realizar atención remota o presencial cuando la naturaleza del incidente lo requiera.
- Mantener comunicación permanente con el supervisor y los usuarios durante la atención de los casos.
- Registrar todas las actuaciones realizadas dentro de la plataforma Kaía.
- Adjuntar las evidencias técnicas correspondientes a cada intervención.
- Documentar la solución implementada y la causa del incidente cuando sea identificada.
- Cerrar formalmente los casos una vez validada la solución.
- Generar reportes e indicadores de gestión del servicio.
- Garantizar disponibilidad del equipo técnico para la atención de contingencias conforme a los ANS establecidos.

Nombre del servicio	Soporte Especializado Nivel 3 y Nivel 4
Alcance del Servicio	Prestación de soporte técnico especializado de niveles III y IV para la infraestructura tecnológica institucional de la CRA asociada a datacenter, procesamiento, almacenamiento, virtualización, redes y seguridad de la información, orientado a la atención de incidentes, problemas y eventos de alta complejidad técnica que requieran diagnóstico experto, análisis especializado, escalamiento técnico, recuperación operativa o recomendación de solución sobre componentes críticos definidos por la CRA. El servicio se prestará como capacidad de escalamiento especializado respecto de los demás componentes operativos del contrato, para intervenir cuando la naturaleza, severidad o complejidad del caso exceda la gestión ordinaria de los frentes de monitoreo, administración o soporte regular. En consecuencia, no constituye una mesa de ayuda, ni un servicio de atención a usuario final, ni reemplaza la operación cotidiana de los demás numerales del Anexo Técnico. El alcance cubre atención remota y, cuando la criticidad del caso o la naturaleza de la intervención lo requieran, atención en sitio previamente coordinada con la CRA, así como interacción con fabricantes o terceros cuando ello resulte necesario para la adecuada gestión del caso dentro del alcance contractual. Se excluyen expresamente del alcance de este servicio la atención de niveles I y II, el soporte a estaciones de trabajo, portátiles, periféricos, herramientas ofimáticas, software de productividad y aplicaciones de negocio, salvo cuando la causa raíz del evento corresponda de manera verificable a un componente de infraestructura, datacenter, red o ciberseguridad cubierto por este numeral.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Unidad de facturación del producto/servicio	Servicio Mes
Cantidad	3

DESCRIPCIÓN DEL REQUERIMIENTO

Característica Requerida	Descripción del requerimiento
Características técnicas	• El proveedor deberá atender incidentes, problemas y eventos de alta complejidad técnica sobre los componentes cubiertos, realizando diagnóstico especializado, análisis de causa probable, formulación de acciones de contención o recuperación, ejecución de actividades autorizadas y emisión de recomendaciones técnicas para restablecimiento o estabilización del servicio. • El proveedor deberá actuar como nivel de escalamiento especializado para los demás componentes técnicos del contrato, cuando estos identifiquen casos cuya atención exceda su capacidad operativa ordinaria o requiera conocimientos avanzados sobre infraestructura crítica. • El proveedor deberá intervenir, dentro del alcance autorizado, sobre componentes de datacenter, virtualización, procesamiento, almacenamiento, redes y seguridad perimetral definidos por la CRA en el inventario técnico, priorizando aquellos servicios o activos cuya afectación comprometa la continuidad operativa institucional. • Toda intervención deberá quedar soportada con registro del incidente o problema, diagnóstico realizado, activo afectado, análisis técnico, acciones ejecutadas, evidencias, resultado obtenido, necesidad de escalamiento adicional cuando aplique y recomendaciones emitidas para la CRA. • Cuando el caso requiera interacción con fabricante, tercero o proveedor de licencias o soporte externo, el contratista deberá realizar el escalamiento correspondiente, acompañar técnicamente la gestión y dejar trazabilidad de las actuaciones efectuadas dentro del alcance de este componente. • El proveedor deberá emitir concepto técnico cuando identifique limitaciones de soporte, obsolescencia, incompatibilidades, fallas recurrentes, riesgos de capacidad o debilidades estructurales que no puedan resolverse de manera definitiva dentro de la atención puntual del caso. • El componente no implica por sí mismo la obligación de ejecutar proyectos de modernización, migraciones mayores, sustitución

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Característica Requerida	Descripción del requerimiento
	de plataformas, adquisición de licencias, renovación de soportes de fabricante, remediación estructural total ni administración permanente de todos los activos cubiertos por otros numerales del contrato. El proveedor deberá consolidar en informe mensual los casos escalados, tiempos de atención, actividades ejecutadas, hallazgos recurrentes, riesgos identificados, recomendaciones y necesidades de mejora o tratamiento por parte de la CRA.
Servicio/soporte	- El servicio deberá prestarse mediante atención remota y, cuando la criticidad del caso y la naturaleza de la intervención lo requieran, mediante atención presencial previamente coordinada con la CRA, conforme a la tabla unificada de ANS del Anexo Técnico o al instrumento que la sustituya. - La activación del soporte nivel III y IV deberá producirse a partir de incidentes, problemas o eventos debidamente registrados y escalados por la CRA o por los componentes técnicos del contrato que correspondan, con identificación del activo afectado, descripción del caso, impacto observado y prioridad asignada. - Toda atención deberá quedar registrada en la herramienta de trazabilidad definida por la CRA o en el mecanismo acordado entre las partes, incluyendo fecha y hora de apertura, profesional asignado, análisis técnico, acciones ejecutadas, escalamiento realizado, tiempos de atención y cierre del caso. - Los tiempos de respuesta y atención aplicables a este componente deberán sujetarse a la tabla general de prioridades y ANS del proceso, evitando expresiones abiertas como disponibilidad inmediata, soporte ilimitado o cobertura irrestricta 7x24 si ello no está respaldado por el presupuesto y por el modelo real del servicio. - El soporte cubierto por este numeral corresponde a la atención especializada de casos complejos sobre infraestructura crítica y no implica presencia permanente en sitio, operación continua del datacenter ni atención indistinta de cualquier requerimiento tecnológico de la CRA.

Entregable	Oportunidad
Procedimiento operativo para la gestión de incidentes, requerimientos, solicitudes y cambios, alineado con la operación de la Mesa de Servicios Kaía.	Dentro de los diez (10) días hábiles siguientes al acta de inicio.
Evidencia del registro completo de todos los casos atendidos en	Permanente.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Entregable	Oportunidad
la Mesa de Servicios, incluyendo trazabilidad, tiempos de atención, actividades ejecutadas y cierre formal.	
Informe mensual de operación de la Mesa de Servicios, indicando número de casos atendidos, clasificación por tipo, cumplimiento de ANS, tiempos de respuesta, tiempos de solución, incidentes críticos, casos escalados y oportunidades de mejora.	Mensual.
Reporte consolidado de indicadores del servicio, incluyendo cumplimiento de los niveles de servicio, análisis de tendencias, reincidencias y desempeño operativo.	Mensual.
Informe de contingencias atendidas mediante canales alternos, indicando causa de la contingencia, fecha de regularización y evidencia del registro posterior en Kaía.	Cuando aplique.
Informe final consolidado de la operación de la Mesa de Servicios, incluyendo estadísticas de atención, cumplimiento contractual, lecciones aprendidas y recomendaciones de mejora.	Al finalizar el contrato.

Criterios de aceptación:

La obligación se entenderá cumplida cuando:

- El 100 % de los incidentes, requerimientos, solicitudes y cambios relacionados con el contrato se encuentren registrados en la Mesa de Servicios Kaía o hayan sido regularizados cuando su atención inicial se haya realizado mediante un canal alternativo autorizado.
- Cada caso cuente con trazabilidad completa, incluyendo registro de apertura, clasificación, diagnóstico, actividades ejecutadas, evidencias técnicas, tiempos de atención y cierre formal.
- Se cumplan los tiempos de primera respuesta y de resolución establecidos en los ANS del contrato para cada nivel de criticidad.
- Los incidentes críticos sean atendidos conforme al esquema de disponibilidad definido por la Entidad.
- Los informes mensuales reflejen el desempeño de la Mesa de Servicios y el cumplimiento de los indicadores establecidos.
- El supervisor del contrato valide el cumplimiento de los niveles de servicio y emita el recibido a satisfacción de los entregables.

B. REQUISITOS DE CUMPLIMIENTO

Los siguientes requisitos de cumplimiento aplican de manera transversal a todos los servicios contratados en el presente Anexo Técnico, sin perjuicio de los indicadores, niveles de servicio, entregables o condiciones particulares que se establezcan de forma específica para algún componente. En caso de existir diferencia entre un requisito general y uno

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

particular, prevalecerá el más estricto o el que otorgue mayor nivel de protección, disponibilidad, trazabilidad o control para la CRA.

El contratista deberá medir, consolidar, reportar y soportar el cumplimiento de los indicadores mínimos, los Acuerdos de Nivel de Servicio (ANS) y las obligaciones de reporte definidas en esta sección, con base en información verificable, trazable y auditable por parte de la CRA.

Sin perjuicio de los demás mecanismos contractuales aplicables, cuando en un período mensual se verifique incumplimiento de los ANS o KPI exigibles a este numeral por causas atribuibles al contratista, la CRA podrá aplicar el descuento o penalidad correspondiente sobre el pago del componente afectado, conforme a la verificación efectuada por la supervisión y a la tabla o regla de descuento definida contractualmente. Para esta evaluación no se contabilizarán las indisponibilidades o desviaciones originadas en ventanas de mantenimiento previamente aprobadas, actualizaciones programadas, eventos de fuerza mayor, causas fortuitas, hechos de terceros o condiciones no imputables al contratista, siempre que dichas circunstancias se encuentren debidamente soportadas y validadas por la supervisión. En caso de incidentes de seguridad o ciberataques, la exoneración solo procederá cuando del análisis técnico y de causa raíz se concluya que el evento no fue favorecido por incumplimientos, omisiones o debilidades de gestión atribuibles al contratista dentro del alcance del presente servicio.

1. Indicadores mínimos (KPI) y fuentes de verificación:

El contratista deberá medir, consolidar, reportar y soportar mensualmente los indicadores mínimos de desempeño definidos en el presente numeral, los cuales aplican de manera transversal a los servicios objeto del contrato, sin perjuicio de los indicadores específicos que la CRA establezca para algún componente particular. Los resultados reportados deberán basarse en información verificable, trazable y auditable, proveniente de las herramientas de monitoreo, consolas de administración, sistemas de tickets, bitácoras, actas, registros de seguridad, reportes automáticos y demás fuentes técnicas aplicables.

Los indicadores aquí definidos tendrán como finalidad permitir a la CRA verificar el comportamiento general del servicio, evaluar el cumplimiento de las obligaciones técnicas y contar con información suficiente para la supervisión, control, seguimiento y toma de decisiones durante la ejecución contractual. Ningún indicador se entenderá cumplido por simple manifestación del contratista; en todos los casos deberá existir evidencia suficiente, consistente y verificable.

La medición de los indicadores deberá considerar el alcance real de los servicios prestados durante el período reportado, los activos efectivamente cubiertos, las ventanas de mantenimiento aprobadas, los cambios autorizados, las contingencias ocurridas y las condiciones operativas particulares que hayan incidido en la prestación del servicio. Cuando un indicador no aplique a un servicio o período determinado, el contratista deberá justificarlo de manera expresa en el informe mensual.

La CRA podrá complementar, ajustar o desagregar estos indicadores durante la ejecución

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

contractual, cuando ello resulte necesario para mejorar la supervisión del contrato, armonizar la medición entre servicios o responder a cambios del inventario técnico, siempre que dichos ajustes no alteren de manera sustancial el objeto contractual y queden formalizados mediante el mecanismo que defina la Entidad.

Tabla. Indicadores mínimos (KPI) y fuentes de verificación

Indicador	Definición	Meta mínima	Periodicidad	Fuente mínima de verificación
Disponibilidad del servicio	Porcentaje de tiempo en que los servicios, plataformas o componentes cubiertos por el contrato permanecen disponibles durante el período evaluado, descontando únicamente las ventanas de mantenimiento previamente aprobadas por la CRA.	Según ANS aplicable por criticidad	Mensual	Herramientas de monitoreo, reportes de consola, bitácoras, tickets e informe mensual
Cumplimiento de atención y solución dentro de ANS	Porcentaje de incidentes, requerimientos, problemas o eventos atendidos y cerrados dentro de los tiempos de respuesta y solución definidos en el contrato.	Igual o superior al 95%	Mensual	Herramienta de trazabilidad definida por la CRA, tickets, registros de atención, bitácoras e informe mensual
Cumplimiento del plan de mantenimiento	Porcentaje de actividades de mantenimiento preventivo, correctivo programado, revisión técnica, hardening, actualización o intervención planificada ejecutadas frente a las programadas para el período.	Igual o superior al 90%	Mensual	Cronograma aprobado, actas de ejecución, bitácoras de cambio, reportes técnicos y evidencias
Cumplimiento del plan de actualizaciones y parches	Porcentaje de parches, actualizaciones y correcciones aprobadas o priorizadas para el período que fueron ejecutadas efectivamente sobre los componentes	Igual o superior al 90%	Mensual	Reportes de cambio, evidencias de instalación, bitácoras, reportes de consola e

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Indicador	Definición	Meta mínima	Periodicidad	Fuente mínima de verificación
	cubiertos.			informe mensual
Ejecución de respaldos programados	Porcentaje de copias de seguridad programadas que fueron ejecutadas satisfactoriamente durante el período, incluyendo las asociadas a configuraciones, datos o componentes críticos según aplique.	Igual o superior al 98%	Mensual	Consola de respaldo, logs, reportes automáticos, bitácoras e informe mensual
Efectividad de restauraciones o pruebas de recuperación	Porcentaje de restauraciones o pruebas de recuperación de ejecutadas satisfactoriamente frente a las programadas, requeridas o instruidas por la CRA durante el período.	Igual o superior al 95%	Mensual o cuando aplique	Actas de prueba, evidencias técnicas, reportes de consola, tickets y registros de validación
Gestión de vulnerabilidades	Porcentaje de vulnerabilidades críticas y altas gestionadas, mitigadas, remediadas o formalmente tratadas dentro de los tiempos definidos por la CRA o en el plan de remediación aprobado.	Igual o superior al 90%	Mensual	Reportes de escaneo, matriz de riesgo, plan de remediación, tickets y evidencias de cierre
Registro y cierre de incidentes de seguridad	Porcentaje de incidentes de seguridad atendidos con registro formal, trazabilidad, análisis, acciones ejecutadas y cierre documentado conforme al procedimiento definido por la CRA.	100% de los incidentes gestionados	Mensual	Tickets, informes de incidentes, análisis de causa raíz, logs y evidencias de cierre
Entrega oportuna del informe mensual	Cumplimiento en la entrega del informe mensual consolidado dentro del plazo definido por la CRA y con el contenido mínimo exigido	100%	Mensual	Radicación, correo de entrega, constancia de recibido o medio definido por la

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Indicador	Definición	Meta mínima	Periodicidad	Fuente mínima de verificación
	en el Anexo Técnico.			CRA

Para efectos de interpretación y supervisión, las metas mínimas aquí definidas corresponden a umbrales base de cumplimiento y no limitan la posibilidad de que la CRA establezca, para determinados servicios o componentes, metas superiores o indicadores complementarios de acuerdo con su criticidad, exposición, impacto institucional o condiciones particulares de operación.

Cuando un indicador presente desviaciones, incumplimientos, tendencia negativa o variaciones relevantes frente a la meta esperada, el contratista deberá explicarlo expresamente en el informe mensual, indicando como mínimo las causas identificadas, el impacto generado, las acciones correctivas o preventivas adoptadas y la fecha estimada de estabilización o cierre.

Las fuentes mínimas de verificación señaladas en la tabla no excluyen otras evidencias que la CRA considere pertinentes. En todos los casos, prevalecerá la evidencia objetiva, trazable y verificable sobre cualquier explicación narrativa no soportada.

El cumplimiento de los KPI aplicables al presente numeral será objeto de verificación mensual por parte de la CRA, con base en registros trazables, evidencias técnicas e informe del período. Cuando se verifique incumplimiento atribuible al contratista, la CRA podrá aplicar el descuento o penalidad correspondiente sobre el pago del componente afectado, sin perjuicio de las demás medidas contractuales a que haya lugar. Para esta evaluación no se contabilizarán como incumplimiento las indisponibilidades o desviaciones derivadas de mantenimientos programados previamente aprobados, actualizaciones autorizadas, eventos de fuerza mayor, caso fortuito, hechos de terceros o situaciones no imputables al contratista, siempre que dichas circunstancias se encuentren debidamente soportadas y validadas por la supervisión. En caso de incidentes de seguridad o ciberataques, la exoneración solo procederá cuando del análisis técnico y de causa raíz se concluya que el evento no fue favorecido por incumplimientos, omisiones o debilidades de gestión atribuibles al contratista dentro del alcance del presente servicio.

2. Acuerdos de Nivel de Servicio (ANS) mínimos

Los Acuerdos de Nivel de Servicio definidos en el presente numeral aplican de manera transversal a los servicios objeto del contrato, sin perjuicio de que para determinados componentes la CRA establezca condiciones particulares más exigentes de acuerdo con su criticidad, exposición, impacto operativo o dependencia institucional. En caso de coexistir un ANS general y uno particular para un mismo servicio o evento, prevalecerá el más estricto.

Los tiempos de respuesta y de solución deberán medirse sobre la base de registros formales, verificables y trazables en la herramienta dispuesta por la CRA para la gestión de

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

solicitudes, incidentes, problemas, eventos o requerimientos técnicos. Cuando un evento sea identificado de manera proactiva por el contratista, el tiempo se contará a partir del momento de su detección debidamente soportada; cuando sea reportado por la CRA, el tiempo se contará a partir del registro formal del caso en la herramienta de trazabilidad o por el canal autorizado por la Entidad.

Para efectos de aplicación de los ANS, el contratista deberá clasificar los casos conforme a la prioridad definida en este numeral, registrar la hora de detección o recepción, documentar las acciones ejecutadas, dejar evidencia del escalamiento cuando aplique y formalizar el cierre con el respectivo soporte técnico. Toda clasificación inadecuada, cierre sin evidencia, reapertura recurrente o traslado improcedente de casos podrá ser revisado por la CRA para efectos de medición del cumplimiento.

Los tiempos aquí definidos corresponden a umbrales mínimos exigibles. El contratista deberá organizar sus recursos humanos, herramientas, canales, escalamiento técnico y capacidad de atención remota o presencial de forma que asegure su cumplimiento durante toda la ejecución contractual.

Tabla. Acuerdos de Nivel de Servicio (ANS) mínimos

Prioridad	Descripción general	Tiempo máximo de respuesta	Tiempo máximo de solución	Observaciones
P1	Incidente crítico con afectación total o severa sobre servicios críticos, seguridad de la información, continuidad operativa, conectividad principal, publicación de servicios institucionales o plataformas esenciales para la operación de la CRA.	1 hora	4 horas	Atención 7x24. Requiere escalamiento inmediato, seguimiento continuo y comunicación al supervisor o responsable definido por la CRA.
P2	Incidente alto con afectación parcial importante, degradación significativa del servicio, riesgo alto de indisponibilidad o afectación relevante a componentes institucionales que exigen atención prioritaria.	4 horas	8 horas o 1 día calendario	Atención prioritaria. Puede requerir intervención remota inmediata y atención en sitio cuando la naturaleza del caso lo exija.
P3	Incidente medio o requerimiento técnico con impacto controlado, sin interrupción total del servicio, pero que requiere	8 horas hábiles	3 días hábiles	Aplica a fallas no críticas, ajustes técnicos, errores controlados y requerimientos

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Prioridad	Descripción general	Tiempo máximo de respuesta	Tiempo máximo de solución	Observaciones
	intervención especializada para evitar afectaciones mayores o corregir fallas no críticas.			especializados.
P4	Solicitud de bajo impacto, requerimiento programable, ajuste menor, actividad preventiva, consulta técnica o intervención que puede ser atendida bajo agenda acordada con la CRA.	1 día hábil	5 días hábiles o según cronograma aprobado	Su atención podrá coordinarse conforme a ventana de mantenimiento, agenda o programación previamente autorizada.

Para efectos de disponibilidad, la CRA adoptará una medición diferenciada por criticidad del servicio, con el fin de evitar metas uniformes que no reflejen la realidad operativa de los distintos componentes del contrato. Como criterio mínimo, la disponibilidad mensual exigible será igual o superior al noventa y nueve coma cinco por ciento (99,5 %) para servicios críticos y al noventa y nueve coma cero por ciento (99,0 %) para servicios de soporte o de criticidad media o baja, salvo que un componente particular exija un valor superior.

No se contabilizarán como indisponibilidad, para efectos del cálculo de ANS, las ventanas de mantenimiento previamente aprobadas por la CRA, siempre que hayan sido programadas, comunicadas, ejecutadas dentro del horario autorizado y debidamente documentadas. Tampoco se considerarán incumplimiento los eventos atribuibles exclusivamente a terceros o a decisiones operativas de la CRA, siempre que dicha condición esté técnica y documentalmente demostrada por el contratista y validada por la supervisión.

Cuando un caso no pueda resolverse dentro del tiempo objetivo definido para su prioridad, el contratista deberá escalarlo oportunamente, informar a la CRA antes del vencimiento del ANS, indicar las causas que impiden el cierre, reportar el impacto identificado y presentar un plan de acción con tiempo estimado de solución. La ausencia de comunicación oportuna no exime el incumplimiento del ANS.

Todo incumplimiento de ANS deberá quedar expresamente reportado en el informe mensual, indicando como mínimo el número del caso, servicio afectado, prioridad asignada, tiempos de respuesta y solución, causa raíz, impacto generado, acciones correctivas y preventivas implementadas, y fecha comprometida de cierre o estabilización.

Para efectos de medición de ANS, determinación de incumplimientos y eventual aplicación de descuentos o penalidades, solo se considerarán los eventos, indisponibilidades, degradaciones, retrasos o fallas que resulten atribuibles al contratista dentro del alcance de

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

las obligaciones a su cargo, con base en evidencia técnica verificable, trazabilidad del caso y validación de la supervisión del contrato.

No se contabilizarán como incumplimiento de ANS ni darán lugar a descuento o penalidad, siempre que se encuentren debidamente documentados, justificados y validados por la supervisión, los siguientes eventos: i) ventanas de mantenimiento, actualización, hardening, cambio controlado o intervención programada previamente aprobadas por la CRA; ii) eventos de fuerza mayor, caso fortuito o hecho de un tercero; iii) fallas de servicios públicos, interrupciones de energía externa, afectaciones de planta física, condiciones ambientales o situaciones de infraestructura no administradas por el contratista; iv) indisponibilidades derivadas de decisiones operativas de la CRA o de intervenciones realizadas por terceros no autorizados por el contratista; y v) demás eventos que, conforme al análisis técnico y contractual, se demuestre que no son imputables al proveedor.

En caso de incidentes de seguridad, ciberataques, eventos maliciosos o afectaciones derivadas de amenazas externas, la CRA evaluará la atribución con base en el análisis de causa raíz, los controles exigibles al proveedor, las evidencias del caso, la oportunidad de la respuesta, el cumplimiento de las actividades de monitoreo, hardening, gestión de vulnerabilidades, respaldo, recuperación y demás obligaciones contractuales aplicables. La ocurrencia de un ataque no exime por sí misma al contratista de responsabilidad cuando se evidencie incumplimiento, omisión o gestión deficiente dentro del alcance contratado.

3. Reglas de medición, atribución y aplicación de descuentos o penalidades

La medición de los KPI y ANS definidos en el presente Anexo Técnico se realizará con base en información verificable, trazable y auditable, proveniente de la herramienta de trazabilidad definida por la CRA, de las herramientas de monitoreo, consolas de administración, bitácoras, registros técnicos, evidencias de atención, informes mensuales y demás fuentes aplicables al servicio evaluado.

Para efectos de determinación de incumplimientos y aplicación de descuentos o penalidades, solo se considerarán los eventos, indisponibilidades, degradaciones, retrasos, fallas o desviaciones que resulten atribuibles al contratista dentro del alcance de las obligaciones a su cargo, de conformidad con el análisis técnico del caso, la evidencia disponible y la validación de la supervisión del contrato.

No se contabilizarán como incumplimiento de KPI o ANS, ni darán lugar a descuento o penalidad, siempre que se encuentren debidamente documentados, justificados y validados por la supervisión del contrato, los siguientes eventos:

- a) Ventanas de mantenimiento, actualización, hardening, cambio controlado, pruebas o intervenciones programadas previamente aprobadas por la CRA.
- b) Eventos de fuerza mayor, caso fortuito o hecho de un tercero.
- c) Fallas de servicios públicos, interrupciones de energía externa, afectaciones de planta física, condiciones ambientales o situaciones de infraestructura no administradas por el contratista.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN ANEXO TÉCNICO	
---	---	--

- d) Indisponibilidades, retrasos o afectaciones derivados de decisiones operativas de la CRA, de omisiones de información o acceso por parte de la Entidad, o de intervenciones ejecutadas por terceros ajenos al contratista.
- e) Cualquier otra situación que, con sustento técnico y documental, se demuestre como no imputable al contratista.

En caso de incidentes de seguridad, ciberataques, eventos maliciosos o afectaciones derivadas de amenazas externas, la CRA evaluará la atribución con base en el análisis de causa raíz, la oportunidad de la respuesta, las evidencias del caso y el cumplimiento de las obligaciones contractuales del proveedor en materia de monitoreo, hardening, gestión de vulnerabilidades, respaldo, recuperación, escalamiento, contención y demás controles aplicables al componente afectado. La sola ocurrencia de un ataque no exonerará al contratista cuando se evidencie incumplimiento, omisión, debilidad de gestión o falta de control dentro del alcance contratado.

Cuando la supervisión determine incumplimiento atribuible al contratista sobre uno o más KPI o ANS, la CRA podrá aplicar descuentos o penalidades sobre el pago mensual del componente afectado, sin perjuicio de los demás mecanismos contractuales, correctivos, de mejora o responsabilidades a que haya lugar. La aplicación de dichos descuentos o penalidades deberá quedar soportada en el informe de supervisión, en el informe mensual del contratista o en el documento técnico que haga sus veces, con identificación expresa del caso, indicador o ANS incumplido, evidencia de atribución, impacto generado y valor o criterio de afectación aplicado.

Todo incumplimiento de KPI o ANS deberá quedar expresamente reportado en el informe mensual, indicando como mínimo el número del caso, servicio afectado, prioridad asignada, tiempos de respuesta y solución, causa raíz, impacto generado, acciones correctivas y preventivas implementadas, y fecha comprometida de estabilización o cierre.

4. Formato mínimo del informe mensual.

El contratista deberá presentar, dentro del plazo definido por la CRA, un **INFORME MENSUAL CONSOLIDADO DEL SERVICIO** en formato PDF, acompañado de los anexos editables en Excel o CSV cuando aplique, con el fin de soportar la supervisión técnica, operativa y contractual de las obligaciones a su cargo. El informe deberá reflejar de manera integral el comportamiento de los servicios prestados durante el período reportado, incluyendo resultados, incidencias, evidencias, desviaciones, riesgos, avances, pendientes y acciones de mejora.

El informe mensual deberá elaborarse con base en información objetiva, consistente y verificable, proveniente de las herramientas de monitoreo, consolas de administración, sistemas de tickets, bitácoras de cambio, reportes automáticos, actas de intervención, registros de seguridad, evidencias de respaldo, pruebas de restauración y demás fuentes aplicables a los servicios contratados. La información presentada deberá ser trazable y mantener coherencia entre el cuerpo del informe, los anexos técnicos y los registros fuente.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

La CRA podrá rechazar, devolver o solicitar ajustes al informe cuando evidencie inconsistencias, ausencia de soportes, falta de trazabilidad, diferencias entre los indicadores reportados y los registros técnicos, omisión de incumplimientos o cualquier otra situación que impida validar razonablemente la ejecución contractual del período. La aceptación del informe mensual no subsana incumplimientos materiales del contrato ni reemplaza las facultades de supervisión de la Entidad.

Como contenido mínimo obligatorio, el informe mensual deberá incluir, al menos, los siguientes apartados:

- a) Identificación general del informe. Deberá indicar período reportado, número del contrato, nombre del contratista, componente o servicio cubierto, fecha de entrega, nombre del responsable del informe y alcance del período evaluado.
- b) Resumen ejecutivo. Deberá presentar una síntesis de la situación general del servicio durante el mes, principales novedades, riesgos relevantes, desviaciones significativas, afectaciones presentadas, estado general de cumplimiento y decisiones o acciones que requieran conocimiento del supervisor.
- c) Alcance del servicio en el período. Deberá relacionar los servicios efectivamente prestados, activos cubiertos, inventario monitoreado o administrado durante el período, cambios relevantes en cobertura, novedades de infraestructura y cualquier ajuste autorizado que incida en la interpretación de los resultados del mes.
- d) Tablero de KPI y ANS. Deberá incluir el resultado del período frente a cada indicador y acuerdo de nivel de servicio aplicable, señalando meta, resultado obtenido, variación, estado de cumplimiento y fuente de verificación. Cuando exista incumplimiento o tendencia desfavorable, deberá indicarse expresamente la causa y la acción correctiva correspondiente.
- e) Gestión de incidentes, eventos, problemas y requerimientos. Deberá presentar el consolidado de casos atendidos durante el período, clasificados por tipo, prioridad, activo o servicio afectado, fecha de detección o registro, tiempo de respuesta, tiempo de solución, estado, causa relevante y cumplimiento de ANS. El detalle deberá guardar correspondencia con la herramienta de trazabilidad definida por la CRA.
- f) Disponibilidad, interrupciones y comportamiento operativo. Deberá incluir el cálculo de disponibilidad de los servicios o componentes a los que aplique, el detalle de interrupciones, degradaciones relevantes, ventanas de mantenimiento ejecutadas, afectaciones al servicio, tendencias operativas y análisis de comportamiento cuando exista histórico comparable.
- g) Cambios, mantenimientos, actualizaciones y parches. Deberá indicar las actividades programadas y ejecutadas durante el período, diferenciando mantenimientos preventivos, correctivos, cambios controlados, hardening, actualizaciones, parches, estabilizaciones y ajustes técnicos. También deberá mostrar lo planificado frente a lo ejecutado, los pendientes y los riesgos derivados de actividades no realizadas.
- h) Estado de respaldos y restauraciones. Deberá contener el resumen de copias de seguridad ejecutadas, porcentaje de éxito, fallos presentados, correcciones aplicadas, estado de respaldos de configuraciones críticas, pruebas de restauración realizadas y resultados obtenidos, cuando aplique al componente respectivo.
- i) Gestión de vulnerabilidades, amenazas y riesgos técnicos. Deberá incluir vulnerabilidades detectadas, criticidad, exposición, estado del tratamiento, avances de

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

- remediación, aceptación del riesgo cuando aplique, incidentes de seguridad relevantes, riesgos técnicos identificados y acciones recomendadas para su mitigación. Esta sección deberá articularse con los componentes contractuales de monitoreo, gestión de incidentes, soporte especializado y seguridad de la información cuando corresponda.
- j) Hallazgos, causas recurrentes y análisis de causa raíz. Cuando se presenten fallas relevantes, incidentes repetitivos, indisponibilidades, errores operativos o incumplimientos, el informe deberá incorporar el análisis de causa raíz, los factores contribuyentes, las lecciones aprendidas y las acciones preventivas o correctivas definidas para evitar recurrencia.
 - k) Recomendaciones técnicas y plan de mejora. Deberá incluir recomendaciones priorizadas para estabilización, optimización, seguridad, capacidad, continuidad o mejoramiento del servicio, indicando responsable, fecha objetivo, estado y dependencia de terceros o de decisiones de la CRA cuando aplique.
 - l) Pendientes y compromisos. Deberá consolidar las actividades no cerradas del período, compromisos adquiridos, acciones en curso, bloqueos existentes, escalaciones abiertas y fecha esperada de cierre o siguiente hito de seguimiento.
 - m) Cumplimiento contractual del período. Deberá incluir un apartado específico en el que se identifique de forma expresa qué KPI o ANS no se cumplieron durante el mes, cuáles fueron sus causas, qué impacto generaron, qué acciones correctivas o preventivas se adoptaron y cuál es la fecha comprometida de estabilización o cierre.
 - n) Anexos y evidencias. Deberá adjuntar, como soporte mínimo, tickets, reportes de consola o herramienta, bitácoras de cambio, logs cuando aplique, actas de intervención, capturas o exportables de tableros, reportes de respaldo, evidencias de restauración, matrices de vulnerabilidad, actas de pruebas y cualquier otro soporte necesario para validar el contenido reportado.

El informe mensual deberá presentarse en lenguaje claro, técnico y verificable, evitando afirmaciones genéricas no soportadas. Todo resultado, porcentaje, estado de cumplimiento o conclusión técnica deberá poder relacionarse con una evidencia concreta o con un registro fuente disponible para revisión por parte de la CRA.

Los anexos editables deberán entregarse con estructura ordenada, nombres de campos comprensibles y consistencia con el informe principal, de manera que la CRA pueda reutilizar la información para seguimiento, auditoría, consolidación histórica y control contractual. Cuando existan datos sensibles o de acceso restringido, estos deberán manejarse conforme a las reglas de reserva, confidencialidad y seguridad definidas por la Entidad.

El contratista deberá conservar los soportes que dan origen al informe mensual durante el plazo definido por la CRA y, como mínimo, conforme a las reglas de retención previstas para registros operativos y de seguridad en el Anexo Técnico.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

C. INVENTARIO TÉCNICO CRA

El presente inventario técnico describe la base mínima de activos, plataformas, componentes y servicios tecnológicos institucionales que deberán ser considerados por los proponentes para el dimensionamiento de la oferta y por el contratista para la prestación de los servicios objeto del contrato. Esta sección hace parte integral del Anexo Técnico y constituye referencia obligatoria para efectos de cobertura, operación, monitoreo, soporte, continuidad, seguridad, gestión de vulnerabilidades, administración técnica y supervisión contractual.

La información aquí contenida se presenta con nivel de detalle suficiente para delimitar el alcance contractual y permitir propuestas comparables, sin perjuicio de que ciertos atributos específicos de seguridad o configuración deban mantenerse bajo manejo controlado por la CRA. En consecuencia, el contratista adjudicatario deberá validar y complementar operativamente este inventario durante el primer mes de ejecución, sin que ello implique reducción del alcance base aquí definido.

Cuando por razones de seguridad institucional no resulte procedente publicar de manera abierta información detallada como versiones exactas, seriales, topologías internas, direccionamiento, configuraciones específicas, parámetros de seguridad, estado de parches o relaciones técnicas de dependencia de alto detalle, dicha información será administrada por la CRA de forma controlada, conforme a los criterios de reserva y proporcionalidad recomendados para este proceso.

1. Infraestructura física y datacenter

Tabla. Infraestructura física y datacenter

Componente	Activo / plataforma	Marca / modelo / tecnología	Cantida d conocid a	Estado o referenci a actual	Observación contractual
Servidores físicos	Servidor de propósito institucional	Dell EMC R520	2	En operación institucional	Hace parte del alcance de monitoreo, soporte especializado, mantenimiento, respaldo y continuidad.
Servidores físicos	Servidor de propósito institucional	Dell EMC R740	1	En operación institucional	Hace parte del alcance de monitoreo, soporte especializado, mantenimiento

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Componente	Activo / plataforma	Marca / modelo / tecnología	Cantida d conocid a	Estado o referenci a actual	Observación contractual
					, respaldo y continuidad.
Seguridad perimetral	Firewall principal	FortiGate FG-100F	1	En operación institucion al	Debe ser cubierto por monitoreo, soporte, vulnerabilidad es, correlación de eventos y controles de seguridad.
Energía y respaldo eléctrico	UPS e infraestructura asociada	UPS institucional y componente s asociados	Según inventari o físico vigente	En operación institucion al	El alcance de mantenimiento del datacenter incluye UPS y demás infraestructura asociada definida por la CRA.
Almacenamie nto	Soluciones de almacenamien to asociadas al datacenter	Plataformas presentes en CRA	Según inventari o vigente	En operación institucion al	Deben considerarse dentro del alcance de monitoreo, soporte, respaldo, recuperación y continuidad de servicios.
Infraestructura de datacenter	Componentes físicos complementari os	Infraestructu ra tecnológica asociada	Según inventari o vigente	En operación institucion al	El servicio de mantenimiento incluye inspección, pruebas, diagnóstico, ajuste y soporte sobre la infraestructura física y tecnológica

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Componente	Activo plataforma /	Marca modelo / tecnología	Cantidad conocida	Estado o referencia actual	Observación contractual
					definida por la CRA.

2. Red, conectividad y acceso

Tabla. Red y conectividad institucional

Componente	Activo plataforma /	Marca tecnología /	Cantidad conocida	Estado o referencia actual	Observación contractual
Red LAN	Switches core y de borde	Multimarca definida por la CRA	Según inventario vigente	En operación institucional	El anexo exige monitoreo de disponibilidad, salud, rendimiento, tráfico, interfaces críticas y eventos relevantes.
Red inalámbrica	Controladores y puntos de acceso WiFi	FortiAP y otros componentes definidos por la CRA	Según inventario vigente	En operación institucional	Deben entrar en monitoreo, análisis de tráfico, capacidad, vulnerabilidades.
Conectividad	Enlaces tráfico LAN/WAN/WLAN	Infraestructura de comunicaciones institucional	Según operación vigente	En operación institucional	Debe existir visibilidad sobre utilización de enlaces, ancho de banda, latencia, pérdida de paquetes y comportamiento general de la red.
Servicios expuestos	Puertos, protocolos y	Servicios institucionales	Según inventario	En operación	El monitoreo debe cubrir

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Componente	Activo plataforma /	Marca tecnología /	Cantidad conocida	Estado o referencia actual	Observación contractual
	servicios de red	publicados o habilitados	o vigente	institucional	puertos, protocolos, IP internas, tráfico origen-destino y comportamiento de red.
Identidad y acceso	Dominios locales, AD, DNS y servicios asociados	Microsoft Active Directory, DNS y Azure Cloud	Según inventario o vigente	En operación institucional	El servicio incluye administración, mantenimiento, hardening, monitoreo, revisión de accesos y soporte de dominios locales e internet.

3. Virtualización, servidores lógicos y software base

Tabla. Virtualización y software base

Componente	Activo plataforma /	Marca tecnología /	Cantidad conocida	Estado o referencia actual	Observación contractual
Plataforma de virtualización	Hipervisor actual VMware	VMware	3 hosts con vSphere y 1 vCenter.	En operación institucional	Se requiere soporte de VMware
Máquinas virtuales	VMs institucionales	VMs de servicios CRA	Mínimo 30 VMs como cobertura contractual de BCDR/Backup	En operación institucional	La solución de backup debe cubrir como mínimo 30 VMs y soportar continuidad durante procesos de migración tecnológica.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Componente	Activo / plataforma	Marca / tecnología	Cantidad conocida	Estado o referencia actual	Observación contractual
Sistemas operativos de servidor	Plataforma base	Windows Server	Según inventario vigente	En operación institucional	El servicio de software base aplica expresamente a Windows Server presentes en la infraestructura.
Sistemas operativos de servidor	Plataforma base	Linux Ubuntu	Según inventario vigente	En operación institucional	El servicio de software base aplica expresamente a Linux Ubuntu presentes en la infraestructura.
Software base y operación	Plataformas de infraestructura y seguridad	Kaspersky , Acronis y Fortinet	Según licencias y componentes vigentes	En operación institucional	Forman parte del alcance de administración , mantenimiento, aseguramiento, soporte y optimización.

4. Ciberseguridad, SOC/NOC y registros

Tabla. Seguridad y operación de ciberseguridad

Componente	Activo / plataforma	Marca / tecnología	Cantidad conocida	Estado o referencia actual	Observación contractual
Ecosistema Fortinet	Fortigate FG100f	Fortinet	1	En operación institucional	Forman parte del alcance de administración , mantenimiento

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Componente	Activo / plataforma	Marca / tecnología	Cantida d conocid a	Estado referencia actual	Observación contractual
					o, aseguramient o, soporte y optimización.
WAF	WAF	Debe ser provisto por el contratista de acuerdo con los requisitos técnicos	1 platafor ma mínima	La CRA no dispone actualmente de WAF institucional	El proveedor debe incluir, parametrizaci ón, integración, operación y soporte del WAF.
Operación SOC	Plataforma SIEM	SIEM o equivalente funcional provisto por el contratista	1 platafor ma mínima	La CRA no dispone actualmente de SIEM institucional	El proveedor debe incluir parametrizaci ón, integración, operación y soporte del SIEM.
Operación NOC	Monitoreo centralizado de infraestructu ra	Herramient as del proveedor o integradas con CRA	Cobertur a 24x7	Requerido contractualme nte	Debe cubrir servidores, switches, firewall, enlaces, almacenamien to, servicios críticos y eventos operativos.
Gestión de vulnerabilidad es	Plataforma y operación de evaluación	Herramient a del proveedor o definida por la CRA	Cobertur a sobre activos críticos	Requiere línea base inicial	El alcance incluye firewall, IP públicas, switches, WiFi, servidores críticos, virtualización y endpoints priorizados.
Registros y	Logs de	Logs de	Según	Retención	Se exige

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Componente	Activo / plataforma	Marca / tecnología	Cantidad conocida	Estado referencia actual	Observación contractual
trazabilidad	seguridad	firewall, SOC, AD y plataformas críticas	operación	mínima contractual	retención mínima de 12 meses para logs de seguridad.
Registros y trazabilidad	Logs operativos	Logs de monitoreo, operación y soporte	Según operación	Retención mínima contractual	Se exige retención mínima de 6 meses para registros operativos.
Accesos administrativos	Cuentas administrativas del proveedor	Accesos con MFA y canales cifrados	Según necesidad autorizada	Bajo control institucional	Deben operar con MFA, mínimo privilegio, segregación de funciones, revisión semestral y revocación al cierre.

5. Respaldo, recuperación y continuidad

Tabla. Backup, BCDR y recuperación

Componente	Activo / plataforma	Marca / tecnología	Cantidad conocida	Estado referencia actual	Observación contractual
Backup / BCDR	Plataforma de respaldo en nube	Acronis Cyber Backup Cloud o equivalente	1 plataforma mínima	Cobertura contractual definida	El proveedor debe incluir plataforma, almacenamiento, operación, monitoreo, DRaaS y acceso de la CRA a consola.
Cobertura de	Máquinas	VMs	30	Cobertura	Debe

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Componente	Activo / plataforma	Marca tecnología /	Cantidad conocida	Estado referencia actual	Observación contractual
respaldo	virtuales	institucionales		mínima contractual	garantizarse protección, recuperación y soporte de continuidad sobre mínimo 30 VMs.
Cobertura de respaldo	Endpoints priorizados	Endpoints de la CRA	50	Cobertura mínima contractual	Debe garantizarse protección, recuperación y soporte de continuidad sobre mínimo 50 Endpoints.
Cobertura de respaldo	Microsoft 365	Negocios básica/estándar, Kiosko, E1 y E3	Hasta 300 cuentas	Cobertura mínima contractual	Debe garantizarse protección, recuperación y soporte de continuidad sobre mínimo 300 cuentas de office 365 respaldadas.
Almacenamiento de respaldo	Capacidad en nube	Hasta 20 TB	20 TB	Cobertura mínima contractual	Debe soportar políticas de retención, integridad de copias, replicación y recuperación verificable.
Continuidad	DRaaS y ambiente de contingencia	Plataforma del proveedor	1 esquema mínimo	Requerido contractualmente	Debe permitir levantamiento de VMs/servicios críticos durante pruebas o desastre declarado.

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

6. Bases de datos, aplicaciones y telefonía

Tabla. Plataformas especializadas

Componente	Activo / plataforma	Marca / tecnología	Cantidad conocida	Estado o referencia actual	Observación contractual
Base de datos	Motor institucional	Oracle Database	Número aproximado de instancias de 3 a 5	En operación institucional	Soporte y mantenimiento para 3 instancias sobre la base de datos Oracle de la entidad.
Ambientes de BD	Producción y/o desarrollo	Oracle y componentes asociados	3 instancias, todas en Producción	En operación institucional	Además del soporte se requiere migrar la actual base de datos Oracle 12G de la entidad con todas sus instancias de un servidor Windows server 2012 a un servidor Windows server 2019 o superior, la entidad cuenta con la licencia para este servidor.
Telefonía IP	PBX institucional	Asterisk con troncal SIP	Número aproximado de extensión esperado 120	Configurada, pendiente de hardening y puesta en producción	El contratista asume responsabilidad sobre la configuración existente y define la validez para entrar en operación.
Sitios web y	Dominios y	Dominios	9 dominios	En	El tipo de

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

Componente	Activo / plataforma	Marca / tecnología	Cantidad conocida	Estado o referencia actual	Observación contractual
certificados	aplicativos webs institucionales	CRA	/ aplicativos	operación institucional	certificado SSL/TLS requerido es DV.

7. Reglas de uso del inventario

Los activos, plataformas y componentes aquí relacionados deberán ser considerados como base mínima del alcance técnico del contrato. Cuando una categoría se encuentre expresada con cantidad “según inventario vigente” o “por confirmar”, ello no implica inexistencia del activo, sino que refleja que la CRA mantiene el detalle técnico completo bajo control institucional y que el contratista deberá considerarlo dentro de su capacidad de cobertura, operación y soporte según la naturaleza del servicio.

Las cantidades expresamente indicadas como mínimas contractuales corresponden a umbrales obligatorios de cobertura para la estructuración de la oferta y la ejecución del contrato. En especial, el servicio de respaldo y continuidad deberá contemplar, como mínimo, treinta (30) máquinas virtuales, cincuenta (50) endpoints, hasta trescientas (300) cuentas de Microsoft 365 y hasta veinte (20) TB de almacenamiento en nube, sin perjuicio de los ajustes que se formalicen mediante control de cambios.

Dentro del primer mes de ejecución, el contratista adjudicatario deberá validar el presente inventario con la CRA y consolidar el inventario operativo del servicio, incluyendo criticidad, dependencias, clasificación de activos, cobertura de monitoreo, reglas de correlación, umbrales, matriz de respaldos, planes de recuperación y demás atributos requeridos para la operación efectiva. Esta validación no sustituye el presente inventario base ni podrá utilizarse para restringir el alcance inicialmente contratado.

Toda modificación, incorporación, retiro, reemplazo tecnológico o cambio relevante en los activos cubiertos deberá gestionarse mediante el mecanismo de control de cambios definido por la CRA, conservando trazabilidad, evidencia y actualización de las coberturas contractuales correspondientes.

D. REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN, GOBERNANZA Y CONTROL DEL PROVEEDOR

Los servicios objeto del presente contrato deberán prestarse en el marco del proceso institucional de seguridad de la información de la CRA, de sus políticas, lineamientos, procedimientos internos y del enfoque de mejora continua asociado a la implementación del SGSI institucional. La tercerización de servicios tecnológicos no transfiere a terceros la responsabilidad institucional de la CRA sobre la seguridad de la información, pero sí impone al contratista la obligación de cumplir integralmente los controles, medidas y deberes

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

contractuales que le correspondan dentro de su alcance.

El contratista será responsable contractualmente por la operación segura, trazable y controlada de los servicios a su cargo, y deberá contribuir activamente al cumplimiento de los lineamientos de seguridad, continuidad, disponibilidad, integridad, confidencialidad y trazabilidad definidos por la CRA. Al inicio del contrato, deberá acreditar conocimiento suficiente de las políticas, procedimientos y lineamientos de seguridad institucional que le sean aplicables para la correcta ejecución de sus obligaciones.

Toda actividad realizada por el contratista sobre activos, plataformas, cuentas, configuraciones, registros, respaldos, eventos, incidentes, consolas o componentes tecnológicos de la CRA deberá ejecutarse bajo autorización, trazabilidad, registro verificable, segregación de funciones y sujeción a los controles definidos por la Entidad. Ninguna actividad técnica de administración, soporte, monitoreo, recuperación, ajuste o intervención podrá realizarse por fuera de los canales, perfiles y mecanismos autorizados.

1. Gobernanza y responsabilidad

La CRA conservará en todo momento la dirección institucional sobre la infraestructura, la información, los servicios críticos, las decisiones de riesgo, la aprobación de cambios relevantes y la custodia de los elementos críticos de administración definidos por la Entidad. El contratista actuará como operador especializado dentro de ese marco, con responsabilidad directa sobre la correcta ejecución de los servicios contratados y sobre el cumplimiento de los controles de seguridad que le resulten exigibles.

El contratista deberá designar un responsable técnico y un responsable de seguridad o punto focal equivalente para la interlocución con la CRA en materia de operación, incidentes, accesos, trazabilidad, vulnerabilidades, continuidad y cumplimiento de obligaciones de seguridad de la información. Toda comunicación crítica relacionada con riesgos, incidentes, indisponibilidades, accesos privilegiados o hallazgos relevantes deberá escalararse oportunamente al supervisor del contrato o al responsable que la CRA defina.

2. Subcontratación y terceros

El contratista no podrá subcontratar, delegar o tercerizar actividades que impliquen acceso a la infraestructura, plataformas, redes, consolas, bases de datos, respaldos, credenciales, registros o información de la CRA sin autorización previa y escrita del supervisor del contrato. En caso de subcontratación autorizada, el contratista principal mantendrá íntegramente la responsabilidad contractual, técnica, operativa y de seguridad frente a la CRA.

Todo subcontratista autorizado deberá cumplir, como mínimo, las mismas obligaciones de confidencialidad, seguridad de la información, tratamiento de datos, trazabilidad, gestión de accesos, conservación de evidencias y demás exigencias aplicables al contratista principal. La CRA podrá requerir evidencia documental de dichos compromisos y verificar su

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

cumplimiento dentro del alcance contractual.

3. Control de accesos y cuentas privilegiadas

El contratista deberá operar bajo los principios de mínimo privilegio, necesidad de conocer, segregación de funciones y uso de cuentas auditables para toda intervención sobre la infraestructura y servicios de la CRA. No se permitirá el uso de cuentas genéricas no controladas, accesos compartidos sin trazabilidad o mecanismos que impidan identificar de forma verificable al responsable de una acción administrativa.

Todos los accesos administrativos remotos del proveedor a infraestructura crítica de la CRA deberán utilizar autenticación multifactor MFA y canales cifrados de administración remota, tales como SSH, HTTPS o VPN. Se prohíbe expresamente el uso de protocolos no cifrados para administración remota, tales como Telnet, HTTP o FTP.

Al inicio del contrato, el proveedor deberá entregar al supervisor del contrato el registro de las cuentas administrativas utilizadas o creadas para la prestación del servicio, indicando como mínimo usuario, alcance, activo o plataforma asociada, perfil de acceso, responsable y justificación. Asimismo, deberá realizar revisión semestral de los accesos otorgados, con informe verificable al supervisor, y revocar todas las cuentas y accesos dentro de las cuarenta y ocho (48) horas siguientes a la terminación o vencimiento del contrato, dejando acta verificable de cierre.

Las credenciales críticas de administración de los sistemas prioritarios definidos por la CRA, tales como firewall, hipervisor, Active Directory, almacenamiento u otros componentes críticos, deberán permanecer bajo custodia institucional de la CRA. El contratista podrá utilizarlas dentro del marco autorizado de operación, pero no tendrá custodia exclusiva ni control único sobre dichas credenciales.

4. Confidencialidad, datos personales y manejo de información

El contratista deberá guardar estricta confidencialidad sobre toda la información institucional, técnica, operativa, administrativa, personal o sensible a la que acceda con ocasión de la ejecución contractual, y solo podrá utilizarla para los fines directamente relacionados con el objeto del contrato. Queda prohibida su divulgación, reproducción, extracción, transferencia, uso distinto o entrega a terceros no autorizados por la CRA.

Cuando en desarrollo del contrato el proveedor acceda, trate, almacene, transmita o administre datos personales, deberá hacerlo exclusivamente para la finalidad contractual y en cumplimiento de las obligaciones aplicables en materia de protección de datos personales. El contratista deberá tratar los datos personales a los que tenga acceso exclusivamente para la ejecución del objeto contractual y conforme a las instrucciones impartidas por la C.R.A., absteniéndose de utilizarlos para fines distintos o de transferirlos, cederlos o divulgarlos a terceros sin autorización previa y expresa de la Entidad. Asimismo, deberá implementar y mantener las medidas técnicas, administrativas y organizacionales necesarias para garantizar la confidencialidad, integridad, disponibilidad y seguridad de la información, así como notificar a la C.R.A., dentro de las 24 horas siguientes a su

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

conocimiento, cualquier incidente de seguridad, vulneración o evento que comprometa o pueda comprometer datos personales o información institucional.

La información técnica sensible de la infraestructura de la CRA, incluyendo topologías, direccionamiento, configuraciones, reglas de seguridad, respaldos, credenciales, bitácoras detalladas, resultados de análisis o cualquier otro contenido que pueda comprometer la seguridad institucional, deberá manejarse bajo criterios de acceso restringido, confidencialidad, integridad, trazabilidad y necesidad de conocer.

5. Monitoreo, registros, incidentes y auditoría

El contratista deberá garantizar que los registros, logs, evidencias, tickets, bitácoras, actas, reportes y demás soportes generados durante la ejecución contractual se conserven con controles de acceso, integridad, disponibilidad y trazabilidad durante el período definido por la CRA. Para efectos del contrato, se establece una retención mínima de doce (12) meses para logs de seguridad y de seis (6) meses para logs operativos, salvo obligación legal o técnica superior.

Todo incidente de seguridad, evento relevante, desviación operacional crítica, incumplimiento de control o hallazgo de vulnerabilidad que afecte o pueda afectar la disponibilidad, integridad o confidencialidad de la infraestructura o de la información de la CRA deberá ser registrado formalmente, gestionado con trazabilidad completa y reportado oportunamente conforme a los procedimientos y canales definidos por la Entidad. Cuando corresponda, deberá incluir análisis de causa raíz, línea de tiempo, acciones ejecutadas, evidencias, impacto, estado, cierre y lecciones aprendidas.

La CRA podrá realizar directamente o contratar auditorías técnicas independientes sobre la operación del proveedor durante la vigencia contractual, con preaviso razonable definido por la Entidad, con el fin de verificar cumplimiento técnico, seguridad, trazabilidad, operación de controles, calidad del servicio y observancia de las obligaciones del contrato. El contratista deberá facilitar la información y evidencias requeridas dentro del alcance contractual, sin afectar la confidencialidad de otros clientes cuando opere sobre plataformas compartidas.

6. Pruebas, mejora y cumplimiento

El contratista deberá planificar, ejecutar y documentar, durante la vigencia contractual, como mínimo dos (2) pruebas o simulacros de continuidad, recuperación y respuesta ante incidentes, coordinados con la C.R.A., que permitan validar la capacidad de recuperación de los servicios tecnológicos críticos. Cada ejercicio deberá generar como mínimo acta, evidencias de ejecución, resultados, métricas de eficacia, hallazgos, conclusiones y un plan de mejora con acciones, responsables y fechas de cumplimiento.

Toda lección aprendida derivada de incidentes reales, simulacros, pruebas de continuidad, fallas relevantes, vulnerabilidades críticas o incumplimientos de control deberá quedar documentada en formato verificable e incorporarse al informe mensual del período correspondiente. El registro deberá incluir, como mínimo, descripción del evento, causa

	OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	
	ANEXO TÉCNICO	

raíz, impacto, controles aplicados, acción correctiva, acción preventiva, responsable y fecha de seguimiento.

El incumplimiento de las obligaciones previstas en esta sección podrá dar lugar a requerimientos formales, planes de acción obligatorios, observaciones de supervisión, reporte de incumplimiento contractual y demás consecuencias previstas en el contrato, sin perjuicio de las acciones legales, disciplinarias, fiscales, civiles o penales a que haya lugar.