ANEXO TECNICO 01 ESPECIFICACIONES TÉCNICAS SEGURIDAD PERIMETRAL

SOLUCIÓN DE NEXT GENERATION FIREWALL RENOVACIÓN FIREWALLS PA – 450

RENOVACIÓN DE LA SUSCRIPCIÓN Y CONTRATO DE SOPORTE PREMIUM - FIREWALL PA (Seguridad Informática perimetral)

Servicio de renovación y soporte técnico por 12 meses para la plataforma de seguridad perimetral compuesta por:

Ítem	Número de Producto	Número de Serial	Cantidad
FW-1	**PAN-PA-450**	**0-23201011564**	**1**
FW-2	**PAN-PA-450**	**0-23201011003**	**1**

Los servicios para renovar corresponden a:

No	Cantidad	DESCRIPCIÓN / SKU	SERIAL
1	1	PAN-PA-450-BND-CORESEC-R PA-450, Precision AI Network Security Subscription Renewal Bundle (Advanced Threat Prevention, Advanced URL Filtering, Advanced Wildfire, Advanced DNS Security and SD-WAN), 1 year (12 months)	0-23201011564
2	1	PAN-PA-450-BND-CORESEC-R PA-450, Precision AI Network Security Subscription Renewal Bundle (Advanced Threat Prevention, Advanced URL Filtering, Advanced Wildfire, Advanced DNS Security and SD-WAN), 1 year (12 months)	0-23201011003
3	1	PAN-SVC-PREM-450-R PA-450, Premium support, 1 year (12 months), term, renewal	0-23201011003
4	1	PAN-SVC-PREM-450-R PA-450, Premium support, 1 year (12 months), term, renewal	0-23201011564

El proveedor prestará el servicio de soporte correspondiente al SKU PAN-SVC-PREM-450-R PA-450, Premium Support, 1 year (12 months), de acuerdo con las condiciones establecidas de los niveles de soporte, incluyendo disponibilidad 24/7 para todas las severidades de incidentes, tiempos de respuesta específicos según la criticidad del incidente y el acceso a ingenieros especializados para una resolución rápida y efectiva de problemas. Además, el proveedor garantizará la entrega de actualizaciones de software, mejoras de seguridad y reemplazo de hardware, conforme a las políticas del fabricante.

ANEXO TECNICO 01 ESPECIFICACIONES TÉCNICAS SEGURIDAD PERIMETRAL

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS REQUERIDAS	CUMPLE	NO CUMPLE
1.0	**GENERALIDADES**		
1.1	Para todos los equipos y accesorios (hardware y software) del presente proceso el servicio de soporte debe ser por un (1) año con reemplazo de partes de fábrica 24x7x4 y actualización del software adquirido a través del contratista a la última versión estable liberada por fabricante, para lo cual el oferente deberá adjuntar certificación firmada por el representante legal o quien haga sus veces.		
1.2	Todas las licencias que requieran los equipos para su funcionamiento deben quedar activas por un término de un año, suministrando los documentos de fabricante que las avale.		
1.3	Se deberá proporcionar una cuenta de acceso al portal oficial de soporte del fabricante, donde la Entidad tendrá la potestad de dar seguimiento a los casos abiertos de soporte.		
2	**EXPERIENCIA:** Con el propósito de mitigar riesgos operativos y garantizar la idoneidad en la ejecución del objeto contractual, el proponente deberá acreditar su capacidad operativa mediante el cumplimiento de los siguientes criterios de experiencia: Alcance y Similitud: El oferente deberá aportar certificaciones de contratos ejecutados cuyo objeto sea igual, similar o complementario a la implementación y administración de soluciones de seguridad perimetral y protección de endpoints. Temporalidad: Los contratos aportados deben haber sido ejecutados y terminados (o tener un acta de recibo a satisfacción) dentro de los últimos cinco (5) años anteriores a la fecha de cierre del presente proceso, garantizando así la vigencia técnica del proponente frente a amenazas cibernéticas actuales. Cantidad de Certificaciones: La experiencia se deberá acreditar mediante un mínimo de dos (2) y un máximo de cinco (5) certificaciones de contratos celebrados con entidades públicas o privadas. Suficiencia Financiera en Experiencia: La sumatoria del valor de los contratos aportados (expresados en SMMLV o en la moneda del proceso) deberá ser igual o superior al 100% del presupuesto oficial asignado para la presente contratación. [NOTA] Las certificaciones presentadas deben permitir la validación clara del objeto, valor, fecha de ejecución y cumplimiento satisfactorio de las obligaciones, con el fin de asegurar que el proponente cuenta con la solidez necesaria para la correcta prestación del servicio.		
3	**EXPERIENCIA DEL PERSONAL:** Con el objetivo de garantizar la correcta implementación, optimización y puesta en marcha de las soluciones de seguridad perimetral, el proponente deberá presentar un equipo de profesionales que cumpla con los siguientes criterios de experiencia y suficiencia técnica: Alcance de la Experiencia: Cada profesional asignado al proyecto deberá acreditar experiencia específica en actividades de implementación, despliegue, arquitectura de configuración y tunning (ajuste fino) de la solución tecnológica ofertada.		

	Certificación de Participación: El oferente deberá anexar a la propuesta una (1) certificación por cada profesional, la cual deberá ser expedida por la empresa o entidad (pública o privada) donde se ejecutó el proyecto. Dicha certificación debe detallar de forma clara las funciones técnicas desempeñadas. Temporalidad de la Experiencia: La experiencia certificada debe haberse desarrollado dentro de los últimos tres (3) años anteriores a la fecha de cierre del proceso, asegurando que el personal posee conocimientos actualizados sobre las versiones vigentes y vectores de ataque contemporáneos. Naturaleza de los Proyectos: Los proyectos certificados deben ser iguales o similares al objeto de la presente contratación, demostrando capacidad para gestionar infraestructuras de seguridad crítica bajo estándares de alta disponibilidad. Nota: La Entidad se reserva el derecho de validar la vigencia de las certificaciones técnicas del fabricante que posean los profesionales, con el fin de asegurar que cuentan con el respaldo oficial de la marca ofertada.		
4	**CERTIFICACIÓN DEL FABRICANTE** El proponente deberá presentar una certificación oficial emitida por el fabricante Palo Alto Networks, en la cual conste que el proponente es un Canal Certificado y Autorizado, condición que lo acredita como idóneo para diseñar, implementar, instalar y poner en funcionamiento la solución de NGFW (Next Generation Firewall) y Cortex XDR ofertada. Dicha certificación deberá evidenciar que el proponente cuenta con la homologación de partner en el nivel más alto de membresía del fabricante, correspondiente al nivel **Diamond Innovator** dentro de su programa de canales. La certificación deberá encontrarse vigente al momento de la presentación de la oferta.		
5	**SEGURIDAD DE LA INFORMACION**		
5.1	El proponente debe acreditar que cuenta con certificación vigente bajo la norma **ISO/IEC 27001 – Sistema de Gestión de Seguridad de la Información**, expedida por un organismo certificador acreditado. El proponente se obliga a mantener dicha certificación vigente durante toda la ejecución del contrato y a aportar, cuando la Entidad lo requiera, los documentos que evidencien su validez y alcance.		

1.2 SOPORTE TÉCNICO ESPECIALIZADO 5x8

El proveedor brindará Soporte Técnico Especializado por un término de 12 meses en un modelo 5x8 a través de un Centro de Soporte Autorizado (CAS) de Palo Alto Networks, asegurando que dicho centro brinde una atención personalizada y localizada garantizando los siguientes servicios:

- **a. Atención y resolución de incidentes.** El Proveedor atenderá de manera oportuna y eficiente las solicitudes de soporte técnico presentadas por la INC, ya sea de forma presencial o remota. La atención se realizará a través de un canal de comunicación establecido entre las partes, garantizando la trazabilidad de las solicitudes y la asignación de recursos necesarios para su resolución.
- **b. Atención de Solicitudes de Servicio.** El Proveedor atenderá solicitudes de servicio de

consulta o asesoría relacionados con la configuración de la plataforma, cambios de configuraciones, generación de reportes de uso, monitoreo proactivo y cualquier otra solicitud que permita optimizar y mejorar, mas no limitarse a:

- Políticas de Seguridad
- Configuración de Puertos
- Calidad de Servicio (QoS)
- VPN SSL
- VPN Site to Client
- VPN site to Site
- NAT
- Enrutamiento
- Usuario

La cantidad máxima de casos mensuales para solicitudes de servicios, consultorías y cambios de configuración es de 10, que pueden ser acumulables y consumibles dentro de la ejecución del contrato de 12 meses hasta de 120 casos.

c. Mesa de Servicios. El proveedor deberá contar con una Mesa de Servicios activa y operativa, la cual servirá como el punto único de contacto para la recepción, registro, gestión y seguimiento de todas las solicitudes de servicio, incluyendo incidentes, problemas y consultas relacionadas con la plataforma. La atención deberá realizarse a través de los siguientes canales:

Canal	Disponibilidad
Línea de atención telefónica	5 x 8
Correo electrónico	5 x 8
Celular de soporte	7 x 24
Herramienta Web	5 x 8

El proveedor se compromete a asegurar que estos canales cuenten con el personal y herramientas necesarias para gestionar los casos de manera eficiente y a proporcionar un sistema de registro de casos para realizar el seguimiento y reporte de todas las solicitudes.

d. Soporte del Fabricante: Soportar consultas técnicas y gestión de problemas con el fabricante.

e. Soporte Técnico en Sitio: Disponer del personal necesario para brindar soporte en sitio cuando la naturaleza del incidente lo requiera o a solicitud de la INC para la resolución de problemas críticos o de alta complejidad que no puedan resolverse de forma remota. El proveedor deberá garantizar la disponibilidad del personal para atención en sitio en los horarios acordados, con los tiempos de respuesta que permitan cumplir los ANS acordados. El alcance del soporte en sitio incluirá diagnóstico, verificación de hardware y software, ajustes de configuración y cualquier otra actividad necesaria para la resolución de incidentes. En caso de requerir apoyo especializado, el personal en sitio contará con canales de escalación a especialistas remotos.

f. Reemplazo de Partes y Piezas: Apoyar y coordinar el proceso de reemplazo de partes.

g. Actualización de Software: Asistir y guiar a la INC en el proceso de actualización de software, asegurando la correcta implementación de los parches de seguridad y mejoras de rendimiento, conforme a las recomendaciones del fabricante. Proporcionar orientación técnica durante la instalación de las actualizaciones, conforme a las recomendaciones del fabricante y las políticas del contrato de soporte vigente. Realizar verificaciones post-actualización para garantizar el correcto funcionamiento del sistema y optimizar la seguridad y el rendimiento de la infraestructura.

h. Consultas Técnicas: Proporcionar asesorías técnicas a la INC para orientar en la

adopción de las mejores prácticas en el uso de la plataforma soportada. Estas asesorías pueden ser capacitaciones sobre la infraestructura de seguridad implementada. (Se incluyen hasta 2 capacitaciones remotas, cada una de 4 horas para 4 personas).

i. **Generar Reportes de gestión e indicadores:** El proveedor deberá elaborar y entregar un reporte mensual de gestión que permita evaluar el desempeño y la seguridad de la infraestructura administrada. Los reportes deberán incluir análisis de tendencias o patrones relevantes basados en los datos históricos generados por las plataformas permitiendo identificar comportamientos anómalos, mejoras potenciales y riesgos emergentes, contribuyendo a una mejor toma de decisiones por parte de la INC. Al inicio del contrato, las partes acordarán la estructura, las métricas y los indicadores específicos que serán incluidos en el informe, asegurando que estén alineados con las necesidades de la INC y sean generados por las plataformas administradas. Las métricas, datos e indicadores utilizados en los reportes serán aquellos que las plataformas administradas puedan generar de manera nativa. Para cualquier reporte específico o personalizado que no sea generado directamente por las plataformas, se deberá llevar a cabo un proceso de evaluación de viabilidad técnica y factibilidad operativa antes de comprometer su entrega.

j. **Documentación y reporte de actividades.** El proveedor deberá notificar y reportarlas actividades realizadas en la plataforma producto de la gestión a su cargo. El reporte deberá incluir el nivel de detalle necesario que le permita a la INC garantizar la transferencia de conocimiento, así como la calidad y trazabilidad de las actividades realizadas.

1.3 SOPORTE TÉCNICO POR DEMANDA 7X24

El Proveedor se compromete a ofrecer soporte en horario no hábil bajo un modelo de horas por demanda, con un total de hasta 40 horas contratadas para cubrir las necesidades de la INC fuera del horario estándar 5x8. Los servicios proporcionados en este soporte 7x24 serán los mismos que en el soporte regular 5x8, incluyendo asistencia técnica, actualización de software, consultas técnicas y demás actividades descritas en el contrato. Definición del Horario No Hábil: De lunes a viernes: Desde las 06:00 pm hasta las 08:00 am del día siguiente. Sábado: Desde las 00:00 hasta las 11:59 pm. Domingo: Desde las 00:00 hasta las 08:00 am del lunes siguiente. Este soporte está destinado a garantizar la continuidad y disponibilidad de los servicios críticos del de la INC en horarios extendidos, asegurando respuesta y asistencia oportuna en caso de incidentes que se presenten durante los periodos no hábiles. Se descontará 1 hora por cada hora consumida en horarios no hábil de lunes a viernes o consumida en fines de semana y festivos y horarios nocturnos.

ANEXO TECNICO 01 ESPECIFICACIONES TÉCNICAS SEGURIDAD PERIMETRAL

UPGRADE SOLUCIÓN DE ENDPOINT PROTECTION CORTEX XDR PRO

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS REQUERIDAS	CUMPLE	NO CUMPLE
1	**DESCRIPCIÓN**		
1.1	Cantidad: 340 Licencias. Marca: Upgrade de licenciamiento para la plataforma Cortex XDR Pro (PAN-XDR-ADV-EP) Cada uno de ellos con las siguientes características:		
1.2	La entidad requiere una solución de Extended Detection & Response (XDR), tecnología que extiende las capacidades de respuesta fuera del endpoint tradicional (EDR)		
1.3	La tecnología debe incluir acciones de respuesta a incidentes y permitir la integración con soluciones de SOAR (Security Orchestration Automation & Response)		
1.4	La solución debe ser reconocida como líder en el último reporte del año 2024 de Forrester Wave: Endpoint Security as a Service		
1.5	La solución debe haber participado en las rondas de pruebas de detección de TTPs de MITRE ATT&CK (APT3, APT29) y debe haber participado en la prueba de detección y protección del año 2021 (Carbanak & FIN7)		
2	**Prevención contra exploits**		
2.1	Detección y prevención del mecanismo de identificación de propiedades de un sistema por parte de un exploit kit (técnica conocida como exploit kit fingerprinting) sin necesidad de utilizar firmas, patrones o heurísticas.		
2.2	Detección de técnicas de explotación sin necesidad de utilizar firmas, patrones o heurísticas, enfocadas principalmente en la prevención de exploits lógicos, procesos vulnerables y exploits del sistema operativo, para sistemas Microsoft Windows.		
2.3	Mitigación de vulnerabilidades conocidas, desconocidas y día cero.		
2.4	Soporta la identificación de distintas técnicas de explotación de vulnerabilidades, entre las que se encuentran Return Oriented Programming, Heap Spray, Jit Spray, Shell link, Structured Exception Handler, etc)		
2.5	Protección de aplicaciones contra las técnicas de explotación de manera predeterminada y "out-of-the-box".		
2.6	Entre las aplicaciones predeterminadas se encuentran: Firefox, Internet Explorer, Microsoft Word, Microsoft Excel, varias versiones de Flash Player, Microsoft Silverlight entre otras.		
2.7	Capacidad de utilizar los módulos de protección contra técnicas de explotación en cualquier aplicación o proceso, incluyendo aquellas desarrolladas internamente.		
2.8	Capacidad de crear un snapshot de forma automática de la memoria RAM al momento de prevenir la ejecución de una técnica de explotación, con la finalidad de proporcionar datos forenses sobre el evento.		
2.9	Capacidad de realizar un análisis avanzado del estatus de la memoria cuando se genere una alerta por prevención de ejecución de exploits.		

ANEXO TECNICO 01 ESPECIFICACIONES TÉCNICAS SEGURIDAD PERIMETRAL

2.10	Es posible configurar perfiles de protección en modo de prevención o monitoreo.		
2.11	Terminación del proceso en el cual fue identificado el intento de ejecución de una técnica de explotación siempre y cuando no sea un proceso crítico del sistema operativo.		
2.12	Prevención de técnicas de explotación que utilizan Dylib-Hijacking para Mac OS.		
2.13	Prevención de técnicas de explotación que utilizan ROP para Mac OS.		
2.14	Prevención de técnicas de explotación que utilizan JIT para Mac OS.		
2.15	Prevención de técnicas de explotación que buscan secuestrar el flujo de control de un proceso mediante el monitoreo de intentos de enumeración de la distribución de la memoria para sistemas operativos Linux.		
2.16	Prevención de técnicas de explotación que buscan redireccionar los flujos de entrada y salida estándares a sockets de red para sistemas operativos Linux.		
2.17	Prevención de técnicas de explotación que utilizan return-oriented programming para sistemas operativos Linux.		
2.18	Prevención del uso de ciertas áreas de memoria que son usualmente utilizadas para almacenar el payload de un ataque utilizando técnicas de heap spray, para sistemas operativos Linux.		
2.19	Protección contra webshells de PHP para servidores Linux.		
2.20	Cuenta con políticas de prevención de técnicas de explotación, así como de compatibilidad, de manera predeterminada, con la finalidad de mejorar la experiencia del usuario final y reducir la creación de falsos positivos.		
2.21	Capacidad de proporcionar la protección contra la explotación de vulnerabilidades sin necesidad de tener una conexión a la consola.		
3	**Identificación de ataques post-explotación.**		
3.1	Identificación y prevención de intentos de escalar privilegios a nivel de Kernel. Esta protección debe de poder ser utilizada en agentes Windows, Mac y Linux.		
3.2	Detección y terminación de comportamientos considerados como maliciosos mediante el análisis continuo de la cadena de eventos que sucedan en un endpoint. Esta detección debe considerar varios eventos y no sólo un evento para poder proporcionar un veredicto de la actividad maliciosa. La detección debe utilizar varias reglas preconfiguradas, las cuales deben de tener la capacidad de analizar varios eventos y no sólo un evento.		
3.3	La protección no debe depender de una conexión a la consola de administración.		
4	**Prevención contra malware conocido.**		
4.1	Generación de hashes de procesos en ejecución y verificación de veredictos en una nube de inteligencia de amenazas.		
4.2	Envío de ejecutables cuando su hash es desconocido para su análisis en un sandbox ubicado en la nube, con la finalidad de determinar si son maliciosos o benignos. Esta protección debe estar disponible para sistemas operativos Windows, Mac, Linux y Android.		
4.3	Capacidad de prevenir contra shells reversos (reverse shell) para sistemas operativos Linux.		
4.4	Capacidad escanear la computadora comparando los hashes de los archivos ejecutables que estén almacenados en la computadora y consultar su veredicto en una nube de inteligencia de amenazas.		
4.5	Capacidad de enviar los archivos clasificados como maliciosos a cuarentena, ya sea que hayan sido identificados al momento de intentar ejecutarse o al momento de ser identificados mediante un escaneo.		

ANEXO TECNICO 01 ESPECIFICACIONES TÉCNICAS SEGURIDAD PERIMETRAL

4.6	Debe contar con un módulo de prevención de ransomware, el cual debe evitar un proceso de encripción identificando intentos de modificación de archivos.		
4.7	Capacidad para proteger contra ataques de minería de bitcoins para dispositivos Linux, detectados por su comportamiento.		
5	**Prevención de malware desconocido.**		
5.1	Debe utilizar un modelo matemático generado a partir de aprendizaje de máquina para comparar una gran cantidad de características de un archivo ejecutable, de manera estática, para determinar si es malicioso. Esta protección debe estar disponible para sistemas operativos Windows, Linux y Mac.		
5.2	Prevención de ejecución de procesos utilizando su hash, de manera que el administrador puede determinar qué aplicaciones pueden ser ejecutadas.		
5.3	Capacidad de identificar si la macro contenida en un documento de Word o Excel es maliciosa, sin necesidad de tener que ejecutar la macro ni observar su comportamiento o ejecución, para determinar si es maliciosa.		
5.4	Capacidad de proporcionar protección contra malware desconocido sin necesidad de tener una conexión a la consola ni a Internet.		
5.5	Capacidad de proporcionar protección contra malware sin necesidad de contar con firmas, patrones y/o heurísticas.		
5.6	Debe ser posible configurar las políticas en modo de prevención o monitoreo.		
5.7	Debe de permitir poner los archivos detectados como maliciosos en una cuarentena, ya sea de manera automática o bajo demanda.		
5.8	Deberá de prevenir la ejecución de archivos DMG maliciosos conocidos y examinar en un servicio de análisis en la nube aquellos archivos DMG desconocidos. Si el veredicto de este análisis es malicioso, deberá de bloquear ejecuciones posteriores.		
6	**Escaneo de archivos ejecutables.**		
6.1	Permite realizar el escaneo de archivos ejecutables sin la necesidad de firmas.		
6.2	Permite programar el escaneo de archivos de manera semanal o mensual.		
6.3	Permite definir el día y la hora en la cual se iniciará el escaneo.		
6.4	El consumo de recursos al momento de realizar el escaneo no debe de impactar en la experiencia del usuario.		
6.5	Permite habilitar el escaneo de dispositivos de almacenamiento removible.		
6.6	Permite crear listas blancas de carpetas para que sean excluidas del proceso de escaneo.		
6.7	Permite poner en cuarentena los archivos identificados como maliciosos, si es que la política está configurada de esta manera.		
6.8	El escaneo de archivos deberá de poder analizar los archivos desconocidos de forma estática para determinar si son maliciosos, así como enviar estos archivos desconocidos al servicio de análisis en la nube para que sean analizados.		
7	**Cifrado de discos duros**		
7.1	Esta funcionalidad deberá de estar soportada para sistemas operativos Mac y Windows.		
7.2	El producto deberá de proporcionar visibilidad hacia agentes de sistemas operativos Windows que cifran las unidades de almacenamiento mediante el uso de Bitlocker.		
7.3	El producto deberá de poder aplicar las configuraciones de Bitlocker creadas en el directorio activo de la organización a las computadoras con sistema operativo Windows.		

ANEXO TECNICO 01 ESPECIFICACIONES TÉCNICAS SEGURIDAD PERIMETRAL

7.4	El producto deberá de proporcionar visibilidad hacia agentes de sistemas operativos Mac que cifran las unidades de almacenamiento mediante el uso de FileVault.		
7.5	El producto deberá de poder aplicar las configuraciones de FileVault a las computadoras con sistema operativo Mac.		
8	**Protección contra el robo de contraseñas.**		
8.1	Proporciona una protección en memoria contra el uso de la herramienta de extracción de contraseñas Mimikatz o similares.		
9	**Restricciones de ejecución.**		
9.1	Restricciones de ejecución de archivos a partir de cierta carpeta.		
9.2	Restricciones de ejecución de archivos a partir de recursos compartidos.		
9.3	Restricciones de ejecución de archivos a partir de dispositivos USB o CD/DVD.		
9.4	Restricciones granulares de ejecución de procesos hijo definiendo el proceso padre y los procesos hijo a restringir o permitir.		
9.5	Restricciones granulares de ejecución de procesos hijo sin necesidad de contar con una conexión a la consola de administración.		
9.6	Cuenta con políticas de restricción de creación de procesos hijo configuradas de manera predeterminada.		
9.7	Capacidad de crear excepciones para permitir la ejecución de archivos a partir de ciertas carpetas.		
9.8	Capacidad de crear excepciones para permitir la creación de procesos hijo.		
9.9	Capacidad de crear excepciones para permitir la ejecución de archivos a partir de carpetas dentro de los dispositivos de almacenamiento removibles.		
9.10	Es posible configurar perfiles en modo de prevención o monitoreo.		
10	**Restricción de uso de puertos USB.**		
10.1	Debe permitir generar perfiles que gestionen las siguientes características de bloqueo de puertos USB cuando se conecten los siguientes tipos de dispositivos: discos duros, unidades lectoras de CD-ROM externas con conexión USB, dispositivos de almacenamiento removibles portátiles con conexión USB, unidades lectoras de discos floppy externas con conexión USB, adaptadores de red en formato USB.		
10.2	Debe permitir generar perfiles de excepciones para poder conectar dispositivos en puertos USB utilizando los siguientes parámetros: tipo de dispositivo (discos duros, unidades lectoras de CD-ROM externas con conexión USB, dispositivos de almacenamiento removibles portátiles con conexión USB, unidades lectoras de discos floppy externas con conexión USB), tipo de permiso a asignar (lectura/escritura o sólo lectura), fabricante (debe de contener una lista predeterminada), producto (debe de contener una lista predeterminada), y número de serie. Los parámetros tipo de dispositivo, tipo de permiso y fabricante deben de ser mandatorios.		
10.3	Debe permitir la creación de políticas que utilicen los perfiles de bloqueo y de excepciones generados y sin ser excluyentes.		
10.4	Las políticas generadas deben de poder asignarse a una computadora en particular o a un grupo de computadoras definido previamente.		
10.5	Debe de permitir la creación de excepciones permanentes utilizando los siguientes parámetros: tipo de dispositivo (discos duros, unidades lectoras de CD-ROM externas con conexión USB, dispositivos de almacenamiento removibles portátiles con conexión USB, unidades lectoras de discos floppy externas con conexión USB), tipo de permiso a asignar (lectura/escritura o sólo lectura), fabricante (debe de contener una lista predeterminada), producto (debe de contener una lista predeterminada), y número de serie. Los parámetros tipo de dispositivo, tipo de permiso y fabricante deben de ser mandatorios. Estas excepciones permanentes no deben de depender de ser aplicadas a una política para que surtan efecto.		

ANEXO TECNICO 01 ESPECIFICACIONES TÉCNICAS SEGURIDAD PERIMETRAL

10.6	Debe permitir la creación de excepciones temporales a partir de una violación registrada.		
10.7	Debe de mostrar las violaciones a las políticas que se hayan registrado mostrando lo siguiente: horario, computadora, usuario, dirección IP, tipo de dispositivo, producto, fabricante y número de serie del dispositivo que intentó conectarse.		
10.8	Esta funcionalidad deberá de estar soportada para sistemas operativos Windows y Mac.		
11	**Firewall de host**		
11.1	Esta funcionalidad deberá de estar disponible para los sistemas operativos Windows y Mac.		
11.2	Las siguientes funcionalidades deberán de estar disponibles para sistemas operativos Windows: - Controlar todas las comunicaciones entrantes y salientes utilizando direcciones IP. - Permitir que las reglas sean aplicadas de acuerdo con la ubicación del dispositivo, por ejemplo, que sólo apliquen si están en la red interna. - El producto debe de poder determinar, mediante la configuración, si el dispositivo se encuentra dentro o fuera de la organización. - La regla podrá especificar direcciones locales o remotas, así como puertos locales o remotos. También se podrá especificar el protocolo dentro de estas cuatro opciones: ICMP, TCP, UDP, ICMPv6.		
11.3	Las siguientes funcionalidades deberán de estar disponibles para sistemas operativos Mac: - Permitir habilitar o deshabilitar el firewall nativo del sistema operativo. - Permitir o bloquear las comunicaciones de red entrantes. - Habilitar el modo stealth - Crear exclusiones por aplicaciones para permitir o bloquear programas de manera específica y utilizando la funcionalidad del sistema operativo conocido como BlundleID		
12	**Captura de datos en el endpoint**		

ANEXO TECNICO 01 ESPECIFICACIONES TÉCNICAS SEGURIDAD PERIMETRAL

12.1	El producto deberá de poder capturar, como mínimo, las siguientes acciones a nivel del endpoint en sistemas operativos Windows: - Proceso ejecutado, incluyendo el tiempo de inicio, el tamaño del archivo asociado. - Actividades de creación, escritura, renombre, eliminación, modificación y creación de enlaces simbólicos de un archivo. - Se deberán de registrar los siguientes parámetros cuando sean cargados archivos DLL: ruta completa, dirección base, id del proceso o hilo que lo está cargando, tamaño de la imagen, firma, valores hash calculados con los algoritmos MD5 y SHA256 del archivo DLL, tamaño del archivo, tiempo de acceso del archivo. - Creación y terminación de los procesos - Inyecciones en hilos de procesos. ID del hilo padre, ID del hilo nuevo o que se ha terminado, proceso que inició el hilo (en caso de ser un proceso distinto). - Las siguientes acciones de red: accept, connect, create, listen, close, bind, con los siguientes parámetros: IP y puerto destino, IP y puerto fuente, conexiones fallidas, protocolo (TCP/UDP), resolver los nombres de computadoras dentro de la red local. - Protocolos de red: peticiones DNS y respuestas UDP, HTTP connect, HTTP disconnect, HTTP proxy parsing. - Estadísticas de red. Volumen al momento de ser enviado a través de un enlace TCP. Volumen recibido a través de un enlace TCP. - Registro. Configuración o eliminación de valores del registro. Creación, modificación, eliminación, adición, restauración y guardar llaves del registro - Sesiones del sistema operativo. inicio de sesión, cierre de sesión, conexión y desconexión. Considerando los siguientes atributos: inicio de sesión interactivo, id de la sesión, estado de la sesión, y si la sesión es local o remota. - Estado de la computadora: inicio, suspendida, reinicio. Con los siguientes atributos: nombre de la computadora, versión del sistema operativo, dominio, estado anterior y actual. - Logs de eventos de Windows.		
12.2	El producto deberá de poder capturar, como mínimo, las siguientes acciones a nivel del endpoint en sistemas operativos Mac: - Creación, escritura, eliminación, renombre, cambio de ruta y apertura de archivos. Con los siguientes atributos: ruta completa del archivo modificado antes y después de su modificación. Generación de hashes con los algoritmos SHA256 y MD5 para el archivo después de su modificación. - Inicio y detención de procesos, con los siguientes parámetros: ID de proceso para el proceso padre, id del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma o el certificado utilizado para firmar el archivo. - Las siguientes acciones de red: accept, connect, connect failure, disconnect, listen, statistics, con los siguientes parámetros: IP y puerto destino, conexiones fallidas, protocolo (TCP/UDP), estadísticas agregadas de envío/recepción para la conexión.		

ANEXO TECNICO 01 ESPECIFICACIONES TÉCNICAS SEGURIDAD PERIMETRAL

12.3	El producto deberá de poder capturar, como mínimo, las siguientes acciones a nivel del endpoint en sistemas operativos Linux: - Para los archivos, las acciones de creación, apertura, escritura y eliminación, incluyendo la ruta completa del archivo y el hash del archivo (para ciertos archivos y sólo si el archivo fue escrito). Copiar o renombrar los archivos, incluyendo las rutas completas tanto del archivo original como del modificado. Las acciones para cambiar el dueño (chown) y el modo (chmod) de los archivos, incluyendo la ruta completa del archivo así como el nuevo dueño o nuevos atributos. - Las siguientes acciones de red: listen, accept, connect, connect failure y disconnect; con los siguientes atributos: dirección IP y puertos fuente para binds explicitos, dirección IP y puerto destino, conexiones TCP fallidas, protocolo UDP/TCP. - Procesos. Creación de procesos, con los siguientes atributos: ID del proceso hijo, id del proceso padre, ruta completa del a imagen del proceso, línea de comando del proceso, valores hash calculados con los algoritmos SHA256 y MD5. Terminación de procesos, incluyendo el ID del proceso.		
13	**Análisis de alertas e investigación de actividad sospechosa**		
13.1	Deberá de contar con un dashboard en nube que permite visualizar alertas generadas de distintas fuentes.		
13.2	Deberá correlacionar alertas, sin importar si estas vengan de datos de endpoint, red o nube y agruparlas dentro de incidentes		
13.3	Deberá de poder mostrar el número total de alertas e incidentes, y debe incluir la capacidad de filtrar la información de forma flexible		
13.4	El producto deberá permitir la creación de una secuencia gráfica que correlacione las alertas individuales con el objetivo de describir la secuencia de un ataque.		
13.5	El producto deberá de mostrar información específica de cada proceso involucrado en la secuencia gráfica.		
13.6	En la pantalla emergente, en caso de estar disponible, deberá de mostrarse los datos relacionado con el perfil de comportamiento y la ejecución del archivo.		
13.7	El producto deberá mostrar una advertencia cuando un ejecutable en particular, que forme parte de la secuencia gráfica, tenga un comportamiento sospechoso.		
13.8	El producto deberá de mostrar datos generales de la ejecución de un proceso que forme parte de la secuencia gráfica, entre los que se encuentran ruta de ejecución, nombre de usuario que ejecutó el proceso, tiempo de su ejecución, entidad que firmó el proceso, valor MD5 del ejecutable relacionado con el proceso, veredicto del análisis del sandbox, valor SHA256 y línea de comandos de la ejecución.		
13.9	El producto deberá mostrar la actividad de cada proceso identificado, en columnas por categorías. Entre las categorías a incluir debe de estar la actividad de red, actividad de los archivos, actividad del registro, módulos ejecutados e intentos de inyección a procesos.		
13.10	El producto deberá utilizar el aprendizaje automático supervisado y no supervisado para establecer líneas de base del comportamiento habitual del usuario y del dispositivo y detectar desviaciones de comportamiento que caracterizan la actividad anómala.		
13.11	El producto deberá de proporcionar la capacidad de decodificar cadenas de caracteres codificadas en base-64 para mostrarlo en texto plano.		
13.12	El producto deberá integrarse con los Firewalls de la entidad, recolectando los logs de red que este produzca.		

ANEXO TECNICO 01 ESPECIFICACIONES TÉCNICAS SEGURIDAD PERIMETRAL

13.13	El producto deberá de poder identificar, de todas las actividades mencionadas anteriormente, aquellas que sean maliciosas o altamente sospechosas y separarlas en una categoría de fácil acceso para el analista.		
13.14	Inteligencia de amenazas compartida para distribuir inteligencia de amenazas de crowdsourcing del servicio de análisis de malware basado en la nube a firewalls, agentes de punto final y servicios de detección y respuesta		
13.15	Para cada una de las actividades mencionadas anteriormente el producto deberá de desplegar los siguientes datos en columnas: fecha, nombre de la computadora, IP del host que generó la alerta, nombre de usuario, sistema operativo del host, tipo de actividad identificada, descripción de la actividad identificada, nombre del archivo asociado, nombre previo del archivo, ruta del archivo, ruta anterior del archivo, valor MD5 del archivo, valor SHA256 del archivo, ruta del archivo que fue el ejecutor del archivo, comando que utilizó el ejecutor del archivo, identificador del proceso que fue el ejecutor del archivo, valor MD5 del ejecutor del archivo que fue la causa raíz de la alerta, valor SHA256 del ejecutor del archivo que fue la causa raíz de la alerta, indicador sobre si el ejecutor de la alerta está firmado, entidad que firma el archivo que fue la causa raíz de la alerta, ruta del archivo que fue la causa raíz de la alerta, comando del archivo que fue la causa raíz de la alerta, valor SHA 256 del archivo que fue la causa raíz de la alerta, indicador sobre si el archivo que fue la causa raíz de la alerta está firmado, entidad que firma el archivo que fue la causa raíz de la alerta.		
13.16	El producto deberá mostrar si existió una inyección de código o si el protocolo RPC es utilizado en otro proceso desde una computadora local o remota.		
13.17	La solución debe correlacionar de forma nativa eventos de endpoint, red, firewall, DNS y nube en una única línea de tiempo de ataque (Attack Causality Chain), sin requerir herramientas externas.		
13.18	El producto deberá proporcionar de manera gráfica la interacción que existe con las direcciones IP que se quieran investigar. Deberá de poder mostrar diferentes opciones de vistas como la ubicación geográfica o los archivos ejecutables que generaron esa comunicación.		
13.19	El producto deberá proporcionar de manera gráfica la interacción que existe entre uno o varios procesos que sean investigados. La gráfica deberá de mostrar la interacción entre los procesos, y si existe una relación entre las computadoras que ejecutan dichos procesos, entre otros aspectos.		
13.20	La solución XDR debe integrarse de manera nativa con los Next Generation Firewalls del fabricante, permitiendo: • Correlación automática entre eventos de red y endpoint • Visibilidad del tráfico asociado a un incidente XDR • Creación de EDL para retroalimentar el firewall perimetral de amenazas detectadas en la red		
13.21	La solución debe incluir Advanced Behavioral Analytics, capaz de: Detectar ataques sin firmas • Identificar movimientos laterales • Detectar Living-off-the-land (LOLbins) • Detectar abuso de credenciales y anomalías de usuario		
13.22	La plataforma debe permitir búsqueda avanzada (Threat Hunting) mediante un lenguaje de consulta que permita: • Consultar eventos históricos • Correlacionar procesos, red, archivos y usuarios		

ANEXO TECNICO 01 ESPECIFICACIONES TÉCNICAS SEGURIDAD PERIMETRAL

	• Realizar investigaciones proactivas		
14	**Configuración y elementos de identificación**		
14.1	La solución debe contar con mecanismos de generación de alertas considerando el comportamiento mostrado por los procesos de las computadoras.		
14.2	Las alertas generadas por el comportamiento de los procesos no deberán de utilizar firmas o heurísticas.		
14.3	Cada alerta generada por el comportamiento de los procesos deberá de tener una descripción del comportamiento identificado.		
14.4	Cada alerta generada deberá de contar con una clasificación de acuerdo con su severidad.		
14.5	La solución debe permitir al analista definir comportamientos de procesos para que generen alertas.		
14.6	La solución debe permitir la generación de excepciones a los comportamientos de los procesos que hayan sido identificados como maliciosos o sospechosos.		
14.7	La solución debe permitir deshabilitar, modificar, exportar o eliminar los comportamientos que generen las alertas por el comportamiento de los procesos.		
14.8	La solución debe permitir importar reglas de comportamientos sospechosos de procesos.		
14.9	La solución debe soportar el uso de indicadores de compromiso tradicionales, incluyendo rutas de archivos, nombres de archivos, dominios, direcciones IP y hashes.		
14.10	La solución debe permitir deshabilitar, modificar, exportar o eliminar un indicador de compromiso mediante un menú contextual.		
14.11	La solución debe permitir la gestión de los indicadores de compromiso por comportamiento de procesos e indicadores de compromiso tradicionales mediante la consola de administración.		
14.12	La solución debe permitir respuesta remota desde consola, incluyendo: • Ejecución de comandos remotos • Recolección de artefactos • Análisis forense bajo demanda		
14.13	La plataforma debe permitir aislar el endpoint de la red de forma remota, manteniendo únicamente comunicación con la consola de administración.		
14.14	Capacidad de: • Terminar procesos maliciosos • Eliminar archivos • Poner archivos en cuarentena de forma centralizada		
14.15	La solución debe permitir ejecutar scripts personalizados de respuesta (bash, PowerShell u otros) como parte de la contención del incidente.		
15	**Acciones de respuesta**		

ANEXO TECNICO 01 ESPECIFICACIONES TÉCNICAS SEGURIDAD PERIMETRAL

15.1	La solución debe permitir aislar una computadora desde la propia consola de administración para que sólo exista comunicación entre el agente y la consola. Deberá ofrecer la capacidad para poder agregar comentarios los cuales explican la razón por la cual fue aislada una computadora.		
15.2	La solución debe permitir agregar IPs a listas dinámicas externas para que estas puedan ser consumidas por NGFWs u otras tecnologías		
15.3	La consola permite definir otros procesos y destinos (direcciones IP) a los cuales se pueda conectar la computadora, además de la consola.		
15.4	La consola permite poner en cuarentena, bajo demanda, archivos maliciosos que hayan sido detectados o reportados, pero no bloqueados por las políticas de prevención definidas.		
15.5	El producto deberá de mostrar los detalles de los archivos que han sido puestos en cuarentena. El producto deberá de permitir filtrar los archivos que han sido puestos en cuarentena por nombre de la computadora, dominio, ruta del archivo, fuente de la cuarentena y fecha de la cuarentena.		
15.6	La solución debe permitir exportar todos los detalles de los archivos que hayan sido puestos en cuarentena en un archivo con formato “tab-separated value” (TSV).		
15.7	La solución debe permitir la restauración de uno o más archivos que hayan sido puestos en cuarentena de manera simultánea.		
15.8	La solución debe permitir una conexión inversa al dispositivo afectado, en versiones superiores a Windows 7 SP1, a través de una conexión remota para permitir las siguientes acciones: - Terminar el proceso de ejecución - Suspender o reanudar el proceso de ejecución - Agregar un proceso a un indicador de compromiso (IOC) - Copiar binario en ejecución para futuras investigaciones		
15.9	La solución debe permitir una conexión inversa al dispositivo afectado a través de una conexión remota para permitir ejecutar secuencias de comandos o comandos en Python versión 3 como mínimo.		
15.10	La solución debe permitir una conexión inversa al dispositivo afectado a través de una conexión remota para permitir ejecutar secuencias de comandos o comandos en Powershell.		
15.11	La solución debe permitir explorar las unidades de almacenamiento de manera remota, incluyendo no sólo discos duros sino también dispositivos de almacenamiento removibles. Deberá permitir mover, renombrar, eliminar, descargar y calcular el hash de cualquier archivo como mínimo.		
15.12	La solución debe permitir la creación de listas blancas o negras		
15.13	La solución debe permitir agregar la información del incidente asociado cuando un archivo sea puesto en una lista blanca o una lista negra.		
15.14	La plataforma debe permitir acciones automáticas basadas en el score de riesgo, tales como: • Aislar endpoint • Bloquear hash • Bloquear IP o dominio • Escalar incidente automáticamente		
16	**Administración y revisión de eventos.**		
16.1	Administración de políticas centralizado, vía una consola web.		
16.2	La consola puede clasificar los eventos en tres niveles de acuerdo con su severidad: bajo, medio y alto.		
16.3	La consola de administración identifica claramente los eventos que han sido reportados y/o bloqueados y aquellos que han sido detectados.		

ANEXO TECNICO 01 ESPECIFICACIONES TÉCNICAS SEGURIDAD PERIMETRAL

16.4	Capacidad para clasificar el estado de los incidentes en cuatro distintos niveles de severidad: alto, mediano, bajo e informacional.		
16.5	Capacidad para clasificar el estado de las alertas en cuatro distintos niveles de severidad: alto, mediano, bajo e informacional.		
16.6	Capacidad de poder agrupar las alertas relacionadas en incidentes, así como proporcionar un contexto del mismo.		
16.7	Capacidad de poder extraer los elementos importantes o relevantes de las alertas, y mostrarlos a manera de resumen en la pantalla de análisis del incidente.		
16.8	La consola deberá de proporcionar información detallada bajo demanda de los eventos identificados como exploits.		
16.9	Permite la actualización y desinstalación del agente a partir de la consola.		
16.10	Permite utilizar cualquier aplicación de un tercero para poder realizar la instalación del agente.		
16.11	Cuenta con integración con Active Directory para la gestión de computadoras y configuración de políticas.		
16.12	Cuenta con la capacidad de poder crear perfiles granulares.		
16.13	Cuenta con la capacidad de poder crear políticas basadas en los perfiles creados.		
16.14	Cuenta con la capacidad de poder aplicar políticas a usuarios, grupos, computadoras o unidades organizacionales de Active Directory.		
16.15	Cuenta con la capacidad de crear grupos virtuales que pueden alimentarse de forma estática y dinámica.		
16.16	La alimentación dinámica de los grupos virtuales podrá ser de forma estática y dinámica, siendo posible configurar para la forma dinámica el nombre de la computadora y dirección IP como mínimo.		
16.17	Cada evento de prevención o notificación cuenta con información básica como tipo de evento, módulo que realizó la prevención, detalles de ese módulo, nombre de la computadora, nombre del usuario, sistema operativo, versión del agente, proceso que generó el evento de prevención, ruta de ejecución del proceso que generó el evento de prevención (en caso de estar disponible), horario y fecha del evento, información forense (en caso de estar disponible).		
16.18	La consola deberá de ser proporcionada bajo un esquema software as a service.		
16.19	Cuenta con un dashboard donde se muestran los incidentes de seguridad que no han sido atendidos (clasificados de acuerdo con su criticidad en alta, media y baja), un resumen sobre los incidentes de seguridad, la cantidad de endpoints que tienen instalado el agente (clasificados por su plataforma), la cantidad de licencias disponibles y la versión del agente.		
16.20	Cuenta con un dashboard donde se describen las características de los incidentes de seguridad que se han generado. Este dashboard debe de permitir analizar a mayor detalle las alertas de seguridad, incluyendo los reportes generados por el agente.		
16.21	Integración con una plataforma de ciberseguridad la cual incluya una nube de inteligencia y contextualización de amenazas, a través de un API.		
16.22	Debe permitir gestionar las excepciones en una pantalla específica.		
16.23	Debe permitir crear excepciones a reglas, mecanismos de detección y/o mecanismos de protección desde la consola. Estas excepciones deben de poder aplicarse a una computadora en específico, o a un grupo de computadoras.		
17	**Características del agente.**		
17.1	Agente con un footprint mínimo que no impacte la experiencia de usuario.		

ANEXO TECNICO 01 ESPECIFICACIONES TÉCNICAS SEGURIDAD PERIMETRAL

17.2	Poco almacenamiento en disco debido a que no utiliza firmas, patrones y/o heurísticas.		
17.3	Soporte para las siguientes versiones de sistemas operativos: - Windows XP* (32-bit, SP3 o posterior), Windows Vista (32-bit, 64-bit, SP1 o posterior; FIPS mode), Windows 7 (32-bit, 64-bit, RTM & SP1; excepto Home), Windows Embedded 7 (Standard & POSReady), Windows 8* (32-bit, 64-bit), Windows 8.1 (32-bit, 64-bit; FIPS mode), Windows Embedded 8.1 Pro, Windows 10 Pro (32-bit and 64-bit), Windows 10 Enterprise LTSB, Windows 10 Education, Windows 10 Update 1809, Windows 11 Pro (32-bit, 64-bit), Wndows 11Enterprise, Windows 11 Education, Windows 11 Pro Education, Windows 11 Pro for Workstation, Windows Server 2003* (32-bit, SP2 o posterior), Windows Server 2003 R2 (32-bit, SP2 o posterior), Windows Server 2008 (32-bit, 64-bit; FIPS mode), Windows Server 2008 R2 (32-bit, 64-bit; FIPS mode), Windows Server 2012 (todas las ediciones; FIPS mode), Windows Server 2012 R2 (todas las ediciones; FIPS mode), Windows Server 2016, Windows Server Core option 2012, 2012 R2 y 2016, Windows Server 2016 Datacenter. - OSX 10.10 (Yosemite), OSX 10.11 (El Capitan), macOS 10.12 (Sierra), macOS 10.14. - CentOS 6, CentOS 7, Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 7, Suse for Enterprise 12.1, Suse for Enterprise 12.2, Ubuntu Server 12, Ubuntu Server 14, Ubuntu Server 16		
17.4	Soporte para los siguientes ambientes virtuales: VMware ESX, Citrix XenServer, Oracle Virtualbox, Microsoft Hyper-V.		
17.5	Capacidad para configurar la captura de datos que serán enviados a la nube para su almacenamiento, procesamiento y análisis en una consola de detección y respuesta a incidentes.		
18	**Servicio de Cacería de amenazas**		
18.1	La plataforma debe permitir buscar, programar y guardar consultas para identificar amenazas difíciles de encontrar.		
18.2	Debe ofrecer capacidades de hunting flexibles que permitan descubrir amenazas utilizando un generador de consultas intuitivo, así como construir consultas avanzadas y visualizar resultados de forma ordenada		
19	**Gestión de usuarios**		
19.1	La consola permite la gestión de usuarios mediante roles.		
19.2	La consola cuenta con roles preconfigurados.		

ANEXO TECNICO 01 ESPECIFICACIONES TÉCNICAS SEGURIDAD PERIMETRAL

19.3	Los roles preconfigurados tienen las siguientes características: - Viewer. Cuenta con permisos para revisar toda la consola, pero no puede tomar acciones. - IT Admin. Cuenta con permisos para ver alertas, la gestión e instalación de agentes, las acciones realizadas en la consola, los perfiles, las políticas, el control de dispositivos y las excepciones globales. Puede instalar y gestionar agentes. - IT Admin con privilegios. Cuenta con los mismos permisos que une IT Admin, pero adicionalmente puede realizar sesiones remotas y extracción de archivos de manera remota. - Administrador de seguridad. Puede ver las políticas, perfiles, acciones tomadas en la consola, incidentes, alertas, reglas, gestión de agentes, excepciones globales y el control de dispositivos. Puede realizar ciertas acciones de configuración. - Administrador de seguridad con privilegios. Cuenta con los mismos permisos que el administrador de seguridad, adicionalmente puede interactuar con APIs públicas, la auditoría y la integración de plataformas de inteligencia de amenazas. Puede realizar sesiones remotas y extracción de archivos de manera remota. - Administrador de instalaciones. Puede ver y configurar la gestión e instalación de agentes. - Investigador. Puede ver las alertas e incidentes, así como iniciar un escaneo bajo demanda. - Investigador privilegiado. Puede ver las alertas, incidentes, reglas, políticas, perfiles, acciones en la consola; así como iniciar un escaneo bajo demanda. - Respondiente. Puede ver alertas, incidentes, las acciones en la consola, reglas. Puede responder ante alertas e incidentes, pero no tiene capacidades de realizar sesiones remotas y extracción de archivos de manera remota. - Respondiente con privilegios. Cuenta con los privilegios del respondiente, pero, adicionalmente, puede ver las políticas, perfiles y excepciones globales; puede realizar sesiones remotas y extracción de archivos de manera remota.		
20	**Reportes**		
20.1	Permite la generación de reportes bajo demanda o programados.		
20.2	Formato de reportes generados en PDF, CSV,TSV.		
20.3	La consola mantiene un historial de los reportes que han sido generados para su posterior consulta.		
20.4	La frecuencia para la generación de los reportes programados podrá ser diaria, semanal o mensual.		
20.5	Si la frecuencia para la generación de los reportes es semanal, se puede especificar el día en el cual se generarán los reportes.		
20.6	Si la frecuencia para la generación de los reportes es mensual, el reporte se generará el día seleccionado de cada mes.		
20.7	El rango de tiempo para la generación de los reportes es expresado en días.		
20.8	Se pueden especificar varias direcciones de correo electrónico para que los reportes sean enviados.		
20.9	Para los reportes bajo demanda se podrá especificar el rango de tiempo a considerar.		
20.10	Los reportes pueden ser generados a partir de plantillas predeterminadas, o se puede generar un reporte personalizado utilizando los “widgets” disponibles.		
20.11	Los reportes se pueden enviar a una lista de correos electrónicos.		
21	**Visibilidad y Gestión de Datos**		
21.1	El producto deberá de mostrar el tipo y cantidad de datos que consume el agente en un dashboard específico.		

ANEXO TECNICO 01 ESPECIFICACIONES TÉCNICAS SEGURIDAD PERIMETRAL

21.2	El dashboard mencionado en el punto anterior deberá de mostrar como mínimo los siguientes datos: - La tasa de ingestión diaria de logs. - El consumo diario del producto comparado con la cuota de ingestión permitida. - Datos de ingestión detallados de cada producto.		
21.3	El producto deberá de realizar recomendaciones para la configuración de consumo de ancho de banda por parte del agente.		