



UNIDAD ADMINISTRATIVA ESPECIAL DE LA
JUSTICIA PENAL MILITAR Y POLICIAL

ANEXO TECNICO N° 3.

**SERVICIOS DE GESTIÓN INTEGRAL DE LA RED Y LOS SERVICIOS DE
CONECTIVIDAD**

REQUERIMIENTOS MINIMOS

Nombre Comercial del Bien o Servicio

SERVICIO DE CONECTIVIDAD WAN-LAN-SEGURIDAD

Generalidades

El servicio debe cumplir con todos los requisitos MINIMOS establecidos en la presente ANEXO TÉCNICO.

Requisitos generales

Prestación de servicio de red corporativa WAN-LAN de telecomunicaciones y ciberseguridad para la Unidad Administrativa Especial de la Justicia Penal Militar y Policial de la Justicia Penal Militar y Policial a Nivel Nacional.

Calidad

El servicio debe cumplir con todos los requisitos establecidos en la presente ANEXO TÉCNICO.

ÍTEM	TABLA DE CONTENIDO
1.	REQUERIMIENTOS GENERALES DE LAS SOLUCIONES
2.	REQUERIMIENTOS DE PERSONAL DE GESTION 2.1. Un (1) Gerente de proyecto. 2.2. Dos (2) ingenieros residentes /Administrador de Redes. 2.3. Dos (2) ingenieros de Seguridad Perimetral. 2.4. Un (1) Analista SOC
1. REQUERIMIENTOS GENERALES DE LAS SOLUCIONES	
Para atender los requerimientos de soporte y mantenimiento de la solución, el CONTRATISTA deberá cumplir con las siguientes condiciones:	
1.1. Disponer del personal requerido para la gestión de los servicios ofrecidos, ubicado en la ciudad de Bogotá, en la sede Palacio, de acuerdo con lo que disponga la UAEJPMP.	
1.2. Registrar, en la herramienta de gestión del servicio, todos los requerimientos e incidentes de nivel II reportados por la mesa de servicio de la Entidad.	





UNIDAD ADMINISTRATIVA ESPECIAL DE LA
JUSTICIA PENAL MILITAR Y POLICIAL

- 1.3.** La UAEJPMP asignará al grupo de gestión ubicado en la sede Palacio las extensiones telefónicas de la PBX corporativa, destinadas a la comunicación con las dependencias internas de la UAEJPMP en Bogotá y en otras ciudades.
- 1.4.** Disponer, como mínimo, de una herramienta estándar de gestión de incidentes, que permita la administración de tiquetes, escalamiento, generación de estadísticas y el registro en bitácora de las soluciones implementadas.
- 1.5.** Contar con el personal mínimo exigido, de conformidad con los requisitos establecidos en el presente proceso para la gestión de los servicios de nivel II y nivel III. El CONTRATISTA podrá adicionar personal, sin costo alguno para la UAEJPMP, de acuerdo con el tamaño de la red y el volumen de tiquetes generados.
- 1.6.** Proveer los medios de comunicación móvil que garanticen la conectividad de voz y datos entre los agentes que prestarán el servicio (relacionados en el Anexo Técnico No. 3) durante la ejecución del contrato.
- 1.7.** En caso de que la atención de un incidente requiera soporte técnico en sitio en cualquier sede de la UAEJPMP a nivel nacional, y conforme a los Acuerdos de Niveles de Servicio (Anexo Técnico No. 5), el CONTRATISTA deberá proveer los técnicos necesarios sin costo adicional para la UAEJPMP.
- 1.8.** Los tiquetes generados por la herramienta de soporte del grupo de gestión del CONTRATISTA, a partir de la fecha y hora de reporte del incidente, constituirán la base para el cálculo de los tiempos de disponibilidad e indisponibilidad, sin perjuicio de que la UAEJPMP valide dicha información con las herramientas de gestión implementadas en la solución.
- 1.9.** Todo el recurso humano que participe en el proyecto y tenga presencia laboral permanente en la UAEJPMP deberá acogerse a la reglamentación interna de la Entidad, incluyendo la realización de estudios de seguridad, la presentación de certificados de antecedentes judiciales y el diligenciamiento del formato de identificación y solicitud de acceso oficial, entre otros requisitos establecidos.
- 1.10.** La UAEJPMP únicamente suministrará el espacio físico, los perfiles de navegación y el antivirus institucional en caso de requerirse. El CONTRATISTA deberá proporcionar, sin costo adicional, todos los elementos necesarios para su operación, incluidos sillas, equipos de cómputo con doble pantalla, dispositivos telefónicos, pantallas de mínimo 23 pulgadas para monitoreo en tiempo real, impresoras, papelería y demás dotación requerida para su personal residente durante la ejecución del contrato. Estas necesidades deberán ser determinadas durante la visita técnica al sitio. En caso de que la Entidad disponga una nueva ubicación durante la ejecución del contrato, el traslado, la instalación y la dotación correspondiente serán asumidos por el CONTRATISTA, sin costo adicional.
- 1.11.** Dentro del mes siguiente a la firma del contrato, el CONTRATISTA deberá entregar a la supervisión del contrato las hojas de vida del personal asignado, junto con los soportes de formación académica, experiencia, certificaciones, vínculo laboral y demás documentos que acrediten el cumplimiento de los perfiles exigidos.





UNIDAD ADMINISTRATIVA ESPECIAL DE LA
JUSTICIA PENAL MILITAR Y POLICIAL

- 1.12.** Todo el personal del grupo de gestión deberá estar debidamente identificado con el carné de la empresa y portar uniforme institucional, que incluya como mínimo chaqueta y camisa formal con el logo de la empresa, durante la vigencia del contrato.
- 1.13.** Durante la ejecución del contrato, la supervisión podrá solicitar el cambio del personal asignado, previo informe del supervisor, cuando se presente alguna de las siguientes situaciones:
- a) Insuficiencia de conocimientos, habilidades o capacidades técnicas para la ejecución de los trabajos.
 - b) Actitudes que afecten el cumplimiento de las obligaciones contractuales.
 - c) Incumplimiento de las funciones asignadas.
- 1.14.** En caso de realizarse cambios de personal, el CONTRATISTA deberá informar a la supervisión con un mínimo de cinco (5) días calendario de antelación, presentar la hoja de vida del personal propuesto para validación por parte de la UAEJPMP y, una vez aprobada, disponer del personal en un plazo no mayor a diez (10) días hábiles.
- 1.15.** Durante el periodo de transición por cambio de personal, el CONTRATISTA deberá garantizar la continuidad en la prestación del servicio, previa aprobación de la supervisión.
- 1.16.** El personal que cubra reemplazos por vacaciones de ingenieros residentes, ingeniero de Seguridad Perimetral o analistas de SOC podrá ser contratado directamente por el proveedor o por una filial, siempre y cuando cumpla con los requisitos y funciones definidos para cada rol.
- 1.17.** El CONTRATISTA se compromete a asegurar la transferencia continua de conocimiento hacia el equipo operativo, cubriendo el uso, interpretación y operación de las tecnologías implementadas, así como los procesos específicos del servicio, garantizando la continuidad operativa y el adecuado entendimiento del entorno de la ENTIDAD.

2. REQUERIMIENTOS DE PERSONAL DE GESTION

El CONTRATISTA deberá asignar obligatoriamente al contrato, como mínimo, el siguiente recurso humano, con la disponibilidad requerida para atención en sitio y en la premisa del contratista, conforme a lo establecido en el presente documento.





UNIDAD ADMINISTRATIVA ESPECIAL DE LA
JUSTICIA PENAL MILITAR Y POLICIAL

2.1. Un (1) Gerente de proyecto.

Funciones	Requerimientos
El CONTRATISTA deberá garantizar la asignación de un (1) Gerente de Proyecto con una disponibilidad semanal mínima equivalente a ocho (8) horas durante toda la ejecución del contrato con un porcentaje de dedicación del 20 % mensual, destinada al seguimiento de actividades, revisión de avances, atención de novedades y coordinación con la supervisión de la UAEJPMP. - Coordinar y realizar el seguimiento permanente a las actividades ejecutadas por el CONTRATISTA, garantizando el adecuado desarrollo y cumplimiento de las obligaciones contractuales. - Asumir la responsabilidad sobre la gestión del recurso humano asignado al contrato, asegurando el cumplimiento de los objetivos, entregables y niveles de servicio definidos por la UAEJPMP. - Actuar como punto único de contacto ante la UAEJPMP para todos los asuntos relacionados con la ejecución del contrato y asistir a las reuniones de seguimiento, coordinación y control que sean convocadas por la supervisión. - Consolidar, elaborar y presentar a la supervisión los informes mensuales de gestión, operación del servicio y facturación, conforme a los lineamientos establecidos por la UAEJPMP.	- Con título Profesional y con experiencia mínima de tres (3) años en Gerencia de Proyectos Informáticos. - Certificación vigente de Project Managment Professional (PMP) o posgrado en la especialización en gerencia de proyectos o Gerencia de Proyectos de Tecnología de la Información (TI / IT Project Management) o Gerencia de Proyectos de Telecomunicaciones o Gerencia de Proyectos del Sector Público o Gobierno de TI o postgrados afines. - Deberá ser personal de planta del Contratista (presentar certificación laboral)





UNIDAD ADMINISTRATIVA ESPECIAL DE LA
JUSTICIA PENAL MILITAR Y POLICIAL

- Adoptar oportunamente las medidas preventivas, correctivas y de mejora necesarias frente a solicitudes, incidentes, problemas o riesgos que puedan afectar el cumplimiento de los objetivos contractuales.
- Ejecutar todas las actividades y funciones requeridas para el adecuado cumplimiento del objeto contractual y de las obligaciones derivadas del contrato.
- Servir como canal oficial de comunicación para la gestión de los aspectos administrativos, técnicos y operativos entre la UAEJPMP y el CONTRATISTA.
- Coordinar los aspectos técnicos, operativos y administrativos necesarios para el cumplimiento de las obligaciones contractuales, garantizando la correcta ejecución del proyecto.
- Revisar periódicamente con la UAEJPMP la ejecución del proyecto mediante reuniones de seguimiento, identificando y gestionando los planes de acción, mejora y mitigación necesarios para asegurar su adecuada implementación.
- Garantizar la oportunidad, calidad y efectividad en la atención y respuesta a los requerimientos formulados por la UAEJPMP.
- Identificar, evaluar, gestionar y monitorear los riesgos asociados a la prestación del servicio durante todas las etapas de ejecución del contrato.





UNIDAD ADMINISTRATIVA ESPECIAL DE LA
JUSTICIA PENAL MILITAR Y POLICIAL

- Mantener informada a la UAEJPMP sobre el avance, estado, hitos, riesgos y resultados del proyecto.
- Definir y acordar conjuntamente con la UAEJPMP los mecanismos de comunicación, reporte, seguimiento y escalamiento requeridos para la adecuada gestión del contrato.
- Velar por la confidencialidad, integridad y adecuado uso de la información a la que tenga acceso, en cumplimiento de las obligaciones contractuales y de las políticas de seguridad de la información aplicables.
- Cumplir y hacer cumplir las normas, estándares, lineamientos y buenas prácticas aplicables a la ejecución del contrato.
- Asistir a las reuniones, mesas de trabajo, comités de seguimiento y demás espacios de coordinación que se requieran durante la ejecución contractual o que sean convocados por la supervisión.
- Ejecutar las demás actividades que resulten necesarias para garantizar el adecuado cumplimiento del objeto contractual y de las obligaciones adquiridas por el CONTRATISTA.





**UNIDAD ADMINISTRATIVA ESPECIAL DE LA
JUSTICIA PENAL MILITAR Y POLICIAL**

- 2.2.** Dos (2) Ingenieros Residentes / Administradores de Redes: El CONTRATISTA deberá disponer en la ciudad de Bogotá de dos (2) ingenieros residentes para la prestación presencial del servicio. La cobertura operativa deberá garantizarse de lunes a viernes entre las 07:00 a. m. y las 06:00 p. m., Asimismo, los sábados el contratista deberá garantizar la disponibilidad de al menos un (1) ingeniero residente para la atención de incidentes, requerimientos y actividades operativas, asegurando la continuidad del servicio durante la jornada laboral comprendida entre las 08:00 a. m. y las 12:00 m. La prestación del servicio los días sábados podrá realizarse de manera remota o presencial, según lo acordado previamente con el supervisor del contrato.

Para tal efecto, el CONTRATISTA deberá establecer los turnos, horarios, relevos y demás esquemas de asignación de personal que resulten necesarios para garantizar la cobertura requerida, en estricto cumplimiento de la normativa laboral colombiana vigente, incluyendo lo dispuesto en la Ley 2101 de 2021 y las demás normas que la modifiquen, adicionen o sustituyan, sin que ello genere costos adicionales para la Entidad.

Funciones	Requerimientos
- El Ingeniero Residente / Administrador de Redes será responsable de la administración, operación, monitoreo y optimización de la infraestructura de red WAN y LAN de la UAEJPMP, así como del soporte técnico asociado a la solución de conectividad implementada, garantizando la continuidad, desempeño y seguridad de los servicios de red de la Entidad. - Administrar los servicios y servidores provistos como parte de la solución de conectividad instalada por el CONTRATISTA. - Administrar y operar los equipos de red LAN de la UAEJPMP, asegurando su correcto funcionamiento y disponibilidad. - Llevar y mantener actualizado el inventario de direccionamiento IP de la red corporativa WAN y la	- Con título de Ingeniería, con experiencia mínima de tres (3) años, en Administración de redes WAN o LAN en entornos corporativos. - Experiencia demostrable en la configuración y operación de switches, routers y dispositivos activos de red y gestión de direccionamiento IP, segmentación de red (VLAN). - Con postgrado en redes de datos o telecomunicaciones o Seguridad de Redes o Seguridad Informática o postgrados afines. - Deberán presentar las certificaciones emitidas por el fabricante en el manejo y administración de los equipos de





UNIDAD ADMINISTRATIVA ESPECIAL DE LA
JUSTICIA PENAL MILITAR Y POLICIAL

segmentación (VLAN) de la red LAN de cada una de las sedes, de acuerdo con los lineamientos y solicitudes de la UAEJPMP. - Realizar la configuración, administración y ajustes de la red WAN / SD-WAN/LAN de las sedes, conforme a los requerimientos definidos por la UAEJPMP. - Apoyar el monitoreo permanente de la red a través de la consola de administración centralizada SolarWinds o la herramienta de monitoreo definida por la Entidad. - Brindar apoyo en la gestión de requerimientos e incidentes relacionados con la red LAN activa de las sedes seccionales. - Ejecutar y administrar las copias de respaldo (backup) de las configuraciones y componentes de los equipos que hacen parte de la solución de red; cada vez que se realice un cambio. - Realizar el diagnóstico, análisis y solución de problemas de red, así como la generación, seguimiento y cierre de tickets, cuando se presenten incidentes en la infraestructura de la Entidad. - Elaborar y ejecutar el planeamiento de la capacidad de transmisión de la red corporativa, de acuerdo con el crecimiento y las necesidades operativas de la UAEJPMP. - Evaluar de manera periódica el rendimiento, comportamiento y eficiencia del tráfico de red, proponiendo acciones de mejora cuando sea requerido.	comunicaciones provistos en la solución, durante los primeros tres meses al inicio de la ejecución del contrato, los cuales deberán estar vigentes durante el periodo de ejecución del contrato. - Deberá ser personal de planta del Contratista. (presentar certificación laboral de la empresa) Conocimientos: - Gestión de Herramientas de monitoreo de red. - Operación, gestión y administración de redes LAN, WAN , SD-WAN - Administración de redes IPv4/IPv6 - Manejo de ofimática para mantener la documentación técnica y elaboración de informes de gestión.
--	---





**UNIDAD ADMINISTRATIVA ESPECIAL DE LA
JUSTICIA PENAL MILITAR Y POLICIAL**

- Generar informes de tráfico y desempeño de la red, conforme a los lineamientos establecidos por la UAEJPMP. - Elaborar y presentar los informes mensuales de gestión y operación del servicio de transmisión de datos. - Configurar y administrar el servicio de DHCP en las sedes de la Entidad a nivel nacional los cuales están alojados en los equipos LAN de la entidad.	
---	--

- 2.3.** Dos (2) Ingenieros Administradores de Seguridad Perimetral: El CONTRATISTA deberá disponer en la ciudad de Bogotá de dos (2) ingenieros administradores de seguridad perimetral para la prestación presencial del servicio. La cobertura operativa deberá garantizarse de lunes a viernes entre las 07:00 a. m. y las 06:00 p. m., Asimismo, los sábados el contratista deberá garantizar la disponibilidad de al menos un (1) ingeniero residente para la atención de incidentes, requerimientos y actividades operativas, asegurando la continuidad del servicio durante la jornada laboral comprendida entre las 08:00 a. m. y las 12:00 m. La prestación del servicio los días sábados podrá realizarse de manera remota o presencial, según lo acordado previamente con el supervisor del contrato.

Para tal efecto, el CONTRATISTA deberá establecer los turnos, horarios, relevos y demás esquemas de asignación de personal que resulten necesarios para garantizar la cobertura requerida, en estricto cumplimiento de la normativa laboral colombiana vigente, incluyendo lo dispuesto en la Ley 2101 de 2021 y las demás normas que la modifiquen, adicionen o sustituyan, sin que ello genere costos adicionales para la Entidad.

Funciones	Requerimientos
- El Administrador de Seguridad Perimetral será responsable de la administración, operación, monitoreo y fortalecimiento de la seguridad perimetral y de la información de la UAEJPMP, garantizando la protección de los	- Ingeniero con experiencia mínima de tres (3) años en manejo de plataformas de seguridad informática. - Con certificaciones en el manejo o configuración de equipos de





UNIDAD ADMINISTRATIVA ESPECIAL DE LA
JUSTICIA PENAL MILITAR Y POLICIAL

activos informáticos y de telecomunicaciones, la detección oportuna de amenazas y la respuesta efectiva ante incidentes de seguridad, conforme a las políticas, normatividad y directrices establecidas por la Entidad. - Disponibilidad de tiempo completo, durante toda la ejecución del contrato. - Las actividades deberán organizarse en turnos que garanticen la continuidad del servicio requerido por la UAEJPMP. - Proveer soporte especializado a los requerimientos de seguridad de la información solicitados por la UAEJPMP y que tengan aplicabilidad sobre la solución implementada. - Administrar, gestionar y brindar soporte a la plataforma de seguridad suministrada como parte de la solución descrita en el Anexo Técnico No. 2, conforme a las directrices impartidas por el contratista y por la supervisión del contrato. - Definir, implementar y mantener estrategias de defensa preventivas y reactivas, orientadas a la protección integral de los servicios informáticos de la Entidad. - Mantenerse actualizado respecto a amenazas, vulnerabilidades y herramientas de seguridad, y proponer la adopción de tecnologías y soluciones efectivas para el fortalecimiento del aseguramiento informático.	seguridad, los cuales deberán estar vigentes durante el periodo de ejecución del contrato. - Deberán presentar las certificaciones emitidas por el fabricante en el manejo y administración de los equipos de comunicaciones provistos en la solución, durante los primeros tres meses al inicio de la ejecución del contrato, los cuales deberán estar vigentes durante el periodo de ejecución del contrato. - Deberá ser personal de planta del Contratista. (presentar certificación laboral de la empresa)
--	--





UNIDAD ADMINISTRATIVA ESPECIAL DE LA
JUSTICIA PENAL MILITAR Y POLICIAL

- Informar oportunamente al Grupo de Seguridad Informática de la Entidad cualquier incumplimiento de la normatividad relacionada con el uso de los activos informáticos y de telecomunicaciones.
- Bloquear o suspender los servicios de red de los equipos que representen una amenaza para la seguridad institucional, previa autorización del Grupo de Seguridad Informática o supervisor del contrato.
- Analizar de manera permanente el tráfico de red, los registros (logs) de los sistemas y las alertas generadas por las herramientas de seguridad, con el fin de detectar, prevenir y mitigar posibles ataques.
- Proporcionar la información necesaria ante la ocurrencia de incidentes de seguridad de la información, facilitando una respuesta oportuna, la investigación del evento y la corrección de las causas identificadas.
- Ejecutar labores de fortalecimiento de seguridad (hardening) sobre servidores, enrutadores y switches que conforman la solución requerida.
- Realizar copias de respaldo de configuraciones y archivos de registro (logs) de todas las herramientas de seguridad informática.
- Verificar y documentar, mediante listas de control (checklist), la correcta configuración y





UNIDAD ADMINISTRATIVA ESPECIAL DE LA
JUSTICIA PENAL MILITAR Y POLICIAL

efectividad de las herramientas de seguridad instaladas. - Mantener una bitácora actualizada de incidentes de seguridad y de las acciones correctivas y preventivas aplicadas. - Registrar el análisis y tratamiento de los eventos de seguridad de la información en la herramienta de gestión de casos de la mesa de ayuda de la Entidad. - Documentar los procesos de aseguramiento de la información y las configuraciones realizadas sobre las herramientas de seguridad. - Promover y participar en reuniones periódicas con el Grupo de Seguridad de la Entidad, orientadas al seguimiento y mejora continua de la postura de seguridad. - Apoyar la revisión, ajuste y validación de las políticas, lineamientos y normatividad general en materia de seguridad de la información. - Suministrar a la plataforma SOC los informes de administración, operación y eventos generados por las herramientas y equipos de seguridad. - Monitorear de forma continua los cambios significativos en la exposición de los recursos de información, frente a las amenazas más relevantes. - Administrar de manera integral las políticas de seguridad, la configuración de los dispositivos de seguridad perimetral, filtros de URL, soluciones antivirus, IPS, Anti	
--	--





UNIDAD ADMINISTRATIVA ESPECIAL DE LA
JUSTICIA PENAL MILITAR Y POLICIAL

Spam y VPN, actuando como responsable general de la seguridad de la red institucional. - Elaborar y presentar los informes mensuales de gestión de seguridad, que deberán incluir, como mínimo: - Comportamiento de los servicios de seguridad definidos en el Anexo Técnico No. 2. - Consumo y bloqueos de solicitudes de navegación desde la red LAN/WAN hacia Internet. - Eventos e incidentes de seguridad detectados durante el período. - Recomendaciones técnicas de mitigación y mejora.	
---	--

- 2.4.** Un (1) Analista SOC NIVEL II: con disponibilidad presencial de lunes a viernes con un horario para la prestación del servicio de 08:00 a. m a 5:00 p.m. de lunes a viernes, en la ciudad de Bogotá D.C. disponibilidad frente a la gestión de incidentes de seguridad de la información de la Entidad, el cual puede ser flexible de acuerdo con las necesidades de la entidad. Para tal efecto, el CONTRATISTA deberá establecer los turnos que considere necesarios conforme a lo establecido en la Ley 2101 de 2021, sin generar costo adicional para la Entidad.

El CONTRATISTA deberá garantizar la prestación del servicio de Centro de Operaciones de Seguridad (SOC) bajo un esquema de disponibilidad continua 7x24, asegurando la atención permanente de los eventos e incidentes de seguridad de la información de la Entidad.

Para tal efecto, se deberá asignar un recurso dedicado en sitio durante el horario laboral, de lunes a viernes con una disponibilidad mínima de cinco por diez (5x8), quien deberá contar con pleno conocimiento del alcance, contexto, herramientas y casos asociados al contrato, encargándose del seguimiento operativo, gestión de incidentes y coordinación con la Entidad.

Fuera del horario laboral, el CONTRATISTA deberá garantizar la continuidad del servicio mediante la articulación con los equipos SOC y/o NOC responsables de la operación en horarios no laborales, asegurando una cobertura integral 7x24. Para esto, deberá implementar mecanismos formales de sincronización y transferencia de conocimiento, incluyendo la actualización





**UNIDAD ADMINISTRATIVA ESPECIAL DE LA
JUSTICIA PENAL MILITAR Y POLICIAL**

continúa de incidentes y casos, la documentación de procedimientos y decisiones relevantes, así como la ejecución de procesos de handover entre turnos.

El objetivo de este esquema será garantizar la continuidad operativa, la atención oportuna de incidentes de seguridad y la adecuada gestión del servicio en todo momento, sin generar costos adicionales para la Entidad dentro de las condiciones establecidas.

Funciones	Requerimientos
- Con disponibilidad de tiempo completo y con sede de trabajo en las instalaciones de la Unidad durante toda la ejecución del contrato, el recurso asignado deberá cumplir, como mínimo, con las siguientes funciones y responsabilidades: - Administrar y gestionar los equipos de seguridad del SOC, incluyendo el correlacionador de eventos, conforme a los procesos, procedimientos y actividades definidos para la operación, los cuales deberán ser ejecutados con la validación y visto bueno del CONTRATISTA. - Revisar, definir y ajustar el modelo de seguridad de la plataforma del SOC, de acuerdo con las necesidades operativas y los lineamientos de seguridad establecidos. - Diseñar, configurar y mantener alarmas tempranas en los sistemas de detección de seguridad operados por los analistas del SOC del CONTRATISTA. - Evaluar las consecuencias, agentes de amenaza y vectores de ataque asociados a los incidentes	- Ingeniero con experiencia mínima de dos (2) años en manejo de plataformas de seguridad informática. - El analista del SOC debe contar con conocimientos en el manejo de la plataforma de SOC, los cual se puede acreditar mediante certificaciones en donde se evidencie el manejo de la plataforma, los cuales deberán estar vigentes durante el periodo de ejecución del contrato. - Certificaciones emitidas por el fabricante respecto a la administración o configuración de la herramienta del SOC. - Deberá ser personal de planta del Contratista.(presentar certificación laboral de la empresa)





UNIDAD ADMINISTRATIVA ESPECIAL DE LA
JUSTICIA PENAL MILITAR Y POLICIAL

escalados por los operadores del SOC. - Desarrollar y mantener contenido en los motores de SIEM, incluyendo reglas de correlación, análisis de datos para inteligencia de seguridad, evaluación de indicadores y análisis de tendencias de ataque. - Atender de manera inmediata los incidentes de seguridad clasificados como altos y críticos, de acuerdo con los procedimientos definidos. - Realizar actividades de aseguramiento de la calidad (QA) sobre los informes periódicos generados por el SOC. - Ejecutar los procesos, procedimientos y actividades definidos en materia de seguridad de la información, conforme a los lineamientos establecidos. - Asesorar y participar activamente en las acciones de respuesta a incidentes de seguridad, en coordinación con las áreas correspondientes. - Registrar el análisis y tratamiento de los eventos de seguridad de la información en la herramienta de gestión de casos de la mesa de ayuda de la Entidad. - Actuar conforme a las políticas de seguridad de la información establecidas por la Entidad. - Notificar de forma inmediata al área de seguridad del CONTRATISTA y al supervisor del contrato cualquier incidente de seguridad de la información o la sospecha de su ocurrencia.	
---	--





UNIDAD ADMINISTRATIVA ESPECIAL DE LA
JUSTICIA PENAL MILITAR Y POLICIAL

--	--

Proyecto: Oscar Leonardo Pérez Casilimas.

Reviso: Carlos Ariel Useda Gómez



www.justiciamilitar.gov.co

Palacio de la Justicia Penal Militar y Policial
Carrera 46 No. 20 C - 01 - Puente Aranda
Línea de atención: +57 (601) 5169563 Ext. 1023
Bogotá D.C., Colombia