ÍNDICE

1. DETALLE Y DESCRIPCIÓN DEL OBJETO

CONTRATAR LA PRESTACIÓN DEL SERVICIO ESPECIALIZADO DE CENTRO DE OPERACIONES DE SEGURIDAD (SOC) PARA LA DETECCIÓN, MONITOREO, GESTIÓN DE ALERTAS Y RESPUESTA A INCIDENTES DE CIBERSEGURIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA SECRETARÍA DISTRITAL DE INTEGRACIÓN SOCIAL.

1.1. ALCANCE DEL OBJETO

El contrato comprende la prestación de un Servicio Especializado de Centro de Operaciones de Seguridad (SOC) en modalidad SOC-as-a-Service (SaaS) para la Secretaría Distrital de Integración Social, orientado a garantizar la detección, monitoreo, análisis, gestión de alertas y respuesta a incidentes de ciberseguridad sobre su infraestructura tecnológica, bajo un esquema de operación continua 7x24x365.

El alcance incluye la implementación, configuración, integración y operación de una plataforma tecnológica que integre capacidades de SIEM, SOAR y XDR, así como el monitoreo continuo de eventos de seguridad, análisis de comportamiento, gestión y respuesta a incidentes, automatización de procesos de seguridad y generación de reportes.

Asimismo, contempla la gestión de vulnerabilidades, ejecución de pruebas de penetración, monitoreo de la exposición cibernética, programas de concientización en seguridad, y la entrega de recomendaciones para el fortalecimiento de la postura de seguridad de la entidad.

El servicio incluye soporte, mantenimiento, actualización de la solución, y operación, garantizando el cumplimiento de estándares y buenas prácticas internacionales en seguridad de la información.

2. ALCANCE FUNCIONAL Y CARACTERÍSTICAS GENERALES

2.1. Requerimientos generales

2.1.1 El contratista deberá proveer un servicio especializado de Centro de Operaciones de Seguridad (SOC) bajo la modalidad de SOC-as-a-Service (SaaS), diseñado para fortalecer las capacidades de detección, análisis y respuesta ante incidentes de ciberseguridad de la Secretaría Distrital de Integración Social.

2.1.2 Plataforma Nativa en la Nube: El servicio debe operar sobre una plataforma de software como servicio (SaaS) del fabricante, alojada en infraestructura cloud, eliminando la necesidad de instalación de infraestructura física (on-premise) por parte de la Entidad.

2.1.3 Arquitectura Unificada: La solución propuesta debe integrar de manera nativa y unificada las capacidades de SIEM (Gestión de Información y Eventos de

Seguridad), SOAR (Orquestación, Automatización y Respuesta de Seguridad) y XDR (Detección y Respuesta Extendidas) en una consola única de gestión.

2.1.4 Disponibilidad del Servicio: El monitoreo, detección y gestión de alertas debe garantizar una operación continua de siete días a la semana, veinticuatro horas al día (7x24x365).

2.1.5 Inteligencia Artificial y Aprendizaje Automático: La plataforma debe emplear algoritmos de Inteligencia Artificial (IA) y Machine Learning (ML) para el análisis de comportamiento de usuarios y entidades (UEBA), permitiendo la identificación de anomalías y amenazas desconocidas o de día cero.

2.1.6 Automatización de Respuesta: El sistema debe contar con capacidades de orquestación y automatización para ejecutar acciones de respuesta inmediata ante incidentes críticos, reduciendo los tiempos de mitigación.

2.1.7 Interoperabilidad y Recolección de Datos: La solución debe tener la capacidad de recolectar, centralizar y correlacionar eventos de seguridad (logs) provenientes de diversas fuentes de la Entidad (nube, aplicaciones, endpoints, red, etc.), asegurando la integridad y el no repudio de la información recolectada.

2.1.8 Escalabilidad y Flexibilidad: El servicio debe permitir la adaptación a las necesidades de crecimiento tecnológico de la Secretaría durante la vigencia del contrato, sin afectar la continuidad de la supervisión.

2.1.9 Soberanía y Seguridad de los Datos: El contratista debe garantizar que el almacenamiento y procesamiento de los datos se realice bajo estrictos estándares de seguridad, cumpliendo con la normativa vigente de protección de datos personales (Ley 1581 de 2012).

2.2 Visualización de red

2.2.1 El servicio debe proporcionar una visibilidad completa y en tiempo real de la infraestructura tecnológica de la Entidad.

2.2.2 Visibilidad Híbrida y Multinube: La plataforma debe permitir la visualización centralizada de activos, independientemente de su ubicación, incluyendo entornos on-premise, nubes privadas y nubes públicas (IaaS, PaaS, SaaS).

2.2.3 Mapeo de Activos y Relaciones: Capacidad de identificar y visualizar automáticamente los activos de red, estableciendo mapas de relaciones y flujos de comunicación para detectar vectores de ataque potenciales.

2.2.4 Análisis de Tráfico y Protocolos: Debe permitir la inspección y el análisis de protocolos estándar y propietarios, facilitando la identificación de comunicaciones anómalas o intentos de exfiltración de datos.

2.2.5 Consola Única de Gestión: El contratista debe proveer acceso a una consola centralizada que permita a la Secretaría visualizar el estado de seguridad de su red a través de tableros (dashboards) intuitivos y personalizables.

2.2.6 Contextualización de Datos: La visualización debe enriquecerse con metadatos que permitan identificar el usuario, el dispositivo y la aplicación involucrada en cada evento de red, facilitando la trazabilidad.

2.3 Visibilidad de amenazas

2.3.1 El contratista debe garantizar una capacidad proactiva de detección de amenazas basada en los siguientes requerimientos:

2.3.2 Detección Basada en Comportamiento (UEBA): La solución debe ser capaz de establecer una línea base de comportamiento normal para usuarios y dispositivos, generando alertas automáticas ante desviaciones significativas que sugieran cuentas comprometidas o amenazas internas.

2.3.3 Inteligencia de Amenazas (Cyber Threat Intelligence): El servicio debe integrar fuentes de inteligencia de amenazas globales y locales para identificar indicadores de compromiso (IoCs), tácticas, técnicas y procedimientos (TTPs) de actores maliciosos conocidos.

2.3.4 Alineación con el Marco MITRE ATT&CK: Todas las detecciones y alertas generadas por la plataforma deben estar mapeadas y categorizadas de acuerdo con la matriz MITRE ATT&CK, permitiendo una comprensión clara de la fase del ataque.

2.3.5 Detección de Amenazas de Día Cero: Mediante el uso de análisis heurístico y modelos de aprendizaje automático, la plataforma debe detectar malware y amenazas avanzadas para las cuales no existen firmas previas.

2.3.6 Monitoreo de Superficie de Ataque: Capacidad de visibilizar vulnerabilidades en activos expuestos a internet y monitoreo preventivo en fuentes de la Deep y Dark Web para identificar fugas de información o menciones relacionadas con la Entidad.

2.4 Arquitectura de la solución

2.4.1 La arquitectura del servicio debe ser moderna y eficiente, minimizando el impacto en la infraestructura local de la Secretaría y garantizando la escalabilidad:

2.4.2 Modelo 100% Cloud-Native (SaaS): La arquitectura debe ser nativa en la nube, donde el fabricante es responsable de la disponibilidad, el rendimiento y la actualización de la plataforma SIEM/SOAR/XDR. No se aceptarán soluciones que requieran la instalación de servidores físicos o virtuales de gestión dentro de los centros de datos de la Entidad.

2.4.3 Despliegue de Agentes y Colectores: La solución debe permitir la recolección de logs y eventos mediante agentes ligeros o colectores virtuales de bajo impacto, capaces de transmitir la información de forma segura (cifrada) hacia la nube del SOC.

2.4.4 Gestión de Logs sin Límites Rígidos: La arquitectura debe permitir el almacenamiento y la retención de logs de seguridad conforme a la normativa vigente, asegurando que la capacidad de procesamiento escale automáticamente ante picos de eventos.

2.4.5 Seguridad de la Plataforma: La infraestructura donde reside el SOCaaS debe contar con certificaciones de seguridad reconocidas (como SOC 2 Tipo II o ISO 27001) para garantizar que los datos de la Secretaría están protegidos.

2.4.6 Acceso Seguro: La arquitectura debe soportar acceso seguro para el personal de la Secretaría mediante protocolos de autenticación fuerte (MFA) para la consulta de tableros y reportes.

2.5 Investigaciones avanzadas y autónomas

2.5.1 Investigación Automatizada: La plataforma debe ser capaz de realizar investigaciones autónomas sobre las alertas generadas, recolectando evidencias de múltiples fuentes (endpoints, red, identidad) para presentar un caso de incidente completo y contextualizado.

2.5.2 Correlación Multi-vectorial: Capacidad de unir eventos aparentemente aislados en diferentes capas tecnológicas para identificar campañas de ataque complejas o movimientos laterales.

2.5.3 Línea de Tiempo del Incidente: Generación automática de una línea de tiempo detallada que muestre el origen del incidente (paciente cero), las acciones realizadas por la amenaza y el alcance del impacto.

2.5.4 Búsqueda Proactiva (Threat Hunting): El servicio debe permitir la ejecución de búsquedas proactivas de amenazas ocultas en los datos históricos (logs) basadas en nuevos indicadores de compromiso (IoCs) descubiertos globalmente.

2.5.5 Reducción de Falsos Positivos: Uso de motores de decisión basados en riesgo para filtrar el ruido y asegurar que los analistas del SOC y el personal de la Secretaría se enfoquen únicamente en incidentes con impacto real.

2.6 Notificaciones y reportes

2.6.1 El contratista debe garantizar un flujo de información constante y detallado hacia la Secretaría, mediante los siguientes mecanismos:

2.6.2 Notificaciones en Tiempo Real: Generación de alertas inmediatas ante incidentes críticos y altos, enviadas a través de correo electrónico, consola y/o canales de mensajería acordados (p. ej. Teams), incluyendo detalles técnicos básicos del evento.

2.6.3 Informes de Gestión Mensuales: Entrega de un informe detallado que resuma el estado de la seguridad, volumen de eventos procesados, incidentes detectados, tiempos de respuesta y recomendaciones de mejora.

2.6.4 Tableros (Dashboards) Ejecutivos y Técnicos: Acceso permanente a visualizaciones gráficas que permitan conocer en tiempo real la postura de seguridad, el cumplimiento de ANS y las amenazas más frecuentes.

2.6.5 Reportes de Cumplimiento: Capacidad de generar reportes basados en marcos de trabajo internacionales (ISO 27001, NIST) para facilitar auditorías y procesos de cumplimiento normativo de la Entidad.

2.7 Administración

2.7.1 El control y supervisión de la plataforma se regirá bajo los siguientes términos:

2.7.2 Administración Delegada: El contratista será responsable de la configuración técnica, tunning de reglas de correlación y actualización de la plataforma. La Secretaría mantendrá la supervisión y podrá solicitar ajustes según sus necesidades operativas.

2.7.3 Control de Acceso basado en Roles (RBAC): La plataforma debe permitir definir diferentes niveles de permisos (lector, analista, administrador) para el personal de

la Secretaría que acceda a la consola.

2.7.4 Registro de Auditoría (Audit Log): La consola debe registrar todas las actividades realizadas por los administradores y analistas, garantizando la trazabilidad de los cambios en las políticas o configuraciones.

2.8 Respuesta autónoma

2.8.1 La solución debe integrar capacidades de SOAR para ejecutar acciones de mitigación sin intervención humana en casos críticos:

2.8.2 Playbooks Automatizados: El sistema debe contar con libros de jugadas (playbooks) preconfigurados y personalizables para ejecutar respuestas automáticas ante amenazas conocidas (ej. bloqueo de IP, aislamiento de un endpoint comprometido o deshabilitación de cuentas con comportamiento anómalo).

2.8.3 Integración con Ecosistema Tecnológico: La capacidad de respuesta autónoma debe ser compatible con la infraestructura actual de la Secretaría (Directorios Activos, Firewalls, Antivirus, etc.) mediante conectores y APIs.

2.8.4 Reducción del Tiempo de Respuesta (MTTR): El uso de la respuesta autónoma debe estar orientado a minimizar el tiempo de exposición ante ataques de alta velocidad como el Ransomware.

2.9 Periodo de vigencia y tiempo de entrega

2.9.1 Dada la naturaleza del servicio bajo modelo SaaS, los tiempos se definen de la siguiente manera:

2.9.2 Fase de Implementación y Puesta en Marcha: El contratista dispondrá de un plazo máximo de treinta (30) días calendario para completar la configuración inicial contados a partir de la firma del acta de inicio, que incluye:

- Despliegue de agentes y colectores.
- Integración de fuentes de logs prioritarias.
- Configuración de tableros de control y reglas de correlación iniciales.
- Validación de conectividad y flujo de eventos.

2.9.3 Vigencia del Servicio: El servicio de SOC-as-a-Service tendrá una duración de doce (12) meses.

El plazo máximo para la fase de implementación (configuración y puesta en marcha) del servicio de SOC-as-a-Service será de treinta (30) días calendario, una vez finalizada y recibida a satisfacción la fase de implementación, se dará inicio formal a la fase de Operación 7x24 (monitoreo, detección y respuesta continua) que tendrá una duración de doce (12) meses. Por lo anterior el plazo total de ejecución del contrato que se derive del presente anexo técnico será hasta de trece (13) meses.

2.9.4 Inicio de la Operación 7x24: Una vez finalizada y recibida a satisfacción la fase de implementación, se dará inicio formal a la etapa de monitoreo, detección y respuesta continua.

2.10 Soporte

2.10.1 El contratista debe garantizar el soporte técnico necesario para la correcta continuidad del servicio:
2.10.2 Soporte Técnico de la Plataforma: Atención de incidentes relacionados con la disponibilidad y el rendimiento de la consola SIEM/SOAR/XDR, con canales de atención 7x24 (portal web, correo electrónico y línea telefónica).
2.10.3 Mantenimiento Evolutivo: Inclusión de todas las actualizaciones de firmas, motores de IA, y nuevos conectores que el fabricante libere durante la vigencia del contrato, sin costo adicional para la Secretaría.
2.10.4 Acompañamiento Técnico: Disponibilidad de especialistas para asistir a la Secretaría en la interpretación de alertas complejas o en la realización de ajustes en las políticas de seguridad de la plataforma.

2.11 Garantía de Disponibilidad y Continuidad del Servicio (SLA):

2.11.1 El contratista deberá asegurar la operatividad del ecosistema SaaS bajo las siguientes condiciones:
2.11.2 Disponibilidad de la Plataforma: El contratista garantiza una disponibilidad mínima mensual del 99.9% para el acceso a la consola de gestión y el procesamiento de eventos.
2.11.3 Actualización Continua: El proveedor es responsable de aplicar todas las actualizaciones de seguridad, parches y mejoras de funcionalidades de la plataforma SaaS sin costo adicional y sin afectar la continuidad del monitoreo.
2.11.4 Soporte Técnico Especializado: Garantía de soporte técnico nivel 3 directo con el fabricante para resolver problemas relacionados con el funcionamiento de la plataforma SIEM/SOAR/XDR.
2.11.5 Respaldo de Configuraciones: El contratista debe realizar respaldos periódicos de las reglas de correlación, dashboards y configuraciones personalizadas para la Secretaría, asegurando su recuperación inmediata ante cualquier falla del servicio cloud.

2.12 Condiciones adicionales:

2.12.1 Para garantizar la calidad y transparencia del servicio, el contratista deberá cumplir con:
2.12.2 Transferencia de Conocimiento Operativo: Al finalizar la implementación, el contratista realizará sesiones de transferencia de conocimiento dirigidas al personal técnico de la Secretaría, enfocadas en el uso de la consola, interpretación de reportes y flujo de escalado de incidentes.
2.12.3 Confidencialidad de la Información: Todo el personal asignado por el contratista deberá suscribir acuerdos de confidencialidad estrictos, dada la sensibilidad de los datos y registros de seguridad que procesará el SOC.
2.12.4 Propiedad de los Datos: Se establece explícitamente que todos los logs, registros de eventos y reportes generados son propiedad exclusiva de la Secretaría Distrital de Integración Social. El contratista deberá facilitar la descarga o migración de esta información al finalizar el contrato si así se requiere.

2.12.5 Reuniones de Seguimiento: Realización de comités técnicos mensuales para revisar la postura de seguridad, el cumplimiento de los ANS y la evolución de las amenazas detectadas en el entorno de la Entidad.
2.12.6 El contratista deberá entregar todas las soluciones / equipos en los sitios/sedes indicadas por la entidad.
2.12.7 Brindar soporte y gestión de las plataformas a contratar.
2.12.8 El servicio de SOC se debe implementar y su respectiva operación tanto en herramientas, recurso humano y de espacios físicos con los controles de seguridad física y lógica, en las instalaciones del contratista.
2.12.9 El contratista deberá realizar la instalación y configuración de los equipos con personal certificado por el fabricante con el cual se esté presentando.
2.12.10 Todas las plataformas deberán ser de propósito específico, no se aceptan soluciones genéricas.
2.12.11 El contratista deberá ser partner aprobado con los Fabricantes de los equipos o soluciones a instalar, para esto deberá entregar con la oferta la carta certificada de los fabricantes mínimo con un mes de vigencia dirigida a la entidad.
2.12.12 Las actividades de instalación, configuración y puesta en producción de las plataformas ofertadas deberán ser realizadas por personal certificado por el fabricante a nivel profesional y arquitecto o su equivalente según el fabricante para esto se deben aportar las respectivas certificaciones
2.12.13 El contratista debe mantener actualizado el Firmware de todos los componentes ofertados de acuerdo con las últimas versiones estables liberadas por el fabricante a solicitud del supervisor del contrato.
2.12.14 El oferente debe contemplar en su oferta todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, refrigerios, entre otros) requerida para que el personal asignado al proyecto pueda cumplir sus funciones.

3. GENERALIDADES

La Subdirección de Investigación e Información, en el marco de sus responsabilidades institucionales, debe garantizar la disponibilidad, integridad y seguridad de la infraestructura tecnológica y de los sistemas de información de la Secretaría Distrital de Integración Social – SDIS, mitigando los riesgos asociados a amenazas externas e internas.

La creciente sofisticación de los ciberataques exige la adopción de servicios robustos y de última generación bajo modelos de operación continua, que permitan visibilidad integral, detección proactiva de amenazas avanzadas y mecanismos efectivos de respuesta automatizada ante eventos que comprometan la confidencialidad, integridad o disponibilidad de la información institucional. Esta necesidad está alineada con la Ley 1581 de 2012 sobre protección de datos personales, y con los lineamientos y políticas vigentes aplicables a entidades públicas del Distrito Capital en materia de seguridad digital, privacidad de la información y gestión institucional.

En atención a lo anterior, la Secretaría Distrital de Integración Social requiere la contratación de un **Servicio Especializado de Centro de Operaciones de Seguridad (SOC) bajo la modalidad SOC-as-a-Service (SaaS)**. Este servicio debe operar sobre una plataforma nativa en la nube

que integre de manera unificada capacidades de **SIEM, SOAR y XDR**, incorporando inteligencia artificial, análisis de comportamiento de usuarios y entidades (UEBA), visualización avanzada y respuesta autónoma. A diferencia de modelos tradicionales, esta solución debe permitir la supervisión 7x24x365 sin depender de infraestructura física local por parte de la Entidad, optimizando la detección de amenazas conocidas y desconocidas mediante el procesamiento y correlación de eventos en la nube del fabricante.

El servicio deberá proporcionar capacidades avanzadas para el monitoreo continuo, la identificación de anomalías, la orquestación de respuesta y la generación automática de acciones de mitigación frente a incidentes de ciberseguridad. Todo ello bajo un esquema de alta disponibilidad, garantizando la soberanía de la información y el cumplimiento estricto del marco normativo vigente en materia de seguridad digital para el sector público.

El presente proceso de contratación tiene como finalidad asegurar la continuidad operativa de los servicios tecnológicos institucionales, a través de una operación integral que reduzca la superficie de exposición, mitigue los riesgos de seguridad informática y fortalezca el nivel de madurez en ciberseguridad de la Entidad, sin restringir la pluralidad de oferentes ni fabricantes que cumplan con los requisitos definidos en este documento.

El CONTRATISTA deberá ejecutar el contrato de conformidad con las especificaciones técnicas establecidas en este anexo, la propuesta económica presentada para el proceso, y las instrucciones impartidas por el SUPERVISOR del contrato. Asimismo, deberá dar cumplimiento a todas las actividades necesarias para asegurar la correcta ejecución del objeto contractual y el alcance definido.

Durante la ejecución, la supervisión técnica será ejercida de forma permanente por parte del SUPERVISOR de la SECRETARÍA o quien este designe, según los procedimientos establecidos por la misma. Todas las reuniones de seguimiento, revisiones técnicas, ajustes o recomendaciones serán registradas mediante actas y/o grabaciones, conforme a los procedimientos institucionales.

Toda comunicación relacionada con el desarrollo del contrato, modificación de requerimientos, validaciones técnicas o coordinación operativa deberá canalizarse exclusivamente a través del SUPERVISOR del contrato y/o quien este designe.

NOTA: El SUPERVISOR del contrato y/o quien este designe, durante cualquier etapa de la ejecución contractual, podrá citar al CONTRATISTA para revisar los aspectos técnicos, de programación, seguimiento, evaluación o cualquier otro componente relacionado con el cumplimiento del contrato. Todos los asuntos tratados en dichas reuniones deberán ser registrados mediante actas y/o grabaciones de las sesiones virtuales, las cuales se anexarán al expediente contractual conforme a los procedimientos institucionales.

En caso de que, en virtud de las reuniones realizadas, surja la necesidad de modificar lo establecido en el contrato, se tendrá en cuenta lo prescrito en el Manual de Contratación de la Entidad y demás normas que regulan la materia.

4. CONDICIONES Y CARACTERÍSTICAS TÉCNICAS ESPECÍFICAS

El contratista deberá garantizar el cumplimiento de las siguientes condiciones de idoneidad y capacidad técnica para asegurar la correcta prestación del servicio de SOC-as-a-Service:

4.1 Vigencia y disponibilidad del servicio:

- La solución deberá estar disponible bajo un esquema de operación continua 7x24, incluyendo atención en fines de semana, días festivos y turnos nocturnos.
- El servicio deberá cubrir la infraestructura de red definida por la Entidad, permitiendo el monitoreo y la respuesta en tiempo real conforme al alcance contratado.
- El licenciamiento, soporte, monitoreo, actualizaciones y mantenimiento deberán mantenerse activos durante todo el periodo contractual, conforme a lo estipulado en el presente documento.

4.2 Condiciones del contratista y soporte:

- El contratista deberá garantizar soporte técnico especializado 7x24 a través de canales telefónicos, electrónicos, remotos y presenciales.
- En caso de falla del componente físico o lógico, el contratista deberá gestionar su reparación o sustitución de acuerdo con las condiciones de la garantía ofrecida.
- El contratista será responsable de gestionar la operación de la solución ante contingencias, asegurando la restauración de la configuración y funcionalidad conforme al plan de respaldo y garantía.
- El soporte deberá garantizar cumplimiento con niveles de servicio establecidos por la Entidad o definidos contractualmente, trazabilidad de incidentes, atención oportuna y documentación completa de cada caso.

4.3 Certificaciones y Experiencia del Contratista (Oferente)

El proponente debe demostrar su capacidad técnica y operativa mediante el cumplimiento de los siguientes requisitos mínimos, los cuales deberán estar vigentes al momento de la presentación de la propuesta:

- Certificación ISO 27001:2022: El oferente debe contar con la certificación de su Sistema de Gestión de Seguridad de la Información (SGSI) vigente, con una antigüedad mínima de un (1) año.
- Membresía FIRST: El oferente debe ser miembro activo y vigente del Forum of Incident Response and Security Teams (FIRST), garantizando que sigue estándares internacionales en la respuesta a incidentes.
- Certificación ISO 20000-1 e ISO 22301: El oferente debe contar con certificaciones en Gestión de Servicios de TI y Gestión de Continuidad del Negocio, respectivamente.
- Informe SOC 2 Tipo II: El proponente debe presentar el informe SOC 2 (Nivel 2) Tipo II, que valide la eficacia operativa de sus controles de seguridad, disponibilidad y confidencialidad.

4.4 Recurso Humano Certificado

El contratista deberá disponer y garantizar, durante toda la ejecución del contrato, incluido el periodo de implementación, puesta en marcha y operación del SOC, de un equipo de trabajo con la formación, experiencia y competencias necesarias para la adecuada prestación del servicio. En consecuencia, el personal mínimo requerido deberá estar vinculado y disponible desde el inicio de la ejecución contractual y mantenerse durante toda la vigencia del contrato, asegurando su participación conforme a las funciones, dedicación y responsabilidades definidas para cada perfil. El personal mínimo requerido es:

4.4.1 Un (1) Gerente de proyecto:

EDUCACIÓN	EXPERIENCIA	DEDICACIÓN
Ingeniero de sistemas electrónicos o afines a carreras de tecnologías informáticas. Estudios de postgrado en gerencia, gestión o dirección de proyectos o con certificado PMP Debe contar con al menos una de las siguientes certificaciones: • PMP • ITIL Foundations v4 • SCRUM vigente	Experiencia mínima de cinco (5) años como Gerente o director de proyectos TI	La dedicación dentro del proyecto será del 30% durante el tiempo de la implementación y 10% para el tiempo de la operación del servicio y/o cuando sea requerido por parte de la entidad.

4.4.2 Un (1) Especialista de Seguridad:

EDUCACIÓN	EXPERIENCIA	DEDICACIÓN
Ingeniero de sistemas electrónico o afines a carreras de tecnologías informáticas. Especialización o Maestría en Seguridad de la información o Gerencia Informática o Seguridad en redes Debe contar con las siguientes certificaciones:	Al menos cinco (5) años realizando auditorías tecnológicas	La dedicación o disponibilidad del 100% durante la vigencia del proyecto.

• ISO 27001:2022 vigente • CISPP (Certified Information Systems Security Professional) de ISC2 • CISM (Certified Information Security Management) de ISACA • CEH (EC-Council Certified Ethical Hacker)		

4.4.3 Un (1) Líder de ciberseguridad:

EDUCACIÓN	EXPERIENCIA	DEDICACIÓN
Ingeniero de sistemas electrónicos o afines a carreras de tecnologías informáticas. Especialización o Maestría en Seguridad de la información o Gerencia Informática o Gerencia de Proyectos informáticos o telecomunicaciones. Que cuente con las siguientes Certificaciones relacionadas: • CISPP (Certified Information Systems Security Professional) de ISC2 • CISM (Certified Information Security Management) de ISACA • CEH version 13 AI (EC-Council Certified Ethical Hacker) • ECIH (EC-Council Certified Incident Handler) • CRISC (Certified in Risk and Information	Experiencia al menos 10 años, en el campo de ciberseguridad demostrable con la certificación laboral.	Ingeniero dedicado 20%, en modalidad híbrida (presencial y virtual), en horario laboral de lunes a viernes de 8:00 am a 5:00 y cuando sea requerido por la entidad para un evento de incidente de seguridad en horario no hábil.

Systems Control) de ISACA • Google Cloud Certified Professional Cloud Security Engineer		

4.4.4 Dos (2) Analistas SOC

EDUCACIÓN	EXPERIENCIA	DEDICACIÓN
Ingeniero de sistemas electrónicos o afines a carreras de tecnologías informáticas. Que cuente con las siguientes Certificaciones relacionadas: • CompTIA Security+ CySA+ • Microsoft SC-200 • EC-Council CSA	Experiencia al menos 1 año, en el campo de ciberseguridad demostrable con la certificación laboral.	Ingeniero dedicado 100%, en modalidad híbrida (presencial y virtual), en horario laboral de lunes a viernes de 8:00 am a 5:00 y cuando sea requerido por la entidad para un evento de incidente de seguridad en horario no hábil.

4.5 Características de los Servicios Especializados

El servicio debe incluir de forma obligatoria las siguientes capacidades:

- Gestión de Vulnerabilidades: Escaneo continuo y priorización de riesgos en activos y aplicaciones web de la Entidad.
- Pruebas de Penetración (Pentesting): Ejecución de pruebas sistemáticas para identificar debilidades explotables, siguiendo metodologías reconocidas.
- Gestión de Exposición Cibernética: Monitoreo preventivo en la Deep y Dark Web (para 2 dominios y hasta 100 correos VIP) para identificar fugas de credenciales o información sensible.
- Simulaciones de Phishing: Ejecución periódica de campañas de concientización para evaluar y fortalecer la cultura de seguridad de los usuarios.

4.6 Seguimiento y Documentación Técnica

El contratista deberá mantener un registro detallado de todas las actividades:

- Bitácora de Incidentes: Documentación técnica de cada amenaza detectada y la ruta de resolución aplicada.
- Manual de Operación: Documento que defina los flujos de comunicación y escalado entre el SOC y la Secretaría.

4.7 Ficha técnica del servicio

4.7.1 Ficha técnica SOC como servicio.
La SDIS requiere adquirir, instalar, configurar e implementar un Centro de Operaciones de Seguridad (SOC) que permita la supervisión continua, detección, análisis y respuesta ante eventos e incidentes de seguridad de la información y que cuente con los siguientes servicios: • Servicio de correlación, monitoreo de alertas, prevención, orquestación y automatización, • Análisis de comportamiento de usuarios o entidades • Servicio de respuesta Incidentes • Identificación y gestión de vulnerabilidades • Pruebas de penetración (Penetration Testing) • Servicio de gestión de la exposición cibernética • Equipo mínimo de trabajo
Mantener las plataformas y herramientas actualizadas que componen el servicio de SOC bajo las mejores prácticas de ciberseguridad y los servicios estratégicos de la secretaria de Integración Social
Servicios profesionales para la entrega, instalación y configuración de cada uno de los elementos que componen el servicio propuesto, conforme a las especificaciones definidas en este documento.
El servicio debe garantizar monitoreo de seguridad continuo, detectando y gestionando amenazas en tiempo real las 24 horas, los 7 días de la semana durante doce (12) meses.
El servicio de bebe estar alienado bajo marco de seguridad y buenas prácticas aplicables, marcos de referencia, estándares internacionales y buenas prácticas reconocidas como: • ISO: 27001:2022 • ISO: 20000 • ISO: 22301 • SOC2 • FIRST-CSIRT • ITIL, NIST (CSF) o CERT
4.7.2 Servicio **de correlación, monitoreo de alertas, prevención, orquestación y automatización**

Agregación, normalización, correlación, almacenamiento seguro, análisis y comunicación en las acciones a tomar, para los datos de los usuarios, dispositivos, aplicaciones e infraestructura, tanto locales en premisas y en nube, con los siguientes activos: Activos (120) y Eventos por Segundo (80) (Servidores, dispositivos de red, PCs, aplicaciones)
El servicio debe contar con una solución de **SIEM en modalidad SOC-as-a-Service (SaaS)** y que cumpla con los siguientes requerimientos: • La plataforma de SIEM debe ser tipo SaaS, no se aceptan soluciones en colocation o en premisas. • Monitoreo de hasta Acitvos (120) y Eventos por Segundo 80, durante doce (12) meses, incluyendo funcionalidades de SIEM, SOAR e integración de XDR en única consola. • Monitoreo y análisis de comportamiento de UEBA, para mil (1.000) usuarios • Servicio de Onboarding sobre la plataforma tipo SIEM propuesta • La solución debe ser compatible con Syslog • La solución de SIEM debe estar como lider en el cuadrante de Gartner para SIEM • La solución debe contar al menos 213 conectores aprobados por el fabricante de SIEM • La solución debe soportar el análisis de comportamiento de usuarios y de entidades (UEBA), de los registros y alertas recopilados de todos los orígenes de datos conectados, analizados, de esta forma genera perfiles de comportamiento de línea de base de las entidades de la organización como usuarios, dispositivos, direcciones IP y aplicaciones. • La solución debe de contar con integraciones a los servicios de Microsoft con los que cuenta la entidad. • La solución debe contar con inteligencia sobre amenazas de forma navita. • El portal debe contar con las optimizaciones de SOC y cobertura basadas en amenazas, para recomendar y priorizar el impacto sobre las amenazas. • El servicio orquestación (**SOAR**) sobre los eventos de forma nativa en la misma plataforma de correlación de Eventos SIEM, no se aceptan soluciones con máquinas virtuales hostiadas o en premisas. • La herramienta deberá tener automatización de tareas de enriquecimiento, respuesta y análisis recurrentes y predecibles que sean responsabilidad del centro de operaciones de seguridad SOC.
La plataforma propuesta debe integrar inteligencia artificial y automatización para correlacionar eventos y responder amenazas eficientemente, optimizando el tiempo de respuesta y mejorando la precisión.
La solución propuesta debe ser líder en SIEM, enfocándose en la prevención e integración de actualizaciones continuas, acciones automatizadas, configuraciones optimizadas y recomendaciones basadas en mejores prácticas para fortalecer las defensas y prevenir ataques futuros.
La solución propuesta debe incluir el servicio de detección, respuesta y la investigación en caso de que se presente un incidente de seguridad.
La solución ofertada deberá emplear un único servicio MDR/MPR para gestionar toda la infraestructura de TI.

La solución ofertada deberá incluir un portal web intuitivo que ofrezca total transparencia sobre la actividad del servicio, con una vista detallada de todos los incidentes.
Se requiere que el servicio cuente con la capacidad de respuesta ante los incidentes de manera centralizada y unificada en los diferentes activos que componen la red empresarial.
La solución ofertada deberá estar en la capacidad de implementarse rápidamente mediante una integración sencilla con el stack de seguridad y el ecosistema existente de la SDIS
La solución deberá estar en la capacidad de realizar evaluaciones regulares de la postura de seguridad de la organización, permitiendo ajustes y mejoras continuas en la infraestructura de seguridad de la secretaria de integración Social
La solución propuesta deberá incluir la generación de informes periódicos que ayuden a la SDIS a entender su postura de seguridad y a cumplir con las normativas aplicables dentro de la organización.
4.7.3 El oferente del servicio de SOC debe cumplir con las siguientes certificaciones como parte de la prestación del servicio:
• **ISO27001**: El oferente debe presentar junto con su propuesta el certificado ISO 27001 del 2022 o superior (SGSI) para su proceso de SOC, con al menos un (1) año de vigencia al cierre de presentación de la propuesta. • **FIRST:** El oferente debe presentar junto con su propuesta la evidencia en la página oficial del FIRST (Forum of Incident Response and Security Teams) la membresía vigente de su SOC, con una vigencia mínima de 1 año de vigencia al cierre de presentación de la propuesta. • **ISO: 20000:** El oferente deberá presentar junto con su propuesta la evidencia de certificación vigente bajo la norma ISO/IEC 20000-1 para la prestación de servicios de gestión de servicios de TI, aplicable al servicio de SOC (Security Operations Center) ofrecido. • El oferente deberá presentar junto con su propuesta la evidencia de certificación vigente bajo la norma **ISO 22301** para Gestión de la Continuidad del Negocio, aplicable a la prestación del servicio de SOC (Security Operations Center). • El oferente deberá presentar junto con su propuesta la **evidencia del informe SOC 2 Tipo II (Nivel 2)** vigente, emitido por un auditor independiente, que certifique la efectividad operativa de los controles, aplicables a la prestación del servicio de SOC (Security Operations Center). • El proponente deberá acreditar, junto con su propuesta, la **certificación vigente como partner, distribuidor autorizado** del fabricante de la plataforma tecnológica SaaS sobre la cual se presta el servicio de SOC ofertado, la cual deberá operar en la nube del fabricante e integrar en una única consola capacidades de SIEM, SOAR y XDR.
4.7.4 Servicio de respuesta Incidentes
Reactivo • Debe incluir información para diferentes tipos de amenazas incluyendo: • Firewall • IPS • Aplicaciones • Perdida de datos

- Malware
- Botnes
- Acceso no autorizado
- denegación de servicios
- Revisión de control cada 6 meses
- Preparación y Alineación de Respuesta a Incidentes
- Revisión del Plan de Respuesta a Incidentes

Remediación en tiempo real

- Recopilación y encriptación de logs
- Comprimir y almacenar los logs
- actualización de los logs cada 30 días
- Consulta de los logs atreves del portal de respuesta a incidentes

Servicios de respuesta a incidentes:

- Gestión y organización de incidentes
- Búsqueda de amenazas
- Contención de amenazas
- Análisis forense digital (disco/memoria/registros/red)
- Análisis de malware
- Análisis de correo de phishing
- Comunicación de incidentes a la gerencia
- Informes personalizados para su organización

4.7.5 Servicio de concientización de seguridad

El servicio de concientización de seguridad hasta (4.800) usuarios, cumplir los siguientes criterios y requerimientos:

Capacitación Personalizada en Ciberseguridad:

- Módulos de aprendizaje a medida según los roles y perfiles de riesgo de los empleados.
- Contenido atractivo e interactivo para maximizar la retención y la efectividad.

Simulaciones de Ataques de Phishing:

- Escenarios reales de ataques de phishing para evaluar y mejorar la concientización de los empleados.
- Campañas personalizables para reflejar las últimas ciberamenazas.

Evaluaciones de Riesgos de Seguridad:

- Evaluación continua del nivel de concientización de los empleados en ciberseguridad.
- Información práctica para identificar y abordar las vulnerabilidades de seguridad.

Soporte Multilingüe y Global:

• Selección de idioma con un solo clic para experiencias de capacitación localizadas. • Educación continua en ciberseguridad.
4.7.6 Pruebas de penetración (penetration testing)
• Pruebas de penetración en cualquier parte de su infraestructura hasta (120) activos, para evaluar la resistencia a amenazas internas, externas, inalámbricas, físicas, de aplicaciones web o de ingeniería social. • Pruebas de penetración a nivel de atacante para replicar todo tipo de ataques, incluyendo amenazas persistentes avanzadas (APT) y ataques de tipo estado-nación. • Ejecución sistemática de las etapas de un ataque, incluyendo la planificación, el reconocimiento, la obtención y el mantenimiento del acceso, y la exposición de la cadena de ataque. • Entrega de hallazgos que incluyan un cuadro de mando del ataque, un guion gráfico, una lista priorizada de problemas y la identificación de controles de seguridad eficaces. • El servicio de incluir un equipo de resiliencia de Ciberseguridad por sus siglas en ingles CRT, un grupo de profesionales en seguridad ofensiva que evalue las capacidades defensivas de la entidad. • Evaluar la seguridad de los sistemas y activos de la infraestructura interna incvluyendo sus entornos de Active Directory (AD) y Azure.
4.7.6. Servicio de gestión de vulnerabilidades
• Servicio gestionado de los activos por profesionales experimentados • Servicio continuo de detección y evaluación con los diferentes sensores y escáneres • Análisis de los activos y de las aplicaciones web hasta que hacen parte del servicio de SOC (120) activos. • priorización automatizada de vulnerabilidades • Visualización de los riesgos en tiempo real • Seguimiento de vulnerabilidades • Puntuación y categorización del riesgo • Identificación de vulnerabilidades que pueden requerir atención • revisión y priorización de las vulnerabilidades sin resolver y las prioriza según el riesgo, el impacto y el esfuerzo de remediación. • Cada vulnerabilidad descubierta es necesario implementar algún tipo de resolución • Seguimiento y la generación de informes de vulnerabilidades • Lecciones aprendidas
4.7.7 Servicio de gestión de la exposición cibernética
El servicio de exposición de superficie de ataque externo para la entidad requiere cubrir los siguientes casos de uso:

La solución debe permitir la identificación, monitoreo y análisis de información sensible expuesta o comercializada en más de 8.000 fuentes de Deep Web y Dark Web, incluyendo foros clandestinos, marketplaces, repositorios de filtraciones, sitios de intercambio de credenciales y otras plataformas asociadas a actividades cibercriminales. La solución debe contemplar licenciamiento hasta 2 dominios
La solución debe permitir la identificación, monitoreo y alerta temprana de credenciales comprometidas (usuarios, correos electrónicos y contraseñas) expuestas o comercializadas en más de 8.000 fuentes de Deep Web y Dark Web, incluyendo foros clandestinos, marketplaces de datos filtrados y repositorios asociados a actividades cibercriminales. La solución debe contemplar licenciamiento hasta 2 dominios
La solución debe permitir el monitoreo de amenazas y posibles compromisos asociados a usuarios VIP o perfiles críticos de la entidad, incluyendo la detección de exposición, filtración o comercialización de información personal, credenciales o datos sensibles en Internet, Deep Web y Dark Web. El servicio debe contemplar en su licenciamiento hasta 100 emails de cuentas vip
La solución debe permitir la identificación y monitoreo de dominios similares, typosquatting o dominios fraudulentos que suplanten la marca o servicios de la organización, utilizados con fines maliciosos como phishing o fraude digital. La plataforma deberá incluir la gestión del proceso de takedown del dominio malicioso, ya sea de forma automatizada o mediante gestión especializada del fabricante, garantizando que el servicio sea facturado únicamente cuando el retiro del dominio fraudulento sea exitoso. La solución debe contemplar licenciamiento hasta 2 dominios

5. SEGUIMIENTO AL SERVICIO CONTRATADO

La ejecución del servicio objeto del presente proceso se desarrollará como un Proyecto Integral, permitiendo una gestión y un control adecuados sobre el avance y el logro de los objetivos y alcance propuesto, aplicando buenas prácticas de gestión de proyectos reconocidas internacionalmente (p. ej., PMBOK o equivalentes).

Durante la ejecución contractual, el seguimiento se llevará a cabo conforme a los siguientes lineamientos:

a. Seguimiento general al cumplimiento contractual:

- El CONTRATISTA deberá presentar un plan de trabajo inicial durante la reunión de inicio del contrato, incluyendo cronograma, matriz de comunicaciones y plan de mantenimiento preventivo y correctivo, en el formato institucional que defina y suministre la SDIS.
- El SUPERVISOR del contrato realizará reuniones de seguimiento con una periodicidad mínima mensual, o según la necesidad operativa de la Entidad.

- El CONTRATISTA deberá entregar informes de gestión periódicos que incluyan: reportes de servicio, incidentes atendidos, cambios aplicados, actualizaciones de configuración y licencias, y estado de cumplimiento de hitos del proyecto.
- Todos los acuerdos y observaciones se registrarán en actas suscritas y, cuando aplique y esté autorizado por la Entidad, grabaciones anexadas al expediente contractual.
- Cualquier situación que implique modificación de tiempos, recursos o alcance técnico será tratada conforme a lo establecido en el Manual de Contratación de la Entidad y demás normas vigentes.

b. Seguimiento específico al servicio.

Para la evaluación de la calidad del servicio, se establecen los siguientes indicadores clave de desempeño (KPIs), los cuales serán medidos mensualmente:

Indicador	Descripción	Meta / Nivel Mínimo
MTTN (Time to Notify)	Tiempo transcurrido desde la detección de una alerta crítica en la plataforma hasta la notificación oficial a la SDIS.	Críticos: < 15 min. Altos: < 30 min.
MTTA (Time to Acknowledge)	Tiempo en que un analista del SOC toma el incidente y comienza la fase de investigación.	< 20 minutos para incidentes de alta prioridad.
Disponibilidad SaaS	Tiempo de actividad de la plataforma de monitoreo y consola de gestión (SIEM/SOAR).	99.9% de disponibilidad mensual.
Efectividad de Reglas	Relación entre alertas reales vs. falsos positivos mediante el tuning constante de la plataforma.	Reducción mensual progresiva del ruido operativo.

c. Metodología de Seguimiento Operativo

La supervisión de la Secretaría realizará el seguimiento a través de:

1. **Acceso a la Consola de Gestión:** El supervisor tendrá acceso con perfil de auditor/lector para verificar en tiempo real el flujo de eventos y el estado de las investigaciones abiertas.
2. **Bitácora Electrónica de Incidentes:** El contratista debe mantener un registro (Ticket Log) donde se evidencie la trazabilidad completa de cada incidente, desde la detección hasta el cierre (Post-Mortem).
3. **Verificación de Playbooks:** Trimestralmente, el contratista deberá demostrar la efectividad de al menos dos (2) procesos de respuesta automatizada (SOAR) configurados para la Entidad.

5.1. INICIO

Una vez suscrita el acta de inicio por las partes, el CONTRATISTA deberá participar en la reunión de inicio del proyecto, la cual será convocada por el SUPERVISOR del contrato o quien esté designe, y deberá contar con la participación del equipo designado por la SDIS y los representantes técnicos del CONTRATISTA.

Durante esta sesión se deberán establecer:

- Los canales oficiales de comunicación entre las partes.
- Los niveles de escalamiento para la atención de soporte técnico.
- La fecha de entrega de los siguientes planes por parte del CONTRATISTA:

  - Plan de trabajo general
  - Plan de mantenimiento preventivo y correctivo,
  - Plan de transferencia de conocimiento.

Los planes deberán elaborarse conforme lo defina la SDIS.

5.2. PLANEACIÓN.

Una vez perfeccionado el contrato y suscrita el acta de inicio, el contratista deberá ejecutar una fase de planeación orientada a asegurar la transición operativa hacia el nuevo modelo de SOC-as-a-Service, cumpliendo con los siguientes hitos:

5.2.1. Plan de Trabajo Detallado

El contratista entregará, dentro de los primeros diez (10) días hábiles, un cronograma detallado que incluya las fases de:

- **Alistamiento:** Definición de accesos, conectividad y perfiles de usuario en la consola SaaS.
- **Despliegue Técnico:** Instalación de agentes, configuración de colectores y habilitación de conectores (APIs) con las fuentes de datos de la Secretaría.
- **Tuning y Estabilización:** Ajuste de reglas de correlación para reducir falsos positivos y calibración de los motores de Inteligencia Artificial.
- **Entrega Operativa:** Formalización de los protocolos de escalado y notificación.

5.2.2. Definición del Modelo de Gobierno y Comunicación

El contratista, en conjunto con la Supervisión del contrato, definirá:

- **Matriz de Contactos:** Identificación del personal clave en la Secretaría (Infraestructura, Aplicaciones, Seguridad) para la notificación de incidentes 7x24.
- **Matriz de Escalado:** Procedimientos claros para la respuesta ante incidentes según su criticidad (Baja, Media, Alta, Crítica).

- **Protocolos de Respuesta:** Definición de las acciones que el SOC puede tomar de forma autónoma (vía SOAR) y aquellas que requieren autorización previa del Supervisor.

5.2.3. Levantamiento de Activos Críticos y Casos de Uso

Como parte de la planeación, el contratista deberá:

- **Inventariar fuentes de datos:** Identificar los logs prioritarios (Active Directory, Firewalls, EDR, Nube, etc.) que deben ser integrados a la plataforma SIEM/XDR.
- **Diseñar Casos de Uso:** Definir, de común acuerdo con la Secretaría, los escenarios de amenaza específicos que se desean monitorear prioritariamente (ej. intentos de exfiltración de datos, accesos no autorizados a bases de datos de integración social, comportamientos anómalos de usuarios VIP).

5.3. EJECUCIÓN.

Durante la fase de ejecución, el CONTRATISTA será responsable de implementar las actividades técnicas y administrativas definidas en el plan de trabajo, garantizando el cumplimiento de los entregables, cronogramas y estándares definidos en el presente anexo técnico y/o en el contrato.

Las actividades mínimas que deberá desarrollar incluyen:

A. Aseguramiento de calidad:

- Aplicación de acciones correctivas y preventivas para mitigar desviaciones técnicas u operativas detectadas durante la implementación.
- Entrega de documentación técnica completa, respaldos de configuración y evidencias de las actividades realizadas.
- Registro y trazabilidad de la configuración, el comportamiento operativo y los ajustes realizados en la solución durante la vigencia del contrato.

B. Entregables mínimos de la fase de ejecución:

- Documento de Cronograma de Actividades del Proyecto entregado en la sesión de inicio del proyecto.
- Documento de Definición de Alcance donde se listarán todos los prerrequisitos, condiciones y alcances técnicos identificados y establecidos en la fase de Planeación y Diagnóstico.
- Documento de Diseño de Alto Nivel de la arquitectura del servicio a implementar.
- Documento con el Plan de Implementación del servicio.
- Documento de Entrega de la Solución

C. Condiciones generales para la ejecución del servicio:

- Las capacidades requeridas (SIEM, SOAR, XDR, UEBA, respuesta autónoma, threat

hunting e investigación automatizada) deberán estar disponibles desde el inicio del servicio, ya sea de forma nativa o mediante integraciones previamente habilitadas y operativas. Lo anterior con el fin de garantizar una operación continua y evitar dependencias de implementaciones progresivas durante la ejecución del contrato.

- El servicio deberá integrarse con las fuentes de información disponibles en la Entidad (identidad, endpoints, aplicaciones, red, entre otras) y, en caso de ser necesario, el contratista deberá contemplar los mecanismos para habilitar la recolección de la telemetría requerida. Lo anterior con el fin de garantizar la adecuada operación del SOC y el cumplimiento de las capacidades funcionales definidas.
- El servicio operará bajo un modelo de gobierno compartido, donde el contratista ejecuta la operación, monitoreo y automatización de respuestas conforme a procedimientos previamente acordados, y la Entidad mantiene la validación y aprobación de acciones críticas.
- Las acciones de respuesta estarán definidas por niveles de criticidad: las acciones automatizadas de bajo impacto podrán ejecutarse de forma autónoma por el contratista, mientras que las acciones de mitigación, contención o bloqueo que puedan afectar la operación requerirán validación previa de la Entidad.
- El servicio contemplará un esquema de retención, disponibilidad y uso de logs históricos alineado con las capacidades de monitoreo, hunting, investigación avanzada y análisis de comportamiento. Estos parámetros serán definidos en la fase de implementación, considerando volúmenes de información, criticidad de las fuentes y necesidades operativas de la Entidad.

5.4. SEGUIMIENTO Y CONTROL.

El seguimiento y control del contrato se realizará de manera continua durante toda su ejecución, con el fin de verificar el cumplimiento de los compromisos técnicos, administrativos y contractuales establecidos en el presente anexo.

El CONTRATISTA deberá presentar informes de gestión mensuales sobre el avance de las actividades, el cumplimiento del cronograma y los entregables comprometidos, así como las acciones de mejora implementadas, conforme a los formatos e instrumentos institucionales que defina y suministre la SDIS.

Adicionalmente, se deberá cumplir con las siguientes condiciones:

- Se programará una reunión mensual de seguimiento, en los primeros ocho (8) días hábiles de cada mes, con la participación del SUPERVISOR del contrato o quien esté designe, y un representante del CONTRATISTA.
- El CONTRATISTA deberá remitir previamente al SUPERVISOR la presentación y el informe de avance, como mínimo cinco (5) días hábiles antes de la reunión, incluyendo:
  - ✓ Cumplimiento del cronograma y estado de los hitos correspondientes al periodo reportado.
  - ✓ Reporte consolidado de eventos e incidentes detectados por la solución, cambios aplicados y configuraciones realizadas.
  - ✓ Identificación de riesgos y medidas de mitigación aplicadas durante el periodo.

- ✓ Avances en la ejecución de las actividades de capacitación y cumplimiento de los entregables técnicos establecidos.

- El CONTRATISTA será responsable de elaborar el acta de cada reunión, en la que se registrarán los temas tratados, compromisos adquiridos, acciones de mejora, validaciones realizadas y observaciones del SUPERVISOR sobre el informe presentado.

5.5. PROCESOS DE CIERRE.

a. Cierre del Contrato:

Al finalizar la ejecución contractual, el CONTRATISTA deberá presentar un informe final de ejecución, que consolide la información técnica, administrativa y financiera del contrato, así como la entrega organizada de todos los activos de información generados durante la ejecución, incluyendo documentación técnica, configuraciones, respaldos y registros de soporte.

Este informe y sus anexos deberán ser entregados en formato digital, conforme al formato institucional definido por la Secretaría Distrital de Integración Social y bajo los lineamientos del sistema de gestión documental de la Entidad. La revisión y aprobación del informe estarán a cargo del SUPERVISOR del contrato.

El informe deberá contener, como mínimo:

- Actas de reuniones, presentaciones y compromisos.
- Informes técnicos y de gestión.
- Entregables documentales (manuales, procedimientos, informes de configuración, evidencias de licencias activadas).
- Registros de incidentes, soluciones aplicadas y acciones correctivas.
- Copia del respaldo de configuración final de la solución de detección y respuesta en red basada en inteligencia artificial.
- Resumen ejecutivo de cumplimiento del cronograma, actividades de capacitación y entregables técnicos.

b. Liquidación del Contrato:

El CONTRATISTA deberá apoyar activamente a los funcionarios y contratistas de la Secretaría Distrital de Integración Social durante el proceso de liquidación contractual, atendiendo los requerimientos de información y documentación que se generen en esta etapa.

En caso de ser requerido, el CONTRATISTA deberá indicar y adelantar las gestiones necesarias para la ampliación de la vigencia de las garantías otorgadas, hasta la fecha efectiva de liquidación del contrato, cuando a ello haya lugar, de conformidad con las condiciones contractuales establecidas.

5.6. ACUERDOS DE NIVELES DE SERVICIO

Servicio / Indicador	ANS	Sanción por Incumplimiento
Disponibilidad de la plataforma SOC	≥ 99.5% mensual	Descuento del 2% del valor mensual del servicio por cada 0.5% por debajo del ANS
Monitoreo del servicio	Operación 7x24x365	Descuento del 1% del valor mensual por cada interrupción no programada superior a 1 hora
Tiempo de notificación incidente crítico	≤ 15 minutos	Descuento del 1% del valor mensual por cada incumplimiento evidenciado
Tiempo de atención incidente alto	≤ 30 minutos	Descuento del 1% del valor mensual por cada incumplimiento evidenciado
Tiempo de contención incidente crítico	≤ 1 hora	Descuento del 2% del valor mensual por cada incumplimiento evidenciado
Escalamiento a la entidad	≤ 30 minutos	Descuento del 0.5% del valor mensual por cada incumplimiento
Disponibilidad soporte técnico	Atención 7x24	Descuento del 1% del valor mensual por indisponibilidad comprobada superior a 2 horas
Tiempo de respuesta soporte crítico	≤ 1 hora	Descuento del 1% del valor mensual por cada caso incumplido
Actualización de firmas y reglas	≤ 24 horas desde liberación crítica	Descuento del 0.5% del valor mensual por cada evento incumplido
Entrega de informes mensuales	Dentro de los primeros 5 días hábiles del mes	Descuento del 0.5% del valor mensual por retraso superior a 3 días hábiles
Retención de logs	Mínimo 12 meses	Descuento del 2% del valor mensual por pérdida parcial o total de registros
Disponibilidad dashboard	≥ 99.5% mensual	Descuento del 1% del valor mensual por cada caída superior a 2 horas

Servicio / Indicador	ANS	Sanción por Incumplimiento
Ejecución de playbooks SOAR	≥ 95% efectividad	Descuento del 1% del valor mensual cuando la efectividad mensual sea inferior al ANS
Gestión de vulnerabilidades críticas	Reporte ≤ 24 horas desde detección	Descuento del 1% del valor mensual por incumplimiento evidenciado

ANDREA ELIANA SALAZAR PEREZ
Subdirectora de Investigación e Información

Elaboró: Juan Alberto Giraldo Zuluaga – Subdirección de Investigación e Información
Revisó: Andrés Mauricio Betancourt Lasprilla – Subdirección de Investigación e Información

REGISTRO DE FIRMAS ELECTRONICAS

01. ANEXO_TÉCNICO SOC

SECRETARÍA DISTRITAL DE INTEGRACIÓN SOCIAL

gestionado por: azsign.com.co

Id Acuerdo: 20260907-100444-059295-58474431

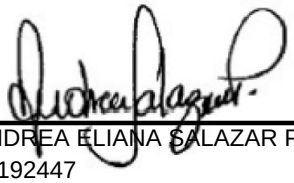
Estado: Finalizado

Creación: 2026-09-07 10:04:44

Finalización: 2026-09-07 10:29:59

Escanee el código para verificación

Firma: FIRMA

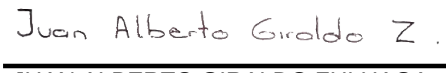


ANDREA ELIANA SALAZAR PÉREZ
52192447
aesalazarp@sdis.gov.co
Subdirectora de Investigación e Información
Secretaría Distrital de Integración Social

Revisión: REVISA

ANDRES MAURICIO BETANCOURT LASPRILLA
11257988
abetancourtl@sdis.gov.co
CONTRATISTA SII
SECRETARÍA DISTRITAL DE INTEGRACIÓN SOCIAL

Elaboración: ELABORA



JUAN ALBERTO GIRALDO ZULUAGA
1053802541
jgiraldoz@sdis.gov.co
Contratista
Secretaría Distrital de Integración Social

REGISTRO DE FIRMAS ELECTRONICAS

01. ANEXO_TÉCNICO SOC

SECRETARÍA DISTRITAL DE INTEGRACIÓN SOCIAL

gestionado por: azsign.com.co

Id Acuerdo: 20260907-100444-059295-58474431

Creación: 2026-09-07 10:04:44

Estado: Finalizado

Finalización: 2026-09-07 10:29:59

Escanee el código para verificación

TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Elaboración	JUAN ALBERTO GIRALDO ZULUAGA jgiraldoz@sdis.gov.co Contratista Secretaría Distrital de Integración Social	Aprobado	Env.: 2026-09-07 10:04:45 Lec.: 2026-09-07 10:08:10 Res.: 2026-09-07 10:08:26 IP Res.: 179.1.200.194 Canal: Email
Revisión	ANDRES MAURICIO BETANCOURT LASPRILLA abetancourtl@sdis.gov.co CONTRATISTA SII SECRETARÍA DISTRITAL DE INTEGRACIÓN SOCIAL	Aprobado	Env.: 2026-09-07 10:08:26 Lec.: 2026-09-07 10:10:02 Res.: 2026-09-07 10:10:34 IP Res.: 167.0.156.32 Canal: Email
Firma	ANDREA ELIANA SALAZAR PÉREZ aesalazarp@sdis.gov.co Subdirectora de Investigación e Información Secretaría Distrital de Integración Social	Aprobado	Env.: 2026-09-07 10:10:34 Lec.: 2026-09-07 10:29:57 Res.: 2026-09-07 10:29:59 IP Res.: 181.225.71.228 Canal: Email