ANEXO TECNICO Nº 2.

SERVICIOS DE CIBERSEGURIDAD Y PROTECCIÓN DE LA INFRAESTRUCTURA TIC

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

1. REQUERIMIENTOS GENERALES DE LAS PLATAFORMAS

La Unidad Administrativa Especial de la Justicia Penal Militar y Policial (UAEJPMP) requiere la prestación del servicio de red corporativa de telecomunicaciones de amplia cobertura (WAN) y red de área local (LAN), soportada en plataformas de última tecnología disponibles en el mercado, que garantice la transmisión segura de datos y el cumplimiento de los Acuerdos de Niveles de Servicio establecidos en el presente ANEXO TÉCNICO_N° 5_NIVELES DE SERVICIO, MÉTRICAS Y TIEMPOS DE ATENCIÓN (ANS).

Para tal efecto, el CONTRATISTA deberá:

1.1. Presentar la plataforma propuesta con una descripción detallada de la arquitectura y de la funcionalidad que soportará el servicio, incluyendo las especificaciones técnicas de los equipos, la cual deberá ser presentada previo a la implementación de la tecnología de conectividad y seguridad y estará sujeta a aprobación por parte de la UAEJPMP.

1.2. Elaborar y presentar la topología de red y el dimensionamiento de los dispositivos para la Justicia Penal Militar y Policial, de manera previa a la implementación de la tecnología de conectividad y seguridad, los cuales deberán ser aprobados por la UAEJPMP.

1.3. El contratista deberá presentar el diagrama gráfico de la topología de red, en el cual se describa claramente la cobertura de la plataforma y el esquema típico de acceso correspondiente a la categoría a implementar.

1.4. La plataforma propuesta deberá incluir el hardware, software, licenciamiento, personal calificado y, en general, todos los recursos necesarios para la adecuada prestación del servicio, la gestión integral de la plataforma y el desarrollo del proyecto.

1.5. La tecnología ofrecida deberá soportar los protocolos IPv4 e IPv6, conforme a las especificaciones definidas por el IETF y los RFC vigentes, para la prestación del servicio de internet.

1.6. En caso de que la implementación de la plataforma requiera componentes activos y/o pasivos adicionales para soportar los servicios de seguridad, el contratista

deberá suministrarlos, instalarlos, configurarlos y ponerlos en operación como parte integral de la plataforma, sin costos adicionales para la entidad.

1.7. El contratista deberá instalar, configurar, implementar y poner en correcto funcionamiento el servicio de seguridad bajo tecnología requerida, el cual deberá contemplar, como mínimo, los siguientes componentes:

a) Canales de datos.
b) Canales de internet dedicados.
c) Soluciones de seguridad.
d) Plataforma de administración y gestión de la plataforma SD WAN.
e) Servicio de personal especializado disponible durante el proceso de implementación y configuración del servicio para la Justicia Penal Militar y Policial.
f) Gestión del tráfico sobre la red WAN y segmentación de la red.

1.8. Los dispositivos utilizados para la plataforma deberán ser nuevos, en óptimas condiciones de operación, escalables, aptos para montaje en rack o bandeja para rack, e incluir todos los elementos y accesorios necesarios para su correcta instalación, puesta en operación y funcionamiento.

1.9. Para verificar este requerimiento, el contratista deberá presentar los certificados del fabricante donde acredite que los equipos son nuevos, no remanufacturados y que no se encuentra fuera de venta ("End of sale"). Adicionalmente, deberá presentar la certificación del fabricante donde acredite que los equipos cuentan con los servicios de soporte técnico ("end of support"), así como, que cuenta con la disponibilidad de repuestos y garantía durante el tiempo de ejecución del contrato.

1.10. Los dispositivos de conectividad, seguridad y servidores suministrados en el marco del contrato deberán sincronizarse con el servicio NTP de la entidad, correspondiente a la hora legal colombiana.

1.11. Todos los equipos provistos como parte de la plataforma deberán contar con soporte técnico directo por parte del fabricante. Este requisito será aplicable a todos los componentes de la plataforma, incluyendo, entre otros, concentradores, switches, equipos de seguridad, servidores y software.

1.12. La UAEJPMP, cuando lo considere necesario, podrá verificar la capacidad y desempeño de los dispositivos utilizados por el contratista, con el fin de garantizar el cumplimiento de los parámetros técnicos exigidos y la viabilidad del objeto contractual.

1.13. El Contratista debe realizar la migración de las configuraciones, políticas, reglas y demás características de los equipos de seguridad perimetral existentes propiedad

de la Unidad y en servicio del contratista a los nuevos equipos suministrados en el contrato.

1.14. La plataforma deberá contar con todos los componentes dedicados para la red de la UAEJPMP. No se aceptan soluciones de tipo **multitenant.**

1.15. Configuración y alistamiento del software, hardware y firmware, garantizando su actualización a la última versión estable aprobada por el fabricante.
1.16. Implementación de la plataforma conforme a las mejores prácticas del fabricante, considerando una arquitectura de red segura.
1.17. Puesta en producción de la plataforma ofertada, asegurando su correcta operación.
1.18. Estabilización de la plataforma, mediante ajustes y verificaciones posteriores a la puesta en producción.
1.19. El CONTRATISTA debe realizar transferencia de conocimiento al Supervisor y funcionarios de apoyo del contrato sobre la operación y gestión de los equipos de seguridad perimetral y de monitoreo instalados en el contrato.
1.20. Entrega a satisfacción de la entidad, con validación del cumplimiento de los requerimientos establecidos.
1.21. El contratista deberá mantener Backups de la configuración de los equipos y en caso de falla por un parche o actualización podrá hacer un rollBack del Servicio.

Nota 1. La arquitectura actual de la UAEJPMP corresponde a una topología de estrella extendida, en la cual todos los nodos —relacionados en el ANEXO TÉCNICO Nº 4 SEDES INCLUIDAS EN EL ALCANCE DEL CONTRATO convergen hacia la sede Fortaleza (Bogotá D.C.) y Palacio (Bogotá D.C.), mediante un canal MPLS, para la prestación de los servicios internos de la entidad (aplicaciones) y el acceso a internet.
Nota 2. La descripción gráfica de la arquitectura actual de la plataforma será entregada al contratista adjudicatario al inicio del contrato.

2. REQUERIMIENTOS DE COBERTURA PARA LA PRESTACIÓN DEL SERVICIO DE SEGURIDAD.

Se deberán suministrar los servicios de seguridad requeridos por la UAEJPMP en la ciudad de Bogotá, correspondiente en el data center principal Fortaleza y Palacio data center alterno. Para tal efecto, se deberán contemplar, como mínimo, los siguientes componentes:

2.1. La fase de instalación plataforma de seguridad en mínimo deberá realizarse de la siguiente manera:

Fase	Tiempo máximo de Ejecución
Fase 1: Sedes categoría 1	Cuatro (4) meses

2.2. Una plataforma de seguridad en alta disponibilidad para la Sede Fortaleza Bogotá y la Sede Palacio Bogotá, que permita la gestión integral de los ámbitos de seguridad, el filtrado de contenido, así como la gestión y el monitoreo de los servicios de seguridad, con capacidad para atender al menos 3.500 usuarios, incluyendo el licenciamiento correspondiente y el suministro de la plataforma necesaria para garantizar la continuidad, disponibilidad y calidad del servicio.

2.3. La plataforma de seguridad descrita en el ITEM 3. Servicio De Seguridad Perimetral Y Protección Del Tráfico De Internet Mediante Firewall, deberá estar implementada en alta disponibilidad en el Nodo Fortaleza Bogotá y en la sede Palacio Bogotá, garantizando que, en caso de falla del cluster principal ubicado en la sede Fortaleza Bogotá, el tráfico sea redirigido de manera automática al datacenter de la sede Palacio Bogotá, y viceversa, asegurando así la continuidad del servicio.

2.4. Para el tráfico de Internet, la plataforma deberá operar en modo activo-activo, de tal forma que, ante la falla de cualquiera de las sedes, la sede restante asuma la totalidad de la carga de la Entidad sin afectar la prestación del servicio. El proceso de failover se realizará a nivel de enrutamiento hacia la otra sede Categoría 1 operativa.

2.5. Para el tráfico de datos y aplicaciones, se deberán contemplar esquemas activo-pasivo y activo-activo, de acuerdo con los requerimientos de la Entidad.

2.6. La solución deberá garantizar la cobertura del servicio de seguridad para el total de usuarios, dispositivos y crecimiento proyectado de la entidad, tomando como referencia un entorno de al menos. 3500 usuarios y/o dispositivos, con base en el acumulado de los siguientes ítems:

- funcionarios activos en el Directorio Activo:1569
- Conexiones de equipos: 1.500
- Holgura de crecimiento: 200

2.7. El contratista deberá presentar una descripción detallada del esquema a implementar, incluyendo el hardware y software utilizados, así como las especificaciones técnicas que caracterizan la implementación de la plataforma.

2.8. El contratista deberá garantizar el soporte técnico y el licenciamiento de la plataforma durante todo el tiempo de ejecución del contrato.

2.9. El contratista deberá entregar los esquemas y estructuras por implementar, integrando la conectividad de las sedes Categoría 1.

2.10. El contratista deberá entregar las características técnicas de todas las plataformas de seguridad propuestas para el cumplimiento del servicio.

3. SERVICIO DE SEGURIDAD PERIMETRAL Y PROTECCIÓN DEL TRÁFICO DE INTERNET MEDIANTE FIREWALL.

Se requiere la prestación de un servicio de seguridad que contemple, como mínimo, los siguientes componentes:

3.1. Servicios de ubicación.

a) La plataforma deberá incluir, como mínimo, los siguientes servicios de seguridad: seguridad externa mediante firewall perimetral, gestión del tráfico de Internet, tráfico de datos, detección y prevención de intrusos (IDS/IPS), Red Privada Virtual (VPN), antivirus perimetral, navegación segura.

b) Para los componentes que el contratista implemente on premise, la plataforma deberá instalarse en los gabinetes dispuestos por la UAEJPMP, correspondientes a un (1) rack en el nodo Fortaleza Bogotá y un (1) rack en la sede Palacio Bogotá.

En consecuencia deberán ser instalables en rack, el contratista podrá ofrecer la funcionalidad requerida mediante un único appliance físico o múltiples appliances o instancias virtuales, suministrando el hardware, software y licenciamiento de propósito específico necesarios, sin que ello genere costos adicionales para la UAEJPMP.

3.2. Servicios de Firewall

a) La Entidad requiere que toda la plataforma on premise en Palacio y Fortaleza en Bogota D.C. de seguridad perimetral esté basada en firewalls de nueva generación (NGFW), que brinden protección externa perimetral e interna, así como funcionalidades de IPS, antivirus y navegación segura, implementadas en alta disponibilidad tanto en el nodo Fortaleza Bogotá como en la sede Palacio Bogotá. con capacidad mínimas de:

a) Rendimiento de Firewall IP (paquetes de 512 Bytes): 100 Gbps.
b) Rendimiento de Firewall IP (paquetes de 1518 Bytes): 60 Gbps.
c) IPS Throughput:20 Gbps
d) Sesiones simultáneas o concurentes:10 Millones.
e) SSL Inspection Throughput: 11 Gbps.
f) NGFW Throughput: 15 Gbps
g) Doble fuente de poder

3.3. Arquitectura de conectividad

a) La plataforma deberá contar con una arquitectura que permita la protección de dos (2) servicios de Internet independientes, ubicados en distintas localizaciones geográficas: Nodo Fortaleza Bogotá y Nodo Palacio Bogotá.

3.4. Balanceo y continuidad

a) La plataforma deberá permitir el balanceo automático de los canales de Internet y, en caso de falla de alguno de ellos, garantizar la continuidad del servicio. Cada canal deberá contar con un firewall perimetral de propósito específico.

3.5. Administración centralizada

a) Los servicios de filtrado de URL y seguridad en la navegación deberán ser administrados de forma centralizada entre Fortaleza Bogotá y Palacio Bogotá, garantizando el cumplimiento de los Acuerdos de Niveles de Servicio (ANS) establecidos en el ANEXO TÉCNICO No. 5.

3.6. Integración con la red WAN

a) Las políticas de navegación deberán integrarse con los **servicios de la red WAN**, permitiendo la aplicación efectiva de controles sobre el tráfico de Internet.

3.7. Accesos a la plataforma de gestión.

a) Se deberá contemplar el acceso a la plataforma de gestión y administración por parte del contratista desde el nodo Fortaleza y Palacio de la UAEJPMP, así como acceso en modalidad de consulta para el personal de seguridad designado por la UAEJPMP. El contratista deberá garantizar que sus oficiales de seguridad cuenten con los permisos necesarios para la administración y control de la plataforma.

3.8. Características del firewall NGFW

3.8.1. El firewall de nueva generación deberá permitir protección externa, perimetral e interna, IPS, antivirus y navegación segura, soportado sobre una plataforma en alta disponibilidad en el nodo Fortaleza Bogotá y la sede Palacio Bogotá.

3.8.2. El servicio de seguridad externa deberá implementarse mediante zonas de seguridad y políticas entre zonas y redes, cumpliendo como mínimo con las siguientes características:

a) Topología de conexión que garantice la seguridad de los accesos a Internet.

b) Funcionalidades de Firewall, Control de Aplicaciones, Antimalware, Bloqueo por Hash, IPS y Web Filter.
c) Uso de las últimas versiones estables de software y licenciamiento disponible en el mercado.
d) Sistema operativo de uso específico.
e) Diseño acorde con los anchos de banda exigidos y las características técnicas mínimas requeridas.
f) Integración con el Directorio Activo de la Entidad (Windows Server 2019 o superior), con capacidad mínima para 2.000 usuarios.
g) Configuración de políticas a cargo del contratista, previa aprobación de la supervisión del contrato.
h) No afectar el rendimiento de la red, garantizando los tiempos de respuesta definidos en el ANEXO TÉCNICO No. 1. REQUERIMIENTOS TÉCNICOS DE CONECTIVIDAD WAN Y LAN.
i) Generación de alertas en tiempo real y control de acceso en las capas de red, transporte y aplicación.
j) Filtrado por puerto, protocolo, aplicación y tipo de tráfico, con capacidad de ensamblaje y análisis de paquetes fragmentados.
k) Analizador de logs que permita automatizar el procesamiento de bitácoras y apoyar la gestión del SOC suministrado por el contratista.
l) Capacidad técnica suficiente para soportar el tráfico de Internet requerido, incluso bajo condiciones de alta carga.
m) La solución deberá permitir que funcionalidades como NGFW, SD-WAN, SIEM, SOAR, protección de nube y servicios SASE operen dentro de un ecosistema tecnológico integrado, compartiendo telemetría, inteligencia, políticas y capacidades de respuesta desde una plataforma unificada.
n) La solución deberá incorporar capacidades de análisis dinámico de archivos y sandboxing para la detección de amenazas desconocidas y malware zero-day, mediante mecanismos de detonación y análisis avanzado de archivos sospechosos en ambientes aislados (sandbox), permitiendo la identificación de comportamientos maliciosos, generación automática de firmas y protección en tiempo real contra amenazas avanzada
o) La solución NGFW deberá incorporar capacidades de prevención de amenazas desconocidas mediante motores de Machine Learning e Inline Deep Learning integrados directamente en la plataforma firewall, permitiendo el bloqueo en línea (inline) de malware desconocido, ataques fileless y amenazas Zero-Day sin depender exclusivamente de firmas tradicionales.
p) La plataforma deberá permitir capacidades de prevención inline orientadas a reducir el riesgo de compromiso inicial (“Patient Zero”), mediante análisis avanzado y prevención automatizada de amenazas desconocidas en tiempo real.
q) La solución deberá generar y distribuir automáticamente mecanismos de protección y firmas de seguridad en tiempo real o en cuestión de segundos hacia los dispositivos NGFW conectados, permitiendo respuesta rápida frente a amenazas emergentes y Zero-Day.

La plataforma deberá permitir la generación de reportes y estadísticas, como mínimo, sobre:

a) Consumo de navegación en Internet.
b) Top de usuarios con mayor consumo.
c) Peticiones a Internet bloqueadas.
d) Identificación de páginas con riesgo de seguridad.
e) Detección de uso de *proxies*.
f) Casos de spam, malware o virus detectados.
g) Recomendaciones y conclusiones.

En caso de que dichos reportes no se generen de forma estándar, el contratista deberá diseñarlos e implementarlos.

Nota: La topología actual de la Entidad será entregada al contratista adjudicatario.

El contratista podrá proponer, si lo considera pertinente, una arquitectura específica que integre múltiples herramientas en un único dispositivo, siempre que se cumplan los requerimientos técnicos establecidos.

3.9. Servicio de seguridad perimetral.

En la prestación de los servicios de seguridad de firewall, el CONTRATISTA deberá cumplir con las siguientes obligaciones:

3.9.1. Suministrar los servicios de prevención de intrusiones (IPS), antivirus, Hash y navegación segura, soportados sobre una plataforma en alta disponibilidad, en los nodos de Fortaleza y en la sede Palacio Bogotá. En consecuencia, el servicio de firewall perimetral podrá ser aprovisionado mediante appliances físicos o zonas de seguridad y políticas entre zonas y redes, siempre que cuenten con el software y el licenciamiento necesarios para garantizar la correcta prestación del servicio.

3.9.2. Suministrar la documentación del esquemas y estructuras de la plataforma, debidamente estructurada y alineada con los requerimientos de la UAEJPMP.

3.9.3. Ofrecer la configuración, puesta en operación y administración de la plataforma, garantizando el cumplimiento de los requerimientos establecidos en el presente documento.

3.9.4. Optimizar, implementar y documentar las políticas de seguridad que serán instaladas en los firewalls requeridos.

3.9.5. Hardware de propósito específico, con la última versión estable del software, incluyendo sus respectivas actualizaciones durante toda la ejecución del contrato.

3.9.6. El contratista deberá establecer en el esquemas y estructuras e implementación de la plataforma a proveer el número de interfaces físicas a proveer de tipo: 1Gbps en cobre 100/1000 BaseT, 1Gbps Base-SX SFP Multimodo, Ethernet 10G Base-SR SFP+ Multimodo, 25 o 40 Gigabit Ethernet, lo que requiera la plataforma para garantizar el correcto funcionamiento y conexión con la plataforma de la UAEJPMP, con capacidad de manejo de VLAN por interface. En caso de que el esquema propuesto requiera un número mayor de interfaces el Contratista debe proveerlos sin costo adicional.

3.9.7. Soporte de alta disponibilidad, permitiendo arquitecturas de clúster activo-pasivo y activo-activo, con sincronización de estados de conexión, de tal forma que, ante la falla de un nodo, el impacto no sea percibido por los usuarios ni por las aplicaciones.

3.9.8. Implementación de arquitecturas de hardware con balanceadores de carga de firewall (Firewall Load Balancers).

3.9.9. Capacidad para realizar funciones de enrutamiento de nivel 3.

3.9.10. Autenticación de usuarios y verificación de autorizaciones contra las políticas de seguridad, permitiendo el establecimiento de conexiones únicamente cuando se cumplan dichas políticas, incluso a nivel de aplicación.

3.9.11. Interfaz gráfica de usuario (GUI), vía web (HTTP/HTTPS) o mediante aplicación cliente, que haga parte de la arquitectura nativa de la plataforma para la administración local, soportando protocolos de seguridad vigentes. La plataforma deberá contar con registro de eventos de seguridad, monitoreo de recursos del sistema y estadísticas de eventos y tráfico.

3.9.12. Diseño que permita ejercer funciones de punto central de seguridad, servidor de redes privadas virtuales (VPN) y terminación de túneles de cifrado.

3.9.13. Mecanismos de cifrado que cumplan con los estándares internacionales AES y 3DES, garantizando la integridad, confidencialidad y autenticidad de la información transmitida.

3.9.14. Compatibilidad, en caso de ser requerido, con los firewalls o equipos de enrutamiento de las sedes de Categoría 2 y 3, con Tipos de Servicio 1, incluyendo VPN y túneles de seguridad.

3.9.15. Capacidad para crear controles de acceso basados en protocolos, puertos y direcciones IP predefinidas.

3.9.16. Soporte de NAT dinámico y NAT estático.

3.9.17. Control de tráfico basado en origen (dirección IP, usuarios y grupos), destino (dirección IP, FQDN, URL o categoría), servicio, aplicación, categoría de aplicaciones y categoría de URLs.

3.9.18. Suministrar la totalidad de los patch cords de cobre, fibra y los transceptores SFP y SFP+ requeridos dentro de la solución de conectividad y seguridad a implementar, garantizando la correcta operación del servicio.

3.9.19. De considerarlo procedente, el CONTRATISTA podrá proponer una arquitectura específica, integrando múltiples herramientas de seguridad en un solo dispositivo.

3.9.20. Funciones de seguridad orientadas a la protección del tráfico de Internet, destinadas a garantizar la navegación segura de los usuarios de la UAEJPMP.

3.9.21. Suministrar la documentación del diseño de la plataforma, debidamente estructurada y alineada con los requerimientos de la entidad.

3.9.22. Ofrecer la configuración, puesta en operación y administración de la plataforma, asegurando el cumplimiento de los requerimientos exigidos en el presente documento.

3.9.23. Realizar la optimización, implementación y documentación de las políticas de seguridad que serán instaladas en los firewalls requeridos.

3.9.24. Contar con la última versión estable del software liberada por el fabricante.

3.9.25. Disponer de un sistema operativo de uso específico, diseñado para funciones de seguridad perimetral.

3.9.26. Suministrar el licenciamiento necesario para soportar como mínimo 3.000 usuarios, garantizando la posibilidad de crecimiento futuro sin que ello implique costos adicionales para la UAEJPMP.

3.9.27. Implementar la plataforma en alta disponibilidad, permitiendo arquitecturas de clúster tanto activo-pasivo como activo-activo, con sincronización del estado de las conexiones entre los nodos, de tal forma que, ante la falla de un nodo, el impacto no sea percibido por los usuarios ni por las aplicaciones.

3.9.28. Soportar funciones de enrutamiento de nivel 3 (Layer 3).

3.9.29. Soportar autenticación de usuarios, verificación de autorizaciones contra las políticas de seguridad y habilitación de conexiones conforme al cumplimiento de dichas políticas en la capa de aplicación.

3.9.30. Disponer de una interfaz gráfica de usuario (GUI), vía web (HTTP/HTTPS) o mediante aplicación cliente, que haga parte de la arquitectura nativa de la plataforma y permita la administración local de las políticas de seguridad.

3.9.31. Contar con registro de eventos de seguridad, monitoreo de recursos del sistema y generación de estadísticas de eventos y tráfico.

3.9.32. Suministrar certificados digitales para la habilitación de la funcionalidad de inspección SSL (SSL Inspection) en las estaciones de trabajo, a través del Directorio Activo administrado por la entidad.

3.9.33. Realizar el registro y análisis de eventos de seguridad, recursos del sistema y estadísticas de eventos y tráfico, tanto en la plataforma provista por el CONTRATISTA como en la herramienta de gestión de casos de la mesa de ayuda de la entidad, para los requerimientos que deban ser implementados.

3.9.34. El contratista deberá suministrar una solución de visibilidad centralizada sobre la navegación, los objetos transferidos y las amenazas asociadas al tráfico web de los usuarios. La solución deberá integrarse con la plataforma de logs y reportes solicitada, permitiendo una visión global de eventos y amenazas. El cumplimiento podrá realizarse mediante funcionalidades nativas de proxy, inspección, análisis, control y reporte .

3.9.35. La solución deberá incorporar capacidades de inspección de tráfico cifrado, incluyendo sesiones SSL/TLS y SSH, que permitan aplicar controles de filtrado URL, control de aplicaciones, prevención de fuga de información (DLP), antivirus e IPS.

3.9.36. Implementar control de tráfico basado en:

a) Fuente: dirección IP, usuarios locales y grupos.

b) Destino: dirección IP, FQDN, URL o categoría.

c) Servicio: acceso web, acceso a archivos, servicios de correo y red, autenticación, acceso remoto, tunneling, VoIP, mensajería, web proxy y otras aplicaciones.

d) Aplicación, categoría de aplicaciones y categoría de URLs.

3.9.37. Realizar inspección de tráfico cifrado mediante SSL, como mínimo, para los protocolos HTTP, IMAP y SMTP.

3.9.38. Permitir la captura de paquetes asociada a políticas de seguridad implementadas, con opción de exportación en formato PCAP.

3.9.39. Ejecutar escaneo profundo de tráfico SSH, sobre todos o un rango específico de puertos configurados para dicho análisis.

3.9.40. Suministrar los logs de seguridad al SOC o SIEM suministrado por el contratista, conforme a los lineamientos definidos.

3.9.41. Si el CONTRATISTA lo considera procedente, podrá proponer una arquitectura específica, integrando múltiples herramientas de seguridad en un solo dispositivo.

3.10. Servicio de seguridad para el tráfico de datos con capacidades de detección y prevención de intrusiones

El contratista deberá contemplar en la plataforma para las sedes de Fortaleza Bogotá y Palacio Bogotá, las siguientes características mínimas:

3.10.1. Implementar un Sistema de Detección de Intrusos basado en red (NIDS – Network Intrusion Detection System), el cual deberá monitorear todo el tráfico que circule por los segmentos de red, con el fin de identificar intentos de uso indebido, accesos no autorizados o actividades maliciosas.

3.10.2. Dicho sistema deberá reportar las amenazas detectadas, identificar intentos de vulneración de la red y contar con la funcionalidad de bloqueo de la fuente del ataque.

3.10.3. Implementar un Sistema de Prevención de Intrusos (IPS), el cual deberá aplicar los controles de acceso necesarios en el perímetro de la red una vez el IDS detecte un intento de ataque.

3.10.4. El sistema de detección y prevención de intrusos deberá implementarse en línea de manera que el tráfico sea recibido directamente por el componente IDS/IPS para su inspección. En caso de falla del sistema, este deberá permitir el paso del tráfico sin afectar la transmisión de los datos soportados por la plataforma provista.

3.10.5. Permitir la selección del sistema operativo, protocolo, nivel de severidad y objetivo, para la configuración de los perfiles de IPS.

3.10.6. El IPS deberá soportar, como mínimo, las siguientes acciones: permitir, monitorear, bloquear, resetear sesiones, almacenar copias de los paquetes que coincidan con firmas, y realizar cuarentena basada en la dirección IP del atacante, con temporización configurable en días, horas o minutos.

3.10.7. El sistema de protección contra intrusos deberá identificar patrones de tráfico anómalos que no cumplan con los requerimientos de los protocolos y estándares establecidos.

3.10.8. Contar con actualización automática de firmas IPS, permitiendo recibir actualizaciones de forma inmediata cuando los centros de actualización emitan nuevas versiones, así como realizar consultas periódicas para verificar la disponibilidad de firmas actualizadas.

3.10.9. La funcionalidad de detección y prevención de intrusos deberá estar completamente integrada a la plataforma de seguridad provista.

3.10.10. La interfaz de administración del sistema IDS/IPS deberá estar integrada a la consola de administración del appliance de seguridad, sin requerir consolas adicionales, y deberá permitir la protección del servicio mediante políticas de control de acceso.

3.10.11. Detectar ataques mediante variaciones de protocolo, así como a través de firmas de ataques conocidos, utilizando técnicas basadas en firmas y en tasa de eventos (signature based / rate based).

3.10.12. Estar basado en el análisis de firmas sobre el flujo de datos de la red, permitiendo además la configuración de nuevas firmas para cualquier protocolo.

3.10.13. Soportar la actualización automática de firmas para el sistema de detección de intrusos.

3.10.14. El sistema IDS/IPS deberá mitigar los efectos de ataques de denegación de servicio (DoS).

3.10.15. Disponer de los siguientes métodos de notificación:

a) Alarmas visualizadas en la consola de administración del appliance.
b) Alertas enviadas por correo electrónico.

3.10.16. Contar con capacidad de cuarentena, permitiendo bloquear el tráfico posterior a la detección de un posible ataque.

3.10.17. Definir políticas de detección y prevención de intrusiones para tráfico IPv4 e IPv6, a través de sensores debidamente configurados.

3.10.18. El sistema IDS/IPS deberá analizar todos los segmentos físicos y virtuales que se definan en el diseño de la plataforma elaborado por el CONTRATISTA.

3.10.19. El IPS deberá incluir un mínimo de 2.000 firmas de detección de ataques, que brinden protección tanto contra ataques orientados a servidores como a clientes.

3.10.20. Detectar y bloquear, como mínimo, los siguientes tipos de amenazas: comunicaciones salientes (outbound) con malware, intentos de tunneling y ataques de explotación (exploit attacks).

3.10.21. Todos los módulos y funcionalidades de seguridad deberán enviar sus traps SNMP y registros syslog al correlacionador de eventos de seguridad suministrado por el contratista.

3.11. Servicio de conectividad segura mediante red privada virtual (VPN)

El CONTRATISTA deberá contemplar que la plataforma incluya una **instancia dedicada para el servicio de Red Privada Virtual (VPN)**, la cual deberá cumplir, como mínimo, con los siguientes requisitos de seguridad, capacidad y operación:

3.11.1. Requisitos Generales de Seguridad

a. La plataforma VPN deberá incorporar funcionalidades de prevención de intrusiones (IPS), antivirus y filtrado de URL, aplicables al tráfico cursado a través del servicio.
b. Deberá implementar controles de contenido que garanticen las condiciones de seguridad requeridas para este tipo de acceso, especialmente para los sistemas misionales, conforme a la configuración y políticas vigentes de la Entidad.

3.11.2. Capacidades Técnicas de la Plataforma VPN

La plataforma que soporte la plataforma VPN deberá cumplir, como mínimo, con las siguientes capacidades técnicas:

a) Debera de estar en capacidad de soportar un mínimo de mil (1.000) usuarios VPN SSL y cien (100) túneles VPN IPSec. El CONTRATISTA deberá suministrar el licenciamiento requerido para cumplir con este requisito.
b) Soportar certificados digitales RSA X.509 para la implementación de VPN cliente-sitio (client-to-site).
c) Soportar VPN IPSec sitio-a-sitio y cliente-sitio.
d) La solución de conectividad y seguridad deberá soportar el protocolo IKEv2, así como los mecanismos estándar necesarios para el establecimiento, negociación y operación de túneles VPN.
e) Deberá admitir la implementación de VPN utilizando algoritmos de cifrado AES-256, AES-128 y 3DES.
f) Deberá soportar, como mínimo, los grupos Diffie-Hellman 1, 2, 5 y 14.
g) Deberá incorporar algoritmos de integridad MD5, SHA-1 y SHA-256.
h) En modo interfaz, la VPN IPSec deberá asignar direcciones IP, permitir el enrutamiento mediante rutas asociadas y poder definirse como interfaz de origen o destino dentro de las políticas de firewall.
i) Permitir la implementación de VPN SSL sin requerir licenciamiento por usuario.
j) La solución deberá soportar protocolos seguros para acceso remoto cifrado, como mínimo TLS 1.2 y TLS 1.3, de acuerdo con las mejores prácticas vigentes de seguridad.

k) Soportar modos de operación web y túnel para VPN SSL.
l) Soportar el uso de certificados RSA X.509 para VPN SSL.
m) Validar estaciones de trabajo con sistema operativo Windows, verificando el sistema operativo, firewall y antivirus antes de permitir el acceso mediante VPN SSL.
n) Verificar la presencia de antivirus y firewall personal, propios o de terceros, en los equipos que establecen conexión VPN SSL.
o) Definir múltiples portales SSL, asignados según el grupo de pertenencia del usuario, que funcionen como interfaz gráfica de acceso.
p) La interfaz de acceso remoto deberá permitir la personalización y publicación de aplicaciones, servicios o recursos autorizados, de acuerdo con el perfil del usuario y las políticas definidas por la Entidad
q) Soportar la funcionalidad de Escritorio Virtual.
r) La solución deberá incorporar controles de seguridad para el acceso remoto a escritorios, aplicaciones o recursos críticos, orientados a reducir el riesgo de acceso no autorizado, fuga de información y compromiso de credenciales
s) La plataforma deberá implementar el enfoque de Zero Trust Network Access (ZTNA), otorgando acceso únicamente a aplicaciones y recursos previamente autorizados.
t) La solución NGFW deberá incorporar capacidades de prevención inline de amenazas mediante motores de Machine Learning e Inline Deep Learning integrados nativamente en la plataforma, permitiendo la detección y bloqueo en tiempo real de malware desconocido, phishing avanzado, ataques Zero-Day y amenazas evasivas sin depender exclusivamente de firmas tradicionales.
u) La solución deberá permitir prevención de amenazas conocidas y desconocidas en tiempo real, incluyendo capacidades de detección de amenazas evasivas y malware Zero-Day antes de que estas impacten la red corporativa.
v) La plataforma NGFW deberá incorporar capacidades de detección de amenazas basadas en comportamiento, analítica y machine learning, permitiendo identificar amenazas sin depender exclusivamente de firmas, hashes o mecanismos tradicionales de fingerprinting.
w) La solución NGFW deberá soportar inspección SSL/TLS avanzada incluyendo tráfico TLS 1.3 y HTTP/2, permitiendo análisis de amenazas sobre tráfico cifrado sin afectar el desempeño ni comprometer la privacidad de usuarios autorizados.
x) La solución deberá soportar políticas dinámicas basadas en identidad y comportamiento de usuario, permitiendo automatización de controles de seguridad mediante grupos dinámicos de usuarios e integración con plataformas XDR, UEBA y SIEM.
y) La plataforma NGFW deberá identificar aplicaciones independientemente de puertos, protocolos, cifrado o técnicas de evasión, permitiendo control granular de funciones específicas de aplicaciones y tráfico SaaS.
z) El servicio de protección de DNS debe poder habilitarse sin modificar la configuracion de DNS de la red local o desviar el trafico DNS a servidores externos.

aa) La solución debe ser un servicio que funcione integrado en la plataforma de NGFW, sin requerir adicionar hardware adicional y sin impactar el rendimiento del NGFW.
bb) La solución debe ser capaz de predecir y detener dominios maliciosos de malware basados en algoritmos de generación de dominio (DGA).
cc) Debe utilizar machine learning y/o inteligencia artificial para detectar nuevos dominios nunca antes vistos autogenerados por algoritmos DGA
dd) Debe poseer políticas para bloquear dominios DGA o interrumpir las consultar de DNS a dichos dominios.
ee) Debe detectar e interrumpir robo de datos ocultos o tunelizados en tráfico DNS
ff) Debe permitir como acción ante peticiones DNS maliciosas: alertar, bloquear las conexiones y además responder a la petición con IP sumidero (sinkhole) con el fin de identificar al usuario/equipo realizando consultas DNS maliciosas.
gg) Debe poder clasificar los dominios maliciosos en categorías como: malware, DGA, DNS tunneling, Comando y Control, DNS dinámicos, phising o dominios recientemente registrados.
hh) La solución debe brindar el contexto de cada dominio incluyendo historial completo para informar el origen y reputación de cada dominio.
ii) Debe brindar analítica de cada consulta DNS: frecuencia de visita, marca de tiempo, información del DNS pasiva, WHOIS y cualquier etiqueta de malware asociada.

3.11.3. Autenticación y Control de Acceso

El CONTRATISTA deberá suministrar una plataforma de protección de acceso remoto ZTNA/VPN, que garantice conectividad segura y verificación de cumplimiento. Para este componente se requiere licenciamiento, con autenticación basada en tokens de software.

a) La plataforma deberá proveer autenticación multifactor (MFA) mediante mecanismos como OTP, notificaciones push, certificados digitales, tokens de software
b) La plataforma deberá permitir el uso de segundos factores de autenticación en dispositivos móviles iOS y Android, mediante aplicaciones autenticadoras, notificaciones push o tokens de software compatibles con la solución ofertada
c) Deberá contar con protección contra ataques de fuerza bruta, incluyendo mecanismos de bloqueo automático.
d) La plataforma deberá ser escalable, aprovechando los dispositivos existentes de los usuarios finales.
e) La plataforma deberá reducir el riesgo de robo de credenciales y ataques de fuerza bruta mediante la implementación de MFA en los accesos de usuario.
f) Deberá soportar usuarios locales y usuarios integrados con directorios corporativos tales como LDAP, Active Directory y RADIUS.

3.12. Auditoría y Arquitectura

a) El CONTRATISTA deberá realizar seguimiento y auditoría de las actividades de los usuarios, registrando accesos y acciones ejecutadas, con el fin de generar reportes y remitir dicha información a la plataforma SOC suministrada por el mismo.
b) En caso de considerarlo pertinente, el CONTRATISTA podrá proponer una arquitectura específica, integrando múltiples herramientas de seguridad en un único dispositivo, siempre que se garantice el cumplimiento integral de los requisitos técnicos aquí establecidos.

3.13. Servicio de protección antivirus perimetral.

Los servicios de seguridad de firewall de nueva generación deberán contar con un módulo de antivirus perimetral, implementado en alta disponibilidad en el nodo Fortaleza Bogotá y en la sede Palacio Bogotá. En consecuencia, el servicio de Gateway Antivirus provisto deberá cumplir, como mínimo, con los siguientes requerimientos:

3.13.1. Analizar, controlar el acceso y detener ataques en tiempo real sobre, al menos, los siguientes protocolos: HTTP, IMAP, POP3, FTP y SMTP.
3.13.2. Mitigar amenazas provenientes de virus, gusanos, troyanos, ransomware, scareware, spyware, adware, botnets, entre otros tipos de malware.
3.13.3. El módulo de antimalware deberá integrarse de forma nativa con la plataforma de seguridad provista.
3.13.4. La plataforma deberá incluir un módulo o componente de antimalware integrado al firewall perimetral.
3.13.5. El antivirus deberá configurarse para realizar la captura y análisis completo de archivos, incluyendo aquellos que presenten múltiples niveles de compresión.
3.13.6. El antivirus deberá permitir la inspección de amenazas en ejecutables Windows embebidos en adjuntos de correo electrónico, así como brindar protección contra malware en dispositivos móviles.
3.13.7. El antivirus deberá operar en tiempo real, contando con el software y licenciamiento necesarios para realizar la categorización de contenido.
3.13.8. El antivirus integrado deberá soportar la inspección y detección de malware en tráfico IPv4 e IPv6.
3.13.9. El antivirus deberá escanear el tráfico asociado a sistemas de archivos compartidos, sin restricciones de licenciamiento.
3.13.10. La plataforma en caso de requerirse deberá soportar la integración con soluciones de Sandbox.
3.13.11. La plataforma deberá incluir mecanismos para detectar y bloquear conexiones hacia redes Botnet y servidores de comando y control (C&C).
3.13.12. La plataforma deberá incluir mecanismo de Identificación y Bloqueo de Malware por Hash (Firmas)
3.13.13. Si el CONTRATISTA lo considera procedente, podrá proponer una arquitectura específica, integrando herramientas de seguridad en uno o varios dispositivos, siempre que se garantice el cumplimiento de los requerimientos establecidos en los anexos técnicos.

3.14. Servicio de plataforma de análisis, registro y gestión centralizada de eventos de seguridad

El contratista deberá entregar la plataforma de seguridad implementada en los nodos de fortaleza y palacio la cual debe integrarse de forma nativa con una plataforma centralizada de recolección, almacenamiento, búsqueda, consulta, análisis y generación de reportes, con la siguiente capacidad mínimas:

3.14.1. Para el nodo Fortaleza Bogotá: Un (1) appliance físico con capacidad de almacenamiento mínimo de 8 TB o retención mínima de logs de doce (12) meses.
3.14.2. Para la sede Palacio Bogotá: Un (1) appliance físico con capacidad de almacenamiento mínimo de 8 TB o retención mínima de logs de doce (12) meses.
3.14.3. La plataforma deberá soportar administración basada en perfiles, permitiendo la asignación de permisos conforme a roles definidos.
3.14.4. La plataforma deberá contar con una vista centralizada, que facilite la detección y el análisis de amenazas en redes, puntos finales, aplicaciones e infraestructura en la nube.
3.14.5. La plataforma deberá permitir el envío de alarmas por correo electrónico, configurables según eventos y niveles de severidad.
3.14.6. La plataforma deberá permitir la creación de módulos personalizados por usuario y por nivel de permisos.
3.14.7. La plataforma deberá permitir la integración con soluciones SIEM de terceros, con el fin de ampliar las capacidades de correlación de eventos y respuesta automatizada.
3.14.8. La plataforma deberá soportar alta disponibilidad (HA), en modos activo-activo o activo-pasivo, garantizando la continuidad del servicio y la tolerancia a fallas.
3.14.9. La plataforma deberá permitir escalabilidad horizontal y vertical, garantizando el crecimiento modular de la capacidad de almacenamiento y procesamiento de eventos.
3.14.10. La plataforma deberá contar con mecanismos de compresión y deduplicación de logs, con el fin de optimizar el uso del almacenamiento.
3.14.11. La plataforma deberá tener la integración con sistemas de autenticación multifactor (MFA), garantizando el acceso seguro de administradores y usuarios.
3.14.12. La plataforma deberá permitir la generación y programación de reportes automáticos en formatos PDF, CSV y HTML, con capacidad de envío por correo electrónico a grupos de usuarios definidos.
3.14.13. La plataforma deberá permitir visualización gráfica avanzada, incluyendo gráficos de tendencias, diagramas de topología y análisis de flujos de tráfico.
3.14.14. La plataforma deberá contar con capacidades para la investigación detallada de incidentes, incluyendo líneas de tiempo de eventos y reconstrucción de sesiones de usuario.
3.14.15. La plataforma deberá integrarse con fuentes de inteligencia de amenazas, permitiendo la correlación en tiempo real de Indicadores de Compromiso (IoC).

3.14.16. La plataforma deberá contar con motores de aprendizaje automático (machine learning) que permitan identificar patrones anómalos y comportamientos sospechosos en usuarios y dispositivos.

3.14.17. La plataforma deberá soportar el firmado digital de logs y reportes, garantizando la integridad y trazabilidad de la información.

3.14.18. La plataforma deberá permitir la segmentación de datos por cliente o unidad de negocio (multi-tenant), habilitando su uso en entornos con múltiples áreas o entidades.

3.14.19. La plataforma deberá contar con una auditoría completa de las acciones realizadas por administradores y usuarios, con generación de reportes exportables.

3.14.20. La plataforma deberá soportar la migración y restauración rápida de configuraciones y bases de datos, permitiendo una recuperación eficiente ante incidentes o fallas.

3.14.21. El CONTRATISTA deberá incluir los servicios de esquemas y estructuras, instalación, configuración, parametrización, puesta en funcionamiento y entrega a satisfacción, realizada por ingenieros certificados por el fabricante de los equipos. El contratista deberá presentar las respectivas certificaciones del grupo de trabajo asignado expedidas por el fabricante de los equipos.

3.14.22. Los esquemas y estructuras de la plataforma a implementar deberán ser revisados y aprobados por el supervisor del contrato.

3.14.23. Al finalizar el contrato, dicha información deberá ser entregada a la Entidad mediante discos externos (SDD) suministrados por el contratista el cual debe contemplar todos los costos o gastos asociados.

3.14.24. Brindar soporte y actualización de la consola de administración, para los componentes que incluyen el producto.

3.14.25. El contratista deberá realizar las pruebas de funcionamiento respectivas para la infraestructura tecnológica, así mismo entregará un documento técnico que especifique las pruebas realizadas en esta fase.

3.14.26. El contratista debe contemplar todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, entre otros) requerida para que el personal asignado al proyecto pueda cumplir sus funciones.

3.14.27. Mantener actualizados los niveles de Firmware de los componentes de acuerdo con las últimas versiones estables liberadas por el fabricante durante la vigencia del contrato.

3.15. SERVICIOS PROFESIONALES

3.15.1. La plataforma deberá incluir servicios profesionales de esquemas, estructuras, instalación, configuración, parametrización, puesta en funcionamiento y entrega a satisfacción, los cuales deberán ser ejecutados por ingenieros certificados por el fabricante. El contratista deberá presentar las certificaciones correspondientes del personal asignado al proyecto.

3.15.2. Los esquemas y estructuras de la plataforma deberán ser revisados y aprobados por el Supervisor del contrato, quien podrá solicitar ajustes o rediseños conforme a las necesidades de la Entidad.
3.15.3. Configuración y alistamiento del software, hardware y firmware a la última versión estable aprobada por el fabricante.
3.15.4. Implementación de la plataforma conforme a las mejores prácticas del fabricante, considerando una arquitectura de red segura.
3.15.5. Puesta en producción de las plataformas ofertadas.
3.15.6. Estabilización de las plataformas implementadas.
3.15.7. Entrega a satisfacción de la Entidad.
3.15.8. El contratista deberá realizar la configuración de políticas, objetos y parámetros necesarios, así como ejecutar pruebas que validen el correcto funcionamiento de la plataforma.
3.15.9. El contratista deberá incluir en su propuesta todos los costos logísticos asociados a la ejecución del proyecto, tales como desplazamientos, transporte, equipos, herramientas y demás gastos necesarios.
3.15.10. El contratista deberá registrar, gestionar y realizar seguimiento a todos los incidentes reportados por la Entidad, determinando su criticidad y el método de replataforma correspondiente.
3.15.11. Niveles de atención requeridos:

- **Nivel I:** atención inicial por agente de mesa de ayuda, mediante checklist y validación conjunta con la Entidad.
- **Nivel II:** atención por ingeniero especializado, de forma remota o presencial.
- **Nivel III:** escalamiento al soporte del fabricante, cuando la incidencia persista.

3.15.12. El soporte deberá ser prestado durante todo el periodo de garantía ofrecido.
3.15.13. El contratista deberá atender y resolver cualquier problema técnico bajo un esquema de atención 7x24x365, con personal especializado en la plataforma.
3.15.14. El contratista deberá adjuntar folletos, catálogos y fichas técnicas de los productos y servicios ofertados.
3.15.15. El contratista deberá documentar todos los procedimientos de instalación, configuración y parametrización de las funcionalidades implementadas, y entregarlos debidamente revisados y aprobados por el Supervisor del contrato.

4. SERVICIOS EN LA NUBE O DATACENTER Y ON PREMISE CONTRATISTA

Para los servicios que el contratista provea en la nube o Datacenter y on premise, deberá garantizar, como mínimo, lo siguiente:

a) Cifrado del tráfico entre la plataforma *on premise* suministrada y la plataforma en la nube.

b) Los accesos de los usuarios de la UAEJPMP, así como del contratista o terceros, deberán contar con controles de acceso mediante autenticación multifactor u otros mecanismos que minimicen el riesgo de accesos no autorizados.
c) Proveer los recursos necesarios para dar cumplimiento a lo requerido en los anexos técnicos.
d) La plataforma de seguridad deberá proteger tanto la plataforma tecnológica de la UAEJPMP como la plataforma provista por el contratista que soporta la plataforma descrita en los anexos técnicos.
e) Proveer los certificados y configuraciones necesarias para permitir accesos confiables, minimizando los riesgos sobre la confidencialidad, integridad y disponibilidad de la información institucional.
f) La plataforma en la nube o Datacenter y on premise, no deberá constituir un impedimento para el cumplimiento integral de los anexos técnicos exigidos.
g) Permitir el acceso a los logs de la plataforma e integración con el SIEM o SOC a suministrar.

5. SERVICIO GESTIONADO DE PROTECCION DE CORREO.

Suministrar, instalar, configurar e implementar una plataforma de protección de correo electrónico en Microsoft 365 como servicio en la nube, la cual deberá cumplir, como mínimo, con las siguientes características técnicas y funcionales:

5.1. Características Generales

a) La plataforma deberá estar basada en tecnología cloud, bajo la modalidad de Software como Servicio (SaaS).
b) Deberá contar con licenciamiento para un mínimo de mil seiscientos (1.600) buzones de correo electrónico.
c) El contratista deberá garantizar la implementación integral de la plataforma, incluyendo configuración, puesta en funcionamiento y pruebas.

5.2. Arquitectura y Funcionamiento

a) La plataforma deberá operar como Gateway SMTP en la nube, integrándose con los servidores de correo electrónico existentes.
b) Deberá actuar como MTA (Mail Transfer Agent) y funcionar de manera transparente, operando como proxy SMTP para el envío y recepción de mensajes.
c) Deberá permitir el análisis en tiempo real del correo entrante y saliente, incluyendo inspección de adjuntos y enlaces.
d) La plataforma deberá integrarse con el servicio de correo electrónico actual de la Entidad, aplicando filtrado bidireccional.
e) Deberá soportar listas blancas y negras a nivel de usuario, dominio y de forma global.

5.3. Seguridad, Protección y Detección de Amenazas

a) La plataforma deberá estar validada en rendimiento y seguridad por laboratorios de pruebas de terceros reconocidos en la industria.
b) Deberá contar con capacidades de Content Disarm & Reconstruction (CDR) para remover o neutralizar código malicioso o contenido no autorizado en archivos adjuntos.
c) La plataforma deberá analizar archivos adjuntos mediante técnicas de inspección antimalware, análisis estático y/o dinámico en sandbox, permitiendo bloquear o poner en cuarentena archivos con contenido malicioso o sospechoso
d) Deberá incluir un Network Sandbox del mismo fabricante, para la identificación y bloqueo de amenazas nuevas o desconocidas.
e) Deberá detectar y bloquear malware y phishing, analizando la reputación de las URLs en el momento del clic (Time-of-Click Analysis).
f) La plataforma deberá contar con mecanismos de detección de suplantación e impersonación de remitentes, incluyendo validaciones de autenticación del mensaje, anomalías de encabezado y análisis anti-phishing sobre remitente, dominio y señales de fraude.
g) La plataforma deberá contar con mecanismos de protección frente a comportamientos anómalos o campañas masivas de correo no deseado, permitiendo detectar, limitar, bloquear o poner en cuarentena mensajes sospechosos conforme a políticas
h) La plataforma deberá incorporar inteligencia de amenazas del fabricante para mejorar de forma continua la detección de spam, phishing y malware emergente.

5.4. Cifrado, Cumplimiento y Privacidad

a) La plataforma deberá permitir cifrado de correo basado en identidad y en políticas configurables, garantizando confidencialidad de extremo a extremo.
b) La plataforma deberá permitir cifrado de mensajes salientes mediante políticas configurables del fabricante, soportando al menos TLS, S/MIME y mecanismos de mensaje seguro.
c) Deberá contar con funcionalidades de Prevención de Pérdida de Datos (DLP).
d) La solución deberá disponer de documentación pública del fabricante sobre controles de seguridad, privacidad y protección de datos aplicables al servicio, así como de las certificaciones corporativas o compromisos de cumplimiento que el fabricante tenga publicados para sus servicios en la nube.

5.5. Gestión, Administración y Reportes

a) La plataforma deberá contar con una consola de administración web unificada, accesible desde cualquier ubicación, con gestión por roles y perfiles.

b) La plataforma deberá permitir sincronización de usuarios y buzones mediante servicios de directorio incluyendo como mínimo Active Directory y/o Microsoft Entra ID.
c) Deberá incluir un módulo de cuarentena accesible al usuario final, con opciones de reporte y liberación controlada de mensajes.
d) Deberá permitir la clasificación avanzada del correo por nivel de riesgo (spam, marketing, phishing, malware, URLs sospechosas).
e) Deberá contar con API REST para fines de monitoreo, automatización y orquestación.
f) La plataforma deberá contar con reportes nativos del fabricante y mecanismos de integración mediante API u otros métodos equivalentes para consulta, extracción o consumo de eventos y resultados de análisis.
g) La plataforma debe permitir integración con SOC o SIEM y sistemas de gestión de incidentes.
h) El contratista debe garantizar la operación y soporte del servicio 24x7x365, contar con personal con experiencia comprobada en administración de soluciones de seguridad de correo electrónico, y ofrecer altos niveles de disponibilidad y respaldo.
i) El contratista debe garantizar que la plataforma cuente con una consola unificada en la nube para monitoreo en tiempo real, configuración de políticas y generación de reportes, con alertas y notificaciones automáticas por correo electrónico ante incidentes.

5.6. Continuidad y Operación

a) La plataforma deberá contar con mecanismos de continuidad para consulta temporal de mensajes entrantes durante indisponibilidad del servicio principal, así como reintentos automáticos de entrega cuando el servicio vuelva a estar disponible
b) Deberá ser capaz de mantener colas de correo ante fallos de conectividad, retrasos o errores de entrega.
c) La plataforma deberá estar respaldada por un laboratorio de investigación y desarrollo con inteligencia de amenazas en tiempo real, garantizando actualizaciones automáticas frente a nuevas campañas de ataque.

5.7. SERVICIOS PROFESIONALES

5.7.1. La plataforma deberá incluir servicios profesionales de diseño, instalación, configuración, parametrización, puesta en funcionamiento y entrega a satisfacción, los cuales deberán ser ejecutados por ingenieros certificados por el fabricante. El contratista deberá presentar las certificaciones correspondientes del personal asignado al proyecto.
5.7.2. Los diseños de la plataforma deberán ser revisados y aprobados por el Supervisor del contrato, quien podrá solicitar ajustes o rediseños conforme a las necesidades de la Entidad.

5.7.3. Configuración y alistamiento del software, hardware y firmware a la última versión estable aprobada por el fabricante.
5.7.4. Implementación de la plataforma conforme a las mejores prácticas del fabricante, considerando una arquitectura de red segura.
5.7.5. Puesta en producción de las plataformas ofertadas.
5.7.6. Estabilización de las plataformas implementadas.
5.7.7. Entrega a satisfacción de la Entidad.
5.7.8. El contratista deberá realizar la configuración de políticas, objetos y parámetros necesarios, así como ejecutar pruebas que validen el correcto funcionamiento de la plataforma.
5.7.9. El contratista deberá incluir en su propuesta todos los costos logísticos asociados a la ejecución del proyecto, tales como desplazamientos, transporte, equipos, herramientas y demás gastos necesarios.
5.7.10. El contratista deberá registrar, gestionar y realizar seguimiento a todos los incidentes reportados por la Entidad, determinando su criticidad y el método de replataforma correspondiente.
5.7.11. Niveles de atención requeridos:

- **Nivel I:** atención inicial por agente de mesa de ayuda, mediante checklist y validación conjunta con la Entidad.
- **Nivel II:** atención por ingeniero especializado, de forma remota o presencial.
- **Nivel III:** escalamiento al soporte del fabricante, cuando la incidencia persista.

5.7.12. El soporte deberá ser prestado durante todo el periodo de garantía ofrecido.
5.7.13. El contratista deberá atender y resolver cualquier problema técnico bajo un esquema de atención 7x24x365, con personal especializado en la plataforma.
5.7.14. El contratista deberá adjuntar folletos, catálogos y fichas técnicas de los productos y servicios ofertados.
5.7.15. El contratista deberá documentar todos los procedimientos de instalación, configuración y parametrización de las funcionalidades implementadas, y entregarlos debidamente revisados y aprobados por el Supervisor del contrato.

6. SERVICIO DE GESTIÓN DE ACCESOS PRIVILEGIADOS.

6.1. Arquitectura General y Acceso Privilegiado

a) La plataforma deberá operar como única puerta de enlace entre la estación de trabajo del usuario y los sistemas administrados para el acceso privilegiado, permitiendo el aislamiento de recursos bajo el enfoque Zero Trust Network Access (ZTNA). El licenciamiento requerido será objeto para el acceso privilegiado por funcionarios con perfiles administradores de la UAEJPMP.

b) La plataforma deberá iniciar las sesiones privilegiadas desde la estación de trabajo del usuario hacia los sistemas gestionados, utilizando múltiples proxies de sesión, a través de un único portal web seguro HTTPS (HTML5).

c) La plataforma deberá soportar un motor distribuido para la administración de contraseñas y sesiones en segmentos de red aislados y regiones geográficas diferentes, manteniendo una administración centralizada de sistemas, políticas y accesos.
d) La plataforma no deberá requerir cambios en la topología de red existente para garantizar que todas las sesiones privilegiadas sean controladas por la plataforma.

e) La plataforma deberá basarse en una arquitectura sin agentes (agentless) para la administración de contraseñas y sesiones privilegiadas.

f) La plataforma deberá ser suministrada como servicio SaaS, y contar con certificaciones de la industria como ISO 27001:2022 y SOC 2 Type II.

g) La plataforma deberá permitir el despliegue de motores de puerta de enlace dentro de redes internas, para el establecimiento de sesiones con sistemas locales.

h) Los nodos de sesión no deberán requerir la recepción de tráfico entrante por ningún puerto TCP o UDP. Toda la comunicación de red deberá ser saliente (outbound), minimizando la superficie de ataque.

i) La plataforma no deberá imponer límites en la cantidad de motores de puerta de enlace desplegables, permitiendo la gestión de contraseñas y sesiones en múltiples redes y centros de datos distribuidos geográficamente.

j) El balanceo de carga de los motores de puerta de enlace deberá ser automático, sin requerir balanceadores externos.

k) Al ser una plataforma SaaS, el fabricante deberá proveer actualizaciones automáticas de seguridad, incluyendo parches y nuevas funcionalidades. En caso de requerirse interrupciones del servicio, deberá existir un mecanismo formal de notificación y autorización.

l) Los respaldos deberán realizarse de forma automática, las grabaciones de sesiones deberán almacenarse en la nube del fabricante y el servicio deberá garantizar una disponibilidad mínima del 99,7 %.

6.2. Descubrimiento de Sistemas y Cuentas

a) La plataforma deberá permitir la carga masiva de sistemas administrados, cuentas privilegiadas, usuarios finales y configuraciones asociadas.

b) Deberá contar con capacidades de descubrimiento automático de sistemas, incluyendo dirección IP, dirección MAC, nombre DNS, sistema operativo, versión, pertenencia a dominio Active Directory, cuentas existentes y privilegios asociados.
c) El descubrimiento de cuentas en Windows deberá incluir cuentas locales, cuentas de dominio que hayan accedido o tengan permisos de acceso, así como sus privilegios.
d) La plataforma deberá permitir la definición de atributos personalizados para sistemas administrados y cuentas privilegiadas.
e) La plataforma deberá gestionar contraseñas de cuentas privilegiadas y no privilegiadas, en sistemas conocidos y no conocidos, incluyendo, como mínimo:
   - Windows
   - Unix / Linux
   - Mac OS
   - Directorios (AD / LDAP)
   - Bases de datos
   - Dispositivos de red
f) El descubrimiento de cuentas y secretos deberá estar listo para usar, sin requerir servicios profesionales.
g) La plataforma deberá contar con un motor de descubrimiento distribuido, capaz de operar en redes aisladas y múltiples regiones geográficas, consolidando los resultados de forma centralizada.
h) La plataforma deberá descubrir Servicios y Tareas Programadas en Windows, permitiendo la gestión automática de las credenciales utilizadas.
i) La plataforma deberá descubrir cuentas de dominio de Active Directory y vincularlas automáticamente con servidores miembros específicos.
j) La plataforma deberá descubrir el software instalado y los puertos abiertos en los sistemas de destino.
k) La plataforma deberá permitir la agrupación de sistemas en función de atributos definidos manualmente o descubiertos automáticamente.
l) La plataforma deberá permitir la agrupación de sistemas y cuentas basada en consultas AD / LDAP.
m) La plataforma deberá enviar notificaciones por correo electrónico al detectar nuevos sistemas o sistemas no accesibles.
n) La plataforma deberá permitir la programación de tareas de descubrimiento e incorporación automática de nuevas cuentas privilegiadas.
o) La plataforma deberá descubrir cuentas locales en SQL Server, habilitando su auto-gestión.
p) La plataforma deberá descubrir instancias de máquinas virtuales en Hyper-V, VMware, Azure y Amazon Web Services.

6.3. Administración de Cuentas Privilegiadas y Gestión de Contraseñas

a) La plataforma deberá permitir cambios automáticos de contraseñas, listos para usar, en plataformas como sistemas operativos, bases de datos, directorios, dispositivos de red y aplicaciones empresariales.
b) Los cambios de contraseñas y secretos no deberán requerir servicios profesionales adicionales.
c) La plataforma deberá permitir la definición de múltiples políticas de contraseñas, aplicables por sistema o por cuenta.
d) La plataforma deberá permitir la aleatorización de contraseñas mediante cuentas de reconciliación, sin requerir conocimiento previo de las credenciales.
e) La plataforma deberá restablecer automáticamente las contraseñas al finalizar el tiempo de acceso autorizado.
f) La plataforma deberá soportar recuperación temporal de contraseñas, con restablecimiento automático al vencimiento.
g) La plataforma deberá permitir el desbloqueo de cuentas al cambiar la contraseña.
h) La plataforma deberá permitir definir la frecuencia de cambio de contraseña basada en fecha y hora.
i) La plataforma deberá permitir el cambio de contraseñas bajo demanda, individual o grupal.
j) La plataforma deberá verificar la integridad de contraseñas, corrigiendo discrepancias y notificando por correo electrónico.
k) La plataforma deberá actualizar automáticamente las contraseñas de Servicios y Tareas Programadas de Windows, con reinicio opcional de servicios.
l) La plataforma deberá permitir la sincronización de contraseñas entre cuentas seleccionadas.
m) La plataforma deberá mantener un historial de contraseñas accesible desde la interfaz web.
n) La plataforma deberá gestionar llaves SSH, incluyendo almacenamiento, rotación y generación (DSA, RSA).
o) La plataforma deberá permitir el cambio de llaves SSH bajo demanda.
p) Tras la rotación de contraseñas, la plataforma deberá ejecutar acciones adicionales, como reinicio de servicios o actualización de bóvedas cloud (Azure Key Vault, HashiCorp).

6.4. Gestión de Sesiones Privilegiadas (Sin VPN)

a) La plataforma deberá supervisar, grabar y controlar sesiones privilegiadas mediante RDP, SSH, HTTPS y otros protocolos, sin exponer contraseñas.
b) La plataforma deberá permitir la configuración de nuevas aplicaciones cliente para monitoreo de sesiones.
c) La plataforma deberá soportar clientes comerciales estándar (RDP, PuTTY, SecureCRT, WinSCP).
d) La plataforma deberá permitir limitar la cantidad de sesiones concurrentes por usuario.

e) La plataforma deberá permitir conexiones directas desde clientes nativos, manteniendo grabación y control.
f) La plataforma deberá mostrar mensajes de advertencia temporizados antes del vencimiento del acceso.
g) La plataforma deberá permitir el cierre forzado de sesiones al finalizar el tiempo autorizado.
h) La plataforma deberá registrar pulsaciones de teclas, permitiendo búsquedas por palabra clave.
i) La plataforma deberá enmascarar contraseñas durante la reproducción de sesiones.
j) La plataforma deberá bloquear comandos SSH prohibidos y notificar eventos críticos.
k) La plataforma deberá permitir búsquedas avanzadas en sesiones grabadas.
l) La plataforma deberá permitir la reproducción de sesiones desde el portal web, sin software adicional.
m) La plataforma deberá soportar reproducción avanzada (línea de tiempo, avance rápido).
n) La plataforma deberá permitir monitoreo en vivo e intervención en tiempo real.
o) La plataforma deberá permitir desactivar la grabación en casos específicos, manteniendo el inicio de sesión automático.
p) La plataforma deberá permitir el uso de cuentas no administradas en sesiones grabadas.
q) La plataforma deberá archivar sesiones por mínimo noventa (90) días, garantizando integridad y cifrado.

6.5. Gobierno, Auditoría, Automatización e Integraciones

a) La plataforma deberá garantizar segregación de funciones (RBAC), flujos de aprobación, auditoría completa, reportes predefinidos, integración con SIEM, ITSM, APIs REST, SDKs, y cumplimiento con Common Criteria, autenticación fuerte, SAML, AD, LDAP y RADIUS.
b) La plataforma deberá soportar integraciones nativas con plataformas de nube, automatización, Kubernetes, CIEM y PEDM.
c) La plataforma deberá ofrecer modelos de licenciamiento flexibles, sin límites de credenciales, secretos ni componentes proxy.
d) Las actualizaciones de software deberán estar documentadas y no requerir servicios profesionales obligatorios.

6.6. Interfaz de usuario

a) La plataforma deberá proporcionar una única interfaz web HTML5, mediante la cual los usuarios puedan realizar actividades relacionadas con el acceso a cuentas

privilegiadas, tales como solicitud de acceso, aprobación, reproducción de sesiones y consulta de trazabilidad y auditoría. Así mismo, la interfaz deberá permitir a los administradores la gestión de cuentas privilegiadas, perfiles de usuario, grupos, organizaciones, roles y políticas.

b) La plataforma deberá contar con una interfaz única de autoservicio, que permita a los usuarios solicitar cuentas y sesiones privilegiadas de manera controlada.
c) La plataforma deberá ofrecer una interfaz de autoservicio que permita al usuario autorizado recuperar credenciales y solicitar sesiones de acceso privilegiado por un periodo de tiempo limitado o de forma puntual.
d) La plataforma deberá permitir al usuario especificar la fecha y hora de inicio, la duración y la justificación al momento de solicitar una contraseña o una sesión de acceso privilegiado.
e) La plataforma deberá permitir al usuario visualizar y consultar solicitudes históricas, activas y pendientes.
f) Todos los módulos de la plataforma PAM, incluyendo el módulo de soporte remoto, deberán estar alojados en un único portal web, con el fin de simplificar la gestión, operación y solicitud de accesos.

6.7. Auditoría y Reportes

a) La plataforma deberá soportar auditoría completa y rendición de cuentas, registrando cada transacción asociada a solicitudes de contraseñas y sesiones privilegiadas.

b) La plataforma deberá registrar todos los cambios realizados por los administradores en la pista de auditoría, incluyendo, como mínimo: nombre de usuario, fecha y hora, actividad realizada, dirección IP y valores anteriores y nuevos.

c) La plataforma deberá proporcionar, de forma nativa y sin requerir componentes adicionales ni costos adicionales, los siguientes informes predefinidos:

- Informe de antigüedad de contraseñas, indicando la última fecha de cambio por cada cuenta administrada.
- Informe de actividades de usuario, con detalle transaccional de solicitudes y aprobaciones de contraseñas y sesiones.
- Informe de derechos de acceso, que detalle qué usuarios tienen acceso a qué cuentas.
- Informe de actividad de cambio de contraseñas, incluyendo motivo y resultado.
- Informe de programación de cambios de contraseña, con detalle de próximos cambios programados.

- Informe de inventario de activos, con listado de sistemas administrados y no administrados, agrupados por sistema operativo.
- Informe de inventario de cuentas, que incluya cuentas administradas y no administradas.
- Informe delta de cuentas, con altas y bajas por periodos diarios, semanales y mensuales.
- Informe de cuentas administradas versus no administradas.
- Informe de uso de cuentas de servicio, indicando los sistemas que utilizan cuentas de servicio para iniciar servicios de Windows.

d) La reportería de todos los módulos del PAM, incluyendo el módulo de soporte, deberá estar disponible en el mismo portal web, garantizando una visibilidad integral de las actividades privilegiadas.

6.8. Autenticación, Seguridad y Cumplimiento

a) La plataforma no deberá contener credenciales embebidas o codificadas que no puedan ser administradas.

b) La plataforma deberá integrarse con múltiples métodos de autenticación empresarial, incluyendo Active Directory, LDAP, Smart Card, RADIUS y otros mecanismos de autenticación robusta.

c) La plataforma deberá permitir autenticación integrada con Windows Active Directory y SAML, habilitando inicio de sesión único (SSO).

d) La plataforma deberá permitir la integración simultánea con múltiples directorios AD y/o LDAP.

e) La plataforma deberá admitir autenticación fuerte mediante RADIUS con doble factor (2FA).

f) La plataforma deberá permitir la revocación temporal de usuarios, evitando que estos realicen solicitudes de acceso privilegiado. Dicha revocación no deberá implicar la deshabilitación ni el bloqueo de la cuenta en AD o LDAP.

6.9. Automatización mediante API

a) La plataforma deberá exponer sus funcionalidades mediante un conjunto completo de servicios RESTful API, listos para usar, sin requerir componentes adicionales ni costos adicionales.

b) La plataforma deberá ofrecer un Kit de Desarrollo de Software (SDK) que permita atender casos especiales mediante el uso de APIs, facilitando el acceso

programático y en tiempo real a las contraseñas, sin necesidad de utilizar la interfaz gráfica del producto.

c) La plataforma deberá proporcionar RESTful APIs que permitan la administración programática de la plataforma, incluyendo, entre otros: creación, modificación y eliminación de sistemas y cuentas administradas, gestión de políticas de acceso, administración de usuarios, recuperación de credenciales y solicitud y lanzamiento de sesiones privilegiadas.

d) La plataforma deberá incluir documentación completa de las APIs, así como ejemplos de uso en, al menos, algunos de los siguientes lenguajes: Python, C#, Java, PowerShell, Ruby y Unix Shell Script.

6.10. Integraciones

a) La plataforma PAM deberá permitir integración nativa con otras soluciones PAM, tales como PEDM (Privileged Elevation and Delegation Management) y CIEM (Cloud Infrastructure Entitlement Management), para el control dinámico de privilegios en estaciones de trabajo, servidores y entornos cloud.

b) La plataforma deberá permitir integraciones nativas con plataformas de automatización, como Automation Anywhere y Blue Prism, para procesos que requieran accesos privilegiados.

c) La plataforma deberá permitir integraciones con External Secrets Operator y Secrets-Agent de Kubernetes.

6.11. Licenciamiento

a) La plataforma PAM deberá ofrecer dos modalidades de licenciamiento: por usuario (User-Based) o por dispositivo administrado (Asset-Based).

b) En caso de que la Entidad decida cambiar el modelo de licenciamiento posterior a la adquisición, dicho cambio deberá ser posible sin penalidades, permitiendo la migración entre modelos User-Based y Asset-Based.

c) El licenciamiento no deberá limitar la cantidad de cuentas privilegiadas ni secretos que puedan ser almacenados y gestionados; estos deberán ser ilimitados.

d) El licenciamiento no deberá limitar la cantidad de componentes proxy requeridos para el establecimiento de sesiones, procesos de descubrimiento o cambios automáticos de contraseñas.

6.12. SERVICIOS PROFESIONALES

6.12.1. La plataforma deberá incluir servicios profesionales de diseño, instalación, configuración, parametrización, puesta en funcionamiento y entrega a

satisfacción, los cuales deberán ser ejecutados por ingenieros certificados por el fabricante. El contratista deberá presentar las certificaciones correspondientes del personal asignado al proyecto.

6.12.2. Los diseños de la plataforma deberán ser revisados y aprobados por el Supervisor del contrato, quien podrá solicitar ajustes o rediseños conforme a las necesidades de la Entidad.

6.12.3. Configuración y alistamiento del software, hardware y firmware a la última versión estable aprobada por el fabricante.

6.12.4. Implementación de la plataforma conforme a las mejores prácticas del fabricante, considerando una arquitectura de red segura.

6.12.5. Puesta en producción de las plataformas ofertadas.

6.12.6. Estabilización de las plataformas implementadas.

6.12.7. Entrega a satisfacción de la Entidad.

6.12.8. El contratista deberá realizar la configuración de políticas, objetos y parámetros necesarios, así como ejecutar pruebas que validen el correcto funcionamiento de la plataforma.

6.12.9. El contratista deberá incluir en su propuesta todos los costos logísticos asociados a la ejecución del proyecto, tales como desplazamientos, transporte, equipos, herramientas y demás gastos necesarios.

6.12.10. El contratista deberá registrar, gestionar y realizar seguimiento a todos los incidentes reportados por la Entidad, determinando su criticidad y el método de replataforma correspondiente.

6.12.11. Niveles de atención requeridos:

- **Nivel I:** atención inicial por agente de mesa de ayuda, mediante checklist y validación conjunta con la Entidad.
- **Nivel II:** atención por ingeniero especializado, de forma remota o presencial.
- **Nivel III:** escalamiento al soporte del fabricante, cuando la incidencia persista.

6.12.12. El soporte deberá ser prestado durante todo el periodo de garantía ofrecido.

6.12.13. El contratista deberá atender y resolver cualquier problema técnico bajo un esquema de atención 7x24x365, con personal especializado en la plataforma.

6.12.14. El contratista deberá adjuntar folletos, catálogos y fichas técnicas de los productos y servicios ofertados.

6.12.15. El contratista deberá documentar todos los procedimientos de instalación, configuración y parametrización de las funcionalidades implementadas, y entregarlos debidamente revisados y aprobados por el Supervisor del contrato.

7. SERVICIO DE DETECCIÓN DE AMENAZAS EN REDES PÚBLICAS

Requerimientos Generales

7.1. La UAEJPMP requiere contar con capacidades de detección de amenazas en redes públicas, por lo cual solicita la adquisición de un servicio integral de monitoreo y protección de marca, el cual deberá cumplir, como mínimo, con las siguientes condiciones:

a) Protección de la marca para el dominio institucional.
b) Protección de al menos catorce (14) cuentas de ejecutivos y/o directivos de la Entidad.
c) Disponibilidad de un servicio de takedown, con un mínimo de veinte (20) incidentes gestionados por año.
d) Para la protección de ejecutivos y directivos, la plataforma deberá contar con capacidades avanzadas de monitoreo que incluyan reconocimiento facial basado en inteligencia artificial, permitiendo la comparación entre imágenes oficiales de los directivos y perfiles sospechosos detectados en redes sociales, con el fin de identificar posibles casos de suplantación visual.

7.2. El CONTRATISTA debe ejecutar acciones de detección y gestión de incidentes de suplantación de marca, incluyendo actividades de takedown de contenidos maliciosos (phishing, dominios fraudulentos, sitios web falsos u otros abusos de marca).

7.3. Para incidentes clasificados como críticos, el CONTRATISTA garantizará un tiempo máximo de inicio y gestión efectiva del proceso de takedown de hasta treinta (30) minutos contados a partir de la identificación o notificación del incidente.

7.4. El CONTRATISTA deberá contar con mecanismos automatizados, procedimientos establecidos y acuerdos con terceros (proveedores de hosting, registradores, plataformas, entre otros) que permitan cumplir con este nivel de servicio.

7.5. La plataforma deberá incorporar capacidades de inspección multimodal basadas en inteligencia artificial que permitan la identificación de abuso de marca mediante análisis simultáneo de imagen, texto y estructura de página, de manera que sea posible detectar fraudes aunque el contenido no contenga referencias textuales directas a la marca.

7.6. El servicio de monitoreo de marca deberá garantizar una detección integral y una respuesta oportuna, orientada a proteger la integridad, reputación y confianza asociadas a la marca de la UAEJPMP.

7.7. La plataforma deberá contar con capacidades avanzadas de detección de phishing, incluyendo la vigilancia de páginas falsas y URLs de redireccionamiento que utilicen indebidamente la marca de la UAEJPMP para aparentar legitimidad y engañar a los usuarios, induciéndolos a suministrar información sensible como credenciales, datos personales o financieros.

7.8. La plataforma deberá permitir la identificación del uso fraudulento de la marca, garantizando protección frente a asociaciones indebidas que puedan engañar, confundir o perjudicar a los usuarios de la Entidad.

7.9. La plataforma deberá permitir la detección de perfiles falsos en redes sociales, mediante la vigilancia de cuentas que utilicen indebidamente la marca para engañar a los usuarios.

7.10. La plataforma deberá contar con un módulo específico de monitoreo y detección de software malicioso tipo Banker Trojan, con capacidades de seguimiento de campañas activas que distribuyan este tipo de malware utilizando indebidamente la marca de la entidad.

7.11. La plataforma deberá permitir la identificación de dominios similares o look-alike que utilicen variaciones del nombre de la marca.

7.12. La plataforma deberá monitorear dominios en diferentes TLD que utilicen la marca con fines potencialmente fraudulentos.

7.13. La plataforma deberá realizar monitoreo del uso de la marca en plataformas de pago, con el fin de identificar posibles fraudes.

7.14. La plataforma deberá realizar el seguimiento de anuncios patrocinados que utilicen la marca de la UAEJPMP en el buscador de Google.

7.15. La plataforma deberá monitorear páginas web indexadas en motores de búsqueda y tiendas oficiales de aplicaciones, que ofrezcan descargas de aplicaciones o APKs que utilicen la marca de la UAEJPMP de manera indebida, fraudulenta o con fines maliciosos.

7.16. La plataforma deberá contar con la capacidad de identificar aplicaciones móviles falsas.

7.17. La plataforma deberá contar con capacidades de detección de piratería en línea, identificando productos falsificados o la distribución ilegal de contenido que pueda afectar la credibilidad de la marca UAEJPMP.

7.18. La plataforma deberá permitir la detección e inicio oportuno de procesos de takedown en marketplaces globales, con el fin de preservar la integridad de la marca y mitigar impactos económicos.

7.19. La plataforma deberá monitorear en tiempo real los anuncios patrocinados publicados en los principales motores de búsqueda (incluyendo Google Search Ads) que utilicen la marca de la entidad de manera indebida, con capacidad de alerta y gestión de remoción.

7.20. La plataforma deberá contar con mecanismos para la detección y remediación de distribución indebida de contenido protegido por derechos de autor en plataformas

de streaming y sitios de intercambio de contenido, incluyendo el uso de notificaciones DMCA y herramientas de Content ID para plataformas de video.

7.21. Algunas de las plataformas en las cuales se podrán realizar actividades de detección y remediación incluyen, entre otras:

a) Facebook.
b) YouTube.
c) eBay.
d) TikTok.
e) Amazon.

7.22. La plataforma deberá realizar monitoreo proactivo de la Surface Web, Deep Web y Dark Web, con el fin de detectar, analizar y responder a amenazas externas dirigidas a cuentas de alto valor.

7.23. La plataforma deberá permitir el monitoreo de información personal identificable (PII) de los ejecutivos y directivos de la UAEJPMP que pueda encontrarse expuesta en Internet.

7.24. La plataforma deberá contar con la capacidad de eliminar de forma expedita información personal expuesta (PII) en sitios de intermediarios de datos, así como de cerrar perfiles falsos en redes sociales, fortaleciendo la postura de seguridad de la Entidad.

7.25. La plataforma deberá permitir el descubrimiento de credenciales filtradas asociadas a los ejecutivos y directivos.

7.26. La plataforma deberá contar con capacidades de protección de la superficie de ataque, orientadas a prevenir la exposición de información confidencial que pueda derivar en ataques de spear phishing, ingeniería social u otras amenazas, para mínimo cuatro (4) IP públicas.

7.27. La plataforma deberá permitir la identificación de perfiles falsos en redes sociales asociados a los ejecutivos y/o directivos de la UAEJPMP.

7.28. El servicio de takedown deberá permitir la baja de sitios web, perfiles en redes sociales, aplicaciones móviles y nombres de dominio que suplanten a la Justicia Penal Militar en la Surface Web.

7.29. La plataforma deberá contar con inspección apoyada en inteligencia artificial (IA), que permita automatizar el análisis de múltiples señales para clasificar, priorizar y gestionar procesos de takedown de manera eficiente.

7.30. El servicio deberá permitir la notificación y gestión ante registradores de dominios y/o proveedores de hosting, previa autorización escrita de la UAEJPMP, para la eliminación de dominios maliciosos activos (por ejemplo, sitios de phishing).

7.31. La plataforma deberá contar con un mecanismo de notificación automática, propio del fabricante, que en paralelo al proceso de takedown notifique a un mínimo de quince (15) entidades globales de ciberseguridad (navegadores, proveedores de antivirus), con el fin de reducir la ventana de exposición del fraude mientras se completa la remoción

7.32. La plataforma deberá garantizar que la primera notificación de takedown se envíe en un plazo máximo de diez (10) minutos para al menos el cincuenta por ciento (50%) de los casos, y en un plazo máximo de treinta (30) minutos para al menos el noventa por ciento (90%) de los casos.

SERVICIOS PROFESIONALES

7.33. La plataforma deberá incluir servicios profesionales de diseño, instalación, configuración, parametrización, puesta en funcionamiento y entrega a satisfacción, los cuales deberán ser ejecutados por ingenieros certificados por el fabricante. El contratista deberá presentar las certificaciones correspondientes del personal asignado al proyecto.
7.34. Los diseños de la plataforma deberán ser revisados y aprobados por el Supervisor del contrato, quien podrá solicitar ajustes o rediseños conforme a las necesidades de la Entidad.
7.35. Configuración y alistamiento del software, hardware y firmware a la última versión estable aprobada por el fabricante.
7.36. Implementación de la plataforma conforme a las mejores prácticas del fabricante, considerando una arquitectura de red segura.
7.37. Puesta en producción de las plataformas ofertadas.
7.38. Estabilización de las plataformas implementadas.
7.39. Entrega a satisfacción de la Entidad.
7.40. El contratista deberá realizar la configuración de políticas, objetos y parámetros necesarios, así como ejecutar pruebas que validen el correcto funcionamiento de la plataforma.
7.41. El contratista deberá incluir en su propuesta todos los costos logísticos asociados a la ejecución del proyecto, tales como desplazamientos, transporte, equipos, herramientas y demás gastos necesarios.
7.42. El contratista deberá registrar, gestionar y realizar seguimiento a todos los incidentes reportados por la Entidad, determinando su criticidad y el método de replataforma correspondiente.
7.43. Niveles de atención requeridos:

- **Nivel I:** atención inicial por agente de mesa de ayuda, mediante checklist y validación conjunta con la Entidad.
- **Nivel II:** atención por ingeniero especializado, de forma remota o presencial.

- **Nivel III:** escalamiento al soporte del fabricante, cuando la incidencia persista.

7.44. El soporte deberá ser prestado durante todo el periodo de garantía ofrecido.
7.45. El contratista deberá atender y resolver cualquier problema técnico bajo un esquema de atención 7x24x365, con personal especializado en la plataforma.
7.46. El contratista deberá adjuntar folletos, catálogos y fichas técnicas de los productos y servicios ofertados.
7.47. El contratista deberá documentar todos los procedimientos de instalación, configuración y parametrización de las funcionalidades implementadas, y entregarlos debidamente revisados y aprobados por el Supervisor del contrato.

8. SERVICIO DE PRUEBAS DE INTRUSIÓN

8.1. ALCANCE DEL SERVICIO DE PENTESTING.

a) La Unidad Administrativa Especial de la Justicia Penal Militar y Policial requiere contratar un servicio de pruebas de seguridad informática (Pentesting) sobre la infraestructura y los servicios tecnológicos que soportan los procesos críticos misionales y de comunicaciones de la entidad.
El servicio deberá cubrir, como mínimo 6 servidores on premise, cuarenta (40) servidores virtuales con sistemas operativos Windows y Linux, así como mínimo cuatro (4) portales web alojados en ambientes de computación en la nube (AWS u homologables).
b) El contratista deberá ejecutar **dos (2) ejercicios anuales** de Pentesting, así como un (1) ejercicio de retesting, durante la vigencia del contrato, con el fin de verificar la efectividad de las acciones de mitigación implementadas.
c) El tipo de prueba requerido para la prestación del servicio será Pentesting de Caja Gris (Gray Box).
d) El servicio de Pentesting deberá permitir la identificación, validación y explotación controlada de vulnerabilidades técnicas, tanto desde fuentes externas (Internet) como desde la red interna, de acuerdo con los servicios y activos tecnológicos previamente definidos por la Entidad.
e) El servicio contratado deberá contribuir al cumplimiento de los requisitos normativos y regulatorios aplicables, incluyendo, entre otros, el Modelo de Seguridad y Privacidad de la Información (MSPI) y la Política de Gobierno Digital, o aquellas que las modifiquen o sustituyan.

8.2. ACTIVIDADES MÍNIMAS DEL SERVICIO

8.2.1. El servicio de Pentesting deberá contemplar, como mínimo, las siguientes actividades:

a) Suscripción de acuerdos de confidencialidad.
b) Gestión de accesos, autorizaciones y permisos requeridos.
c) Contextualización funcional y técnica del entorno evaluado.
d) Acceso controlado a la infraestructura, incluyendo pruebas de conectividad mediante VPN cuando aplique.

8.2.2. El servicio de Pentesting deberá incluir las siguientes actividades:
a) Identificación de activos tecnológicos activos.
b) Identificación de sistemas operativos.
c) Escaneo de puertos y servicios expuestos.
d) Identificación de aplicaciones y servicios en ejecución.
e) Detección de vulnerabilidades potenciales.
f) Generación del inventario inicial de vulnerabilidades.

8.2.3. El servicio de Pentesting deberá contemplar las siguientes actividades:
a) Análisis detallado del inventario de vulnerabilidades.
b) Identificación y validación de vulnerabilidades.
c) Enumeración técnica de las vulnerabilidades detectadas.
d) Categorización de vulnerabilidades de acuerdo con su nivel de severidad y criticidad.

8.2.4. El servicio de Pentesting deberá contemplar, de manera controlada, las siguientes actividades:
a) Pruebas sobre mecanismos de autenticación.
b) Pruebas de control de acceso.
c) Pruebas de exposición, captura o manipulación de datos, sin afectar la disponibilidad de los servicios.Pruebas sobre mecanismos de autenticación.
d) Pruebas sobre mecanismos de gestión de sesiones.
e) Pruebas de control de acceso.
f) Pruebas de exposición, captura o manipulación de datos, sin afectar la disponibilidad de los servicios.

8.2.5. El servicio de Pentesting deberá incluir, como mínimo, los siguientes productos y actividades:
a) Elaboración y entrega de la matriz de vulnerabilidades, con su respectiva clasificación y recomendaciones de mitigación.
b) Notificación inmediata a la Entidad en caso de identificación de vulnerabilidades críticas.
c) Elaboración y entrega de informe técnico, con el detalle de las pruebas realizadas, metodología utilizada y hallazgos.
d) Elaboración y entrega de informe ejecutivo, orientado a tomadores de decisión.
e) Presentación formal de los resultados a la Entidad.

9. SERVICIOS CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

9.1. REQUERIMIENTOS SERVICIO DE SOC CONTRATISTA

9.1.1. El contratista deberá prestar el servicio desde un Centro de Operaciones de Seguridad (SOC) ubicado en la ciudad de Bogotá D. C. (Colombia). La conexión se realizará mediante una conexión segura, utilizando los canales de conectividad definidos en el contrato. Así mismo, el contratista deberá prestar el servicio de administración, gestión y monitoreo de la seguridad informática sobre la plataforma tecnológica de la Unidad Administrativa Especial de la Justicia Penal Militar y Policial (UAEJPMP), a través de un Centro de Operaciones de Seguridad (SOC) con operación 7x24x365 o bajo el esquema "Follow the Sun". Para tal fin, el contratista deberá suministrar, administrar y operar una plataforma de correlación, análisis, detección y respuesta, o una plataforma equivalente de analítica y operaciones de seguridad, que permita la recolección, normalización, correlación, investigación y respuesta a eventos de seguridad.

9.1.2. 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.

9.1.3. Los procesos de gestión y operación deben estar basados en las mejores prácticas de acuerdo con los modelos de ITIL, CSIRT, ISO27001, NIST entre otros.

9.1.4. El SOC debe contar con equipo de respuesta a incidentes que sea miembro FIRST, debe demostrar la membresía del FIRST.

9.1.5. Certificación ISO/IEC 27001:2022, con alcance específico a servicios de SOC y/o ciberseguridad.

9.1.6. Certificación ISO 22301:2019, con alcance específico a servicios de SOC y/o ciberseguridad.

9.1.7. Membresía activa en la organización FIRST por un período mínimo de siete (7) años.

9.1.8. El contratista deberá contar con un Centro de Operaciones de Seguridad (SOC) conformado por personal calificado para el monitoreo continuo de los activos de información y la gestión de incidentes de seguridad las 24 horas y deberá garantizar la dedicación al 100% de (1) un analista de nivel II en modalidad 8x5.

9.1.9. EL CONTRATISTA debe disponer de las herramientas para el seguimiento de servicio, análisis de eventos, informes, cuadros de inteligencia y analítica de datos, adicionalmente, se debe contar con una línea de atención telefónica 24x7, correo electrónico y/o la matriz respectiva de escalamiento a través de la cual se pueda establecer comunicación entre las partes.

9.1.10. El servicio debe garantizar la disponibilidad, confidencialidad, integridad, no repudio, auditoria y privacidad de los datos y servicios soportados.

9.1.11. De forma permanente el servicio de monitoreo SOC realizará una valoración de las amenazas existentes en la región y el mundo, determinando cuál de estos exponen a un riesgo a la UAEJPMP, resumiendo los resultados en Boletines o Informes extraordinarios de SOC.

9.1.12. Los servicios de gestión de SOC realizarán seguimiento 7x24 a los ataques originados desde Internet al igual que los originados al interior de la UAEJPMP.

9.1.13. El SOC, debe definir la matriz de escalamiento de común acuerdo con los responsables de seguridad del contratista y de la UAEJPMP, clarificando el nivel de escalamiento según el tipo y nivel de incidente.

9.1.14. El servicio deberá detectar actividades inusuales, recolectar evidencias, correlacionar los eventos para el escalamiento y determinar si corresponde a un evento de seguridad, tendencias, falsos positivos, patrones o firmas de intruso las cuales deberán ser notificadas y documentadas.

9.1.15. El CONTRATISTA debe contemplar las herramientas que considere necesarias para contar con la inteligencia artificial para la detección de estos eventos Notificación proactiva de posibles amenazas de Malware, proporcionando soluciones y estrategias de mitigación, tomar medidas para proteger los sistemas y redes afectados o amenazados por la actividad de intrusos, y desarrollar otras estrategias de respuesta o plataforma alternativa.

9.1.16. Servicio de manejo de incidentes de SOC realizando el triage de los incidentes de seguridad mediante agentes de nivel I, II y III, correlación de eventos, respuesta ante incidentes, amenazas y ataques contra la plataforma tecnológica y los sistemas de información de la organización

9.1.17. Detectar y recolectar las evidencias de los eventos anómalos, que ocurran sobre la infraestructura de UAEJPMP y que puedan poner en peligro la seguridad de la misma.

9.2. SERVICIO DE GESTIÓN, MONITOREO Y CORRELACIÓN DE EVENTOS DE SEGURIDAD

9.2.1. El CONTRATISTA deberá suministrar, administrar y operar una plataforma centralizada de analítica y operaciones de seguridad, que permita la integración de múltiples fuentes de datos de seguridad, incluyendo telemetría proveniente de agentes, fuentes cloud y registros vía syslog; así como la recolección, ingesta, normalización, correlación, búsqueda, investigación y gestión de eventos de seguridad. La solución deberá permitir además la gestión de casos, automatizaciones y acciones de respuesta.

9.2.2. La solución propuesta deberá operar en entornos híbridos, incluyendo infraestructura on-premise, nube privada y/o nube pública, y deberá permitir la gestión centralizada, así como la ingesta, normalización y correlación de eventos de seguridad provenientes de múltiples fuentes integradas, tales como endpoints,

servidores, sistemas de identidad, servicios en la nube y recursos distribuidos en entornos locales y cloud.

9.2.3. La plataforma deberá estar desplegada en infraestructura en la nube, bajo modalidad Software as a Service (SaaS) del fabricante o Infraestructura as a Service (IaaS) en nube pública, garantizando alta disponibilidad del servicio y el cumplimiento igual o superior al 99,7%.

9.2.4. El contratista deberá proporcionar los recursos de cómputo requeridos (máquinas físicas y/o virtuales) en cada uno de los centros de datos Fortaleza y Palacio, para el despliegue de colectores de logs en esquema de alta disponibilidad, contemplando como mínimo un (1) colector por cada Data Center.

Este esquema deberá garantizar la continuidad en la recolección de eventos de seguridad, incluso ante la eventual falla de una de las sedes.

9.2.5. La plataforma deberá contar con capacidades de conectividad que permitan la integración de datos desde múltiples fuentes relevantes, mediante conectores nativos, APIs o colectores de logs. Deberá soportar, al menos, la ingesta de información proveniente de: endpoints, servidores, servicios en la nube, redes, sistemas de identidad, correo electrónico, dispositivos de seguridad, aplicaciones corporativas y otros sistemas críticos para la organización.

9.2.6. La plataforma deberá contar con licenciamiento de forma nativa con capacidades de UEBA (User and Entity Behavior Analytics), SOAR (Security Orchestration, Automation and Response) y deberá ofrecer modelo de licenciamiento por capacidad de ingesta fija en GB/día o EPS.

9.2.7. La plataforma deberá disponer de un catálogo robusto de acciones automatizadas para actividades de investigación, contención, remediación y respuesta.

9.2.8. La plataforma deberá incorporar capacidades de analítica basadas en inteligencia artificial y aprendizaje automático que permitan:
- Identificación de incidentes relevantes
- Priorización de alertas
- Generación de casos de seguridad consolidados
- Ejecución de acciones de respuesta automatizada.

9.2.9. La Plataforma debe disponer de un repositorio centralizado de datos administrado por el fabricante, que permita:
- Almacenamiento de telemetría de seguridad.
- Búsqueda e investigación de eventos.

- Correlación de información.
- Soporte a analítica avanzada.

9.2.10. La plataforma deberá incorporar capacidades de inteligencia artificial y machine learning para:

- Correlación automatizada de eventos
- Reducción de falsos positivos
- Agrupamiento inteligente de alertas
- Priorización de incidentes
- Análisis de causa raíz
- Automatización de la respuesta.

9.2.11. La plataforma deberá estar en la capacidad para realizar el servicio de monitoreo y correlación, como mínimo los siguientes dispositivos con capacidad de crecimiento:

- Números de equipos de cómputo en servicio en Bogotá:1300
- Numero de servidores on premise virtuales:40
- Numero de servidores on premise físicos:8
- Numero de servidores en AWS: 20
- Aplicaciones en AWS:15
- Numero de servicios WEB :5
- Numero de equipos de red LAN:130
- Numero de solución Trellix: Endpoint Security 1300 licencias de usuarios, Data Loss prevention (DLP) 170 licencias, ePolicy Orchestrator (ePO) consola de administración, Network Security (NX) AWS y Fortaleza, IPS (Intrusion Prevention System) 2 equipos IPS con una Manager virtualizado. los eventos de seguridad de las estaciones de usuario deberán ser enviados al SIEM desde la consola de la solución de Endpoint Protection / EDR de la Entidad (consolidados, enriquecidos y filtrados por la propia plataforma de endpoint) y no de forma directa desde cada estación individualmente.

9.2.12. la plataforma deberá permitir la ingesta, normalización, correlación y análisis de
eventos de seguridad provenientes de Microsoft 365, de los servicios existentes en AWS y de dispositivos de red on-premise, incluyendo mecanismos de recolección mediante API y recepción de logs vía syslog a través de colectores.

9.2.13. La plataforma propuesta debe contar con capacidades de análisis avanzadas, incluyendo aprendizaje automático y modelos de comportamiento, para identificar amenazas conocidas y desconocidas, reducir falsos positivos y priorizar alertas relevantes para su investigación.

9.2.14. La plataforma deberá contar con un repositorio centralizado de datos (data lake) diseñado para la seguridad, con capacidad mínima de almacenamiento para

la Entidad de mínimo 5 TB mensuales de telemetría o 100 GB logs por dia para la ingesta, normalización y retención de grandes volúmenes de eventos provenientes de múltiples fuentes (endpoint, red, nube, identidad y aplicaciones empresariales, entre otros), sin degradar el rendimiento de análisis ni la disponibilidad de consultas.

9.2.15. La plataforma deberá garantizar la retención de logs por un período mínimo de doce (12) meses, noventa (90) días hot/warm y 9 meses congelados.

9.2.16. La plataforma debe incluir una herramienta visual e interactiva que represente de manera gráfica las relaciones entre entidades involucradas en un incidente de seguridad (como usuarios, direcciones IP, endpoints y archivos). Esta funcionalidad debe facilitar la comprensión del alcance de la amenaza, identificar la causa raíz y apoyar el análisis contextual durante las investigaciones, permitiendo a los analistas visualizar el flujo de eventos y sus correlaciones.

9.2.17. La plataforma deberá generar de manera automática y nativa una línea de tiempo cronológica unificada (Smart Timeline o equivalente) por cada usuario y entidad (host, cuenta de servicio, dirección IP, dispositivo) involucrados en una investigación, sin requerir que el analista escriba consultas en lenguajes propietarios (SPL, KQL, ESQL u otros). La línea de tiempo deberá presentar todos los eventos correlacionados de la sesión, sus puntajes de riesgo individuales y acumulados

9.2.18. La plataforma deberá incluir un mínimo de 1.500 modelos de detección preconstruidos por el fabricante, basados en técnicas de aprendizaje automático supervisado y no supervisado. Estos modelos deberán estar disponibles para su activación inmediata, sin necesidad de desarrollo adicional, escritura manual de reglas ni contratación de servicios profesionales por parte de la Entidad o el contratista. Adicionalmente, estos modelos deberán actualizarse de forma automática a través del contenido proporcionado por el fabricante durante toda la vigencia del contrato.

9.2.19. La plataforma deberá implementar risk scoring acumulativo por sesión de usuario y por entidad, donde múltiples eventos de bajo riesgo individual sumen un puntaje agregado que dispare alertas cuando supere un umbral configurable.

9.2.20. Todas las labores de configuración de la plataforma de monitoreo y correlación de eventos y la generación de los casos de uso para el monitoreo SOC deberán ser ejecutadas por el personal asignado en el contrato.

9.2.21. La Plataforma debe realizar publicaciones periódicas de inteligencia actualizada, como reportes técnicos, recomendaciones urgentes, alertas sobre

amenazas emergentes, análisis de actores de amenazas y actividades maliciosas, accesibles desde la plataforma.

9.2.22. La plataforma deberá proveer un mecanismo de enriquecimiento automatizado de alertas que, al identificar entidades como direcciones IP, hashes de archivos, hashes de programas, dominios o URLs, incorpore información de inteligencia adicional obtenida de fuentes internas y externas.

9.2.23. La Plataforma debe ofrecer integración con fuentes externas de inteligencia, para validar la reputación de los indicadores observados.

9.2.24. La plataforma deberá disponer de APIs de inteligencia de amenazas que permitan la consulta y descarga automatizada de indicadores de compromiso (IoCs) e informes de inteligencia, en formatos estructurados y de forma segura.

9.2.25. El CONTRATISTA deberá suministrar, administrar y operar una plataforma que permita la recolección y análisis de datos provenientes de logs, endpoints y telemetría de red, incluyendo metadatos de tráfico, registros normalizados de comunicaciones y NetFlow, con capacidades de correlación, investigación y detección de eventos de seguridad.

9.2.26. La plataforma deberá contar con mecanismos para la detección y prevención de amenazas como:

- Malware conocido y desconocido, incluyendo amenazas de día cero.
- Técnicas y tácticas de adversarios (TTPs), con referencia al marco MITRE ATT&CK.
- Actividades sin archivos (fileless), mediante detección basada en comportamiento o indicadores de ataque.
- Ejecución de scripts maliciosos, comandos sospechosos, drivers no autorizados, manipulación de registros y procesos anómalos.
- Comportamientos asociados a ransomware, incluyendo actividades preparatorias o de ejecución maliciosa identificables en la telemetría disponible.
- Movimientos laterales, acceso no autorizado y posibles actividades asociadas al compromiso de credenciales, observables en la telemetría integrada.
- Capacidades de respuesta y remediación sobre equipos soportados, tales como detención de procesos sospechosos, exploración de carpetas, eliminación de archivos y ejecución remota de comandos para investigación y contención.

9.2.27. La plataforma deberá realizar la recolección, integración, normalización, análisis, almacenamiento, inteligencia de amenazas y visualización mediante tableros, soportando la incorporación de nuevas fuentes de datos, agentes y colectores adicionales de acuerdo con las necesidades de crecimiento, de UAEJPMP , sin afectar la disponibilidad del servicio.

9.2.28. La Plataforma podrá ser provista en entornos híbridos como on-premise o nube privada o nube pública, con conectividad segura hacia las fuentes de datos mediante mecanismos de comunicación cifrada, sin comprometer la seguridad o integridad de la información de UAEJPMP.

9.2.29. La plataforma deberá tener capacidad para integrar en su monitoreo los servicios de la entidad de seguridad de endpoint Trellix.

9.2.30. La plataforma deberá soportar una ingesta de 6 TB mensual/165 GB por día o 3500 EPS.

9.2.31. La plataforma debe tener capacidad de correlacionar eventos entre capas para una detección más precisa.

9.2.32. La plataforma deberá contar con capacidades nativas de detección de comportamiento anómalo de cuentas y entidades observadas en la telemetría integrada, mediante correlación, detectores o analítica contextual, sin requerir herramientas externas.

9.2.33. La plataforma debe permitir la integración con otros sistemas de seguridad mediante APIs, conectores y protocolos estandarizados.

9.2.34. UAEJPMP y el contratista verificaran los recursos mínimos necesarios para el correcto funcionamiento de la sonda que operará como colector de logs, asegurando la disponibilidad de infraestructura, conectividad y acceso a los sistemas requeridos para la recolección, transmisión y almacenamiento de la información.

9.2.35. La plataforma debera permitir la ingesta de fuentes multientorno: on-premise, cloud e híbrido.

9.2.36. La plataforma deberá contar con capacidades de automatización para la detección, clasificación y priorización de alertas e incidentes de seguridad, así como para la generación automática de reportes. Además, deberá permitir la notificación de eventos mediante correo electrónico y su gestión a través del sistema de tickets provisionado por el contratista.

9.2.37. La plataforma deberá tener capa de inteligencia de amenazas propia (IoCs, IoAs) para ayudar durante la Investigación de una alerta o incidente, proporcionando la contextualización del ataque/brecha.

9.2.38. La plataforma deberá tener recolección en tiempo real de logs desde múltiples fuentes, incluyendo dispositivos de red, seguridad, servidores, aplicaciones, servicios en la nube entre otros, mediante agentes, colectores o conectores que garanticen la operatividad completa de los servicios a monitorear.

9.2.39. La plataforma deberá permitir la correlación avanzada de eventos mediante reglas personalizadas, detectores avanzados y modelos de comportamiento, para apoyar la identificación de actividades maliciosas o anómalas, incluyendo escenarios de compromiso de cuentas, movimientos laterales, exfiltración de datos, comportamientos inusuales de usuarios y otras técnicas asociadas al marco MITRE ATT&CK.

9.2.40. El acceso a la consola deberá incluir soporte para autenticación multifactor (MFA) e integración con sistemas de autenticación SSO.

9.2.41. La plataforma deberá contar con un mecanismo de protección para evitar la desinstalación no autorizada de los sensores o agentes instalados. Este

mecanismo deberá requerir, al menos, una validación desde la consola central por parte de un usuario con perfil autorizado.

9.2.42. El servicio deberá incluir soporte técnico, gestión de actualizaciones, parches, y mantenimiento preventivo y correctivo de la plataforma.

9.2.43. Generación La plataforma deberá permitir la generación de informes, tableros y evidencias configurables para apoyar procesos de auditoría, gobierno, seguimiento y cumplimiento de controles de seguridad de la información, mediante reportes personalizados y programados construidos a partir de eventos y detecciones, así como el uso de plantillas predefinidas, dashboards personalizables y exportación de resultados.

9.2.44. Integración con fuentes de inteligencia de amenazas nacionales e internacionales para enriquecer la detección y priorización de eventos.

9.2.45. Una vez integrada toda la plataforma tecnológica, el contratista configurará y afinará la herramienta de correlación para mejorar su funcionalidad, tomando como base al menos los siguientes eventos:

a) Actividades asociadas a la administración de cuentas de usuario final (UserID).
b) Actividades asociadas a cuentas de altos privilegios, automáticas de procesos o asignadas a usuarios administradores (root, sa, administrator).
c) Ejecución de comandos especiales sobre sistemas operativos.
d) Ejecución de comandos especiales sobre bases de datos (dump,drop, delete, insert, update).
e) Cambios de parámetros técnicos, de configuración o de seguridad.
f) Cambios de configuración horaria.
g) Cambios no autorizados en recursos tecnológicos críticos.
h) Actividades de conexión de cuentas de usuario final o administradores.
i) Actividades asociadas a manipulación de bitácoras técnicas (LOGs) o interrupciones en el envío de los LOGs.
j) Actividades asociadas a conexión de acceso remoto.
k) Actividades asociadas a la no efectividad de controles en el ejercicio del monitoreo transaccional.

9.2.46. Ante pérdida de conectividad entre los colectores on-premise y la plataforma, los colectores deberán mantener buffer local con capacidad mínima de setenta (70) horas de eventos al volumen nominal de ingesta proyectado, con reenvío automático y ordenado al restablecerse la conexión, sin pérdida de eventos ni alteración de la línea de tiempo. Los colectores deberán generar alertas de salud al SOC ante (i) pérdida de conectividad superior a cinco (5) minutos, (ii) buffer local superior al 60% de capacidad, (iii) caída del proceso de recolección.

9.2.47. Todas las acciones realizadas por los analistas del SOC del contratista en la consola del SIEM (consultas, modificaciones de reglas, cambios de severidad, cierre de incidentes, ejecución de playbooks SOAR, acciones de respuesta sobre activos de la Entidad) deberán quedar registradas en una bitácora de auditoría con los siguientes atributos mínimos: (i) identificación del analista, (ii) timestamp

en hora legal colombiana, (iii) acción ejecutada, (iv) objeto afectado, (v) resultado. La bitácora deberá conservarse por mínimo seis (6) meses, ser inmutable y accesible para auditoría por parte de la Entidad mediante consola dedicada o exportación periódica.

9.2.48. El CONTRATISTA debe realizar transferencia de conocimiento al Supervisor y funcionarios de apoyo del contrato sobre el servicio aplicado del modelo de operación del SOC, tanto a nivel del CONTRATISTA como del implementado para la ENTIDAD, asegurando su correcta ejecución, supervisión y alineación con los procedimientos y niveles de servicio establecidos.

9.2.49. La plataforma deberá permitir la creación de consultas personalizadas, así como la generación de tableros y reportes configurables. Estas consultas o reportes deberán poder programarse y notificar su disponibilidad automáticamente por correo electrónico a usuarios autorizados.

9.2.50. La plataforma deberá proporcionar visibilidad completa del entorno tecnológico de la organización a través de una consola de administración centralizada. Esta visibilidad debe incluir información en tiempo real e históricos sobre activos, accesos y aplicaciones, accesibles desde la consola central de la plataforma.

9.2.51. El servicio de monitoreo SOC deberá mantener sincronizados todos los relojes de la herramienta con la hora legal colombiana, suministrada por el Instituto Nacional de Metrología de Colombia (https://inm.gov.co/servicios/hora-legal/).

9.2.52. Las herramientas adicionales que deba utilizar el contratista, tales como hardware, software, firmware, utilitarios o appliances, deben cumplir con la regulación de derechos de autor y propiedad intelectual. Así mismo, deben contar con soporte, mantenimientos y actualizaciones del fabricante o proveedor.

9.2.53. Dentro del plan de trabajo deberá especificar la metodología que utilizará para administrar, configurar, monitorear y gestionar el servicio de monitoreo objeto del presente contrato, especificando etapas, recursos, entregables, herramientas y técnicas a utilizar.

9.2.54. El Contratista deberá contar con personal profesional titulado en Ingeniería de Sistemas, Electrónica o Telecomunicaciones o afines, con más de 2 años de experiencia en operaciones de SOC, administración de plataformas de gestión y correlación de eventos de seguridad y monitoreo continuo de seguridad, capaz de gestionar alertas, incidentes y análisis de información de manera eficiente, asegurando la disponibilidad y confiabilidad del servicio.

9.2.55. Nota: El UAEJPMP se reserva el derecho de ajustar aspectos de la metodología.

9.2.56. La plataforma

9.2.57. La solución

9.2.58. La solución

9.2.59. FABRINCTAS

Elaboro: Ingeniero Oscar Leonardo Perez Casilimas