Lote 4 SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
1	**SOLUCIÓN SIEM-SOAR**		
1.1	Con el objetivo de fortalecer las capacidades institucionales en la gestión, detección y respuesta ante incidentes de seguridad de la información, se requiere una solución integral de SIEM y SOAR, que permita la correlación avanzada de eventos, la detección oportuna de amenazas cibernéticas y la orquestación automatizada de respuestas, por lo cual, la solución deberá ser escalable, soportar un crecimiento progresivo de la capacidad de procesamiento de eventos (EPS). Lo anterior bajo un modelo de despliegue que puede ser on-premise o Cloud o híbrido, permitiendo la interoperabilidad y el aprovechamiento de la arquitectura tecnológica existente, sin perjuicio de la adopción de nuevos esquemas de licenciamiento o suscripción, como también la incorporación de nuevos componentes de hardware, que permitan mejorar el desempeño, la escalabilidad y la eficiencia operativa de la solución, teniendo en cuenta los requerimientos técnicos del proceso. La solución deberá permitir la integración de cualquier fuente de información de las diferentes marcas que operan la ciberseguridad en La Policía Nacional de Colombia, para uso continuo con derecho a actualizaciones y nuevas versiones (upgrade) por un término de veinticuatro (24) meses y que cumpla las siguientes características: Se deberá entregar una solución con funciones de Security Information and Event Management (SIEM) junto con la funcionalidad de Security Orchestration, Automation, and Response (SOAR), en la que todos los componentes deben ser de un mismo fabricante, con el fin de garantizar la integración nativa, la simplificación operativa, la reducción de la complejidad técnica y la optimización de la gestión, soporte y mantenimiento de la solución. El almacenamiento para la administración y operación de la solución podrá implementarse en un esquema on-premise, cloud o híbrido, garantizando una capacidad de retención y consulta de información (logs y eventos) de mínimo noventa (90) días. Para tal efecto, el proponente podrá contemplar, de ser necesario, el uso e integración de la infraestructura de almacenamiento existente en la Policía Nacional (una unidad NAS con capacidad de 200 TB), siempre que se garantice su compatibilidad, desempeño y adecuada integración con la solución propuesta La solución propuesta deberá contar con reconocimiento en el mercado en funcionalidades de SIEM y SOAR. Para tal efecto, el oferente deberá presentar informes o estudios de analistas independientes que respalden dichas capacidades. Se aceptarán,		

Lote 4 SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	entre otros, reportes emitidos por Gartner y/o Forrester y/o GigaOm u otras firmas reconocidas del sector (No superiores a dos (2) años), en los cuales la solución ofertada esté incluida dentro de las categorías de SIEM-SOAR. No se aceptarán como soporte documentos, reportes o certificaciones elaborados por el propio fabricante. Junto con la propuesta, el oferente deberá adjuntar documentación oficial emitida por el fabricante (casa matriz), que sustente de manera clara y verificable el funcionamiento de la solución de SIEM y SOAR, así como el cumplimiento de la totalidad de las especificaciones técnicas requeridas en el presente proceso. No se aceptará documentación distinta a la oficial del fabricante.		
2	**FUNCIONALIDADES DEL SIEM Y SOAR**		
2.1	El oferente debe hacer entrega de un certificado de casa matriz en el que se certifique que la solución ofertada de SIEM-SOAR cumple con todos los requerimientos técnicos solicitados. Por lo anterior, el oferente debe especificar la marca de la solución a ofrecer, así: **Marca:**		
2.2	La solución, en su funcionalidad de SIEM, deberá soportar una capacidad mínima de procesamiento de veinte mil (20.000) eventos por segundo (EPS) o, en su defecto, una ingesta promedio equivalente de al menos un (1) terabyte (TB) por día, garantizando el desempeño, la estabilidad y la disponibilidad de la plataforma.		
2.3	La solución deberá permitir la recepción o ingesta de datos provenientes de cualquier fuente de información, así como la creación y configuración de *parsers* definidos durante la fase de implementación inicial del proyecto, permitiendo el apoyo de asistencia basada en inteligencia artificial del fabricante de la solución. Asimismo, la solución deberá contar con capacidad de absorber picos de ingesta o recepción significativamente superiores al requerido, garantizando en todo momento la recepción, retención y posterior procesamiento de los datos sin pérdida de información. Lo anterior siempre que el volumen promedio diario de ingesta o recepción se mantenga dentro de los parámetros establecidos en el presente proceso.		
2.4	En caso de que la solución sea de tipo cloud, deberá contar con una instancia dedicada y aislada para la Policía Nacional de Colombia, en la cual se gestione las funcionalidades de SIEM y SOAR. Dicha instancia deberá soportar como mínimo diez (10) usuarios con acceso a la plataforma, asociados a los dominios @correo.policia.gov.co y @policia.gov.co.		

Lote 4 SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	Adicionalmente, la solución deberá contar con autenticación multifactor (MFA) para el acceso de los usuarios, garantizando mecanismos de control de identidad y seguridad en el ingreso a la plataforma En caso de que la solución sea de tipo on-premise, deberá permitir la integración con el Directorio Activo institucional para la gestión centralizada de identidades y control de accesos. En cualquiera de los casos, la solución deberá disponer de una consola de administración basada en web para el acceso de los usuarios.		
2.5	En caso de que la solución sea de tipo on-premise, deberá contar con una arquitectura de hardware certificada por el fabricante de la solución ofertada, que permita el fortalecimiento de las capacidades institucionales. Para tal efecto, el proponente podrá considerar la infraestructura tecnológica existente, la cual también deberá ser validada y certificada por el fabricante (casa matriz). En relación con lo anterior, la solución deberá contemplar como mínimo los siguientes componentes de hardware, dispuestos en dispositivos separados: 1. Un (1) dispositivo para la consola de gestión de la solución. 2. Un (1) dispositivo para el procesamiento de datos. 3. Un (1) dispositivo para la recolección de eventos. Podrán incorporarse dispositivos adicionales, de acuerdo con el diseño arquitectónico de la solución ofertada, siempre que estos se encuentren certificados por el fabricante para su inclusión dentro de la arquitectura propuesta. En caso de que la solución sea de tipo cloud o híbrida, se deberá entregar junto con la propuesta la certificación de la arquitectura de la solución emitida por el fabricante (casa matriz). Asimismo, la solución deberá contar con un componente on-premise para la recolección de datos, para lo cual el proponente podrá hacer uso de la infraestructura tecnológica existente, siempre que esta sea compatible y validada por el fabricante dentro del diseño de la arquitectura propuesta. En caso de que alguno de los componentes de la arquitectura no soporte los requerimientos establecidos en el presente proceso durante el período de soporte y garantía, deberá ser reemplazado por otro de mayor capacidad, garantizando la continuidad y calidad del servicio, previa validación y concepto del fabricante		

Lote 4 SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	(casa matriz), sin que ello implique costos adicionales para la Policía Nacional de Colombia. Las especificaciones de la infraestructura tecnológica existente serán detalladas en el ítem de soporte correspondiente, con el fin de que puedan ser verificadas y validadas por el fabricante (casa matriz) para efectos de la certificación de la arquitectura requerida. La certificación de casa matriz respecto de la arquitectura deberá ser entregada junto con la propuesta, e incluir los datos de contacto del fabricante en Colombia, con el fin de permitir su verificación. En caso de que los componentes de la infraestructura tecnológica existente no sean avalados y certificados por el fabricante, el contratista deberá suministrar e implementar la infraestructura necesaria para soportar los requerimientos de la solución, la cual deberá contar con la respectiva certificación del fabricante (casa matriz), debiendo ser presentada por el oferente junto con la propuesta.		
2.6	La solución deberá permitir el monitoreo continuo de eventos y la gestión de la seguridad, organizados por dominios funcionales tales como autenticación, malware/antivirus, detección de intrusiones, firewalls, tráfico de red y acceso VPN, entre otros. Asimismo, deberá incorporar capacidades de detección basadas en IA/ML (Inteligencia Artificial/Machine Learning) que complementen los mecanismos tradicionales de correlación y reglas.		
2.7	La solución deberá permitir la configuración de reglas de correlación personalizadas, clasificando los eventos detectados y generando alertas tipificadas conforme al marco de MITRE ATT&CK, mediante su representación en matrices y mapas de calor que faciliten el análisis y la priorización de amenazas.		
2.8	La solución deberá permitir la gestión de eventos mediante consultas avanzadas, así como la construcción de tableros (dashboards) dinámicos basados en condiciones y criterios configurables, que faciliten el análisis de la información y fortalezcan los procesos de cacería de amenazas (*threat hunting*).		
2.9	La solución deberá contar con capacidad de ingesta de datos mediante conectores configurables y personalizables, que permitan la parametrización e integración de cualquier fuente de información, incluyendo, pero sin limitarse a, mecanismos basados en APIs, syslog, agentes, archivos planos, bases de datos y servicios en la nube. Asimismo, deberá permitir el desarrollo, modificación y despliegue de conectores personalizados cuando no existan integraciones nativas.		
2.10	La solución deberá contar con una funcionalidad de inteligencia de amenazas (*Threat Intelligence*) nativa, que permita el		

Lote 4 SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	enriquecimiento y la contextualización de eventos de seguridad dentro de los procesos de investigación, detección y correlación. Dicha funcionalidad deberá ser provista por el mismo fabricante de la solución ofertada, garantizando su integración nativa y operación unificada. Asimismo, deberá permitir la integración y gestión de fuentes de inteligencia de amenazas internas y externas (feeds), incluyendo la administración de indicadores de compromiso (IoC), tales como direcciones IP, dominios, URLs, hashes y otros artefactos relevantes, los cuales deberán ser utilizados en los procesos de correlación, detección y respuesta automatizada.		
2.11	La funcionalidad de inteligencia de amenazas deberá permitir la consulta, ingestión e inclusión de indicadores de compromiso (IoC) mediante integración vía API, de forma manual y automática, así como su visualización en tiempo real. Asimismo, deberá soportar la actualización continua de dichos IoC y su aplicación en procesos de detección, correlación e investigación, incluyendo su uso dentro de reglas de correlación y flujos de respuesta automatizada (playbooks), con el fin de fortalecer la capacidad de mitigación de amenazas. Se deberá integrar con la MISP-PONAL.		
2.12	La solución deberá permitir la investigación avanzada de eventos basada en telemetría, comportamientos y análisis contextual, incorporando capacidades de analítica avanzada e inteligencia artificial para el descubrimiento de patrones, anomalías y amenazas. Asimismo, deberá habilitar capacidades de *threat hunting* mediante búsquedas interactivas sobre grandes volúmenes de datos, sin restricciones funcionales que limiten su uso operativo dentro de la plataforma.		
2.13	La solución deberá contar con un módulo de reportería personalizable, que permita la generación de reportes y tableros analíticos con filtros avanzados y visualizaciones gráficas tales como mapas de calor, geolocalización, gráficos de flujo (*flow charts*), tendencias, gráficos de barras y tablas dinámicas, entre otros. Estos elementos deberán actualizarse constantemente y permitir la exportación de la información en formato PDF, entre otros.		
2.14	La solución deberá incorporar de forma nativa capacidades para la gestión de incidentes, incluyendo la delegación de casos, el seguimiento, los escalamientos, la documentación detallada de cada incidente y el proceso de triage. Asimismo, deberá permitir la asignación basada en roles, la trazabilidad completa del ciclo de vida del incidente y el registro de auditoría de todas las acciones ejecutadas dentro de la plataforma.		
2.15	Deberá permitir la creación y personalización de reglas de correlación adaptadas a los requerimientos de la organización, con capacidad para combinar múltiples fuentes de datos, con el fin de obtener una comprensión integral de los incidentes de seguridad, permitiendo la asistencia de inteligencia artificial en el		

Lote 4 SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	diseño, optimización o recomendación de dichas reglas. Asimismo, deberá contar con reglas predefinidas asociadas a tecnologías de múltiples fabricantes, las cuales deberán ser modificables de acuerdo con las necesidades institucionales.		
2.16	La solución deberá permitir el desarrollo de casos de uso de cumplimiento mediante la ingesta de datos y la configuración de reglas de correlación. Asimismo, deberá soportar la implementación de múltiples casos de uso de seguridad documentados, ajustables a las necesidades de la organización.		
2.17	La solución podrá contar, de forma opcional, con funcionalidad de UEBA (User and Entity Behavior Analytics) mediante un sensor nativo del fabricante de la solución ofertada, para su despliegue en los controladores de dominio de la institución, con el propósito de obtener información de auditoría del Directorio Activo.		
2.18	La solución deberá contar de forma nativa con conectores propios de diversos fabricantes, que permitan la integración de las diferentes fuentes de información de la institución. La ingesta de eventos de seguridad provenientes de aplicaciones, bases de datos, servidores, infraestructura de comunicaciones e infraestructura de seguridad deberá realizarse mediante agentes o métodos de recolección nativos soportados por la herramienta ofertada		
2.19	La solución deberá contar con capacidad de integración mediante API REST bidireccional, que permita la ejecución de acciones, la activación de *playbooks* y la consulta de detecciones, incidentes o casos gestionados.		
2.20	La solución deberá contar con un mecanismo de comunicación seguro basado en el protocolo SSL/TLS a través del puerto 443. Asimismo, deberá incluir la funcionalidad de restricción de acceso a la consola mediante listas de direcciones IP permitidas		
2.21	La solución deberá permitir la creación de *parsers* para fuentes de información no estándar, cuando por necesidad de la institución se requiera su inclusión en los procesos de analítica, correlación y tratamiento de la información. Esta funcionalidad deberá soportar el uso de scripts, expresiones regulares (regex) y capacidades nativas de la solución, con el fin de facilitar la normalización y estructuración de los datos. Asimismo, la creación de *parsers* deberá incluir funcionalidades de pruebas y validación, que permitan verificar la correcta extracción y asignación de campos. Adicionalmente, la solución deberá contar con un asistente basado en inteligencia artificial que apoye la creación, optimización y mejora de *parsers* a partir del análisis de muestras de logs.		
2.22	La solución podrá contar, de forma opcional, con la capacidad de desplegar colectores o conectores nativos para la ingesta de información mediante agentes de software del mismo fabricante de la solución ofertada, que operen sobre determinadas fuentes		

Lote 4 SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	de datos, permitiendo el envío de logs hacia la solución, ya sea en modalidad on-premise, cloud o híbrida.		
2.23	En caso de que la solución sea de tipo cloud o híbrido, para aquellas fuentes de datos que no permitan el despliegue de agentes de software para el envío de logs hacia la solución en la nube, deberá contar con la capacidad de recibir la información mediante un colector o conector nativo on-premise, que funcione como pasarela para la transferencia de datos hacia la nube. En caso de que la solución sea de tipo on-premise, deberá contar con un recolector de eventos dedicado para la recepción de logs provenientes de diferentes fuentes, independiente de los demás componentes del sistema. Según sea el caso, los componentes deben estar incluidos dentro de la certificación de la arquitectura emitida por el fabricante, que deberá ser presenta con la propuesta.		
2.24	Los colectores o conectores deberán contar como mínimo con la capacidad de recolección de datos mediante Syslog, consultas SQL, archivos locales, registros de eventos de Windows (Windows Event Log), *journal* de sistemas Linux y APIs (REST u otros mecanismos de integración soportados por la solución), entre otros métodos de recolección.		
2.25	La solución deberá contar con una vista que permita visualizar el consumo de eventos provenientes de las diferentes fuentes de datos, así como el estado de los colectores o conectores, indicando si presentan actividad o inactividad. Asimismo, deberá generar alertas cuando no se reciban eventos durante un período de 24 horas, registrando la última hora de ingesta o recepción. De igual forma, deberá permitir la visualización de la cantidad de datos ingeridos o recepcionados por día y su distribución por fuente de datos.		
2.26	Los colectores o conectores deberán permitir el filtrado de logs antes de su envío a la solución, independientemente de la modalidad de despliegue (on-premise, cloud o híbrida), con el fin de descartar registros que no aporten valor, optimizando la gestión de la información y el uso de los recursos asociados al presente proceso.		
2.27	La solución deberá tener la capacidad de normalizar, filtrar, deduplicar, correlacionar, categorizar e identificar incidentes de seguridad, así como generar las notificaciones correspondientes a los eventos o incidentes detectados.		
2.28	La solución deberá permitir la búsqueda de los datos en tiempo real, con rangos de tiempo definidos, tales como: minutos, horas, días o meses con el fin de realizar monitoreo. Las búsquedas deben mostrar los datos en poco tiempo para no afectar la respuesta del manejo de los incidentes.		
2.29	La solución deberá ser capaz de transformar los eventos en gráficas, reportes y vistas que permitan monitorear las métricas		

Lote 4 SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	importantes para la organización. Estás vistas deberán ser completamente personalizables		
2.30	La solución deberá permitir la visualización de la postura de seguridad de la organización mediante tableros consolidados que integren múltiples dominios de seguridad, tales como endpoint, red, autenticación, tráfico, entre otros.		
2.31	La solución deberá permitir el uso simultáneo de la plataforma por distintos usuarios, sin interferencia entre casos de uso ni degradación del desempeño.		
2.32	La solución deberá permitir el uso de tableros (dashboards) interactivos, habilitando la navegación, el filtrado y el pivoteo hacia análisis detallados o consultas subyacentes por medio de drill-down		
2.33	La solución deberá contar con la capacidad de generar gráficos de tendencias y visualización de datos, IoCs, los cuales podrán representarse en formatos como tablas, gráficos de flujo (tipo Sankey), gráficos de columnas, mapas de calor y mapas de geolocalización, entre otros, con el fin de facilitar el análisis visual de la información. Estas visualizaciones deberán actualizarse en tiempo real		
2.34	La solución deberá contar con un módulo de analítica que permita la identificación de incidentes de seguridad en la organización, considerando la visibilidad sobre múltiples fuentes de datos integradas, tales como EDR, entornos cloud, gestión de identidades, correo electrónico, navegación web, red, firewalls y VPN, entre otros. Dicho módulo deberá permitir, como mínimo: • Detectar malware conocido y desconocido, incluyendo amenazas de día cero. • Detectar tácticas, técnicas y procedimientos (TTPs) conforme al marco MITRE ATT&CK, asociados a la explotación de vulnerabilidades. • Detectar indicadores de ataque (IoA) e indicadores de compromiso (IoC). • Identificar actividades sospechosas en sistemas, tales como procesos, registros, scripts, comandos, controladores (drivers), entre otros. • Identificar movimientos laterales y accesos indebidos de credenciales. • Detectar ataques y explotación de vulnerabilidades, incluyendo aquellos de tipo día cero. • Contar con capacidades de respuesta y remediación mediante la integración con las funcionalidades de SOAR.		
2.35	La solución deberá incluir un módulo de automatización tipo SOAR, del mismo fabricante de la solución ofertada, que permita la creación, el desarrollo y ejecución de *playbooks* para la automatización de actividades de respuesta sobre las fuentes de		

Lote 4 SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	datos. Dicho módulo deberá soportar acciones tales como el aislamiento de dispositivos, el enriquecimiento con inteligencia de amenazas, *auto-triage*, notificaciones personalizadas e integración con plataformas de inteligencia, entre otras. Asimismo, deberá permitir la ejecución remota de scripts como parte de los procesos de respuesta y remediación. Dichos *playbooks* deberán poder ejecutarse de forma automática, bajo demanda o de manera programada.		
2.36	La funcionalidad SOAR, en caso de ser on-premise, deberá ser desplegada en un componente de hardware independiente, para lo cual se podrá hacer uso de la infraestructura actual o de un nuevo dispositivo. Esta condición deberá estar contemplada en la certificación de la arquitectura emitida por el fabricante de la solución, la cual deberá ser entregada por el oferente junto con la propuesta.		
2.37	La funcionalidad de SOAR deberá contar con un tablero de gestión que permita visualizar las ejecuciones de *playbooks* correspondientes, el cual deberá evidenciar como mínimo: • La cantidad de ejecuciones de *playbooks* originadas a partir de alertas, detecciones o incidentes. • La cantidad de ejecuciones derivadas de aprobaciones de usuarios. • La tendencia de ejecuciones de *playbooks* exitosas y fallidas. • El *top* de ejecuciones según el tipo de disparador o mecanismo de iniciación de los *playbooks*. • El listado de las ejecuciones más recientes, así como aquellas ejecutadas bajo demanda.		
2.38	La solución deberá contar con capacidades de respuesta orquestada, integrando múltiples vectores de seguridad, tales como EDR, antivirus, entornos cloud, gestión de identidades, correo electrónico, navegación web, VPN, red y firewalls, entre otros, con el objetivo de prevenir, contener y mitigar el impacto de incidentes de seguridad de la información. Para tal efecto, deberá contar con una biblioteca de *playbooks* preconstruidos y un conjunto amplio de acciones de respuesta disponibles con documentación técnica de las integraciones del módulo SOAR.		
2.39	Las acciones del módulo SOAR deberán poder ejecutarse mediante APIs, *playbooks* nativos o a través de la integración con el SIEM		
2.40	La funcionalidad de SOAR deberá contar con trazabilidad de la ejecución de cada *playbook*, permitiendo comprender las actividades realizadas, los procesos de decisión y la identificación de errores para la mejora continua de su diseño y respuesta. Asimismo, deberá incluir un módulo de auditoría que permita registrar quién realizó cambios, cuándo se efectuaron y qué modificaciones se aplicaron, manteniendo el versionamiento de los *playbooks* y la posibilidad de restaurar versiones anteriores.		

Lote 4 SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
2.41	La solución SIEM-SOAR deberá contar con capacidades de inteligencia artificial propias del fabricante de la solución ofertada, orientadas a optimizar el desempeño de cada uno de los componentes funcionales de la plataforma, de acuerdo con su rol dentro de la arquitectura de seguridad de la solución ofertada.		
2.42	La solución SIEM-SOAR deberá contar con capacidades de asistencia basadas en inteligencia artificial mediante lenguaje natural, que permitan: • Realizar consultas y búsquedas de información dentro de la solución, tales como listados de dispositivos con características específicas, aplicaciones de riesgo, vulnerabilidades e indicadores de compromiso (IoCs), con el fin de reducir los tiempos de investigación de los analistas. • Consultar ejecuciones de scripts y obtener explicaciones en lenguaje natural sobre su funcionamiento y significado. • Generar consultas para la ejecución de búsquedas, agilizando los procesos de cacería de amenazas. • Solicitar apoyo en la creación y diseño de flujos de automatización (*playbooks*). Esta funcionalidad deberá estar disponible como apoyo para analistas de SOC, CSIRT y demás personal encargado del análisis e investigación de incidentes de seguridad, con un esquema de uso medido mensualmente durante la vigencia del contrato.		
2.43	La solución SIEM-SOAR deberá permitir la activación de los productos adquiridos de manera escalonada, de forma que no se afecte la continuidad operativa durante el proceso de implementación, hasta el inicio de los veinticuatro (24) meses de funcionamiento requeridos, incluso ante eventuales contratiempos que puedan presentarse durante el despliegue de la solución.		
2.44	La solución SIEM-SOAR deberá contar con capacidades de detección, investigación y respuesta ante amenazas (TDIR), integrando las funcionalidades requeridas en el presente proceso, con el fin de gestionar de forma centralizada las operaciones de seguridad.		
2.45	La solución deberá contar con capacidad de escalabilidad, de manera que permita a la institución fortalecer su postura de seguridad o incorporar nuevas herramientas tecnológicas en el futuro.		
2.46	Todo el licenciamiento requerido para el funcionamiento de la solución ofertada deberá ser suministrado por el contratista.		
3	**SOPORTE**		
3.1	Mínimo dos (2) años en sitio o virtual (Cra 59 No. 26 -21 Oficina de Tecnologías de la Información) según el requerimiento del supervisor, para verificación del estado de la solución SIEM-SOAR y su infraestructura, actualizaciones, onboarding,		

Lote 4 SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	aplicación de mejores prácticas, optimización de red, y demás requerimientos relacionados con la solución a partir del 24/12/26. El soporte deberá ser 5x8, 5 días de la semana y 8 horas diarias y deberá anexar junto con la propuesta los números de contacto para las solicitudes de soporte, con escalamiento a fabrica cuando se amerite. El contratista deberá presentar, a solicitud del supervisor del contrato, un reporte detallado y actualizado del soporte brindado, en temas de configuraciones realizadas en atención a los requerimientos de soporte solicitados.		
3.2	En caso de que se haga uso de la infraestructura tecnológica existente, se deberá renovar el soporte por un periodo de dos (2) años, a partir del 24/12/2026, para los siguientes equipos, con las características que se indican a continuación: 1 Servidor HPE DL360 Gen11 8SFF CTO de serie 3M1D1V146H, procesador Intel® XEON® Silver 4514Y 2.00 GHz, 128 GB de RAM 3 TB de disco. 1 Servidor HPE StoreEasy 1670 MS WS IoT22 de serie 2M2D1W01DH, procesador Intel® Xeon® Bronze 3408U 1.80 GHz, 64 GB de RAM, 200 TB de disco Se podrán fortalecer las capacidades de los dispositivos mencionados, siempre que dicha ampliación esté contemplada dentro de la certificación de la arquitectura de la solución emitida por el fabricante, la cual deberá ser entregada por el oferente junto con la propuesta. En todo caso, el soporte deberá iniciar a partir del 24/12/2026. Es de resaltar que la infraestructura actual estará disponible a partir del 24/12/2026; en tal caso, el contratista deberá prever el uso de equipos temporales, independientemente de que la solución sea on-premise, cloud o híbrida.		
3.3	En caso de darse continuidad a la solución actual bajo la modalidad on-premise, se deberán considerar los requisitos para el fortalecimiento de las capacidades institucionales de SIEM-SOAR, para lo cual se deberá renovar el soporte, mantenimiento y actualizaciones de la licencia SIEM (FSMP000000018807), incluyendo el incremento a veinte mil (20.000) EPS y los demás requerimientos técnicos establecidos en el presente proceso, que garanticen el despliegue óptimo de la solución. De igual forma, se deberá renovar el soporte, mantenimiento y actualizaciones de la licencia del SOAR (FSOAR4715328538) conforme a los requerimientos solicitados.		
3.4	Si la solución es en modalidad cloud o hibrida de igual forma el periodo de soporte iniciará a partir del 24/12/2026.		
4	**GARANTÍA**		

Lote 4 SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
4.1	Mínimo dos (2) años de garantía en sitio, en la dirección Cra. 59 No. 26-21, Oficina de Tecnologías de la Información. En caso de falla de alguno de los equipos de la solución, deberá ser reemplazado e instalado en un plazo no mayor a veinte (20) días hábiles, durante el cual el contratista deberá ejecutar las acciones necesarias para evitar la indisponibilidad total del servicio. Lo anterior no generará costo adicional para la Policía Nacional de Colombia. La garantía debe iniciar a partir del 24/12/2026.		
4.2	En caso de que alguno de los equipos presente degradación en el desempeño o en la calidad del servicio, deberá ser reemplazado bajo garantía, sin costo adicional para la Policía Nacional de Colombia. Para tal efecto, se realizarán validaciones conjuntas entre el contratista y el fabricante, con el fin de determinar si la afectación obedece a limitaciones de desempeño del equipo frente a los requerimientos de la solución ofertada, procediendo, en caso afirmativo, con el respectivo cambio en garantía.		
4.2	El proponente deberá acreditar que es partners vigente del fabricante de la solución ofertada para el año de la presente contratación. Para ello, deberá anexar una carta o certificación oficial emitida por el fabricante, en la cual se indique expresamente que el proponente cuenta con la calidad de partners autorizado y vigente para la comercialización, implementación y/o soporte de la solución ofrecida. Esta certificación deberá contar con datos de contacto de Colombia para verificación.		
4.3	El oferente deberá garantizar que la solución ofertada cuenta con soporte técnico oficial del fabricante y acceso a actualizaciones de software y firmware si es el caso, durante el período mínimo de garantía.		
4.4	Los componentes ofertados, independientemente del modelo de la solución (on-premise, cloud o hibrido) no deberán estar próximos a su fin de ciclo de vida (End of Life - EOL) ni a su fin de soporte (End of Support - EOS) según la política del fabricante. El contratista deberá garantizar que los productos cuentan con soporte oficial durante la vigencia del presente contrato.		
4.5	Si la solución es en modalidad cloud o hibrida de igual forma el periodo de garantía iniciará a partir del 24/12/2026.		
5	**ESPECIFICACIONES TÉCNICAS PARA LA INSTALACIÓN DE EQUIPOS EN EL CENTRO DE DATOS DE LA POLICÍA NACIONAL.**		
5.1	Los siguientes requerimientos técnicos deberán ser tenidos en cuenta para la instalación de servidores en el Centro de Procesamiento de Datos de la Policía Nacional ubicado en la Carrera 59 No. 26-21 CAN – Bogotá D.C., estos requerimientos podrán ser verificados en la visita técnica voluntaria establecida en el pliego de condiciones. El contratista deberá conocer la topología de conexión y la disponibilidad en infraestructura		

Lote 4 SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	suficiente para conectar los equipos, para lo cual esta será verificada mediante la visita técnica establecida en el pliego.		
5.2	La infraestructura tecnológica a instalar en el centro de datos de la Policía Nacional debe ser tipo RACK en formato de 19" (*el estándar de 19" se refiere a la distancia de ancho que hay entre los perfiles interiores del armario)*		
5.3	La infraestructura tecnológica a instalar en el centro de datos de la Policía Nacional deberá contar con doble fuente de alimentación. A su vez debe contar con la conexión de acceso no presencial en el centro de datos (Utilidad de gestión y/o administración remota)		
5.4	La infraestructura tecnológica a instalar en el centro de datos de la Policía Nacional deberá tener contrato de garantía y/o soporte vigente durante el tiempo de permanecía en el centro de datos.		
5.5	El contratista certificará los enlaces de la Fibra Óptica y cableado estructurado en cobre que sean instalados en el centro de cómputo de la Policía Nacional, como complementos necesarios para el correcto funcionamiento y conectividad de la solución tecnológica.		
5.6	Si la solución supera los requerimientos técnicos presentes en el Centro de Datos de la Policía Nacional (disponibilidad de enlaces de cobre y/o fibra óptica al igual que potencia eléctrica, para la instalación de nuevos equipos). El contratista deberá proveer además de los equipos a instalar, la infraestructura física necesaria para toda la interconexión de la solución.		
5.7	La solución de infraestructura física de cableado a instalar deberá hacerse con productos de cobre y fibra del mismo fabricante Instalado en el Centro de Datos de la Policía Nacional, para efectos de mantener la homogeneidad y compatibilidad de la solución instalada y así poder tramitar para estos nuevos enlaces la garantía dada por el fabricante que es de 25 años. Es importante también indicar que el proveedor que instale la infraestructura física de cableado en cobre y/o fibra óptica requerida sea un integrador avalado y certificado por el fabricante SIEMONS para desarrollar diseño e instalación de sus productos.		
5.8	La solución de cobre y/o fibra óptica a instalar debe ser administrable y monitoreada (solución Inteligente), por tal razón todos los elementos a instalar deben cumplir con las especificaciones técnicas.		
5.9	PDU DE RACK O GABINETE		
5.10	Los equipos suministrados no deberán superar la carga máxima eléctrica distribuida en cada PDU de rack o gabinete, el contratista deberá realizar las conexiones al componente eléctrico para garantizar el adecuado funcionamiento de los equipos.		
5.11	PDU Gabinetes 30Amp de mínimo 30-(C13) 6-(C19) NEMA L6-30P - Rango de temperatura de operación normal a plena carga deberá ser de mínimo 45° hasta 60° Centígrados, monitoreable de fábrica (controlador de PDU Ethernet de mínimo 10/100/1000 o 10/100 base T con IPv4 o IPv6 verticales con una capacidad		

Lote 4 SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	mínima de carga de 4.5Kw o superior. Estas deberán ser de la misma marca y modelo de las que se encuentran instaladas actualmente en el Centro de Datos de la Policía Nacional.		
5.12	Voltaje de entrada aceptable: 200-240 VAC, Voltaje de salida: 200/240 VAC.		
5.13	Las salidas o receptáculos deben estar codificados por color, de acuerdo al grupo de receptáculos y disyuntor.		
5.14	Longitud del cable de entrada: Mínimo 3 Metros.		
5.15	Corriente máxima por salida: (C13) 10A, (C19) 16A por cada receptáculo.		
5.16	Cantidad de interruptores automáticos internos: 2		
5.17	Tipo de disyuntor: 1 o 2 polos hidráulico-magnético		
5.18	Norma UL y/o CE (certificado europeo) y/o CSA y/o EMC, Medioambiental ROHS.		
5.19	Las Pdu de Rack deben tener una capacidad de distribución de poder bifásica y deberán ser energizadas por el contratista en su totalidad hacia los tableros de distribución. Las PDU deberán poderse comunicar a través de los protocolos SNMP y proveer los archivos de los MIB'S que permitan la lectura de los diferentes parámetros de monitoreo de cada una de las PDU para integrarse con las herramientas de monitoreo de la Policía Nacional.		
5.20	La PDU monitoreables deberán ser configuradas para el monitoreo de las siguientes variables de consumo: • Potencia • Voltaje • Corriente • Kilovatios por hora • Factor de Potencia • Frecuencia • KVA		
5.21	SOLUCIÓN DE COBRE CABLE UTP EN CATEGORIA 6A		
5.22	Debe cumplir o superar las especificaciones de la norma ANSI/TIA-568-2-D, el estándar IEEE 802.3an-2006 de requerimientos de canal para soportar 10GBASE-T.		
5.23	Deberá soportar por lo menos las siguientes aplicaciones: 100 Mb/s Ethernet 10GBase-T, 100Base-TX (Fast Ethernet), 1000base-T (Gigabit Ethernet); IEEE 802.3, ANSI X3.263; 1.2Gb/s ATM; Token Ring 4/16 para Voz y Datos.		
5.24	Deberá existir compatibilidad mecánica y eléctrica de los productos y cables de la Categoría 6A, con las categorías anteriores.		
5.25	El forro debe ser continuo, sin porosidades u otras imperfecciones, con especificación de su cubierta o chaqueta type LSZH (UL o ETL) de acuerdo a la norma IEC 60332-3. Retardante de llama, no generar gas toxico y libre de halógenos (LSZH).		
5.26	El cable deberá ser de construcción tubular en su apariencia externa (redondo). Dentro del cable, los conductores de cobre deben estar trenzados en pares firmemente y estos deben tener		

Lote 4 SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	separación individual para mejorar su desempeño. El cable deberá ser calibre No. 23 AWG, debe ser elaborado por el mismo fabricante de la conectividad y estar probados por laboratorio ETL para Categoría 6A respectivamente.		
5.27	Los enlaces con cables de cobre deberán ser de 4 pares trenzados sólidos, del tipo F/UTP (blindado). La conexión final a los patch panels correspondientes se deberá hacer con el método de conexión T568B.		
5.28	No se aceptarán cables con conductores pegados u otros métodos de ensamblaje que requieran herramientas especiales para su terminación.		
5.29	Deberá poseer un elemento que ayude a reducir los efectos de alíen Cross Talk		
5.30	El forro del cable debe ser color azul y tener impresa, como mínimo, la siguiente información: nombre del fabricante, número de parte, tipo de cable, número de pares, tipo de listado (LSZH), y las marcas de mediciones secuenciales para verificación visual de longitudes.		
5.31	El cable deberá permitir en su instalación al menos un radio mínimo de curvatura de 4 veces su diámetro externo a una temperatura de 0ºC sin ocasionar deterioro en forro o aislantes.		
5.32	Velocidad de propagación >69% de 10 a 500 Mhz, Debe poseer una impedancia característica de 100Ω, +/- 15% hasta 100Mhz, +/- 22% entre 100 – 350Mhz y +/- 32% entre 350 – 500Mhz de respuesta para ancho de banda de acuerdo con el ANSI/TIA 568-2-D para categoría 6 A.		
5.33	Debe cumplir con IEEE 802.3af, IEEE 802.3at y los requerimientos de 802.3bt		
5.34	La clasificación de flamabilidad de la chaqueta debe cumplir con IEC 60332-3, 60754-2, 61034-2		
5.35	Para la instalación de los enlaces de cobre en los EDA´s (Patch panels modulares angulados) se deberán utilizar herrajes de patch panels ZMAX, Empty, Shielded, 48 Openings, Angled, 1U, Black, Fixed Wire Manager, de la misma marca del fabricante instalado en el centro de datos de la Policía Nacional		
5.36	Para la instalación de los enlaces de cobre en los HDA´s (Patch panels modulares angulados) se deberán utilizar herrajes de patch panels inteligentes del tipo MapIT, Empty, Shielded, 24 Openings, Angle, 1U, Black, Fixed Wire Manager, Keystone, Referencia Siemon: M-SPPA-K24ENS, los cuales deberán estar conectados a un panel de control maestro MapIT, 24 Port, 1U, Black, de la misma marca del fabricante instalado en el centro de datos de la Policía Nacional. Es importante que el proveedor verifique si existe disponibilidad de puertos de conexión en el panel de control maestro, en caso de que no haya disponibilidad será necesario instalar un panel de control maestro adicional.		

Lote 4 SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
5.37	Para los herrajes de patch panel del sistema inteligente ubicados en los HDA´s los cables de cobre deberán ser instalados en tomas o jacks RJ-45 ZMAX, Shielded, Category 6A, RJ45, Keystone, Black, Tool-Less, T568A/B, de la misma marca del fabricante instalado en el centro de datos de la Policía Nacional.		
5.38	Para los herrajes de patch panel ubicados en los EDA´s los cables de cobre deberán ser terminados en tomas o jacks RJ-45 ZMAX, Shielded, Category 6A, RJ45, Panel Mount, Tool-Less, T568A/B, de la misma marca del fabricante instalado en el centro de datos de la Policía Nacional.		
5.39	Para la habilitación de los servicios en los EDA´s será necesario utilizar patch cords RJ45 a RJ45, Category 6A, S/FTP, T568A/B, Stranded, CM/LSOH-1, White Cable, Clear Boot, 7 Feet, Bulk Pack. Para la habilitación de los servicios en los HDA´s será necesario utilizar patch cords del sistema inteligente MapIT, RJ45 a RJ45, Category 6A, U/FTP, T568A/B, Stranded, LSOH-1, Blue Cable, Blue Boot, 2 Meters, de la misma marca del fabricante instalado en el centro de datos de la Policía Nacional.		
5.40	Todos los componentes de cobre (cables y conectividad) que se instalen nuevos deberán ser debidamente identificados y marquillados cumpliendo las normas ANSI/TIA-606-C, y deberán ser probados con un equipo de certificación avalado por el fabricante del cableado de cobre, y este a su vez deberá contar con certificado de calibración vigente expedido por el fabricante del equipo, las pruebas se deberán hacerse para enlace permanente y cumpliendo con los límites de medición de la ISO 11801.		
5.41	Para la conexión de COBRE ADMINISTRACION se requiere que el contratista instale: Copper, Patch Cord, RJ45, RJ45, Category 6A, S/FTP, T568A/B, Stranded, CM/LSOH-1, White Cable, Clear Boot, 7 Feet, Bulk Pack,3 Meter, No. parte ZM6A-S07-06B 19SIZM6AS0706B , Marca Siemon. Que sean necesarios para la conexión total de los puertos del equipamiento tecnológico.		
5.42	SOLUCIÓN DE FIBRA OPTICA		
5.43	Los enlaces con cables de fibra óptica pre-conectorizados deberán ser MTP/MTP de 12 hilos, del tipo multimodo OM4, y velocidades de hasta 10 Gbseg hasta 550 metros sobre enlaces dúplex (2 hilos) o velocidades de hasta 40 Gbseg sobre 4 enlaces dúplex (8 hilos).		
5.44	Estos cables de fibra deben ser Plug & Play, Trunk, 12 Strand, RazorCore, XGLO, Multimode, Female MTP Base 12 Solution, Female MTP Base 12 Solution, Polarity C, OM4, 50/125, Aqua, LSOH-3C, Pulling Eye, XX Meter, de la misma marca del fabricante instalado en el centro de datos de la Policía Nacional donde XX corresponde a la distancia en metros.		
5.45	Para la conexión de los enlaces de fibra óptica en los HDA´s 3 (Bandeja de alta densidad) se deberán utilizar bandejas de fibra óptica u ODF´s del tipo LightStack, Rack Mount, 1U, Sliding		

Lote 4 SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	Access, 12 Openings, Black, de la misma marca del fabricante instalado en el centro de datos de la Policía Nacional.		
5.46	Para la conexión de los enlaces de fibra óptica en los EDA´s (Bandeja de conexión) se deberán utilizar bandejas de fibra óptica u ODF´s del tipo inteligente MapIT, G2 Smart, Enclosure, 1U, Multimode, 48 Fiber, Aqua, LC, MTP, OM4, Black, de la misma marca del fabricante instalado en el centro de datos de la Policía Nacional.		
5.47	Como el sistema de fibra óptica es inteligente y está característica se realiza en los gabinetes EDA's bajo una topología de cross conexión se deben utilizar también bandejas u ODF´s (Bandeja de Cross conexión) de fibra óptica del tipo inteligente MapIT, G2 Smart, Enclosure, 1U, Multimode, 48 Fiber, Aqua, LC a LC, OM4, Black, de la misma marca del fabricante instalado en el centro de datos de la Policía Nacional.		
5.48	Para la adecuada conexión de los cables de fibra óptica MTP/MTP a las bandejas de fibra óptica u ODF´s (Cassettes pre conectorizados) es requerido que estos cables sean conectados a cassettes pre conectorizados del tipo MTP a 6 LC dúplex, OM4, multimodo, de la misma marca del fabricante instalado en el centro de datos de la Policía Nacional.		
5.49	Para la conexión de equipos en los EDA´s y HDA´s se deberán utilizar patch cords entre las bandejas inteligentes de cross conexión de los EDA´s a los puertos de los equipos y las bandejas de alta densidad a los puertos de los switches de fibra en los HDA´s, estos patch cords deberán ser dúplex, XGLO, Multimode, LC BladePatch a LC BladePatch, RFP, OM4, 50/125, Aqua, LSOH-3C, 2 Meter, de la misma marca del fabricante instalado en el centro de datos de la Policía Nacional.		
5.50	Adicionalmente, como la topología de conexión en los EDA´s es de cross conexión y el sistema es inteligente, es requerido utilizar patch cords dúplex del tipo inteligentes entre la bandeja que recibe los cables troncales de fibra MTP/MTP en cassettes pre conectorizados y la bandeja de cross conexión que habilita los servicios de los equipos, estos patch cords deben ser del tipo MapIT, Duplex, XGLO, Multimode, LC a LC, OM4, 50/125, Aqua, OFNR, 1 Meter, de la misma marca del fabricante instalado en el centro de datos de la Policía Nacional.		
5.51	En caso de instalar enlaces nuevos de fibra óptica el contratista deberá verificar si hay disponibilidad de espacio en las bandejas de alta densidad de los HDA´s, en las bandejas inteligentes de los EDA´s, y en las bandejas inteligentes de cross conexión de los EDA´s, en caso de no tener disponibilidad deberán instalar bandejas nuevas con las especificaciones técnicas anteriormente descritas.		
5.52	Todos los componentes de fibra óptica (cables y conectividad) que se instalen nuevos deberán ser debidamente identificados y marquillados cumpliendo las normas ANSI/TIA-606-C, y deberán ser probados con un equipo de certificación avalado por el		

Lote 4 SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	fabricante del cableado de cobre, y este a su vez deberá contar con certificado de calibración vigente expedido por el fabricante del equipo, las pruebas deberán hacerse para enlace permanente y cumpliendo con los límites de medición de la ISO 11801.		
5.53	Para la conexión de FIBRA SAN, se requiere que el contratista instale: Fiber, Jumper, Duplex, XGLO, Multimode, LC BladePatch, LC BladePatch, RFP, OM4, 50/125, Erika Violet, LSOH-3C, 3 Meter. No. Parte FBP-LCLC5V-02EH o 19SIFBPLCLC5V02EH, Marca Siemon. Que sean necesarios para la conexión total de los puertos del equipamiento tecnológico.		
5.54	Para la conexión de FIBRA LAN, se requiere que el contratista instale: Fiber, Jumper, Duplex, XGLO, Multimode, LC BladePatch, LC BladePatch, RFP, OM4, 50/125, Aqua, LSOH-3C, 3 Meter. No. parte FBP-LCLC5V-02AH 19SIFBPLCLC5V02AH. Marca Siemon. Que sean necesarios para la conexión total de los puertos del equipamiento tecnológico.		
6	**TRANSFERENCIA DE CONOCIMIENTO**		
6.1	Se deberá brindar transferencia de conocimiento certificada por el contratista con acompañamiento del fabricante, para diez (10) funcionarios previa coordinación con el supervisor, en los siguientes roles: administración, manejo y análisis de la información entregada por la herramienta. Esta capacitación deberá tener una intensidad horaria mínima de veinticuatro (24) horas hábiles. Se deberá brindar acceso a recursos de capacitación en línea sin límite por parte del fabricante, para los funcionarios de la entidad durante la vigencia del contrato.		
7	**DERECHOS DE AUTOR**		
7.1	En atención al numeral 15 del capítulo IX “Parámetros y recomendaciones adicionales que orientan el cumplimiento del régimen jurídico del derecho de autor y los derechos conexos de la Circular conjunta No. 004 del 24/04/2006 de la Procuraduría General de la Nación y la Unidad Administrativa Especial Dirección Nacional de Derechos de Autor, el proponente deberá presentar con la oferta una certificación de distribuidor autorizado o certificado de autenticidad y certificado de registro de soporte lógico – software, expedido por la Dirección Nacional de derechos de autor.		
7.2	El contratista deberá entregar un certificado de Fabricante donde se evidencie la autenticidad del software contratado con vigencia máxima de 30 días y relacionándose al proceso en mención.		
8	**COMPONENTE AMBIENTAL**		
8.1	El oferente deberá presentar el certificado de consulta del Registro Único de Infractores Ambientales (RUIA), expedido a través del enlace oficial del Ministerio de Ambiente: https://vital.minambiente.gov.co/SILPA_UT_PRE/RUIA/Consultar		

Lote 4 SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	Sancion.aspx?Ubic=ext.,; En caso de presentarse como unión temporal o consorcio, deberá aportarse el certificado RUIA de cada uno de sus integrantes. Así mismo, este certificado deberá ser presentado durante la ejecución del contrato cuando el supervisor lo requiera, con el fin de verificar la existencia o no de sanciones ambientales vigentes.		
8.2	El oferente deberá verificar la necesidad de permisos, licencias, concesiones o autorizaciones ambientales de acuerdo a su actividad comercial y, de ser legalmente exigibles, obtenerlos y presentar el documento emitido por la autoridad ambiental competente. En caso de que no aplique deberá declararlo el representante legal bajo la gravedad de juramento, asumiendo plenamente las consecuencias legales, ambientales y contractuales que se deriven del incumplimiento. Se deberán mantener vigentes durante toda la ejecución del contrato.		
10	**ACUERDO DE CONFIDENCIALIDAD**		
10.1	Si la Policía Nacional considera pertinente someter a estudio de seguridad al contratista, éste permitirá y facilitará todos los medios que la Entidad le solicite para este fin. El Contratista se obliga a no suministrar información que obtenga o conozca con ocasión de la ejecución del contrato y que se encuentra marcada como confidencial; así como sobre los lugares a los cuales tenga acceso con ocasión de su servicio y sea revelada información marcada como confidencial. El contratista deberá firmar un acuerdo de confidencialidad y no revelación de la información, para lo cual deberá diligenciar el formulario “ACUERDO DE CONFIDENCIALIDAD”.		
11	**COMPROMISO ANTICORRUPCIÓN**		
11.1	Cumplir con el compromiso de anticorrupción durante la ejecución del contrato manifestando que se encuentra dispuesto a suministrar la información propia que resulte necesaria para aportar transparencia al mismo y si se comprueba el incumplimiento del contratista, sus empleados, representantes, asesores o de cualquier otra persona que actúe en su nombre, es causal suficiente para la terminación anticipada del contrato, para lo cual deberá diligenciar el formulario “COMPROMISO ANTICORRUPCIÓN”.		
12	**SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO.**		
12.1	El contratista deberá cumplir con la implementación del sistema de Gestión de Seguridad y Salud en el Trabajo, para lo cual deberá diligenciar el formulario “SISTEMA DE GESTIÓN DE LA SEGURIDAD Y SALUD EN EL TRABAJO”.		
12.2	El oferente deberá acreditar el cumplimiento de los Estándares Mínimos del Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST), en los términos establecidos por el Decreto 1072 de 2015 y por la Resolución 0312 de 2019 del Ministerio del Trabajo, mediante la presentación de la calificación oficial		

Lote 4 SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	radicada ante la Administradora de Riesgos Laborales ARL y/o ante el Ministerio del Trabajo de conformidad con la circular 027 de 2026, correspondiente al año inmediatamente anterior a la fecha de cierre del presente proceso de selección.		
12.3	El contratista debe acreditar, mediante los soportes documentales pertinentes, el cumplimiento de las obligaciones legales relacionadas con el pago de los aportes al Sistema de Seguridad Social Integral, prestaciones sociales y afiliación y pago a la Administradora de Riesgos Laborales ARL de sus trabajadores en misión al objeto contractual.		
12.4	**EXPERIENCIA DEL PERSONAL** Se requiere mínimo de una (01) persona quien debe acreditar estudios en ingeniería de sistemas o electrónica, experiencia mínima de cinco (5) años en instalación y puesta en funcionamiento de la solución ofertada objeto del presente proceso. Deberá contar con mínimo tres (03) de las siguientes certificaciones vigentes, así: • CEH version 13 AI (EC-Council Certified Ethical Hacker) • ECIH (EC-Council Certified Incident Handler) • FCSS equivalente al NSE7 • CISPP (Certified Information Systems Security Professional) de ISC2 • CDPSE (Certified Data Privacy Solutions Engineer) de ISACA Para lo cual, el oferente deberá presentar con la propuesta, la siguiente documentación: - Hoja de vida - Diploma - Tarjeta profesional vigente de alguna de las ingenierías solicitadas (mínimo 2 años de experiencia a partir de la expedición de la tarjeta profesional) - Una (01) certificación que evidencie el manejo e implementación de la herramienta por parte del fabricante. - Una (01) certificación en el manejo e implementación de la solución ofertada de SIEM-SOAR, donde se evidencie experiencia mínima de dos (2) años en instalación y puesta en funcionamiento de la misma. - Tres (03) certificaciones que evidencie el manejo e implementación de la herramienta por parte del fabricante.		

<table>
<tr><th colspan="4">Lote 4 SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM</th></tr>
<tr><th>ÍTEM</th><th>DESCRIPCIÓN</th><th>CUMPLE</th><th>NO CUMPLE</th></tr>
<tr><td>13</td><td colspan="3">EXPERIENCIA DEL PROPONENTE</td></tr>
<tr><td></td><td>EXPERIENCIA GENERAL PROPONENTE NACIONAL O EXTRANJERO CON SUCURSAL O REPRESENTACIÓN EN COLOMBIA -RUP

El Registro Único de Proponentes es el instrumento a través del cual se verificará el requisito de experiencia del proponente, para tal efecto las personas naturales, las personas jurídicas, las uniones temporales, los consorcios u otra forma de asociación que participen en este proceso, deberán acreditar la experiencia con mínimo uno (01) máximo tres (03) contratos celebrados y ejecutados con entidades públicas y/o privadas, identificados con alguno de los siguientes códigos UNSPSC y que su valor sumado sea igual o superior a 571.13 SMMLV, equivalente al 50% del presupuesto oficial, así:

<table>
<tr><th>CLASIFICACIÓN UNSPSC</th><th>SEGMENTO</th><th>FAMILIA</th><th>CLASE</th><th>VALOR EXPRESADO EN SMMLV</th></tr>
<tr><td>43233200</td><td>Difusión de Tecnologías de información y telecomunicaciones</td><td>Software</td><td>Software de seguridad y protección</td><td>571.13</td></tr>
</table>
</td><td></td><td></td></tr>
<tr><td>13.1</td><td>NOTA 1: si los contratos acreditados fueron realizados bajo la modalidad de Consorcio, de Unión Temporal u otras formas de asociación, se tomará para la verificación, el porcentaje (%) de participación en la ejecución del contrato del oferente que haga parte del Consorcio, de la Unión Temporal u otras formas de asociación, y luego sumará el valor obtenido para así establecer el total acreditado. Para lo anterior, deberá presentar el documento que acreditó la conformación del Consorcio, la Unión Temporal u otras formas de asociación, donde deberá constar el porcentaje de participación de cada uno de los integrantes para la ejecución del contrato.

NOTA 2: en el caso de proponentes plurales, todos sus integrantes deben registrar experiencia en el RUP con alguno de los códigos UNSPSC antes señalados.

NOTA 3: en la presentación de la oferta, el oferente deberá diligenciar y entregar el formulario “EXPERIENCIA GENERAL DEL PROPONENTE”, donde relacionará los contratos para la evaluación.

EXPERIENCIA ESPECÍFICA PROPONENTE NACIONAL O EXTRANJERO CON SUCURSAL EN COLOMBIA</td><td></td><td></td></tr>
</table>

Lote 4 SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	El proponente que vaya a proveer los bienes o servicios objeto del presente proceso de contratación, trátese de personal natural o jurídica, deberá anexar mínimo una (01) máximo tres (03) constancias (certificaciones o actas de liquidación) de contratos celebrados y ejecutados con entidades públicas y/o privadas, cuyo objeto sea igual o similar al objeto de la presente contratación “HERRAMIENTA DE DETECCIÓN Y PREVENCIÓN DE AMENAZAS EN LA RED” o relacionados con seguridad de APIS, documentos que como mínimo deberán tener la siguiente información: 1. Nombre del contratista 2. Nombre del contratante 3. Objeto del contrato 4. Valor del contrato 5. Fecha de suscripción y fecha de inicio del contrato 6. Fecha de terminación del contrato 7. Personal de contacto para verificar la información: teléfono fijo o celular, correo electrónico institucional, logo (en caso de certificación). 8. Estado del contrato: ejecutado o liquidado. 9. Si es certificación, deberá estar suscrita por el funcionario competente para tal fin. 10. Manifestación clara y explícita donde se evidencie que el contratista cumplió a cabalidad con el objeto del contrato. 11. Porcentaje del valor del contrato que ejecutó como miembro de un consorcio, unión temporal u otra forma de asociación. **NOTA 1:** en cumplimiento del artículo 2.2.1.2.4.2.18 del Decreto 1082 de 2015, el Decreto 1860 de 2021 el cual reglamentó parcialmente la Ley 2069 de 2020 "Por medio de la cual se impulsa el emprendimiento en Colombia” y el artículo 1º del Decreto 0287 de 2026 “Por el cual se modifican los artículos 2.2.1.2.4.2.6., 2.2.1.2.4.2.7. y 2.2.1.2.4.2.8. del Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación”, se toma como criterio diferencial para las MiPymes y los emprendimientos y empresas de personas con discapacidad, el número de contratos para la acreditación de la experiencia. Por tanto, deberán anexar mínimo una (01) máximo cuatro (04) constancias (certificaciones o actas de liquidación) que cumplan con lo antes relacionado. **NOTA 2:** la experiencia específica presentada deberá estar registrada en el Registro Único de Proponentes, no serán tenidas en cuenta aquellas constancias de contratos que no se encuentren registrados.		

Lote 4 SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	NOTA 3: si la información relacionada en el (RUP) para acreditar la experiencia no se puede verificar**,** la entidad se reserva la facultad de solicitar información adicional. **NOTA 4**: no se aceptarán auto certificaciones. **NOTA 5**: no se tendrán en cuenta las certificaciones de contratos en ejecución. **NOTA 6:** no se aceptan certificaciones con enmendaduras o que presenten inconsistencias no subsanadas. **NOTA 7:** cuando los documentos no indiquen su valor en SMMLV o si estos son de años anteriores a 2026, se hará la respectiva conversión de acuerdo al año en que terminó el contrato. La verificación será realizada por el comité evaluador técnico. **NOTA 8:** si los contratos acreditados fueron realizados bajo la modalidad de consorcio, unión temporal u otras formas de asociación, se tomará para la verificación, el porcentaje (%) de participación en la ejecución del contrato del oferente que haga parte del consorcio, unión temporal u otras formas de asociación, y luego sumará el valor obtenido para así establecer el total acreditado. Para lo anterior, deberá presentar el documento que acreditó la conformación del consorcio, unión temporal u otra forma de asociación, donde deberá constar el porcentaje de participación de cada uno de los integrantes en la ejecución del contrato. **NOTA 9:** en el caso de proponentes plurales, todos sus integrantes deben registrar experiencia en el RUP según el código UNSPSC requerido en el presente proceso de selección. **NOTA 10**: en el caso que el proponente haya participado en procesos de fusión o escisión empresarial, debe tomar para estos efectos, exclusivamente los contratos que le hayan asignado en el respectivo proceso de fusión o escisión, para ello debe aportar el certificado del contador público o del revisor fiscal (si la persona jurídica tiene revisor fiscal) que así lo acredite. La Policía Nacional se reserva el derecho de hacer las verificaciones que considere necesarias en la documentación presentada, con el fin constatar el contenido de la misma. **NOTA 11:** en la presentación de la oferta, el oferente deberá diligenciar y entregar el formulario “EXPERIENCIA DEL PROPONENTE”, donde relacionará los contratos para la evaluación.		

Lote 4 SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	La Policía Nacional se reserva el derecho de hacer las verificaciones que considere necesarias en la documentación presentada, con el fin constatar el contenido de la misma.		