1. **Especificaciones técnicas, Requisitos del Proveedor:** Para dar cumplimiento al objeto contractual, el contratista deberá tener en cuenta las especificaciones técnicas de los servicios a adquirir que son requeridas por parte de la ETITC y que son establecidas en el presente documento, es de aclarar que no se aceptaran propuestas parciales:

ITEM	SERVICIO	MEDIDA	CANTIDAD	PERIODICIDAD
01	**SERVICIO DE CENTRO DE OPERACIONES DE SEGURIDAD Y RESPUESTA A INCIDENTES DE SEGURIDAD SOC**	**TIEMPO DE SERVICIO**	**3**	**MESES**
1.1	**IMPLEMENTACIÓN Y DESPLIEGUE:** Implementar y operar para la ETITC, el centro de operaciones de seguridad, automatización SOC, que vigile de manera permanente y analice los eventos o incidentes de seguridad de la información de forma permanentemente con un monitoreo de disponibilidad las 24 horas del día, los 7 días de la semana (7X24X365) con el fin de realizar la gestión y el monitoreo de la seguridad informática de las plataformas y herramientas tecnológicas misionales que administra la entidad. 1. A partir de la firma del contrato el proveedor tendrá 30 días calendario para realizar el 100% del despliegue del servicio SOC incluyendo la instalación y configuración de las herramientas que hagan parte de la oferta comercial. 2. En caso de que se presente algún retraso en el despliegue aducido al proveedor, este deberá compensar los días adicionales de servicio. 3. El contratista y la ETITC suscribirán acta de inicio donde se socializara Roadmap u hoja de ruta del proyecto.			
1.2	**PLATAFORMA DE GESTIÓN A UTILIZAR POR PARTE DEL CONTRATISTA** El proveedor deberá incluir en su propuesta una plataforma 100% web, bajo modalidad servicio (SaaS o equivalente), para la gestión de incidentes de seguridad de la información, que permita el registro, análisis, seguimiento, documentación y trazabilidad de eventos e incidentes de ciberseguridad. La plataforma deberá estar alineada con las buenas prácticas establecidas en la norma ISO/IEC 27035 para la gestión de incidentes de seguridad de la información, y deberá permitir como mínimo: • La gestión integral del ciclo de vida de los incidentes de seguridad (registro, clasificación, análisis, contención y cierre).			

- La administración y documentación de playbooks o procedimientos de respuesta.
- La gestión y almacenamiento de evidencias asociadas a los incidentes.
- El registro y seguimiento de actividades de contención, análisis y recuperación.
- La gestión de planes de recuperación ante desastres y pruebas asociadas.
- La generación de reportes, métricas y trazabilidad de la gestión de incidentes.
- El sistema debe incluir una licencia para usuarios ilimitados y grupos de usuarios ilimitados.
- El proveedor debe parametrizar el sistema según las necesidades y políticas de la entidad.
- Entre los aspectos del DRP que el sistema debe permitir documentar se encuentran: las actividades de activación y normalización indicando duración y responsables, RTO, RPO, Tiempos de Interrupción, entre otros. Adicionalmente, debe permitir cargar documentos relacionados con las actividades.
- El sistema debe permitir la programación y gestión de simulacros donde quede plenamente documentadas las pruebas y sus resultados en cuanto a la gestión de incidentes y el DRP.
- Dada la necesidad de garantizar la integración de la gestión de la seguridad, no se podrán presentar varios sistemas que cumplan de manera independiente las funciones solicitadas.

El proveedor debe adjuntar a su propuesta la ficha técnica del Sistema que será suministrado, el tipo de suscripción y el país en donde se hospeda la plataforma y en general en donde indique claramente el cumplimiento de cada uno de los aspectos seleccionados.

La plataforma podrá corresponder a una solución especializada tipo gestión de incidentes de seguridad (Incident Response), SOAR o herramienta equivalente, siempre que cumpla con las capacidades anteriormente descritas.
La presente exigencia ***no corresponde a una herramienta de mesa de ayuda o gestión de tickets de soporte técnico (Service Desk),*** salvo que dicha funcionalidad haga parte de una solución integral que permita cumplir con los requisitos de gestión de incidentes de seguridad establecidos.

El proveedor deberá garantizar la entrega de la documentación completa generada durante la ejecución del contrato, incluyendo incidentes gestionados, playbooks, evidencias, pruebas y demás registros, al momento de finalización del contrato.

Propiedad y entrega de la información
Toda la información, registros, evidencias, configuraciones, playbooks, reportes, métricas, bitácoras e información generada, procesada o gestionada en el marco de la prestación del servicio SOC, ***será de propiedad exclusiva de la ETITC***.
El proveedor deberá garantizar, durante la ejecución del contrato y especialmente al momento de su finalización:

- La entrega completa, organizada y estructurada de toda la información generada durante el servicio.
- La entrega en formatos abiertos, reutilizables y accesibles para la ETITC.
- La transferencia de conocimiento sobre el uso, gestión e interpretación de la información.
- La eliminación controlada de la información en los sistemas del proveedor, garantizando la no retención no autorizada.

La información deberá ser entregada sin restricciones de acceso, licenciamiento o dependencia tecnológica que limite su consulta o uso posterior por parte de la ETITC.
El incumplimiento de esta obligación será considerado como un ***incumplimiento contractual***.

Gestión de Playbooks, Planes y Pruebas

Los playbooks, planes de recuperación ante incidentes de seguridad y pruebas programadas deberán ser gestionados bajo un modelo de responsabilidad compartida entre el proveedor del servicio SOC y la ETITC.
En este sentido:

- El proveedor será responsable de:
  - Diseñar, documentar, proponer y mantener actualizados los playbooks de respuesta a incidentes.
  - Estructurar los planes de respuesta y recuperación técnica ante incidentes de seguridad.
  - Definir, ejecutar y documentar las pruebas programadas.

- La ETITC será responsable de:
  - Validar y aprobar los playbooks y planes propuestos.
  - Definir el contexto organizacional, niveles de impacto y prioridades del negocio.
  - Autorizar las acciones que puedan afectar la operación institucional.

Todas estas actividades deberán ser gestionadas a través de la plataforma dispuesta por el proveedor, garantizando su trazabilidad, actualización y disponibilidad durante la ejecución del contrato.

- La información generada será de propiedad exclusiva de la ETITC y deberá ser entregada al finalizar el contrato conforme a lo establecido en el presente anexo.

1.3	**CORRELACIÓN DE EVENTOS Y SIEM** El contratista deberá Gestionar las herramientas y consolas de administración de sistemas entregados por la ETITC en el cumplimiento del contrato, para lo anterior la ETITC entregará al SOC consolas de herramientas implementadas de correlación SIEM and Threat Intelligence, consola de EndPoint Security, directorio activo y consola de Microsoft 365 para la atención de incidentes de ciberseguridad. Para la prestación del servicio de Centro de Operaciones de Seguridad (SOC), se establece una **matriz de responsabilidades compartidas**, mediante la cual se asignan de forma clara las funciones entre ETITC (*en adelante, el Contratante*) y el proveedor del SOC (*en adelante, el Proveedor*), para la administración coordinada de las plataformas de ofimática y de seguridad de la entidad de la Escuela. Este modelo adopta el principio de responsabilidad compartida, en virtud del cual el Proveedor deberá asumir las funciones operativas y técnicas relacionadas con la detección, el monitoreo y la respuesta a incidentes, mientras que el Contratante conservará la responsabilidad sobre la gobernanza, la gestión del riesgo, la clasificación de la información y la toma de decisiones estratégicas. En el dominio de Identidad y accesos, el Contratante será responsable de definir el contexto organizacional, la creación y gestión de usuarios, la identificación de activos críticos, los requisitos regulatorios aplicables y las políticas de seguridad. Por su parte, el Proveedor deberá contribuir en el marco de la administración compartida, mediante la ejecución de actividades tales como: (i) la aplicación de controles de seguridad asociados a usuarios, (ii) el inventario técnico de los activos monitoreados y (iii) el apoyo en la identificación de riesgos relacionados con las plataformas de ofimática y los diferentes dispositivos protegidos por las plataformas de seguridad de la entidad. En el dominio de seguridad de dispositivos finales, el Proveedor deberá implementar y administrar los controles técnicos de seguridad, incluyendo la configuración segura de Microsoft 365 (p. ej., controles de acceso, políticas de

	seguridad y protección del correo) y la gestión del antivirus (despliegue, actualización y definición/aplicación de políticas de protección). El Contratante, por su parte, definirá las políticas de acceso, aprobará configuraciones críticas y garantizará las actividades de concienciación de los usuarios. En el dominio de detección y monitoreo, el Proveedor será responsable del monitoreo continuo 24/7, la correlación de eventos, el análisis de registros (logs) y la detección de actividades anómalas, tanto en la plataforma Microsoft 365 como en los dispositivos finales (endpoints). Lo anterior incluye la gestión de las alertas generadas por las herramientas de seguridad y su priorización de acuerdo con su criticidad. En el dominio de respuesta y contención, el Proveedor ejecutará los procedimientos de respuesta a incidentes de primer nivel, incluyendo actividades de contención, erradicación y recuperación técnica inicial, conforme a los playbooks definidos y al alcance establecido en la matriz de responsabilidades compartidas. Para tales efectos, el Contratante proporcionará usuarios con permisos de administración sobre las plataformas de Office 365 y del antivirus, que permitan la ejecución de acciones de contención de primer nivel. El Contratante participará en la toma de decisiones relacionadas con el impacto al negocio, la comunicación interna y externa, y la aprobación de acciones que puedan afectar la operación (por ejemplo, el bloqueo de cuentas o el aislamiento de equipos). Adicionalmente, el Contratante ejecutará las acciones de respuesta a incidentes correspondientes a contención y erradicación de nivel dos (2) y superiores. En el dominio de recuperación y continuidad del negocio, el Contratante liderará la restauración de los procesos de negocio y la continuidad operativa. El Proveedor apoyará mediante el suministro de información técnica, el análisis posterior al incidente y la formulación de recomendaciones orientadas a fortalecer los controles y evitar recurrencias.
1.4	**CONFIGURACIÓN DE HERRAMIENTAS** La configuración de la plataforma de ofimática (Microsoft Office 365) y de las herramientas de seguridad asociadas a la prestación del servicio de Centro de Operaciones de Seguridad (SOC), incluida la solución de protección antivirus, podrá ser objeto de ajustes y modificaciones como consecuencia de la transición, incorporación del proveedor del servicio SOC. Las modificaciones referidas tendrán como finalidad alinear la operación de seguridad con los modelos operativos, metodologías, capacidades tecnológicas y buenas prácticas del proveedor entrante, así como con los requisitos específicos definidos por Contratante. Dichos ajustes podrán comprender, de manera enunciativa y no limitativa, cambios en políticas y estándares de seguridad, reglas de detección, configuraciones de monitoreo, umbrales de alertamiento, integraciones entre herramientas, y procedimientos y mecanismos de respuesta a incidentes. Todo cambio de configuración deberá ejecutarse bajo un esquema de gestión de cambios y configuraciones, de manera planificada, controlada, documentada y previamente autorizada por el Contratante, garantizando la continuidad del servicio, la integridad, confidencialidad y disponibilidad de la información, y la protección de los activos tecnológicos. En todo caso, los ajustes deberán

	observar las políticas y directrices de seguridad del contratante, los requisitos legales y regulatorios aplicables, y los marcos de referencia reconocidos, incluyendo la norma ISO/IEC 27001:2022, según resulte pertinente. El Proveedor será responsable de identificar, proponer y sustentar técnica y documentalmente los cambios requeridos, bajo un enfoque de mejora continua y gestión del riesgo. El Contratante conservará la facultad de revisar, solicitar ajustes, aprobar o rechazar las modificaciones propuestas, considerando su impacto operativo, contractual y en el nivel de riesgo aceptable; en consecuencia, el Proveedor no implementará cambios sin la aprobación previa y expresa del Contratante, salvo en los casos de contención urgente de incidentes conforme a los procedimientos acordados. Finalmente, todo cambio deberá quedar debidamente registrado como parte de la gestión de configuraciones y cambios, incluyendo, como mínimo, la solicitud, el análisis de impacto, la evaluación de riesgos, las aprobaciones, el plan de implementación, la evidencia de ejecución, las pruebas/validaciones y el plan de reversión, asegurando trazabilidad, auditoría y la posibilidad de retorno al estado anterior cuando sea necesario.
1.5	**HORARIO Y FORMAS DE ATENCIÓN:** • Atención de lunes a domingo de 00:00 a 23:59 (24x7) • Desde una línea telefónica • 100% en español • Atención desde un lugar físico en Colombia • El proveedor debe incluir en la propuesta una plataforma 100% web que permita documentar y gestionar los incidentes de seguridad de la información, los playbooks, los planes de recuperación de desastres y las pruebas programadas, conforme a lo requerido en la guía técnica ISO 27035 para gestión de incidentes. • El proveedor debe suministrar el acceso a una aplicación 100% web para la gestión de los casos de soporte y las acciones del SOC.
1.6	**ACUERDO DE NIVEL DE SERVICIO Y ATENCIÓN:** El contratista deberá cumplir con los acuerdos de nivel de servicio (ANS) y la matriz de escalamientos para la atención de los casos de soporte e incidentes de seguridad de la información que sean establecidos por la ETITC A continuación, se describen los niveles que integran la matriz de escalamiento para la atención de ETITC y del proyecto, así como los roles del personal a cargo. • **Nivel 1 – Analista de Monitoreo SOC**: Atención inmediata por parte de los operadores de nivel 1(atención remota). Monitoreo continuo, clasificación de alertas, análisis inicial, notificación y escalamiento. • **Nivel 2 – Analista Especialista SOC:** Escalamiento a nivel 2 con respuesta en máximo de 30 minutos (atención remota). Análisis avanzado, correlación, diagnóstico del incidente, recomendación y ejecución de contención de primer nivel. • **Coordinador del SOC:** Intervención de nivel 2 y coordinadores del SOC para la atención de incidentes en curso en máximo 45 minutos (atención

	remota). Gestión integral del incidente, aseguramiento del cumplimiento de ANS, coordinación con la ETITC y elaboración de informes. • Reuniones de seguimiento mensual de manera presencial o virtual con el o los Coordinadores del SOC. • El contratista deberá informar de manera prioritaria e inmediata de acuerdo con la matriz de escalamiento y los ANS definidos, así como alertar sobre los cambios de seguridad, de configuración y críticos que se generen en las plataformas tecnológicas que se están monitoreando. Para esto, se debe hacer y entregar a la ETITC una tabla de alertas, prioridad, tiempos, escalamiento. • El contratista deberá realizar seguimiento a los diferentes incidentes hasta tener un cierre confirmado de los mismos. • La erradicación avanzada, recuperación total del servicio y decisiones de impacto a la entidad son responsabilidad de la ETITC, con acompañamiento técnico del SOC cuando aplique, conforme a la matriz de responsabilidades compartidas.
1.7	**REQUERIMIENTOS DE MONITOREO DE DISPONIBILIDAD Y RENDIMIENTO CON ENFOQUE EN SEGURIDAD** Este componente se limita al monitoreo con fines de seguridad de la información y no implica la operación, administración ni soporte de la infraestructura tecnológica de la ETITC El Proveedor deberá realizar el monitoreo continuo de la disponibilidad, capacidad y comportamiento operativo de los activos tecnológicos incluidos en el alcance del servicio SOC, con el único fin de identificar eventos, anomalías o degradaciones que puedan estar asociadas a incidentes de seguridad de la información o ciberseguridad. Este componente ***no corresponde a un servicio de Centro de Operaciones de Red (NOC)*** ni reemplaza las funciones de operación o administración de infraestructura tecnológica de la ETITC, y se limita exclusivamente al apoyo del proceso de detección y análisis de eventos de seguridad. El monitoreo deberá contemplar, como mínimo, las siguientes actividades: • Seguimiento al estado operativo de las plataformas, sistemas y herramientas de seguridad de la ETITC (disponibilidad, capacidad y comportamiento anómalo), con el fin de identificar posibles afectaciones asociadas a incidentes de seguridad. • Identificación de degradaciones de rendimiento, latencias inusuales o indisponibilidades que puedan indicar ataques de denegación de servicio, consumo anómalo de recursos, fallos provocados por actividades maliciosas u otros eventos de ciberseguridad. • Monitoreo de los canales de comunicación críticos únicamente para detectar anomalías relacionadas con seguridad (por ejemplo, intentos de interrupción intencional del servicio o comportamientos anómalos del tráfico). • Generación y envío de alertas correlacionadas cuando se identifiquen eventos que, por su naturaleza, severidad o recurrencia, puedan

representar un riesgo para la confidencialidad, integridad o disponibilidad de los activos de información.

- Uso de fuentes de inteligencia de amenazas externas debidamente reconocidas (listas de reputación de IP, dominios maliciosos u otros indicadores) para apoyar la validación de eventos detectados y enriquecer el análisis de seguridad.
- El proveedor deberá ejecutar pruebas de **análisis de vulnerabilidades** sobre los servicios web o servidores que requiera la entidad. Deberá atender por lo menos 10 solicitudes mensuales las cuales se informarán por medio de los canales de comunicación establecidos. Los resultados deberán ser enviados máximo en 8 horas hábiles (por cada 5 objetivos) y deberán incluir el reporte de la herramienta de escaneo de vulnerabilidades y el informe de análisis de vulnerabilidades.
- El proveedor deberá ejecutar **pruebas de penetración** de tipo **caja negra** sobre los servicios web o servidores que requiera la entidad. Deberá atender por lo menos 10 solicitudes mensuales las cuales se informarán por medio de los canales de comunicación establecidos. Los resultados deberán ser enviados máximo en 12 horas hábiles (por objetivo) y deberán incluir el reporte de la herramienta de escaneo de vulnerabilidades, el informe de análisis de vulnerabilidades, las técnicas de penetración usadas y los resultados con las debidas evidencias.
- El proveedor deberá ejecutar **pruebas de penetración** de tipo **caja blanca** sobre los servicios web o servidores que requiera la entidad. Deberá atender por lo menos 2 solicitudes mensuales las cuales se informarán por medio de los canales de comunicación establecidos. Los resultados deberán ser enviados máximo en 18 horas hábiles (por objetivo) y deberán incluir el reporte de la herramienta de escaneo de vulnerabilidades, el informe de análisis de vulnerabilidades, las técnicas de penetración usadas y los resultados con las debidas evidencias.

Las herramientas de escaneo de vulnerabilidades usadas por el proveedor debe brindar las mejores garantías de calidad en los resultados. El proveedor debe adjuntar a su propuesta la ficha técnica de las herramientas que usaran para la prestación de este servicio.

Las actividades descritas anteriormente deberán integrarse al proceso general de monitoreo, correlación y gestión de incidentes del SOC, y sus resultados deberán reflejarse en los informes, alertas y entregables definidos en el presente documento, sin asumir responsabilidades propias de la operación TI o del soporte de infraestructura.

1.8	**CAPACIDAD DE CONTENCIÓN DE INCIDENTES:** 1. El proveedor tendrá acceso de visualización directamente a las consolas de gestión de los sistemas cubiertos, de tal forma que las acciones y el monitoreo no dependa exclusivamente de la información recolectada por el SIEM. 2. Cuando se detecten eventos de seguridad en el SIEM que indiquen una anomalía, el SOC nivel 1 deberá validarlos directamente desde la consola del sistema de control, con el fin de analizarlos y determinar si constituyen incidentes de seguridad; únicamente estos últimos estarán sujetos a los tiempos de atención y a las penalidades definidas en los Acuerdos de Nivel de Servicio (ANS) 3. En caso de incidentes de ciberseguridad asociados a los sistemas vigilados, se deberá prestar y ejecutar las acciones de atención y contención rápidas como etapa inicial para la gestión del incidente por parte de la ETITC. 4. La confirmación de un incidente de seguridad se debe realizar en un plazo de máximo de 30 minutos después de detectada la anomalía y debe ser escalada al nivel 2 y al coordinador del SOC de manera inmediata. 5. Las acciones de contención deben ser coordinadas (documentadas y autorizadas) con anterioridad por medio de playbooks (libro de jugadas o guía de acciones). El proveedor debe crear los playbooks que se le soliciten en cuanto a los sistemas cubiertos y debe proponer los que consideren apropiados. 6. Los canales para la comunicación y coordinación de las actividades de contención deberán ser proporcionados por el proveedor. 7. El proveedor debe presentar por medio de una aplicación web los resultados de la gestión de incidentes, los resultados de la contención y la planeación de las pruebas.
1.9	**ATENCIÓN Y GESTIÓN DE INCIDENTES DE SEGURIDAD:** 1. Desde la herramienta de gestión de incidentes de seguridad proporcionada por el proveedor se deben registrar todos los incidentes de seguridad atendidos.

	2. El proveedor debe informar el estado de la gestión de los incidentes por medio de la herramienta web, asignando usuarios y perfiles a las personas que la ETITC necesite informar. Como medio alterno se usará les medios que la ETITC indique como email y Teams. 3. El proveedor debe proporcionar un informe de la gestión del incidente firmado por el profesional correspondiente, donde se registre las actividades y mejoras. 4. En caso de ser requerido, la ETITC podrá citar virtual o presencialmente por lo menos una vez al mes al coordinador del SOC para la presentación del informe (mensual o tras un incidente) o para solicitarle su concepto en la mejora de la gestión de seguridad de la información. 5. La notificación del incidente debe incluir detalles sobre el incidente, la naturaleza del ataque, la fecha y hora en que se detectó, el impacto potencial en la red o sistemas de la ETITC, así como las medidas que se están tomando para mitigar el impacto del incidente. 6. El contratista deberá generar reportes de eventos y de análisis de tendencias, para tomar las acciones preventivas y/o correctivas, tales como: instalación de parches, actualización de versiones, modificación de políticas y configuraciones. Además, debe quedar registros de cuándo, dónde y cómo se presentan los incidentes. Estos análisis deberán apoyarse en capacidades de inteligencia de amenazas (Threat Intelligence), mediante el uso de fuentes de carácter público, comercial o propio, que permitan fortalecer los procesos de detección, correlación y análisis de incidentes. Así mismo, deberá garantizar la trazabilidad de los incidentes, registrando como mínimo cuándo, dónde y cómo se presentan, así como la naturaleza del evento, impacto, acciones ejecutadas y estado de resolución. 7. El contratista deberá ejecutar actividades de Threat Hunting orientadas a la detección proactiva de amenazas. Estas actividades deberán realizarse de manera programada con una periodicidad mínima mensual, sin perjuicio de su ejecución adicional cuando se identifiquen eventos, indicadores de compromiso o alertas que lo ameriten. Cada actividad de Threat Hunting deberá generar entregables que incluyan como mínimo: - Hallazgos identificados - Análisis técnico de eventos - Indicadores de compromiso (IoC) - Recomendaciones de mitigación Las actividades deberán contribuir a un enfoque proactivo en la detección de amenazas avanzadas y a la mejora continua del servicio SOC.
1.10	**CONTINUIDAD DEL SERVICIO:** El proveedor deberá garantizar la continuidad y disponibilidad del servicio de Centro de Operaciones de Seguridad (SOC), asegurando la operación

ininterrumpida, proactiva y predictiva de los procesos de monitoreo, análisis, detección y atención de eventos e incidentes de seguridad de la información.

1. **Infraestructura del servicio SOC:** Garantizar que las plataformas, herramientas y componentes tecnológicos utilizados para la prestación del servicio SOC (incluyendo la plataforma de gestión de incidentes y herramientas complementarias) operen bajo condiciones de alta disponibilidad, redundancia y resiliencia.
   En caso de utilizar infraestructura propia o de terceros, deberá anexar la documentación que evidencie el cumplimiento de estándares de alta disponibilidad, tales como centros de datos nivel III (Tier III) según el Uptime Institute o equivalentes.
   Se precisa que las herramientas de seguridad suministradas por la ETITC (SIEM, Endpoint, Microsoft 365, entre otras) son de propiedad de la Entidad, por lo cual el proveedor no será responsable de la certificación del centro de datos donde estas se encuentren alojadas.

2. **Responsabilidad sobre la operación y detección del servicio SOC**

   Sin perjuicio de lo anterior, el proveedor será responsable de la operación integral del servicio SOC, incluyendo la capacidad de monitoreo continuo, análisis, correlación y detección proactiva y predictiva de eventos e incidentes de seguridad.
   En este sentido, el proveedor deberá:

   - Configurar, ajustar y optimizar reglas de correlación, detección y generación de alertas en las herramientas de seguridad.
   - Diseñar, implementar y mantener playbooks orientados a la detección temprana, contención y respuesta a incidentes.
   - Implementar mecanismos de análisis, aprendizaje y automatización que permitan identificar comportamientos anómalos, degradaciones del servicio o indicadores de compromiso antes de la materialización de incidentes.
   - Realizar monitoreo continuo tanto sobre las herramientas suministradas por la ETITC como sobre herramientas propias utilizadas en la operación del SOC.

   El proveedor será responsable de la detección oportuna de anomalías, degradaciones del servicio o eventos de seguridad, aun cuando estos tengan origen en infraestructura o plataformas de la Entidad.
   La no detección o notificación oportuna de eventos que puedan derivar en incidentes o afectaciones del servicio será considerada como incumplimiento de los Acuerdos de Nivel de Servicio (ANS).

	3. **Continuidad operativa del servicio**: El proveedor deberá contar con las capacidades técnicas, operativas y organizacionales que le permitan garantizar la continuidad del servicio SOC en caso de fallas en la infraestructura, incluyendo: • Disponibilidad de personal 7x24 • Mecanismos de acceso remoto seguro a las plataformas de la ETITC y recuperación ante fallas. • Mecanismos de monitoreo redundante (ETITC + proveedor). • Canales seguros y redundantes de acceso a las herramientas de la Entidad. • Procedimientos de contingencia operativa documentados. El modelo de operación deberá contemplar capacidades de alta disponibilidad a nivel del servicio SOC, independientemente de la infraestructura subyacente. 4. **Instalaciones y operación del servicio:** La ETITC podrá solicitar visitas técnicas a las instalaciones donde se encuentre el equipo operativo del SOC, con el fin de verificar las condiciones de prestación del servicio. 5. **Plan de continuidad del servicio:** El proveedor deberá presentar junto con la propuesta su esquema de continuidad del servicio SOC, el cual deberá incluir: • Escenarios de falla. • Estrategias de recuperación. • Procedimientos de contingencia. • Mecanismos de redundancia operativa. • Indicadores de disponibilidad del servicio. Dicho plan deberá ser aprobado por la ETITC y mantenerse actualizado durante la ejecución del contrato.
1.11	**ENTREGABLES DOCUMENTALES:** Los informes de operación mensuales se deberán entregar dentro de los primeros 5 días hábiles. • Informe mensual de gestión de los servicios y la infraestructura incluyendo el estado de cada uno de los activos monitoreados. • Presentar informe semanal sobre el estado general de los activos monitoreados, cambios y modificaciones en la infraestructura. • Informes de cambios y modificaciones en la infraestructura. • Informe mensual de gestión de los casos de soporte. • Inteligencia de amenazas: con la información recolectada se deberá entregar un informe quincenal y notificación cuando ocurra alguna alerta crítica o incidencia que puede o haya afectado a la entidad, en máximo tres horas a partir de la ocurrencia del evento, que incluya como mínimo:

	- Fecha y hora en la que se descubrió el incidente - Tipo de incidente - Prioridad en el tratamiento - IP origen - IP afectada - Detalle del incidente - Acciones ejecutadas de detención y contención de ataques - Recomendaciones de remediación **Alertas:** Reportes Diarios (Resumen informe mensual) Monitoreo: Reportes Diarios (Resumen informe mensual) Cambios: Reportes Diarios (Resumen informe mensual) Tendencias: Reportes Diarios o semanal según ocurra (Resumen informe mensual) Gestión: Reportes Diarios (Resumen informe mensual) Métricas: Reportes Mensual o a solicitud del supervisor (Resumen informe mensual) Estadísticas: Reportes Mensual o a solicitud del supervisor (Resumen informe mensual)
1.12	**CAPACITACIÓN:** • Se debe dar una capacitación sobre el uso de las herramientas incluidas en la propuesta al personal de soporte interno y a los administradores de los sistemas. • La capacitación debe ser por lo menos de 8 horas. • Se debe dar una capacitación, presencial en una sesión, acerca de buenas prácticas en la atención de incidentes de al menos 2 horas. • Capacitación de al menos 4 horas al equipo de soporte y administración pertenecientes al proceso de gestión de Informática y Telecomunicaciones de la ETITC, al respecto de respuesta de incidentes de seguridad y ciberseguridad. • Se incluirá en el ciclo de capacitaciones al equipo del Csirt Académico, con fines investigativos.
1.13	**PRUEBAS DE GESTIÓN DE INCIDENTES:** El proveedor debe presentar un plan de pruebas para atención, contención y recuperación frente a de incidentes de ciberseguridad guiado por el Coordinador del SOC. Estas pruebas deben ser semestrales. Se deberán realizar como mínimo dos (2) simulaciones de incidentes durante la vigencia del contrato, distribuidas en el periodo de ejecución, pudiendo ajustarse en su programación de común acuerdo con el supervisor del contrato. Las simulaciones deberán evaluar la capacidad de detección, análisis, respuesta y contención frente a eventos de seguridad.

	Cada simulación deberá generar un informe que incluya como mínimo resultados, tiempos de respuesta, análisis de desempeño y recomendaciones de mejora. La ETITC podrá solicitar ajustes al plan de pruebas conforme a las necesidades del servicio.
1.14	**PERSONAL El presente anexo técnico se desarrollara con base en el personal mínimo requerido habilitante según numeral 8.4 del estudio previo**

1. PLAZO PARA LA EJECUCIÓN DEL CONTRATO

El plazo de ejecución será de 3 meses contados a partir de la firma del acta de inicio, previo cumplimiento de sus requisitos de perfeccionamiento y ejecución.

2. ACTIVOS PARA MONITOREAR

Se relacionan a continuación los activos tecnológicos de la Entidad sobre los cuales el correlacionador de eventos del SOC deberá realizar actividades de monitoreo, correlación y análisis.

La información descrita en este numeral corresponde a una aproximación general del entorno tecnológico de la Entidad. En consecuencia, las cantidades, características específicas, versiones y configuraciones detalladas serán suministradas al contratista adjudicatario durante la fase de inicio del contrato, en el marco del proceso de empalme y transferencia de conocimiento.

Lo anterior con el fin de permitir un adecuado dimensionamiento del servicio, sin comprometer la seguridad de la infraestructura tecnológica institucional.

1. Firewall
2. Consola EndPoint Security de la ETITC: Licenciamiento a cargo de la ETTITC
3. Microsoft Directorio Activo sobre Windows Server: Licenciamiento a cargo de la ETTITC
4. Canales internet: Principal y respaldo
5. Canales WAN: 2 MPLS sedes
6. Sistema SOLARWINDS Security Event Manager SWE50 V.2025.4 (SEM) Licenciamiento a cargo de la ETITC
7. Correlación de eventos LevelBlue® USM Anywhere™ standard 30 days Licenciamiento a cargo de la ETITC
8. Aplicaciones institucionales
9. Servicios de Microsoft 365 (Outlook y OneDrive u otros)
10. Servidores físicos y virtuales
11. Consola de Virtualización
12. Sitios web institucionales
13. Otros activos tecnológicos relevantes para la operación del servicio

El contratista deberá garantizar la capacidad de monitoreo sobre estos activos y aquellos adicionales que sean incorporados durante la ejecución del contrato.

El servicio incluirá actividades de ingeniería social orientadas a evaluar el nivel de exposición y concientización de los usuarios, entre las cuales se contemplan:

- Identificación de exposición en fuentes abiertas
- Evaluación de información disponible en redes sociales
- Simulación de intentos de suplantación
- Ejercicios de phishing y vishing
- Validación de controles de acceso cuando aplique

Para la ejecución de estas actividades, el contratista deberá disponer de herramientas especializadas y licenciadas para la simulación de ataques de ingeniería social, que permitan la gestión controlada de campañas, la medición de resultados, la trazabilidad de los eventos y la generación de reportes.

Se deberá realizar como mínimo:

- Hasta 100 pruebas de phishing
- Hasta 50 pruebas de vishing

Las actividades de ingeniería social deberán ejecutarse durante la vigencia del contrato conforme a un plan de trabajo definido conjuntamente entre la ETITC y el contratista.

El volumen establecido de pruebas deberá cumplirse en su totalidad durante la vigencia contractual, pudiendo ser distribuido de manera periódica o escalonada de acuerdo con las necesidades institucionales.

La frecuencia, programación y alcance específico de las campañas serán definidos durante la ejecución del contrato y deberán estar debidamente documentados en los informes del servicio.

ANEXO 01- ATENCION Y ANS (ACUERDOS A NIVEL DE SERVICIO)

CLASIFICACIÓN DE SERVICIOS: El servicio permitirá atender

- Incidentes de Seguridad
- Requerimientos del Servicio SOC

A continuación, se describe en qué eventos el servicio se canalizará como incidente, y en qué eventos como requerimiento. También se describe su nivel de criticidad, dependiendo de cada situación.

- Incidentes de Seguridad: Un incidente corresponde a cualquier evento confirmado de seguridad considerando el impacto sobre la disponibilidad, confidencialidad e

integridad de los activos de información de la ETITC, los incidentes se medirán según su nivel de criticidad (alto, medio bajo).
El servicio de atención de incidentes comprende las actividades de identificación, análisis inicial, confirmación, notificación y ejecución de acciones de contención de primer nivel, conforme a los playbooks y a la matriz de responsabilidades definidas en el contrato.
Las actividades de erradicación avanzada, recuperación total y restablecimiento del servicio serán responsabilidad de la ETITC, con el acompañamiento técnico del proveedor del SOC cuando aplique.
El tiempo de atención corresponde al tiempo máximo para identificación, análisis inicial y notificación, no al tiempo total de solución.

Nivel de Criticidad	Descripción	Tiempo de Atención	Entregable
Alto	Incidente de seguridad con afectación crítica o total de los servicios de la organización, o compromiso grave de información generado por un evento de seguridad informática.	Máximo 15 minutos.	Informe del incidente que incluya como mínimo: • Causa, • Forma de detección • Análisis del evento • Acciones de contención o solución aplicada • Impacto identificado
Medio	Incidente de seguridad con Afectación parcial del servicio contratado. Intermitencia en los servicios de la organización o impacto de nivel medio en la organización generados sobre los activos de información.	Máximo 2 horas.	Informe del del incidente que incluya como mínimo: • Causa, • Detección, • Análisis, • Acciones de contención o solución aplicada
Bajo	Evento de seguridad sin impacto operativo crítico, que no interrumpe los servicios, pero requiere análisis y seguimiento (por ejemplo: intentos de ataque bloqueados o alertas preventivas).	Máximo 4 horas.	Informe del evento incluya como mínimo: • Causa, • Detección, • Análisis, • Solución • Recomendaciones

- Atención de Requerimientos del Servicio SOC

Los requerimientos corresponden a solicitudes relacionadas con ajustes de configuración, parametrización y cambios autorizados sobre las herramientas y plataformas incluidas en

el alcance del servicio SOC, los cuales serán atendidos conforme a su nivel de criticidad y previa autorización del supervisor del contrato.
Los requerimientos serán gestionados según su nivel de criticidad y prioridad operativa.

Nivel de Criticidad	Descripción	Tiempo de Atención	Entregable
Alto	Solicitud de adición, modificación y/o cambio de parámetros debido a que afecta a la Organización asociadas a nuevas funcionalidades o cambios internos prioritarios.	Máximo 30 minutos.	Correo electrónico de confirmación y registro en el Informe Mensual de Requerimientos.
Medio	Solicitud de adición, modificación y/o cambio de parámetros debido a que afecta de forma parcial la operación de la Organización.	Máximo 2 horas.	Correo electrónico de confirmación y registro en el Informe Mensual de Requerimientos
Bajo	Solicitud de adición, modificación y/o cambio de parámetros que no inciden en el funcionamiento operativo de la organización.	Máximo 6 horas.	Correo electrónico de confirmación y registro en el Informe Mensual de Requerimientos

DISPONIBILIDAD DEL SERVICIO SOC

El Contratista deberá cumplir con los acuerdos de niveles de servicio establecidos en el presente documento, en el caso de no cumplirlos, asumirá los descuentos descritos en la *Tabla 1*, estos acuerdos de niveles de servicio se aceptan con la suscripción del contrato.

Ante el incumplimiento por parte del Contratista de los acuerdos niveles de servicio (ANS) establecidos, la Entidad, generará penalizaciones al Contratista que afectarán el valor de la factura del mes correspondiente, para cada uno de los niveles de servicios insatisfechos

Por lo anterior, y con la finalidad de medir la prestación del servicio, se han diseñado dos indicadores de niveles de servicio que Le permiten medir a la ETITC la indisponibilidad del servicio y la oportunidad de la prestación del servicio

ESQUEMA DE PENALIZACIONES

Con el objetivo de garantizar el cumplimiento del Acuerdo de Nivel de Servicio (SLA), se establece el siguiente esquema de penalizaciones aplicable ante incumplimientos atribuibles al proveedor. Las penalizaciones serán calculadas sobre el valor mensual del servicio y se descontarán de la factura correspondiente al mes siguiente al evento.

CONDICIONES GENERALES DE PENALIZACIONES

- Las penalizaciones no son acumulativas por evento y tendrán un tope máximo de 25% del valor mensual.
- Se excluyen de penalización los eventos generados por causas de fuerza mayor, acciones del cliente o fuera del alcance del contrato.
- Todos los incumplimientos deberán ser debidamente documentados y reportados por ambas partes para su validación.
- Las penalizaciones se aplicarán exclusivamente sobre incidentes de seguridad confirmados, entendidos como aquellos que afectan la confidencialidad, integridad o disponibilidad de la información.
  Las alertas o eventos de seguridad no serán sujetos de penalización, salvo que deriven en incidentes que no sean gestionados conforme a los ANS establecidos.

SLA Monitoreado	Parámetro	Penalización por incumplimiento
Identificación y análisis de posibles incidentes de seguridad	< 15 minutos	2% del valor mensual por evento
Escalamiento de incidentes críticos	< 30 minutos	1% del valor mensual por evento
Notificación de incidentes críticos	< 30 minutos	2% del valor mensual por evento
Notificación de incidentes altos	< 1 hora	1% del valor mensual por evento
Notificación de incidentes Medios **Inicio de Respuesta – Incidentes Críticos**	< 4 horas < 1 hora	2% del valor mensual si hay más de 3 eventos fuera de SLA 5% del valor mensual por evento
Inicio de Respuesta – Incidentes Altos	< 2 horas	2% del valor mensual por evento
Disponibilidad de Plataforma SIEM/SOAR/Portal **Gestión de Cambios en Plataforma SIEM**	>99.7% mensual < 24 horas hábiles desde la solicitud	1% por cada 0.1 por debajo del umbral 1% del valor mensual por cada solicitud fuera de SLA

Tabla 1

ACCION	NOMBRE	CARGO/PERFIL	FECHA	FIRMA
Elaboró	Ing. Luis Javier Tovar	Profesional de Seguridad de la Información	31/08/2026	*Luis Tovar*