ANEXO TÉCNICOS No 1 –

Servicios especializados de análisis y monitoreo para la gestión de eventos de ciberseguridad

INTRODUCCIÓN

La Unidad de Búsqueda de Personas dadas por Desaparecidas – UBPD, en su compromiso por salvaguardar la confidencialidad, integridad y disponibilidad de su información, requiere la contratación de un **servicio integral de seguridad gestionada** que articule de forma coherente y operativa las funciones de un **Centro de Operaciones de Seguridad (SOC)**, el **análisis continuo de vulnerabilidades** y un **sistema de control de acceso a la red (NAC)**, consolidando así un entorno de protección robusto y adaptado a las necesidades institucionales.

Este servicio deberá estar soportado en una plataforma de **Security Information and Event Management (SIEM)** robusta, actualizada y reconocida en el mercado, administrada 24/7/365 por personal altamente calificado del proveedor. Dentro del alcance, se incluirá la gestión completa del SIEM (configuración, mantenimiento, actualización, y operación continua), la entrega de alertas en tiempo real, reportes periódicos, análisis detallados de incidentes, y la emisión de recomendaciones estratégicas con base en buenas prácticas internacionales.

Adicionalmente, el proveedor deberá garantizar:

- La integración nativa del SIEM con los sistemas existentes de la UBPD.
- La configuración dinámica de reglas de correlación, flujos de respuesta y políticas de seguridad.
- El uso de tecnologías avanzadas, tales como **machine learning** y **análisis de comportamiento**, para la detección proactiva de amenazas.
- Transferencia de conocimiento a los funcionarios de enlace y acompañamiento técnico por un término menor a 20 horas en plazo máximo de cinco (5) días hábiles. .

Como parte del servicio integral, se incluye un **sistema de análisis de vulnerabilidades en modalidad Suscripción**, administrado directamente por el proveedor, que permita identificar, evaluar, priorizar y gestionar de manera continua los riesgos asociados a vulnerabilidades y configuraciones inseguras en activos de red, entornos internos, aplicaciones web y superficies de exposición externa.

Este componente será parte fundamental del monitoreo centralizado del SOC, permitiendo:

- Escaneos periódicos y automatizados de vulnerabilidades sin interrupción del servicio.
- Evaluación contextual de riesgos para una toma de decisiones informada.
- Priorización de hallazgos con base en criticidad y explotación activa.
- Informes técnicos y ejecutivos con recomendaciones de remediación.
- Sinergia con los procesos de gestión de incidentes para acelerar la contención y resolución de eventos.

El servicio incluirá también una solución de **Network Access Control (NAC)** que garantice el acceso seguro a la red de la UBPD, tanto cableada como inalámbrica, permitiendo que solo dispositivos y usuarios autorizados puedan conectarse a la infraestructura tecnológica.

Esta solución debe permitir:

- La gestión concurrente de hasta **1.200 dispositivos o usuarios**.
- Políticas de acceso dinámicas basadas en el perfil del dispositivo, ubicación, hora de conexión y cumplimiento de políticas.
- Visibilidad completa de los dispositivos conectados a la red y control de cumplimiento de requisitos de seguridad.
- Integración con el SIEM para fortalecer la detección de accesos no autorizados o anómalos.

El proveedor será responsable de la **provisión, instalación, implementación, configuración, puesta en producción, administración y soporte técnico especializado** de la solución NAC, garantizando su operación ininterrumpida, actualización continua y alineación con las políticas institucionales de seguridad.

Para asegurar la calidad y confiabilidad del servicio, se establece que:

- No se aceptarán soluciones genéricas, experimentales o sin respaldo comercial/técnico.
- Las plataformas incluidas deben estar respaldadas por fabricantes reconocidos a nivel internacional, con experiencia comprobada en seguridad de la información.
- Todo el servicio debe estar alineado con estándares internacionales como ISO/IEC 27001, NIST, y el marco MITRE ATT&CK.

El servicio incluirá también bajo la modalidad de suscripción, una solución especializada de Prevención de Pérdida de Datos (DLP, por sus siglas en inglés), que permita implementar controles automáticos y políticas de seguridad orientadas a la detección, bloqueo y reporte de cualquier intento de transferencia o exfiltración de datos sensibles fuera de los entornos autorizados. Esta herramienta deberá operar de manera centralizada y permanente (24/7), permitiendo la supervisión del flujo de información en reposo, en tránsito y en uso, tanto en plataformas locales como en ambientes de nube híbrida.

La adopción de esta tecnología representa una medida estratégica de mitigación de riesgos para la UBPD, dado que fortalece su capacidad institucional para cumplir con el principio de seguridad previsto en la Ley de Protección de Datos Personales, previene incidentes que puedan afectar derechos fundamentales, y reduce la exposición legal y reputacional derivada de potenciales brechas de seguridad. Así mismo, se alinea con los lineamientos del Modelo de Seguridad y Privacidad de la Información del Ministerio TIC y con los estándares internacionales en materia de ciberseguridad.

1. ALCANCE Y CONSIDERACIONES GENERALES

SERVICIO INTEGRAL GESTIONADO DE SEGURIDAD – SOC CON ANÁLISIS DE VULNERABILIDADES Y NAC

La Unidad de Búsqueda de Personas dadas por Desaparecidas (UBPD) requiere contratar un **servicio integral de seguridad gestionada**, que combine en una sola oferta técnica y operativa las capacidades en la modalidad de suscripción de a) un **Centro de Operaciones de Seguridad (SOC)**, b) **análisis continuo de vulnerabilidades** y c) una solución avanzada de **control de acceso a la red (NAC)**, permitiendo así una protección unificada, continua y de alta disponibilidad para toda su infraestructura tecnológica.

Este servicio deberá prestarse por un período mínimo de **un (1) año**, contado a partir de la entrega formal de la implementación e inicio de operaciones del servicio, y no desde la firma del acta de inicio.

1.1. CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

El servicio SOC gestionado será el eje central de la operación de seguridad, garantizando la **correlación efectiva de eventos**, el **alertamiento oportuno** y la **respuesta inmediata** ante incidentes cibernéticos. Este servicio debe contemplar:

- Operación continua **24/7/365** por parte del proveedor.
- Administración completa de una plataforma **SIEM** robusta, actualizada y reconocida, que será provista con todo su licenciamiento como parte integral del servicio.
- Gestión de eventos, incidentes, análisis forense, emisión de recomendaciones y acompañamiento técnico especializado.
- Generación de reportes periódicos y mecanismos efectivos de escalamiento y comunicación.
- Integración del SIEM con otras soluciones de seguridad existentes, incluidas las funciones de análisis de vulnerabilidades y NAC.
- La UBPD acepta diferentes esquemas o modalidades para la prestación del servicio, tales como implementación en infraestructura propia (on-premise), en la nube o en modelo híbrido. Esta flexibilidad de la forma de implementación no implica una disminución de las exigencias; cualquier modelo propuesto deberá cumplir en su totalidad con los requisitos funcionales, técnicos y normativos establecidos, garantizando que las condiciones de operación, calidad, seguridad y continuidad exigidas por la entidad se mantengan sin excepción.

1.2. ANÁLISIS DE VULNERABILIDADES (INTEGRADO AL SOC)

Como componente esencial del servicio integral gestionado de seguridad, el proveedor deberá incorporar una solución de **análisis de vulnerabilidades en la modalidad de suscripción**, administrada directamente desde el Centro de Operaciones de Seguridad (SOC). Esta solución permitirá identificar y gestionar riesgos de seguridad presentes en activos de infraestructura tecnológica, aplicaciones web y superficies de exposición externa, alineándose con las políticas de seguridad de la UBPD.

El análisis de vulnerabilidades deberá contemplar lo siguiente:

- **Ejecución de dos (2) ejercicios de análisis de vulnerabilidades al año**, programados de manera concertada con la UBPD.
- Cada ejercicio debe incluir su respectivo **retest o reescaneo posterior**, para validar la efectividad de las acciones de remediación implementadas por la entidad.
- Cobertura de hasta 1**00 activos IP** y **50 aplicaciones web**, incluyendo:
    - **Activos internos** (servidores, estaciones, dispositivos de red con IP interna o externa).
    - **Aplicaciones web** identificadas por su URL o FQDN.
    - **ASM (Attack Surface Management)** para detección no invasiva de brechas en activos expuestos a Internet.

Adicionalmente, la herramienta deberá permitir:

- Generación de reportes técnicos y ejecutivos por cada ejercicio, con clasificación de riesgos, evidencias, y recomendaciones.
- Integración de los hallazgos con el SIEM para su correlación con eventos e incidentes.

- Gestión centralizada desde el SOC, garantizando el seguimiento a las vulnerabilidades detectadas y la asesoría técnica para su remediación.

1.3. CONTROL DE ACCESO A LA RED (NAC) (INTEGRADO AL SOC)

La solución NAC, también gestionada e integrada dentro del servicio SOC, permitirá **controlar y asegurar el acceso a la red corporativa** (cableada e inalámbrica) únicamente para dispositivos y usuarios autorizados y en cumplimiento con las políticas de seguridad definidas por la UBPD.

El servicio deberá contemplar:

- Capacidad para administrar hasta **1.200 dispositivos o usuarios concurrentes**.
- Verificación del cumplimiento de políticas en los dispositivos (antivirus actualizado, ausencia de software malicioso, parches de seguridad instalados, etc.).
- Integración con el SIEM para correlación de accesos no autorizados o sospechosos.
- Administración continua por parte del proveedor: ajustes de políticas, soporte técnico especializado de segundo y tercer nivel, generación de reportes y alertas.
- Instalación, configuración, puesta en producción y mantenimiento de la solución NAC.
- Licenciamiento completo y actualizaciones funcionales incluidas en modalidad de suscripción durante todo el periodo contractual.

1.4. DATA LOSS PREVENTION - DLP

La solución DLP, también gestionada e integrada dentro del servicio SOC, contempla el suministro, configuración, operación y soporte de dicha solución bajo un modelo de servicio por suscripción con una duración mínima de un (1) año. El alcance incluye:

- Implementación de la solución DLP, asegurando su integración con la infraestructura tecnológica de la UBPD.

- Aplicación de políticas de prevención de pérdida de datos (DLP) basadas en contenido, usuarios, roles y contexto, con capacidad de detección de datos sensibles en tránsito, en uso y en reposo.

- Cobertura sobre los principales canales de riesgo: correo electrónico, navegación web, almacenamiento en red, puertos USB, impresoras y sistemas en la nube.

- Integración con soluciones existentes de seguridad perimetral.

- Provisión de reportes automatizados, alertas en tiempo real, trazabilidad de incidentes y bitácoras de auditoría con fines normativos y de gestión del riesgo.

- Acceso al panel de administración, monitoreo continuo 24/7, y servicio de soporte técnico especializado incluido dentro de la suscripción.

2. ESPECIFICACIONES TÉCNICAS

2.1. SERVICIO DE SIEM Y SOC	
1. GENERALIDADES	
	El contratista deberá contar con un (1) SOC – SECURITY OPERATION CENTER operativamente propio (no tercerizado) y sus instalaciones. Para lo cual deberá entregar certificación emitida por el representante legal del oferente, indicando la titularidad de los derechos de propiedad del centro de operaciones de seguridad (SOC). La entidad podrá solicitar y/o programar una visita a las instalaciones con el fin de corroborar la información aportada y ubicación.
	El oferente debe estar certificado mínimo en ISO 27001:2022, ISO 9001:2015 y mantener la certificación vigente durante la vigencia de la suscripción, además los servicios prestados deberán estar alineados bajo la metodología de ITILV4.
	El oferente debe evidenciar a la entidad la membresía vigente al año 2025 de FIRST (Forum of Incident Response and Security Teams). Para lo cual debe presentar evidencia emitida por FIRST e indicar nombre del CSIRT registrado y url del mismo, https://www.first.org/ y adicional se deberá presentar carta de patrocinadores miembros vigentes de FIRST con la recomendación correspondiente como CSIRT
	El SOC debe estar siempre disponible 7 x 24 con analistas de seguridad y esquema de escalamiento de incidentes desde el centro de monitoreo. El contratista deberá incluir en la oferta documento describiendo el servicio.
	La solución SIEM (Security Information and Event Management) que soporta el SOC deberá estar licenciada en modalidad de suscripción, con garantía y soporte ante fabricante por el tiempo que dure la ejecución, para lo cual se deberá adjuntar certificación de fabricante. La solución SIEM debe ser 100% compatible con las herramientas de seguridad on-premise con que cuenta la Entidad.
	El SOC debe contar con una arquitectura en alta disponibilidad que asegure una inmediata recuperación ante la falla de uno de sus componentes.
	El contratista deberá dar suministro del soporte y garantía de fábrica en horario 7x24x365 por el periodo de vigencia de la suscripción para la plataforma SIEM que soporta el SOC.
	El SIEM utilizado por el SOC debe aparecer clasificado como "Retador" o "líder" en el cuadro mágico de Gartner (SIEM) en el último reporte.
	El servicio debe ser prestado en idioma castellano (español), que facilite la interacción de las áreas de operación con el personal del Entidad.
	El contratista debe implementar, administrar, operar, soportar y actualizar la plataforma para el Monitoreo y correlación de los eventos de seguridad.
	El SOC debe prevenir y enfrentar las diferentes situaciones de riesgos de seguridad de la información y ciberseguridad, al contar con un monitoreo proactivo, que garantice la debida gestión y optimización de las configuraciones de las tecnologías con las que cuente El Entidad, en los componentes del alcance del proyecto.
	La solución de SOC deberá contar con un sistema de base de datos que asegure que la solución soporte grandes volúmenes de datos sin afectar su estabilidad.
	Cuando sea necesario, se deben parsear los logs generados por los activos de la plataforma de red y cómputo, para que se les puedan aplicar las reglas de correlación que se establezcan.

	Para todos los equipos requeridos para la prestación del servicio, deben asegurarse por parte del Contratista, que estos cuenten con el debido mantenimiento, soporte y garantía en caso de fallas, con lo cual se asegura su reemplazo inmediato. Toda la solución debe estar vigente en temas de garantía y soporte por los fabricantes o distribuidores. Adjuntar con la presentación de la oferta certificaciones emitidas por los fabricantes de las plataformas que soportan los servicios, donde conste que el oferente está autorizado para su distribución, uso y que el licenciamiento que hace parte de la solución se encontrará vigente durante la ejecución y sin anuncio de fin de venta y soporte, en los casos en que aplique.
	El SOC, deberá contar con las siguientes características:
	- Actualización constante de la base de datos de contextos, configuraciones, software instalado y servidores corriendo en los dispositivos monitoreados.
	- Análisis constante del desempeño de las aplicaciones lo cual permite definir atención prioritaria a la que más esté afectada mediante transacciones sintéticas.
	- Visor personalizado de log de tráfico.
	El descubrimiento de los dispositivos se debe realizar sin agente y usando protocolos estándares entre ellos SNMP, WMI, VM SDK, OPSEC, JBDC, Telnet, SSH, JMX, Rest api. Una vez descubierto el dispositivo se debe presentar en la CMDB la cual debe estar dentro de la solución SIEM, no puede estar separada.
	Debe estar en capacidad de monitorear los servicios de DNS, FTP/SCP, Generic TCP/UDP, ICMP, JDBC, LDAP, SMTP, IMAP4, POP3, POP3S, SMTP, SSH y Web — HTTP, HTTPS,
	- Herramienta de búsqueda sobre los logs de tráfico.
2. DIMENSIONAMIENTO DEL MONITOREO Y ALERTAMIENTO.	
	El contratista debe contemplar un monitoreo para la cantidad de fuentes descritas en el alcance del presente documento, de acuerdo con las características de las plataformas instaladas por la Entidad, de manera automática y continua y en caso de detectarse una modificación, alta o baja de una fuente, esta será alertada para verificarse si es un cambio autorizado.
	El contratista debe verificar el correcto funcionamiento de los activos de TI definidos por el Entidad, por medio del SOC, para ello realizará un monitoreo 7 x 24 de la solución y configurará alertas automáticas para la temprana identificación de un comportamiento anómalo. El monitoreo debe incluir la evaluación del desempeño (performance), disponibilidad, transacciones sintéticas (transacciones que permiten generar carga sobre los aplicativos), ataques informáticos, ciberataques, uso de interfaces y estatus de procesamiento de los equipos.
	El contratista debe realizar correlación avanzada de eventos de seguridad y ciberseguridad para proteger las plataformas de TI del Entidad definidas, para ello, el contratista deberá monitorear los eventos generados a través de la solución SIEM (Security Information and Event Management) y alertar sobre eventos o comportamientos anormales que se presenten según los logs integrados dentro del SIEM.
	El contratista deberá garantizar el diseño, modelamiento y configuración de mínimo diez (10) casos de uso, los cuales serán definidos en conjunto con la Entidad para la puesta en operación del SOC.
	De acuerdo con el plan de comunicaciones establecido, el contratista debe comunicar a la Entidad de manera inmediata las alertas de eventos que se consideren de alta criticidad y que pongan en riesgo la estabilidad de los servicios de la entidad, lo anterior, producto del monitoreo constante realizado. El Entidad será quien realice las actividades de remediación según las alertas del SOC
	Generación automática de la notificación a la Entidad de los eventos críticos e incidentes por lo menos por dos (2) medios de comunicación diferentes, de acuerdo con lo definido en el plan de comunicación del contrato. En la notificación se debe indicar las recomendaciones a seguir para atender y mitigar el evento o incidente.

	El proveedor debe realizar el acompañamiento en la atención, mitigación y contención de los eventos e incidentes que se presenten, apoyando al Entidad con recomendaciones, buenas prácticas, cierre de brechas, soluciones, configuraciones, entre otros, con el fin de atender oportuna y eficientemente el evento o incidente.
3. FUNCIONALIDADES Y ALCANCE DEL SOC	
3.1 Implementación y gestión del SOC:	
Para la configuración y puesta en marcha del SOC se requiere presentar un plan de actividades que debe ser aprobado por la entidad, el cual debe contener como mínimo:	
3.1.1	Configuración y alistamiento del software y firmware de los componentes requeridos para el SOC a la última versión estable aprobada por el fabricante
3.1.2	Entrega de los componentes requeridos a satisfacción de la Entidad
3.1.3	Afinamiento, estabilización y pruebas de los componentes requeridos, realizado por personal certificado por el fabricante.
3.1.4	Funciones y responsabilidades del personal involucrado, cronograma de actividades y productos a entregar. Cualquier cambio en alguno de estos aspectos deberá ser informado y aprobado por el supervisor
3.1.7	Las actividades de parametrización de conectores y aprovisionamiento de los servicios podrán ser realizadas en sitio o remotamente.
3.1.8	Las reglas de correlación, que no requieran un proceso consultivo ni un conocimiento del negocio fuerte, deben ser creadas por el contratista con una solicitud a la mesa de ayuda del SOC.
3.1.9	El SOC debe contar con capacidad de hacer "Assessment" por lo menos una vez cada seis meses de dispositivos perimetrales, que permita:
	• Tener un panorama real sobre la efectividad de los accesos otorgados por los dispositivos, • Hacer auditoria en los cambios de configuración y permisos • Detectar reglas solapadas, mal usada y sin uso.
	• El contratista debe presentar a la Entidad la metodología y el proceso que utilizará para estas evaluaciones y deberá coordinarla con el Entidad ciñéndose al procedimiento de gestión de cambios de la entidad.
3.2 RECOLECCIÓN Y CORRELACIÓN DE EVENTOS	
3.2.1	El contratista debe contar con una solución de recolección y correlación de eventos debidamente certificada la cuál debe contar con servicios de soporte y mantenimiento por parte del fabricante (o por la firma autorizada por el fabricante), durante el tiempo en que se presten los servicios a la Entidad.
	La supervisión del contrato solicitará las evidencias, que acrediten que el SIEM, cuenta con contrato de soporte y mantenimiento, durante la vigencia de la suscripción y podrá realizar las verificaciones y solicitar las evidencias que considere necesarias.
3.2.3	Debe estar apoyado en un sistema de inteligencia externo que aporte descubrimiento de amenazas avanzadas y sus actores ocultos que contengan listas de reputación o dominios catalogados como sospechosos para la generación de indicadores de compromiso en cualquier parte de la infraestructura de TI incluida en el alcance del presente anexo.
3.2.4	El Correlacionador de Eventos como servicio utilizado por el SOC debe contar con un panel de control de seguridad fácil de utilizar que destaca las amenazas más importantes y de esta manera se genere un flujo de trabajo rápido y eficaz para la investigación y recomendación de la remediación.
3.2.5	Debe conectarse con sistemas de inteligencia basados en intercambio colaborativo o machine learning o similares para descubrir ataques ocultos, entre otros.
3.2.6	Debe garantizar el manejo de protocolos seguros, así como la protección adecuada de la información a transmitir para la prestación y uso del servicio (alguno de ellos puede ser SSL/TLS, VPN, canales dedicados).

3.2.7	Debe ser compatible y soportar por lo menos los siguientes protocolos de colección y/o monitoreo, tales como: syslog, Web HTTP/HTTPS, DNS, FTP/SCP, Generic TCP/UDP, ICMP, IMAP4, JDBC, LDAP, POP3, POP3S, SMTP, SOAP, SSH, Telnet/SSH, SNMP, WMI, JMX, OPSEC, ALE, registros de FTP, SCP, SFTP, o Archivos de logs en sistemas mediante NFS y/o CIFS, entre otros
3.2.8	Deberá soportar correlación cruzada de eventos
3.2.9	Deberá permitir la Integración por medio de Apis con fuentes de información externa sobre amenazas, tales como Dominios de Malware, IP's, URLs, Hash y Nodos de Tor
3.2.10	Deberá soportar integración nativa con fuentes de información de terceros tales como MS365, Forcepoint, AWS, Fortiguard entre otros.
3.2.12	Deberá tener la capacidad de colectar logs de forma segura desde dispositivos remotos
3.2.13	Deberá contar con una Framework de notificación de incidentes el cual deberá estar basado en políticas
	La herramienta de gestión de eventos e información de seguridad que hace parte de la solución como servicio, debe contar con capacidades dentro de sus funciones que faciliten la interoperabilidad o integración con las nuevas tecnologías de seguridad como lo son las soluciones EDR (Endpoint Detección and Response), UEBA (User & Entity Behavior Analytics), asi como las plataformas que proporcionan inteligencia de amenazas (TIP), y plataformas SOAR (Security Orchestration, Automation and Response en caso que en un futuro se requiera habilitar por parte del Entidad
3.2.14	La solución SIEM debe permitir la escalabilidad en cada uno de sus componentes
	La solución de SIEM propuesta debe contar con capacidades de integración nativa, sin requerir desarrollos adicionales, que permitan la correlación y análisis de eventos provenientes de las plataformas de seguridad actualmente implementadas en la entidad, incluyendo soluciones de gestión de firewalls, análisis de tráfico, gestión centralizada de configuraciones y detección y respuesta extendida. Esta integración deberá permitir la recolección automática de logs, eventos y alertas.
3.2.15	Realizar análisis del desempeño y flujo de las aplicaciones vía NetFlow, en el caso que la entidad lo requiera, sin que esto genere costos adicionales para la entidad.
3.2.16	Deberá tener la capacidad de ejecutar scripts de remediación cuando un incidente ocurra
3.2.17	Debe tener la capacidad de detectar desviaciones o anomalías en la línea base definida, el comportamiento de las aplicaciones, equipos, usuarios de la plataforma e IPs.
3.2.18	Los eventos capturados por la funcionalidad de recolección de eventos y la detección de los incidentes deben ser en tiempo real.
3.2.17	Deberá poder realizarse filtros por medio de expresiones regulares.
3.2.18	Debe incluir la generación de indicadores de compromiso para cada activo monitoreado, basándose en los ataques recibidos y el uso de amenazas identificadas.
3.2.19	El servicio debe realizar la detección de uso de eventos s o accesos a la plataforma que no concuerden con el patrón histórico de uso o acceso.
3.2.20	Identificar al menos los siguientes eventos de seguridad, mínimos para monitorear:
	Accesos no autorizados
	Denegación de servicio.
	Explotación de vulnerabilidades.
	Fuerza bruta/login.
	Escaneo de puertos.
	Principales orígenes de ataque.
	Principales destinos de ataque.
	Ubicación geográfica del ataque.

	Orígenes/destinos reportados por fuentes de inteligencia de seguridad.
	Acceso por parte de los usuarios a dominios diferentes a los autorizados.
	Cambios sobre Plataformas (software instalado, desinstalado, cambio de políticas del directorio activo)
	Conexiones (accesos remotos, intentos de conexión)
	Eliminación de logs
	Actividades de cuentas de altos privilegios
	Usuarios (bloqueados, agregados, eliminados, desbloqueados, cambio de contraseñas).
	Reinicio o caída de interfaces, procesos y servicios críticos.
	Cambios en BGP/OSPF/EIGRP
	Caídas de puertos del tipo Storage
3.2.21	Se debe garantizar durante la vigencia de la suscripcion el almacenamiento online de los eventos de seguridad correlacionados, los incidentes de seguridad, el historial de comportamiento y las vulnerabilidades de los activos. A la fecha de finalización de este año, dichos eventos deben ser entregados al Entidad en medio digital.
3.2.22	Los conectores de captura de eventos deberán enviar en todo momento y en tiempo real los eventos recolectados hacia el motor de correlación, salvo que se requiera habilitar bajo demanda de envió asíncrono de eventos.
3.2.23	La transmisión de los datos entre los componentes recolectores de eventos y el motor de correlación deberán utilizar mecanismos de cifrado y de compresión de datos.
3.2.24	El servicio debe estar en la capacidad de comprobar la integridad de los eventos correlacionados.
3.2.25	Los componentes que realizan la recolección de eventos deberán verificar constantemente el estado de la conexión con el correlacionado a través de un mecanismo eficaz que ante la eventual pérdida de la conexión entre el componente de recolección y el motor de correlación, genere de manera inmediata la notificación, adicionalmente el primero deberá almacenar de forma inmediata los eventos bajo una cache de tamaño configurable hasta que se reanude dicha conexión, realizando la transmisión de los eventos hasta vaciar el cache.
3.2.26	La solución debe permitir detectar fluctuaciones en la recepción de logs por fuente de información.
3.2.27	Los componentes que realizan la recolección de eventos deberán tener la capacidad de filtrado de eventos particulares desde el origen, con lo que se reducirá el volumen de eventos que recibirá el motor de correlación.
3.2.28	La solución de recolección y correlación de eventos (SIEM) debe tener la capacidad de ofuscar/eliminar campos sensibles, capacidad de agregación y filtrado.
3.2.29	El servicio debe tener la posibilidad de integrar las vulnerabilidades (detectadas por la Entidad) con el monitoreo y correlación y se deben declarar incidentes ante vulnerabilidades detectadas durante la prestación del servicio
3.2.35	Deberá soportar la correlación de eventos de múltiples fuentes, tales como Firewalls, Servidores, estaciones de trabajo, WAF, Switches, bases de datos, entre otros.
3.2.36	Deberá contar con la característica de monitoreo de HiperVisor tales como VMWARE y HypeV, entre otros.
	La solución SIEM debe tener un motor distribuido de correlación de eventos en tiempo real, con el fin de mejorar la ingesta de datos siendo capaz de manejar múltiples reglas dado el alto grado de eventos
3.2.37	Deberá poder monitorear plataformas de almacenamiento tales como EMC, Bucket VeeamBackup, entre otros a nivel de desempeño y uso de almacenamiento.
3.2.38	Deberá poder monitorear sistemas del tipo directorio activo y Exchange basado en WMI y PowerShell.

3.2.39	Deberá poder monitorear motores de bases de datos SQL Server, Oracle, MySQL entre otras, vía JDBC.
3.2.40	Deberá soportar protocolos de comunicación en IPv4 e Ipv6.
4. GESTIÓN DE INCIDENTES DEL SOC	
4,1	El SOC deberá alertar, atender, clasificar y apoyar activamente la resolución y contención de los incidentes de seguridad y ciberseguridad de la información del Entidad en los cuales se requiera su participación.
4,2	El contratista debe participar y apoyar en la resolución de incidentes de seguridad de la información a través de su grupo de trabajo.
4,3	Cuando se registre eventos o incidentes de seguridad de la información se debe realizar un análisis inicial el cual deberá tener en cuenta lo siguiente:
	Investigación: Quién, Qué, Cómo, Cuándo, Dónde y Por Qué.
	Clasificación: Evento, Incidente.
	Categorización: Ataque Informático, Código Malicioso, Falla, Vulnerabilidad.
	Correlación: Hosts, Red.
	Valoración: Alto, Medio, Bajo
	Elaboración, entrega y seguimiento del plan de trabajo para Investigación, Contención, Erradicación, Recuperación, Prevención y Comunicados a eventos e incidentes.
	Debe dar seguimiento de Eventos e incidentes desde la creación hasta el cierre.
6. TABLEROS DEL SOC **(Dado que el SOC es quien recoge toda la información de las demás herramientas se requiere de este tablero, el cual es compendio de los demás servicios)**	
6,1	La plataforma entregada por el contratista deberá tener:
	• Una consola del tipo Tablero de Gestión en la cual se pueda visualizar en línea, en tiempo real y de forma segura varios tipos de gráficas y tablas, lo cual permita tener una visión global de los incidentes de seguridad, un resumen ejecutivo y un cuadro de mandos, que contemple:
	o El estado de los ANS contratados, o El análisis y acciones ejecutadas por los analistas del SOC.
	o El estado de las plataformas
	o Incidentes registrados y las acciones que ha tomado el SOC y el Entidad para solucionar los eventos de seguridad que se presenten.
	o Vulnerabilidades
	o Trazabilidad de la mitigación del problema con asignación individual a los activos/usuarios.
	• Un módulo para el cálculo de los SLA. Debe estar en la capacidad de calcular el SLA de la disponibilidad de los activos discriminando entre horas laborales y no laborales
	• Un módulo grafico que muestre la infraestructura existente, las conexiones de las mismas y los eventos generados en cada activo.
	• Un tablero que permita identificar en un mapa los incidentes y su ubicación geográfica.
	• Un módulo para revisar las políticas de correlación.
	• Un módulo para la visualización de los agentes instalados y su estado dentro del SOC.
	• Un módulo de visualización para la característica de “base de datos de la gestión de configuración” o CMDB.
	• Un módulo que permita validar el estado del incidente, con sus acciones de remediación y el estado del incidente.
	El contratista debe entregar imagen del Tablero donde muestre esta funcionalidad.
6,2	El tablero debe gestionar todos los incidentes usando un número de ticket, además el ticket debe contar con toda la información relevante del incidente para revisión del Entidad.

6,3	Debe realizar un seguimiento a través de acuerdos de nivel de servicio (ANS) e indicadores clave de desempeño en ingles *Key Performance Indicator* (KPI's) continuamente actualizados.
6,4	Debe permitir realizar configuraciones de vistas resumidas que puedan ser personalizables y que contengan la información técnica de las plataformas que se encuentran bajo gestión.
6,5	Debe contar con vistas de acuerdo con los roles necesarios para los diferentes niveles que indique el Entidad.
6,6	Debe permitir la integración de gestión de vulnerabilidades para llevar el registro de avance y remediación de estas.
6,7	Debe permitir exportar los datos soportando múltiples formatos, incluyendo por lo menos los formatos: csv, xml y pdf.
7. REPORTES DEL SOC (Dado todas las herramientas reportan al SOC, se requieren de los siguientes reportes que genera el SOC y no reportes aislados)	
7,1	Informe de las actividades realizadas del *implementación*, *monitoreo y alertamiento*. Donde se relacionen las acciones de implementación y monitoreo realizadas por el contratista durante el mes con sus correspondientes evidencias que permitan verificar el cumplimiento de los Acuerdos de Nivel de Servicio, donde se relacione el estado de la suscripción, alertas, estado y riesgos de los activos monitoreados.
	Periodicidad: mensual – sujeto a modificaciones según requerimientos del supervisor
7,2	Informe de *incidentes y eventos de seguridad* que hayan sido detectados, atendidos, pendientes y gestionados, con su correspondiente estado, clasificación, acciones de mejora si aplica, descripción de la gestión (acompañamiento) realizada frente a la mitigación ejecutada, descripción de las lecciones aprendidas para futuros eventos e incidentes, descripción de las actividades definidas para la mejora continua.
	Periodicidad: mensual – sujeto a modificaciones según requerimientos del supervisor
7,3	Informe de *incidentes de disponibilidad* que hayan sido detectados, atendidos, pendientes y gestionados, con su correspondiente estado, acciones de mejora si aplica, descripción de la gestión (acompañamiento) realizada frente a la mitigación ejecutada, descripción de las lecciones aprendidas para futuros eventos e incidentes, descripción de las actividades definidas para la mejora continua.
	Periodicidad: mensual – sujeto a modificaciones según requerimientos del supervisor
7,4	Informe de *incidentes de rendimiento* que hayan sido detectados, atendidos, pendientes y gestionados, con su correspondiente estado, acciones de mejora si aplica, descripción de la gestión (acompañamiento) realizada frente a la mitigación ejecutada, descripción de las lecciones aprendidas para futuros eventos e incidentes, descripción de las actividades definidas para la mejora continua. Periodicidad: mensual sujeto a modificaciones según requerimientos del supervisor
7,5	Cuando se presente un evento o incidente crítico el contratista debe entregar en un tiempo no mayor a treinta (30) minutos, un reporte donde se pueda evidenciar por lo menos la siguiente información:
	• Usuario vector
	• IP origen.
	• IP destino
	• Dispositivo (s) comprometido (s).
	• Actividad ejecutada por el atacante.
	• Intentos de ataque.
	• Categoría del evento o incidente.
	• Propuesta de actividades a ejecutar para su contención.

7,6	Los siguientes reportes podrán ser generados de acuerdo con el monitoreo y según los acordado con el supervisor del contrato:
	- Reporte de Incidentes de seguridad.
	- Reporte de Actividades Sospechosas de Usuarios / Equipos / Aplicaciones.
	- Reporte de Integridad de Archivos.
	- Reporte de Cambios de Configuraciones.
	- Reporte de Cambios no Autorizados en los Registros de Windows.
	- Reporte de Violaciones de Políticas de Control de Acceso.
	- Reporte de Incidentes de Disponibilidad.
	- Reporte de Incidentes de Rendimiento o Recursos.
	- Reporte de Incidentes de Caídas en Servicios.
	- Reporte de Incidentes de Caídas en Aplicaciones.
	- Reporte de Cambios en los Registros.
	- Reporte de Cambios en el Software Instalado.
	- Reporte de CMDB a nivel de las plataformas monitoreadas.
	- Reporte de Cumplimiento de acuerdos de nivel de servicios, en inglés Service Level Agreement (SLA´s) de la entidad.
	- Abusos de Privilegios de Navegación.
	- Malware en el mes.
	- Ataques a la infraestructura.
	- Usuarios con Malware
	- Usuarios con Botnets.
	- Usuarios no productivos.
	- Aplicaciones maliciosas en la Red.
	- Exploits Detectados.
	- Usuarios/ Equipos más Riesgoso para la entidad.
	- Categorías más usadas por los usuarios.
	- Destinos maliciosos de la red.
	- Usos de la VPN a horas no laborales.
	- Segmentos de Red comprometidos.
	soportar reportes de cumplimiento tales como PCI-DSS, HIPAA, SOX, NERC, FISMA, GLBA, GPG13, SANS Critical Controls, CISK, COBIT, ITIL, ISO 27001, NERC, NIST800-53, NIST800-171, NESA, KSA ECC.
	- Entre otros
8.	**SERVICIO DE ANALISIS DE VULNERABILIDADES**
8.1	El análisis de vulnerabilidades hará parte integral del servicio de SOC gestionado, sin que la entidad deba adquirir herramientas o licencias adicionales.
8.2	Se deberán ejecutar dos (2) ejercicios anuales de análisis de vulnerabilidades, cada uno con su respectivo reescaneo (retest) para validar las acciones de remediación.
8.3	Requiere una consola para el análisis de activos expuestos a internet y agente virtualizado (máquina virtual) para activos internos.
8.4	Se incluye la cobertura para hasta 100 activos IP y 50 aplicaciones web, que podrán distribuirse entre infraestructura TI, ASM (superficies expuestas) y aplicaciones web.
8.5	El proveedor será responsable de la instalación, configuración, implementación, puesta en producción, administración y soporte completo de la solución durante la vigencia de la suscripción.

8.6	La plataforma debe permitir realizar el análisis programado de vulnerabilidades conforme al cronograma acordado con la entidad, incluyendo el escaneo inicial y su retest.
8.7	El acceso a la plataforma se podrá realizar desde cualquier ubicación con conexión a internet, lo que facilita la colaboración y la gestión remota.
8.8	La solución debe ser escalable, permitiendo la administración de múltiples motores distribuidos y ajustándose a cambios en el volumen de activos.
8.9	La herramienta debe cumplir con estándares y marcos de seguridad reconocidos, tales como BugTraq, CAPEC, CVSS v2/v3, CWE, Exploits Available, OWASP Top 10 y PCI-DSS.
8.10	El proveedor debe ejecutar como mínimo las siguientes actividades: configuración inicial de sensores o agentes, planificación y ejecución de escaneos, interpretación de hallazgos, soporte técnico y acompañamiento mensual.
8.11	Por cada uno de los ejercicios (escaneo inicial y su retest), se deberá entregar un informe técnico y ejecutivo en formato PDF y editable (Word o Excel), incluyendo una reunión virtual para socializar hallazgos y recomendaciones, 5 días hábiles posterior a culminar el escaneo.
8.12	El contenido mínimo de cada informe incluirá: resumen ejecutivo, detalle técnico por activo, análisis de configuraciones inseguras, evidencias del escaneo, recomendaciones estratégicas e historial de acciones tomadas.
9. SERVICIO DE CONTROL DE ACCESO A LA RED NAC	
9.1	La solución de Control de Acceso a la Red (NAC) hará parte integral del servicio de SOC contratado. Todo el licenciamiento, infraestructura, soporte técnico, administración y operación del sistema NAC deberá ser provisto, gestionado y mantenido por el proveedor del SOC, como un componente funcional del mismo.
9.2	La solución de Control de Acceso a la Red (NAC) ofertada deberá contar con capacidad de integración nativa, comprobada y soportada por el fabricante, con las soluciones de ciberseguridad actualmente implementadas en la infraestructura tecnológica de la entidad. Esta integración deberá permitir el intercambio de eventos, políticas, alertas y/o decisiones de control de acceso en tiempo real, de forma automatizada y sin requerimientos de desarrollo a medida
9.3	Incluir protección para 1200 equipos de usuario concurrentes (900 usuarios institucionales y 300 Invitados o dispositivos móviles)
9.4	Ser escalable, permitiendo una ampliar el despliegue inicial, bien sea apilando más licencias de dispositivos o añadiendo más clústers, que puedan cubrir áreas específicas de la red, o zonas geográficas concretas.
9.5	La solución debe integrar todos los componentes físicos y lógicos, licenciamiento propietario o de terceros requeridos para la exitosa implementación, sin generar un costo adicional para la entidad.
9.6	Soportar el perfilado de dispositivos interactuando con el dispositivo mediante HTTP/HTTPS, SSH/Telnet o incluso interaccionando con el dispositivo a través de scripts diseñados a medida.
9.7	Soportar opciones de autenticación flexibles, incluyendo 802.1X, autenticación WEB y autenticación MAC.
9.8	Debe permitir conectarse a la red institucional solo a dispositivos autenticados/registrados, desplegando políticas de seguridad que bloqueen y aíslen dispositivos que no cumplan los controles institucionales, enviándolos a un área de cuarentena sin necesidad de intervención por parte de los administradores de red.
9.9	Permitir la autenticación de usuarios a través de un portal web seguro HTTPS con redireccionamiento automático, tanto en red inalámbrica como en red alámbrica.
9.10	Ser capaz de controlar escenarios en los que hay más de un equipo conectado a un puerto, asociando a cada equipo la VLAN adecuada, siempre que el equipo de acceso lo permita.
9.11	Soportar la evaluación de la postura de seguridad basada en agentes y sin agentes.
9.12	La Solución debe permitir las siguientes opciones de Visibilidad: − Debe permitir la detección de hosts desconocidos. − Debe permitir la identificación de hosts y/o usuarios mediante Portal Cautivo.

	− Debe permitir la identificación de usuarios mediante Active Directory. − Debe permitir la categorización automática de hosts. − Debe recordar el perfil asignado a cada host, y verificar que sigue siendo válido en cada nueva conexión del host. Si el perfil variara, deberá impedir su conexión y notificar inmediatamente sobre el hecho. − Debe permitir la fijación de períodos de tiempo en los que el host está autorizado a operar, y evaluarlos periódicamente. − Debe permitir la importación de un archivo .CSV conteniendo información sobre los hosts a registrar. − Debe permitir la integración con plataformas MDM (MDM de Google) − La solución no debe requerir obligatoriamente el uso de 802.1x para permitir el descubrimiento de hosts en la infraestructura cableada. − Debe permitir determinar el perfil de los hosts descubiertos mediante métodos que no requieran la instalación de agentes incluyendo, al menos, los siguientes: DHCP Fingerprinting, HTTP/HTTPS, Ubicación, SNMP, SSH, Telnet, TCP, UDP, OUI, WMI, WinRM − La solución debe poder reconocer los siguientes sistemas operativos sin necesidad de agentes: DHCP Fingerprinting, HTTP/HTTPS, Ubicación, SNMP, SSH, Telnet, TCP, UDP, OUI, WMI, WinRM" − Debe permitir la designación de un Sponsor que autorice el acceso de un invitado. − Debe permitir la designación de un Sponsor que autorice la categorización de un host.
9.13	Ante una alarma de seguridad debe permitir el bloqueo o aislamiento automático de los hosts comprometidos
9.14	La solución debe poder interoperar con dispositivos de conexión cableada e inalámbrica de los principales fabricantes, incluyendo, como mínimo: Cisco/Meraki, HP/HP Procurve/3Com/H3C/Aruba, Extreme Networks/Enterasys/Motorola/Avaya/Brocade/Foundry Networks, Fortinet/Meru, Juniper, Dell, Alcatel-Lucent, D-Link, Huawei Technology, Ruckus, Riverbed/Xirrus.
9.15	La solución debe permitir distintos roles administrativos, incluyendo la capacidad de limitar y controlar la cantidad de acceso permitido a las funcionalidades disponibles, dependiendo del grupo administrativo de la organización al que pertenezca el usuario.
9.16	La solución debe proveer un log de auditoría de todas las conexiones de la red, tanto cableadas como inalámbricas. Esto debe incluir una interfaz amigable, que permita buscar y generar consultas en la información almacenada. Teniendo en cuenta que el proyecto se va a ejecutar bajo la modalidad de servicio, el Data Center donde se encuentre alojada toda la infraestructura debe estar localizado en Colombia.
9.17	La solución debe incluir un log de auditoría de todas las acciones y cambios realizados al sistema por los usuarios administradores, incluyendo qué se cambió, cuándo se cambió y quién lo cambió.
9.18	Ser capaz de controlar escenarios en los que hay más de un equipo conectado a un puerto, asociando a cada equipo la VLAN adecuada, siempre que el equipo de acceso lo permita.
9.19	La solución debe contar con las siguientes funcionalidades de Reportes: − Debe contar con un Tablero de Control que presente información relevante de manera resumida. − Debe contar con reportes predefinidos que incluyan resultados sobre: Registro de Invitados; Registro de dispositivos; Escaneo de Dispositivos − Debe permitir la generación y archivado de reportes periódicos − Debe permitir el envío automatizado de reportes mediante correo electrónico − Debe contar con reportes de Compliance de PCI. − La información de los reportes debe poder ser exportada en formato HTML, CSV, Excel, XML, RTF o PDF. − Debe permitir la aceptación y eliminación de alarmas del log de forma manual. − Debe permitir la aceptación y eliminación de alarmas del log de forma automática. − Debe permitir la definición de alarmas en función de la ocurrencia de determinados eventos.

9.20	La Solución debe permitir las siguientes opciones de Control y/o Automatización: − La solución no debe requerir obligatoriamente el uso de 802.1x para brindar control de acceso a nivel de Puerto en la infraestructura cableada. − Debe permitir el uso de agentes persistentes, evanescentes (desaparecen luego de realizado en análisis) o pasivos. − La solución debe tener la capacidad de aprovechar la combinación de informaciones sobre la identidad del usuario y el tipo de dispositivo para aprovisionar dinámicamente permisos de acceso basados en roles y distintos niveles de acceso. − Debe permitir la generación de políticas de control, agrupadas jerárquicamente, y determinar la política a aplicar a cada dispositivo en función de una serie de reglas de asignación. − Debe soportar, al menos, los siguientes tipos de información para determinar la política a aplicar: Ubicación, Grupo de Pertenencia, Atributo, Fecha y Hora − La solución debe incluir funcionalidades de Guest Management, permitiendo la creación de perfiles de Invitados y Contratistas. − Debe permitir la creación de plantillas que agrupen a los invitados o contratistas en grupos que tengan distintos permisos de acceso, o períodos de tiempo de acceso permitido. − Debe contar con herramientas que permitan la generación y mantenimiento de este tipo de usuarios y sus claves de acceso. − Debe permitir la creación de Portales de Auto-Registro. − Debe soportar el envío de claves de acceso mediante SMS. − Si un dispositivo no pasa los tests de Compliance, debe ser posible no forzar la remediación, forzar la remediación inmediatamente, enviando al dispositivo a una red de cuarentena, o permitir la remediación retardada, dando un período de tiempo desde la detección inicial de problemas, para la solución de estos. Pasado el período de tolerancia, de persistir los problemas, el dispositivo debe ser puesto en cuarentena inmediatamente. − Debe permitir la existencia de Sponsors que aprueben el ingreso de Invitados o Contratistas a la red, o que eleven los permisos de acceso de ciertos individuos.
9.21	La solución debe permitir la integración de dispositivos de infraestructura de seguridad de terceras partes, incluyendo: CheckPoint, Cyphort, Cisco/SourceFire, FireEye, Fortinet, Juniper/Netscreen, Palo Alto, Qualys, SonicWall, Tenable, AirWatch, MobileIron, MaaS360, Citrix XenMobile, Adtran/BlueSocket.
9.22	La solución debe poder interoperar con dispositivos de conexión cableada e inalámbrica de los principales fabricantes, incluyendo, como mínimo: Cisco/Meraki, HP/HP Procurve/3Com/H3C/Aruba, Extreme Networks/Enterasys/Motorola/Avaya/Brocade/Foundry Networks, Fortinet/Meru, Juniper, Dell, Alcatel-Lucent, D-Link, Huawei Technology, Ruckus, Riverbed/Xirrus.
10. SERVICIO DE DATA LOSS PREVENTION - DLP	
10.1	La solución de Data Loss Prevention (DLP) hará parte integral del servicio de SOC contratado. Todo el licenciamiento, infraestructura, soporte técnico, administración y operación del sistema DLP deberá ser provisto, gestionado y mantenido por el proveedor del SOC, como un componente funcional del mismo.
10.2	La solución de Data Loss Prevention (DLP) ofertada deberá contar con capacidad de integración nativa, comprobada y soportada por el fabricante, con las soluciones de ciberseguridad actualmente implementadas en la infraestructura tecnológica de la entidad. Esta integración deberá permitir el intercambio de eventos, políticas, alertas y/o decisiones de control de acceso en tiempo real, de forma automatizada y sin requerimientos de desarrollo a medida
10.3	protección para 900 EndPoints. Entre Servidores y Usuarios finales
10.4	La solución debe prevenir la exfiltración y pérdida accidental de datos.
10.5	La solución debe proporcionar visibilidad inmediata sobre el movimiento y la actividad de los datos.

10.6	La solución debe proporcionar un agente unificado que consolide todas las funcionalidades de monitoreo y bloqueo.
10.7	La solución debe detectar y responder a la manipulación de datos y actividades anómalas utilizando IA y ML.
10.8	La solución debe tener capacidades de inteligencia artificial o aprendizaje automático.
10.9	La solución debe integrar aprendizaje automático desde el primer día para establecer una línea base de la actividad individual del usuario y utilizar algoritmos de análisis de comportamiento para detectar comportamientos típicos frente a comportamientos novedosos o anómalos.
10.10	La solución debe proporcionar capacidades adicionales de análisis y analítica para ofrecer insights a nivel organizacional.
10.11	La solución debe ser capaz de monitorear amenazas internas y empleados de alto riesgo.
10.12	La solución debe aplicar políticas de riesgo interno con acciones de seguridad proactivas en tiempo real.
10.13	La solución debe identificar y mitigar amenazas internas a través de análisis avanzados de comportamiento de usuarios.
10.14	La solución debe mapear las actividades en un formato de MITRE.
10.15	La solución debe permitir políticas de protección de privacidad de datos como almacenamiento de datos y logs forenses en datacenters de la compañía, colocar seudónimos a los nombres de las cuentas que se están investigando para que el analista no sepa a quien se hace la revisión e incluir la autorización de investigaciones fuera de la caja (out-of-the-box) por parte de analistas.
10.16	La solución debe monitorear y bloquear datos sensibles transferidos a través de navegadores web a dominios públicos externos (por ejemplo, Gmail, Yahoo, Hotmail).
10.17	La solución debe diferenciar entre datos sensibles transferidos a soluciones en la nube empresariales y soluciones en la nube personales (por ejemplo, Google Drive para Empresas vs. Google Drive Personal).
10.18	La solución debe monitorear y bloquear datos sensibles transferidos a dispositivos USB.
10.19	La solución debe monitorear datos sensibles transferidos a través de aplicaciones de terceros (por ejemplo, Putty).
10.20	La solución debe monitorear datos sensibles copiados mediante capturas de pantalla.
10.21	La solución debe monitorear datos sensibles copiados a través de pulsaciones de teclas (por ejemplo, imprimir pantalla).
10.22	La solución debe restringir y monitorear la impresión de archivos en formato PDF o en impresora física
10.23	La solución debe monitorear datos sensibles copiados a nivel de archivo/carpeta.
10.24	La solución debe monitorear datos sensibles copiados a nivel de comando (por ejemplo, símbolo del sistema, terminal).
10.25	La solución debe monitorear datos sensibles copiados/descargados a una máquina virtual sin agente de punto final.
10.26	La solución debe soportar el rastreo de múltiples archivos compartidos por un usuario.
10.27	La solución debe soportar el monitoreo del movimiento de datos sensibles fuera de un conjunto definido de usuarios.
10.28	La solución debe exportar un historial de todo el movimiento de datos dentro de la empresa, incluyendo datos provenientes de fuentes externas.
10.29	La solución debe monitorear la descarga de datos sensibles por un usuario directamente desde una aplicación/servidor de aplicaciones.
10.30	La solución debe proporcionar detalles de los datos sensibles descargados por un usuario durante un período especificado, incluyendo el número total de archivos, volumen de descarga, nombres de archivos y origen.

10.31	La solución debe monitorear servicios y plataformas de correo electrónico (por ejemplo, MS Exchange, Office 365, Gmail, Outlook).
10.32	La solución debe bloquear el montaje de unidades de almacenamiento removibles (por ejemplo, USB, HDD externo).
10.33	La solución debe monitorear y bloquear datos sensibles impresos en impresoras físicas y/o PDF.
10.34	La solución debe proporcionar un dashboard para cumplimiento y auditoría.
10.35	La solución debe soportar la generación de reportes personalizados basados en usuarios específicos.
10.36	La solución debe soportar la generación de reportes personalizados basados en tipos específicos de datos.
10.37	La solución debe soportar la generación de reportes personalizados basados en períodos específicos.
10.38	La solución debe integrarse con otras herramientas de ciberseguridad (e.g., SIEM).
10.39	La solución debe integrarse con Active Directory, Azure AD y soluciones LDAP de terceros.
10.40	La solución debe soportar MFA (Autenticación Multifactor).
10.41	La solución debe soportar SSO (Inicio de Sesión Único) con Active Directory, Entra ID, GCP, Amazon, AWS.
10.42	La plataforma debe monitorear la actividad en aplicaciones de inteligencia artificial (e.g., ChatGPT).
10.43	La solución debe funcionar independientemente de la conexión de red y la ubicación.
10.44	La solución debe monitorear el uso de aplicaciones SaaS, incluyendo herramientas de Shadow AI como Gen-AI, e incorporar educación de usuarios basada en riesgos en el punto de acceso a datos sensibles.
10.45	La solución debe aplicar análisis de comportamiento de usuarios y entidades a gran escala.
10.46	La solución debe utilizar un agente escalable y ligero para recopilar y registrar datos.
10.47	La solución debe educar a los usuarios sobre el manejo adecuado de datos.
10.48	La solución debe proporcionar formación basada en riesgos para mejorar la seguridad de los datos.
10.49	La solución debe incluir notificaciones personalizadas y recordatorios para reforzar la conciencia sobre las políticas de seguridad y dirigir a los usuarios a alternativas aceptables cuando se detecten aplicaciones no autorizadas.
10.50	La solución debe identificar el uso de Shadow AI y detener la carga de datos sensibles.
10.51	La solución debe mapear automáticamente las detecciones a una base de conocimientos de tácticas, técnicas y procedimientos de amenazas internas.
10.52	La solución debe cumplir con los requisitos de residencia de datos.
10.53	La solución debe reducir los costos de ancho de banda al no depender de un motor de escaneo de archivos basado en la nube.
10.54	La solución debe integrarse fácilmente con los sistemas y plataformas existentes en la organización.
10.55	La solución debe ser compatible con dispositivos y plataformas de colaboración.
10.56	La solución debe utilizar tecnología de agente ligero para sistemas operativos Windows, macOS y Linux para una implementación sin problemas y actualizaciones automáticas a escala empresarial.
10.57	La solución debe proporcionar perfiles MDM, transmisión de eventos, webhooks y una API abierta para la integración con herramientas MDM, SIEM, SOAR, de automatización y de mesa de servicio existentes.
10.58	La solución debe identificar y rastrear datos automáticamente según su origen, como sistemas de recursos humanos o repositorios de código fuente.
10.59	La solución debe aplicar políticas de DLP y de riesgo interno basadas en el origen de los datos y si se utilizó una cuenta corporativa o no corporativa para la salida de datos.

10.60	La solución debe proporcionar visibilidad inmediata sin políticas sobre el movimiento de datos y los procesos empresariales.
10.61	La solución debe incluir un asistente de IA que resuma y contextualice los datos asociados con actividades de alto riesgo para acelerar el análisis de incidentes.
10.62	La solución debe mapear las actividades a una base de conocimientos de tácticas, técnicas y procedimientos de amenazas internas.
10.63	La solución debe estar disponible en la nube para facilitar su implementación y escalabilidad.
10.64	La solución debe permitir a las organizaciones activar servicios y obtener visibilidad de riesgos de datos en minutos para proteger datos sensibles desde el primer día.
10.65	La solución debe ayudar a cumplir con requisitos clave de cumplimiento, incluyendo PCI DSS, HIPAA, ISO 27001, NIST, PII, PHI, entre otros.
10.66	La solución debe proporcionar visibilidad profunda en las actividades de los usuarios, el acceso a datos y los sistemas para prevenir la salida de datos sensibles.
10.67	La solución debe abordar los controles de cumplimiento normativo relacionados con la prevención de pérdida de datos con un esfuerzo mínimo utilizando políticas predefinidas de PII/PHI/PCI.
10.67	La solución debe priorizar la privacidad bajo regulaciones como GDPR y CCPA.
	La solución debe utilizar técnicas de minimización de datos integradas, como la seudonimización y el almacenamiento forense localizado, para ayudar a los equipos de seguridad a detectar y mitigar amenazas mientras se protege la confidencialidad de los empleados.
10.68	La solución debe almacenar los registros forenses en centros de datos controlados por el cliente en la región.
10.69	La solución debe minimizar los conjuntos de datos de investigación seudonimizados.
10.70	La solución debe incluir flujos de trabajo de autorización de investigación listos para usar para los analistas.
10.71	La solución debe proporcionar visibilidad de datos, evaluación de riesgos y políticas de protección de datos listas para usar para proteger los activos de información críticos dentro y fuera de la red.
10.72	La solución debe analizar qué datos se están utilizando y cómo, permitiendo determinar la mejor respuesta.
10.73	La solución debe clasificar y rastrear datos en tiempo real para proporcionar visibilidad y protección de datos inmediata, sin necesidad de políticas predefinidas.
10.74	La solución debe utilizar agentes, extensiones de navegador y conectores en la nube para recopilar, enriquecer e indexar automáticamente la actividad a través de diferentes tipos de eventos (autenticación, web, email, aplicaciones, USB, creación de archivos, compartición y descarga de archivos).
10.75	La solución debe aplicar políticas adaptativas basadas en riesgos que consideren factores de riesgo y permitan decidir qué acciones tomar, como notificar a los usuarios a través de Microsoft Teams o Slack, capturar forenses de archivos y pantallas, aislar o bloquear un endpoint, terminar un proceso o bloquear actividades de alto riesgo.
10.76	La solución debe proporcionar un feed de actividad detallado y secuenciado en el tiempo que permita a los analistas ver la actividad de usuarios, datos y dispositivos antes, durante y después de un incidente.
10.77	La solución debe mapear las detecciones de actividades de alto riesgo a una base de conocimientos de tácticas, técnicas y procedimientos de amenazas internas y secuenciarlas automáticamente en incidentes con puntuación de riesgo para priorizar las investigaciones.
10.78	La solución debe permitir a los analistas de seguridad tomar acciones según la gravedad del riesgo, como mostrar un mensaje en pantalla al empleado, tomar una captura de pantalla, terminar un proceso, bloquear conexiones a un dispositivo o bloquear el teclado y el ratón de un dispositivo.
10.79	La solución debe incluir gestión de casos integrada y reportes de riesgos que destaquen comportamientos descuidados, maliciosos y accidentales a lo largo del tiempo, permitiendo evaluar la efectividad de los controles de seguridad e identificar áreas de mejora.

10.80	Los reportes deben poder exportarse fácilmente para compartir con la dirección.
10.81	La solución debe proporcionar visibilidad integral de las interacciones de los usuarios con los datos en la nube y mantener la protección a medida que los datos se mueven fuera de la nube, asegurando la protección continua de la información sensible, independientemente de su ubicación o método de acceso.
10.82	La solución debe construir un inventario completo con puntuación de riesgo de las aplicaciones SaaS y herramientas GenAI utilizadas en toda la organización, con información sobre el ingreso, egreso y credenciales de datos.
	La solución debe fortalecer las defensas contra posibles brechas de datos derivadas de la exposición de datos empresariales a través del uso no autorizado de aplicaciones, incentivando a los empleados a usar herramientas autorizadas.
10.83	La solución debe proporcionar notificaciones personalizadas y recordatorios para reforzar la conciencia sobre las políticas de seguridad y dirigir a los usuarios a alternativas aceptables cuando se detecten aplicaciones no autorizadas. Las notificaciones deben poder enviarse a través de diálogos en el endpoint, correo electrónico, Microsoft Teams y sistemas de mensajería Slack.
10.84	La solución debe proporcionar capacitación basada en riesgos para entrenar a los empleados a tomar las decisiones correctas basadas en la detección de comportamientos inaceptables, reforzar las políticas de seguridad corporativa y promover una buena higiene cibernética.
10.85	La solución debe incluir reglas predefinidas para detectar prácticas de higiene cibernética deficientes, como la carga de archivos confidenciales a ubicaciones inesperadas, la conexión a redes Wi-Fi no seguras, la inserción de dispositivos de hardware maliciosos o el uso de aplicaciones no autorizadas para almacenamiento en la nube o dispositivos USB.
10.86	Sistemas operativos soportados: Windows 10, 11, Windows server 2012 R2 y siguientes, MACOs Mojave 10.14 y siguientes, Red Hat Enterprise Linux 7 y siguientes, Centos / y siguientes, Ubuntu 16.04 LTS y 17.10 y debian 8 y siguientes
10.87	La solución requerida debe incluir la licencia para Control de dispositivos integrada, DLP en linea para web, correo, Cloud Drive y conectores de medio, Clasificación de datos en tiempo real, análisis de riesgo de aplicaciones SaaS y de Inteligencia Artificial generativa, Entrenamiento de riesgos a usuarios finales, Soporte de librerías de cumplimiento regulatorio, etiquetas de microsoft MIP/AIP, archivos forenses, gestión de incidentes y secuencia de tiempo de actividad,
10.88	La solución requerida debe incluir las licencias necesarias para monitoreo de actividades de usuario y equipo final, analítica de comportamiento con Machine learning, detección de manipulación de datos, aislamiento de usuarios finales y bloqueo en tiempo real, detección de incidentes con puntuación de riesgo, captura de pantalla para análisis forense, gestión de caso, librería de detección de riesgo asociado a mapas de Mitre ATT&ck, conectores de integración con Google workspace, Microsoft office 365 y controles de compartir archivos.
10.89	La solución debe incluir un servicio de buenas prácticas llevado a cabo por el fabricante que incluya el análisis inicial, revisión de políticas a implementar, ajuste de la solución, recomendaciones y seguimiento durante el primer mes de implementación y seguimiento mensual y final de la solución implementada. Debe realizarse directamente por el fabricante de la solución, no puede ser realizado por el oferente.
11. SOPORTE	
11.1	El oferente debe contar con una mesa de ayuda certificada en ITIL que permita a la Entidad contactarse con el SOC para la apertura de tickets con al menos en tres formas distintas de comunicación, por llamada a un teléfono fijo o celular, por correo electrónico o por el portal web de generación de tickets. Para lo cual el oferente deberá adjuntar certificación del fabricante de la herramienta usada por la mesa de ayuda donde indique que cuenta al menos 9 procesos de ITIL.

	El servicio se prestará por suscripción para el análisis de activos expuestos a internet y agente virtualizado (máquina virtual) para activos internos.
11.2	Debe incluir el soporte técnico, en la modalidad Estándar 7*24*365 por el periodo en el cual este vigente el servicio por suscripción, es decir un (1) año a partir de la entrega del certificado de derecho de uso del SIEM, teniendo en cuenta los siguientes ítems: 1. El prestador de servicio debe contar con certificación vigente por el ente tercero certificador directamente al fabricante de la herramienta usada por la mesa de ayuda en al menos 9 procesos de ITIL. 2.Se podrá realizar su validación en la página oficial de PeopleCert. El enlace se encuentra a continuación: https://atv.peoplecert.org/tool-vendor-accreditation/ 3. Soporte, mantenimiento y actualización del SIEM, DLP y NAC por un (1) año a partir de su activación. 4. Se debe confirmar la recepción del incidente, entregando un número de caso, en un tiempo máximo de 10 minutos contados a partir de la recepción del incidente. 5. El Contratista debe dar respuesta a los incidentes reportados por el Entidad en un tiempo máximo de dos (2) horas, los cuales pueden ser reportados las 24 horas del día, 7 días de la semana. 6. Número de casos ilimitados 7. Analizar el incidente y, según corresponda, verificar la existencia del problema, identificar la causa raíz y dar solución y/o reportar los avances según los tiempos de gestión definidos. 8. Brindar orientación y asistencia a la entidad para resolver la incidente vía remoto en primera instancia y en caso de no dar solución al incidente, la asistencia debe ser presencial. **NOTA:** El contacto con el canal de soporte se debe realizar única y exclusivamente a través de los profesionales designados por el Entidad, quienes centralizaran, priorizaran y filtraran las solicitudes de soporte de los usuarios de acuerdo con los criterios generales del alcance del soporte.
12. SEGURIDAD	
12.1	Para la prestación del servicio el proveedor debe contar con herramientas y métodos para controlar la fuga de información desde el SOC, tales como herramientas DLP (Prevención de Pérdida de Datos), monitoreo de correo electrónico, bloqueo de puertos USB, etc, para disminuir la probabilidad de fuga de información del Entidad a la que tenga acceso con ocasión de la prestación del servicio.
12.2	Para la prestación del servicio el proveedor debe contar con procesos o procedimientos formales debidamente documentados para dar de baja la información de la Entidad (eliminación segura) ya sea por solicitud de la Entidad (si así se solicita) y una vez finalice la prestación de los servicios de tal forma que se garantice la correcta disposición de la información de la entidad.
	Los documentos podrán ser solicitados por la supervisión del contrato en el Entidad, en cualquier momento durante la ejecución y se podrá solicitar soportes que evidencien las actividades y herramientas utilizadas
12.3	El SOC y en general el proponente debe permitir al Entidad realizar auditorías sobre los procesos, tecnologías y personas que operan en el SOC, en caso de ser requerido, todas las veces que el Entidad lo requiera.

12.4	Dada la naturaleza de las actividades a realizar en desarrollo del objeto contractual, el contratista debe garantizar la integridad y confidencialidad de la información institucional a la cual llegue a tener acceso directamente o por intermedio de terceros, para lo cual el contratista suscribe el respectivo compromiso de confidencialidad que hará parte integral del contrato. El contratista deberá asegurar el cuidado, la confidencialidad y la correcta utilización de la información entregada y generada durante la ejecución del contrato, así como de los elementos que para su ejecución el Instituto ponga a su disposición.
12.5	La información confidencial propiedad de la UBPD, en tal virtud, adoptará todas las medidas necesarias para impedir su duplicación, sustracción, divulgación, alteración, ocultamiento o utilización indebida.
13. ENTREGABLES	
13,1	El contratista debe presentar, dentro de las 2 primeras semanas posterior a la adjudicación del contrato, un plan detallado para la implementación y puesta en funcionamiento del SOC.
13,2	Diseño y modelamiento de mínimo diez (10) casos de uso, los cuales serán definidos en conjunto con la Entidad para la puesta en operación del SOC.
13,3	El contratista deberá entregar el certificado de suscripción al SOC, contado a partir de la firma del acta de inicio.
14,6	El contratista deberá remitir los reportes definidos por la entidad cumpliendo con la periodicidad establecida para ellos.
14,7	El proveedor debe generar recomendaciones y notificaciones preventivas para evitar incidentes de seguridad, notificación de amenazas emergente, presencia de campañas de código malicioso (mundial y local), ransomware, phishing, entre otros que apliquen a la entidad. La información debe ser entregada a la Entidad cada vez que sea pertinente y por lo menos una vez al mes.
14,8	Realizar una transferencia de conocimientos no certificada de veinte (20) horas para mínimo 3 colaboradores de la Entidad, la cual debe incluir como mínimo temas de administración, configuración y afinamiento de los componentes implementados.
14,9	Mensualmente se debe realizar reuniones de seguimiento para la presentación del estado de avance del contrato y la presentación de los informes del mes.
14,1	Disponer y mantener actualizada toda la información de la ejecución del contrato en el repositorio dispuesto por la DTI.
15. PLATAFORMA BASE A MONITOREAR	

15,1	Se requiere una solución de SIEM para la monitorización y gestión de eventos de seguridad de al menos 300 dispositivos o 4050 EPS críticos dentro de la infraestructura de la entidad. La solución deberá ser capaz de correlacionar provenientes de los siguientes elementos:

206	Servidores virtuales (Windows - Linux)
33	Servidores físicos
22	Aplicaciones Web
30	Firewall de perímetro
6	Herramientas de seguridad
1	WAF
Total, Dispositivos	**300**

Yeferson Chassaigne
Experto Técnico 04

Carlos A Hernandez Z
Contratista OTIC

EDGAR ALEXANDER PRIETO MUÑOZ
Firmado digitalmente por EDGAR ALEXANDER PRIETO MUÑOZ
Fecha: 2025.09.09 10:29:35 -05'00'

Edgar A Prieto M
Jefe OTIC