PERÚ | Ministerio de Relaciones Exteriores

REQUERIMIENTO PARA SERVICIOS

CONTRATACIÓN DEL SERVICIO DE SEGURIDAD GESTIONADA PARA EL MINISTERIO DE RELACIONES EXTERIORES

I. TÉRMINOS DE REFERENCIA

1. ÁREA USUARIA

Oficina de Tecnologías de la Información del Ministerio de Relaciones Exteriores.

2. OBJETIVO

La presente contratación tiene por objetivo brindar servicio de seguridad gestionada por un periodo de veinticuatro (24) meses para el Ministerio de Relaciones Exteriores.

3. FINALIDAD PÚBLICA

El Ministerio de Relaciones Exteriores requiere mantener la seguridad informática perimetral para los usuarios del Ministerio de Relaciones Exteriores, que se encuentran en las sedes de Lima, las Oficinas Desconcentradas, los Órganos del Servicio Exterior, la Academia Diplomática y otros de interés de la *Cancillería*, a fin de mitigar ciberataques que atenten contra la continuidad operativa de la entidad, permitiendo así la disponibilidad, integridad y confidencialidad de la información, que es procesada, almacenada y transmitida en la infraestructura tecnológica de la institución.

Es importante señalar que la presente contratación se alinea con la actividad del Plan Operativo Institucional 2024, de acuerdo con el siguiente detalle:

CÓDIGO POI	DESCRIPCIÓN DE LA ACTIVIDAD
AOI00004500019	Gestión de las tecnologías digitales

4. CONSIDERACIONES GENERALES

ITEM	CANTIDAD	UNIDAD DE MEDIDA	DESCRIPCIÓN
1	1	SERVICIO	CONTRATACIÓN DEL SERVICIO DE SEGURIDAD GESTIONADA PARA EL MINISTERIO DE RELACIONES EXTERIORES

CUADRO MULTIANUAL DE NECESIDADES

CMN 2024-2026: **SI**

PLAN ANUAL DE CONTRATACIONES 2024: **11**

4.1. CARACTERÍSTICAS DEL SERVICIO

4.1.1. Seguridad Gestionada

La administración de los equipos de seguridad en su totalidad será administrada por el Contratista en coordinación con la Oficina de Tecnologías de la Información del Ministerio de Relaciones Exteriores, y soportar los protocolos IPV4/IPV6. Las licencias y el soporte de fábrica deberá ser parte del servicio por el tiempo que se estipule en el contrato.

El servicio deberá cumplir con las siguientes características mínimas:

- Solución de Firewall con aprendizaje automático basado en actividad de usuario.
- Solución de Protección de Intrusos.
- Solución de Firewall de aplicaciones WEB.
- Protección a nivel de navegación (tráfico que se efectúa al navegar por internet)
- Protección a nivel del servicio de correo electrónico (correos saliente provenientes de los sistemas de envío de correos)
- Sistema de prevención de actividades ocultas y malintencionadas en el tráfico cifrado.
- Protección a nivel de endpoint centralizado (tráfico efectuado a través de los equipos de cómputo).
- Servicio de Gestión de Eventos de Seguridad.
- Analizar el tráfico de las redes privadas virtuales (VPN) con las misiones.
- Permitir identificación, verificación y categorización del tráfico protocolo para cifrar navegación de páginas web (https) con inspección completa de la capa 7
- Protección de Cuentas Privilegiadas.
- Sistema de Detección de Amenazas con Inteligencia Artificial.
- Centralización de log de auditoría y análisis de la generación de reportes.
- Gestión de administración, configuración y actualización de firmas de los equipos de seguridad.
- Detección y prevención de todo tipo amenazas avanzadas a nivel de nube y on premise.

a) Solución Firewall de Aplicaciones Web

El Contratista deberá proveer Dos (2) Appliance o Equipamiento de protección a las aplicaciones web del Ministerio de Relaciones Exteriores frente a las amenazas externas, realizando detección de amenazas mediante reglas que puedan ser personalizables y/o algoritmos de inteligencia artificial. Deberá contar con alta disponibilidad a nivel de hardware, una consola de gestión de propósito específico en appliance dedicado o virtual, o en su defecto que la gestión pueda ser administrada desde el mismo hardware que realiza la función de WAF y debe ser de tecnología vigente, nuevos y de primer uso. Los componentes serán instalados en el centro de datos, ubicado en el Edificio Raúl Porras Barrenechea, ubicado en el Jirón Ucayali N.° 337, Cercado de Lima y ser de tecnología vigente, nuevos y de primer uso. La entidad proporcionará la conectividad a nivel de switches.

Asimismo, la solución deberá contar con las siguientes características mínimas:

Funcionalidades generales

- Cada componente debe de tener softwares específicos, destinados a la finalidad de Firewall de Aplicación Web (WAF –Web Application Firewall), así como las licencias necesarias para su funcionamiento y protección de servidores y aplicaciones Web.
- Insertar latencia inferior a los 5 milisegundos, con el objetivo de no impactar el performance de las aplicaciones Web.
- Dichos equipos serán conectados mediante cableado UTP RJ45.
- El sistema propuesto debe de ser formado por software y hardware del mismo fabricante.
- El equipamiento, deberá tener las siguientes funcionalidades mínimas:

  ✓ Por lo menos 4 interfaces RJ45 1Gb (deberán soportar funcionalidad bypass).
  ✓ Almacenamiento local de como mínimo 450GB.
  ✓ Espacio máximo en gabinete 2U.
  ✓ Throughput: mínimo de 1 Gbps.
  ✓ Cada equipo tendrá fuentes duales redundantes de tipo hot-swap.

Funcionalidades de red

- Tener LEDs para la indicación del status y actividades de las interfaces.
- La solución deberá tener varios mecanismos de despliegue (deployment) contando como mínimo con puente transparente en línea (Bridge L2), Proxy Reverso. Se

valorará como opcional la capacidad de inspeccionar tráfico en modo "Sniffing", utilizando puertos SPAN de un Switch o algún TAP de red, para poder monitorear el tráfico sin realizar cambios en la red.

- Soportar VLANs del estándar IEEE 802.1q.
- Debe de implementar el protocolo Link Aggregation Control Protocol (LACP) - IEEE 802.3ad.
- Soportar direccionamiento IPv4 y IPv6 en las interfaces físicas y virtuales (VLANs).
- La solución debe de soportar y brindar cluster de alta disponibilidad entre dos equipos en modo Activo-Pasivo y Activo-Activo, de forma que el tráfico siga siendo procesado en caso de fallo del equipo principal.

Funcionalidades de gestión

- El sistema operativo / firmware debe soportar interfaz gráfica web para la configuración de las funciones del sistema, utilizando navegadores disponibles gratuitamente y protocolo HTTPS, y también por CLI (interface de línea de comando), accediendo localmente por puerto de consola, o remotamente vía SSH.
- Debe de soportar administración basada en interface web HTTPS.
- Debe de soportar administración basada en interface de línea de comando vía SSH.
- Tener auto complementación de comandos en la CLI.
- Tener ayuda contextual en la CLI.
- La solución debe de tener un Dashboard con información sobre el sistema (información del cluster, hostname, número de serie, modo de operación, tiempo en servicio, versión de firmware).
- Debe de ser posible visualizar a través de la interfaz gráfica de gestión la información de licencia, firmas y contrato de soporte.
- Debe de ser posible visualizar desde la interfaz de gestión ó CLI la información de uso de los discos de log.
- Debe de incluir herramienta dentro de la interfaz gráfica de gestión (dashboard) que permita visualizar los últimos logs de ataques detectados/bloqueados.
- Debe proveer las siguientes informaciones en la interfaz gráfica de gestión: estadísticas de throughput HTTP en tiempo real, estadísticas de eventos de ataques detectados/bloqueados y los últimos logs de eventos del sistema.
- Tener en la interfaz gráfica estadísticas de conexión concurrente de políticas de seguridad del sistema.
- La configuración de administración de la solución debe permitir la utilización de perfiles.
- Debe de ser posible ejecutar y recuperar backup por la interfaz Web (GUI).
- Debe soportar los protocolos de monitoreo SNMP v1, SNMP v2c e SNMP v3.
- Debe ser capaz de realizar notificación de eventos de seguridad a través de e-mail, traps SNMP y Syslog.
- La solución deberá de soportar almacenar logs localmente en disco y en servidor externo vía protocolo SYSLOG.
- La solución debe tener la capacidad de enviar alertas por email de los eventos basado en severidad y/o categorías.
- La solución debe soportar y estar habilitada, la opción de datos analíticos conteniendo la localización geográfica de los clientes web.
- La consola de gestión deberá permitir la centralización de las políticas, reportes, monitoreo, eventos de seguridad, gestión de los distintos componentes de la solución y el monitoreo de su estado, performance, etc.
- Debe tener la capacidad de generar reportes detallados basados en tráfico/acceso/actividades del usuario.
- La consola de administración deberá soportar todo tipo de gestión sobre el WAF y personalización de reportes granulares que incluyen: servidor y aplicación web protegidos, tipo de ataque, objeto atacado, URL, método HTTP, IP origen, usuario del aplicativo web, rango de tiempo, u otros.

Funcionalidades de autenticación

- Los usuarios deben contar con la capacidad de autenticarse a través del encabezado de autorización HTTP / HTTPS.
- Los usuarios deben de ser capaces de autenticarse a través de formularios HTML embebidos.
- La solución debe tener la capacidad de autenticar usuarios en bases externas remotas LDAP y RADIUS.

Reglamentación y certificaciones

- La solución debe soportar el modelo de seguridad positiva definido por OWASP considerando protección para todas las vulnerabilidades expresadas en el TOP 10.
- Cada componente debe de tener certificación FCC.

Funcionalidades del Web Application Firewall

- Cada componente debe soportar y estar habilitada, la capacidad de identificar y bloquear ataques a través de una base de datos de firmas y reputación IP, actualizado de forma automática.
- Tener mecanismo de aprendizaje automático capaz de identificar todos los contenidos de la aplicación, incluyendo URLs, parámetros de URLs, campos de formularios, detección de BOT y lo que se espera de cada campo.
- El perfil aprendido de forma automática debe de poder ser ajustado.
- La solución debe tener generación de reportes con la información obtenida en auto aprendizaje, con las estadísticas y las políticas de tráfico obtenido, los reportes de ataques, eventos y reportes de chequeo de vulnerabilidades para fines de cumplimiento de reglamentación.
- Cada componente debe tener la capacidad de creación de firmas de ataques personalizables.
- Cada componente debe soportar la capacidad de protección contra ataques del tipo Botnet.
- Cada componente debe soportar detección de ataques de cambios de cookie.
- Identificar y proteger contra ataques del tipo Credit Cart Theft.
- Identificar y proteger contra ataques del tipo Cross Site Request Forgery (CSRF).
- La solución debe tener funcionalidad de protección contra ataques como cross site scripting (XSS).
- Cada componente debe tener la capacidad de protección contra ataques del tipo HTTP header overflow.
- Cada componente debe tener la capacidad de protección contra ataques del tipo Local File inclusion (FLI).
- Cada componente debe tener la capacidad de protección contra ataques del tipo Man-in-the-middle (MITM).
- Cada componente debe tener la capacidad de protección contra ataques del tipo Remote File Inclusion (RFI).
- Cada componente debe tener la capacidad de protección contra ataques del tipo Server Information Leakage.
- Protección contra envíos de comandos SQL ocultos en las requisiciones enviadas a la base de datos (SQL Injection).
- Tener la capacidad de protección contra ataques del tipo Malformed XML
- Cada componente debe tener la capacidad de protección contra ataques del tipo Forms Tampering.
- La solución debe tener funcionalidad de protección contra ataques de manipulación de campos ocultos.
- Tener la capacidad de protección contra ataques del tipo Directory Traversal.
- Cada componente debe tener la capacidad de protección del tipo Access Rate Control.
- Permitir configurar reglas de bloqueo a métodos HTTP no deseados.
- Permitir configurar listas negras de bloqueo y listas blancas de confianza, basadas en dirección IP de origen.

- Permitir la liberación temporal o definitiva (white-list) de direcciones IP bloqueadas por tener originado ataques detectados por la solución.
- Cada componente debe tener la funcionalidad de proteger el website contra acciones de defacement, con la funcionalidad opcional de recuperación automática y rápida del website en caso de fallo.
- Cada componente debe tener la capacidad de investigar y analizar todo el tráfico HTTP para validar si está en conformidad con la respectiva RFC, bloqueando ataques y tráfico no conformes.
- Cada componente debe ser capaz de hacer aceleración de SSL, donde se instalan los certificados digitales en la solución y las requisiciones HTTP sean enviadas a los servidores sin criptografía.
- La solución debe de ser capaz de funcionar como terminador de sesión SSL para aceleración de tráfico.
- Para SSL/TLS offload soportar al menos, TLS 1.0, 1.1 e 1.2.
- La solución debe tener la capacidad de almacenar certificados digitales de CA's.
- La solución debe de ser capaz de generar CSR para ser firmado por una CA.
- La solución debe de ser capaz de chequear los certificados válidos y que no fueron revocados por una lista CRL.
- La solución debe contener las firmas de robots conocidos como link checkers, indexadores de web, search engines, spiders y web crawlers que puedan ser añadidos a los perfiles de control de acceso, así como resetear dichas conexiones.
- La solución debe soportar un sistema de reputación de direcciones IP públicas conocidas como origen de ataques de botnets. Este sistema debe de ser actualizado automáticamente.
- La solución debe permitir la customización o reenvío de solicitaciones y respuestas HTTP en el HTTP Host, Request URL HTTP, HTTP Referer, HTTP Body y HTTP Location.
- La solución debe permitir crear reglas definiendo el orden con que las páginas deben de ser accedidas para prevenir ataques como cross-site request forgery (CSRF).
- La solución debe de tener la capacidad de definir restricción a determinados métodos HTTP.
- La solución debe tener la capacidad de proteger contra detección de campos ocultos.
- Debe generar perfil de protección automáticamente a partir de reporte en formato XML generado por scanner de vulnerabilidades de terceros.
- Debe de ser capaz de hacer compresión del contenido HTTP, para reducir la cantidad de información enviada al cliente.
- Soportar redirección y reescritura de requisiciones y respuestas HTTP.
- Permitir redirección de requisiciones HTTP para HTTPS.
- Permitir reescribir la línea URL del encabezado de una requisición HTTP.
- Permitir reescribir el campo HOST del encabezado de una requisición HTTP.
- Permitir reescribir el campo REFERER del encabezado de una requisición HTTP.
- Permitir redirigir requisiciones para otro website.
- Permitir enviar respuesta HTTP 403 Forbidden para requisiciones HTTP.
- Permitir reescribir el parámetro LOCATION en el encabezado HTTP de una respuesta de redirección HTTP de un servidor web.
- Permitir reescribir el cuerpo ("body") de una respuesta HTTP de un servidor web.
- Permitir añadir el campo X-Forwarded-For para identificación de la dirección IP real del cliente cuando en modo proxy reverso.
- Debe permitir al administrador crear nuevas firmas y/o cambiar las firmas preexistentes.
- Para los eventos de ataques web podrán soportar un análisis de información unificada y contextual pudiendo ser en la nube con capacidad de analizar miles de eventos WAF como tendencias, patrones de amenazas y campañas de ataque en distintos contextos.
- También se aceptará que la plataforma se alimente de una nube de inteligencia que analiza miles de eventos WAF como tendencias, patrones de amenazas y campañas de ataque en 7 Gbps distintos contextos
- La solución debe ser capaz de realizar parches virtuales para mitigar vulnerabilidades críticas sin la necesidad de realizar cambio alguno en el servidor web.

- Cada componente deberá ser otorgado en calidad de alquiler, formando parte del servicio ofertado.

Licencias y suscripción de software

Toda suscripción de software deberá estar cubierta por el periodo de garantía de la solución.

El Contratista será responsable del transporte, recepción, instalación, configuración y puesta en operación de los componentes para la protección a las aplicaciones web. Así como también, el Contratista será el responsable del mantenimiento preventivo y correctivo de los componentes cedidos en calidad de alquiler.

b) Solución Anti-DDoS

El Contratista deberá proveer Un (1) Appliance o Equipamiento de protección ante ataques DDoS, de tecnología vigente, nuevo y de primer uso, de tipo volumétrico, y de capa de aplicaciones, así como también que ejecute actualizaciones con la plataforma centralizada del fabricante. El componente será instalado en el centro de datos, ubicado en el Edificio Raúl Porras Barrenechea, ubicado en el Jirón Ucayali N.° 337, Cercado de Lima. El componente mencionado deberá cumplir con lo siguiente:

Características del equipo

- El sistema debe de ser un appliance dedicado a proporcionar disponibilidad, por lo que no se aceptarán dispositivos que dependan de información de estado de la conexión para poder mitigar, cómo: firewalls, sistemas de prevención y detección de intrusos (IDS/IPS) y las variantes o combinaciones como UTM, NGFW, NGIPS. En caso de tratarse de una solución que involucre varios componentes, ninguno de estos debe depender de la información de estado para poder mitigar (Stateless), por lo que no se aceptaran WAF, IPS, o Firewalls cómo complemento a la solución anti-DDoS dado su naturaleza Stateful.
- Debe incluir al menos 4 interfaces 1GE RJ45.
- Las interfaces de red deben incluir la función de bypass físico o fail-open/fail-close a nivel de RJ45, o la solución debe contar con funciones de alta disponibilidad utilizando 2 equipos de similares características.
- Tener al menos 240GB SSD.
- El equipo deberá tener fuentes duales redundantes de tipo hot swap.
- Debe soportar al menos 1Gbps de throughput con crecimiento mínimo a 7Gbps sin necesidad de cambiar el equipo, solo cambiando la subscripción o licencia.
- La latencia debe ser de menos de 80 microsegundos (us).
- El sistema debe poder incluir un módulo de descifrado de tráfico SSL o TLS integrado en el mismo dispositivo basado en hardware.
- La inspección de tráfico SSL deberá de soportar suites de cifrado ECDH (Curvas Elípticas de Diffie Hellman) y RSA.
- El sistema deberá de prevenir el bloqueo global de CDN o proxys en línea o por derivación

Funcionalidades Generales

- La solución deberá estar basada 100% appliance de propósito específico para identificar y mitigar ataques DDoS en las capas 3, 4 y 7, no se aceptará soluciones basadas en software o hardware genérico y/o open source.
- La detección deberá ser basada en el análisis del comportamiento de los patrones de tráfico.
- El equipo deberá detectar y mitigar los ataques de día cero.
- La detección y mitigación de ataques deberán ser realizados en un CHIP específico para el procesamiento del tráfico o por procesadores dedicados para funciones de tipo servidor.

- La solución deberá de realizar a cabo una evaluación continua, cuando se encuentre bajo un ataque, para minimizar los falsos positivos, lo que garantiza que el tráfico real no sufrirá ningún tipo de interrupción.
- El dispositivo deberá crear automáticamente los límites para el comportamiento del tráfico de red.
- Deberá contar con un modo de aprendizaje para permitir crear perfiles detallados del tráfico de la red.
- Deberá contar un modo de prevención, donde los límites de tráfico aprendido se pueden utilizar para mejorar los perfiles de tráfico.
- Debe tener la capacidad de segmentar los perfiles de seguridad o grupos de protección, proporcionando perfiles completamente independientes uno del otro.
- Las contramedidas/protecciones de la solución deben ser flexibles y no requerir detener/reiniciar el servicio para poder ser activadas/desactivadas o modificadas, deben permitir el cambio en los parámetros de protección mientras se encuentran en ejecución y visualizar el efecto de estos cambios sobre el tráfico hacia los recursos protegidos a través de su interfaz gráfica embebida.
- Los puertos de cobre deben tener un mecanismo de derivación incorporado que permitirá que el tráfico continúe cruzando por el equipo en caso de fallo del mismo.
- Deberá tener un período de tiempo configurable para el bloqueo de direcciones IP que se identificaron como la fuente de los ataques de inundación.
- Deberá ser capaz de proteger a los segmentos de red IPv6.
- Deberá ser capaz de configurar los puertos no estándar para escuchar el protocolo HTTP.
- Deberá ser capaz de configurar direcciones IP para el lanzamiento de las contramedidas.
- Deberá contar con un ajuste de emergencia para la protección contra ataques emergentes o de lo contrario, debe permitir que se ajusten parámetros o niveles de seguridad de manera rápida.

Funcionalidades de inspección de paquetes

- El equipo propuesto deberá tener tecnología de inspección de paquetes para el monitoreo del estado para vectores de ataque específicos.
- El equipo propuesto deberá tener tecnología de inspección de paquetes para el continuo ajuste de los valores para limitar la velocidad de transferencia.
- El equipamiento propuesto deberá contar con una tecnología de inspección de paquetes detallada de cada uno de los paquetes que cruza por el equipo.
- El equipo propuesto debe tener tecnología de inspección de paquetes por análisis heurístico.
- El equipo propuesto debe tener la tecnología de inspección de paquetes por análisis del comportamiento predictivo.

Funcionalidades de chequeo de paquetes

- El equipo propuesto debe tener procesos de verificación con la capacidad de realizar filtros de tráfico utilizando expresiones regulares u métodos de mitigación similares o más avanzados.
- El equipo propuesto debe tener procesos de verificación activa.
- El equipo propuesto debe tener procesos de verificación con el reconocimiento de anomalías.
- El equipo propuesto debe tener procesos de verificación con el análisis de protocolos válidos.
- El equipo propuesto debe tener procesos de verificación con definición de los límites de tasa de transferencia.
- El equipo propuesto debe tener procesos de verificación para crear listas blancas y listas negras.
- El equipo propuesto debe tener procesos de verificación con reconocimiento del estado de la anomalía.
- El equipo propuesto debe tener procesos de verificación con filtrado de ataques del tipo Stealth (opcional)

- El equipo propuesto debe tener procesos de verificación con rastreo de direcciones origen.
- El equipo propuesto debe tener procesos de verificación de legitimidad para comprobar la dirección IP correspondiente (anti-spoofing)

Funcionalidades de prevención de ataques

- El equipo propuesto debe tener mecanismos de prevención contra grandes volúmenes de (inundaciones), que limita el número de conexiones simultáneas y nuevas conexiones.
- El equipo propuesto debe tener mecanismos de prevención contra grandes volúmenes de tráfico (inundaciones), utilizando técnicas para detectar, bloquear, rastrear y reiniciar las conexiones TCP inactivas.
- El sistema deberá de prevenir el bloqueo global de CDN o proxys o en línea o por derivación.
- El equipo propuesto debe tener mecanismos de prevención contra grandes volúmenes de (inundaciones), con la verificación de la legitimidad de la dirección IP.
- El equipo propuesto debe tener mecanismos de prevención contra grandes volúmenes de tráfico (inundaciones), que limite la tasa de paquetes.
- El sistema debe tener la capacidad de cambiar el nivel de protección a alto de manera automática cuando el tráfico total exceda los umbrales definidos.
- La solución deberá tener capacidad de detección por comportamiento realizando una estimación de umbrales adaptativos para parámetros críticos
- El equipo propuesto debe tener mecanismos de prevención contra grandes volúmenes de tráfico (inundación), con rastreo de direcciones de origen.
- El equipo propuesto debe tener mecanismos de prevención contra grandes volúmenes de tráfico (inundaciones) contando con mecanismos de mitigación SYN, ACK, Retransmisiones SYN, DNS.

Funcionalidades de mitigación de ataques

- Ataques de inundación por avalancha TCP/UDP/HTTP.
- El equipo propuesto debe tener mecanismos de mitigación de ataques en la capa 3, contra grandes volúmenes de tráfico (floods).
- El equipo propuesto debe tener mecanismos de mitigación de ataques en la capa 3 en contra de grandes volúmenes de tráfico (inundación) para prevenir las inundaciones protocolos fragmentados.
- Protección ataques volumétricos tipo Chargen o Fraggle Attacks.
- Mitigación de ataques basados en aplicación / Web Servers – HTTP: incorporar firmas o anomalías, expresión regular de carga útil.

.

- Mitigación de ataques basados en aplicación / Servidores SIP: SIP malformado, requerimiento de límite de velocidad SIP (opcional).
- Mitigación de ataques basados en aplicación / Prevención L3-L4: paquetes inválidos, detección inundación ICMP /TCP SYN, expresión regular de carga útil, tasa basada en bloqueo, asignación de tráfico o Mitigación de ataques basados en aplicación / Prevención L3-L4: paquetes inválidos, detección inundación ICMP /TCP SYN, expresión regular de carga útil, tasa basada en bloqueo, asignación de tráfico.
- Mitigación de ataques basados en aplicación / Basados en Volumen: Chargen, Fragmentación ICMP/UDP/TCP, NTP reflexion, SSDP o Mitigación de ataques basados en aplicación / Prevención L3-L4: paquetes inválidos, detección inundación ICMP /TCP SYN, expresión regular de carga útil, tasa basada en bloqueo, asignación de tráfico.
- El equipo propuesto debe tener mecanismos de mitigación de ataques en la capa 3 contra grandes volúmenes de tráfico (inundación) para evitar inundaciones fuente y destino.
- El equipo propuesto debe tener mecanismos de mitigación de ataques en la capa 3 en contra de grandes volúmenes de tráfico (inundaciones), permitiendo creación de políticas de control en la ubicación geográfica y la inclusión de la reputación de la dirección IP.

- El equipo propuesto debe tener mecanismos de mitigación de ataques en la capa 4 en contra de grandes volúmenes de tráfico (inundación), con la prevención en todos los puertos TCP.
- El equipo propuesto debe tener mecanismos de mitigación de ataques en la capa 4 en contra de grandes volúmenes de tráfico (inundación), con la prevención en todos los puertos UDP.
- El equipo propuesto debe tener mecanismos de mitigación de ataques en la capa 4 en contra de grandes volúmenes de tráfico (inundación), con la prevención de todos los tipos y códigos ICMP.
- El equipo propuesto debe tener mecanismos de mitigación de ataques en la capa 4 en contra de grandes volúmenes de tráfico (inundación), para evitar la gran cantidad de conexiones en la capa 4.
- El equipo propuesto debe tener mecanismos de mitigación de ataques en la capa 4 en contra de grandes volúmenes de tráfico (inundación), para prevenir ataques SYN, ACK, RST y FIN.
- El equipo propuesto debe tener mecanismos de mitigación de ataques en la capa 4 en contra de grandes volúmenes de tráfico (inundación), para impedir el establecimiento de conexiones excesivas por origen.
- El equipo propuesto debe tener mecanismos de mitigación de ataques en la capa 4 en contra de grandes volúmenes de tráfico (inundación), para prevenir los ataques enviados por redes de ordenadores zombis o bots.
- El equipo propuesto debe tener mecanismos de mitigación de ataques en la capa 4 en contra de grandes volúmenes de tráfico (inundación), con prevención contra inundaciones que violen el estado de las conexiones TCP.
- El equipo propuesto debe tener mecanismos de mitigación de ataques en la capa 7 en contra de grandes volúmenes de tráfico (inundación), HTTP METHOD: GET, HEAD, OPTIONS, POST.
- El equipo propuesto debe tener mecanismos de mitigación de ataques en la capa 7 en contra de grandes volúmenes de tráfico (inundación), para Floods de User Agent.
- El equipo propuesto debe tener mecanismos de mitigación de ataques en la capa 7 en contra de grandes volúmenes de tráfico (inundación), para Floods de hosts.
- El equipo propuesto debe tener mecanismos de mitigación de ataques en la capa 7 en contra de grandes volúmenes de tráfico (inundación), validando parámetros obligatorios del encabezado HTTP.
- El equipo propuesto debe tener mecanismos de mitigación de ataques en la capa 7 en contra de grandes volúmenes de tráfico (inundación), validando accesos secuenciales de HTTP.
- El equipo propuesto debe tener mecanismos de análisis de reputación de la dirección IP.
- Se debe tener análisis dinámico de la reputación de la dirección de IP.
- Tener las actualizaciones automáticas de bases de datos de reputación de direcciones IP.

Funcionalidades de mitigación de ataques de DNS

- Debe tener mecanismos avanzados de mitigación de ataques de anomalías en el encabezado de DNS.
- Debe tener mecanismos avanzados de mitigación de ataques de DNS Query-response.
- Debe tener mecanismos avanzados de mitigación de ataques del tipo Flood DNS.
- Debe tener mecanismos avanzados de mitigación de ataques del tipo Query-DNS inesperada.
- Debe tener mecanismos avanzados de mitigación de ataques del tipo DNS-Response no solicitado.
- Debe tener mecanismos avanzados de mitigación de ataques de Cache de DNS response sobre flood.
- Debe tener mecanismos avanzados de mitigación de ataques de Flood de DNS Query por origen dentro del TTL.

Funcionalidades de Gestión

- Debe contar con una interface gráfica vía WEB embebida en el appliance basada en SSL (HTTPS) para la administración del equipo.
- Contar con una línea de comandos.
- Se debe permitir la creación de rutas estáticas para que pueda configurarse de forma remota desde cualquier punto de la red.
- El acceso administrativo deberá tener la opción de estar limitado a equipos específicos.
- El equipo debe ser capaz de enviar los registros de logs a un servidor remoto.
- El equipo debe ser capaz de ser supervisado por SNMP para obtener información sobre el sistema.
- El equipo debe ser capaz de enviar correos electrónicos para las alertas del sistema
- Debe ser capaz de autenticar a los usuarios administradores a través de RADIUS.
- Debe ser capaz de crear administradores con acceso total o de sólo lectura.

Funcionalidades de Monitoreo

- Deberá contar con métricas de monitoreo de tráfico por dirección de origen.
- Deberá contar con métricas de monitoreo de tráfico por TCP SYN.
- Deberá contar con métricas de monitoreo de tráfico por conexiones establecidas.
- Deberá contar con métricas de monitoreo de tráfico por TCP SYN por origen.
- Deberá contar con métricas de monitoreo de tráfico por puerto TCP o UDP.
- Deberá contar con métricas de monitoreo de tráfico por paquetes fragmentados.
- Deberá contar con métricas de monitoreo de tráfico por cantidad de accesos a URL.
- Deberá contar con métricas de monitoreo de tráfico por verificación de anti-spoofing.
- Deberá contar con métricas de monitoreo de tráfico de URL asociadas.
- Deberá contar con métricas por interface (opcional)
- Deberá contar con métricas por política de protección (opcional)
- Deberá contar con métricas a nivel de Capa 3: por origen, destino, protocolo, orígenes únicos y paquetes fragmentados (opcional)
- Deberá contar con métricas a nivel de Capa 4: SYN (Paquetes, Por Origen, Por Destino, SYN/ACK, SYN/ACK por destino), TCP, UCP, Conexiones Concurrentes por Origen, Conexiones Nuevas, Sesiones TCP, ICMP (opcional)
- Deberá contar con métricas a nivel de Capa 7: HTTP (Methods, URLS, Hosts, Referers, Cookies, User Agents), DNS (Query, Query por origen, orígenes sospechosos, Fragmentos, QType MX, QType All, QType Zone Transfer, DNS Response Code, DNSSEC), NTP (Request, Responder, Broadcast), DTLS, QUIC (opcional).

Funcionalidades de Reportes

- Deberá contar con reportes de estadísticas por puertos (Paquetes, Bits).
- Deberá contar con reportes de estadísticas de los recursos protegidos (Paquetes, Bits).
- Deberá contar con reportes de estadísticas del número total de paquetes descartados.
- Deberá contar con reportes de estadísticas de paquetes descartados por inundaciones.
- Deberá contar con reportes de estadísticas de paquetes descartados en la capa 7 (HTTP y DNS).
- Deberá contar con reportes de estadísticas de paquetes descartados por listas de control de acceso.
- Deberá contar con reportes de estadísticas de paquetes descartados por anomalías.
- Deberá contar con reportes de estadísticas de capa 3 (origen más activo, destino más activo, paquetes fragmentados, direcciones bloqueadas y por protocolos).
- Deberá contar con reportes de estadísticas de la capa 4 (paquetes SYN, SYN por origen, SYN por destino, conexiones por origen, conexiones por destino, ACK, RST, FIN por destino, conexiones establecidas por destino, nuevas conexiones, puertos TCP, UDP, tipos y códigos ICMP).
- Deberá contar con reportes de estadísticas de la capa 7 (DNS: Consultas, Consultas por Origen, Origenes sospechosos, Contar consultas, Contar por tipo de consultas MX, Consultas totales, Consultas por tipo transferencia de Zona, Consultas Fragmentadas, Respuestas no solicitadas, Consultas no solicitadas, Descartes LQ, Descartes TTL, Descartes por cache, Descartes por IP Forjados, DNS Rcodes).

- Debe contar con un monitoreo gráfico que muestra las estadísticas del rendimiento para cada uno de los puertos de los equipos en paquetes y bits.
- El sistema debe proporcionar estadísticas detalladas para cada protección, mostrando su impacto en el tráfico durante los últimos 5 minutos (opcional), 1 hora, 24 horas, 7 días o un rango de tiempo.
- Debe contar con un monitoreo gráfico que muestra las estadísticas del rendimiento de todos los paquetes descartados por inundaciones, firmas, anomalías y otras amenazas.
- Los gráficos de monitoreo de paquetes descartados se deben mostrar al menos en la capa 3, capa 4 y capa 7.
- Cada componente deberá ser otorgado en calidad de alquiler, formando parte del servicio ofertado.
- El componente que el Contratista instale y utilice para la protección ante ataques DDoS, deberá contar con soporte del fabricante.
- Deberá contar con reportes de Top Attacks - Drop count by DDoS attack event type (opcional).
- Deberá contar con reportes de Top ACL Attacks - Drop count by ACL rules and Global ACL rules (opcional).
- Deberá contar con reportes de Top Attackers - Drop count by Source IP address (opcional).
- Deberá contar con reportes de Top Attacked Subnets - Drop count by Protected Subnet (opcional).
- Deberá contar con reportes de Top ACL Subnets - Drop count by ACLs associated with Protected Subnets (opcional).
- Deberá contar con reportes de Top Attacked Protocols - Drop count by Protocol (opcional).
- Deberá contar con reportes de Top Attacked TCP Ports - Drop count by TCP port (opcional).
- Deberá contar con reportes de Top Attacked UDP Ports – Drop count by UDP port (opcional).
- Deberá contar con reportes de Top Attacked ICMP Type Codes - Drop count by ICMP Type / Code (opcionjal).
- Deberá contar con reportes de Top Attacked HTTP URLs - Drop count by HTTP URL (hash index)(opcional).
- Deberá contar con reportes de Top Attacked HTTP Methods - Drop count by HTTP method (opcional).
- Deberá contar con reportes de Top Attacked HTTP Hosts - Drop count by Host header (hash index) (opcional).
- Deberá contar con reportes de Top Attacked HTTP Referers - Drop count by Referer header (hash index).
- Deberá contar con reportes de Top Attacked HTTP Cookies - Drop count by Cookie header (hash index) (opcional).
- Deberá contar con reportes de Top Attacked HTTP User Agents - Drop count by User-Agent header (hash index) (opcional).
- Deberá contar con reportes de Top Attacked HTTP Servers - Drop count by HTTP server IP address (opcional).
- Deberá contar con reportes de Top Attacked Destinations - Drop count by Destination IP address (opcional).
- Deberá contar con reportes de Top Attacked SPPs - Drop count by SPPs (opcional).
- Deberá contar con reportes de Top Attacked ACL SPPs - Drop count by ACL SPPs (opcional).
- Deberá contar con reportes de Top Attacked DNS Servers - Drop count by DNS server IP address (opcional).
- Deberá contar con reportes de Top Attacked DNS Anomalies - Drop count due to anomalies by DNS server IP address (opcional).
- Deberá contar con reportes de Top Successful Logins (opcional).
- Deberá contar con reportes de Top Failed Logins (opcional).

El Contratista será responsable del transporte, recepción, instalación, configuración y puesta en operación del componente para la protección ante ataques DDoS. Así como también, el Contratista será el responsable del

mantenimiento preventivo y correctivo del componente cedido en calidad de alquiler.

c) Seguridad Perimetral

El Contratista deberá proveer Cuatro (4) Appliance o Equipamiento de Firewall Externos e Internos con políticas de acceso definidas por el Ministerio de Relaciones Exteriores, los equipos deberán tener las funciones antimalware y de prevención de intrusos, así como también estar configurados en alta disponibilidad y ser de tecnología vigente, nuevo y de primer uso. Deberá contarse asimismo con una instancia de Firewall para la granja de servidores que contendrá su módulo IPS para inspección externa e interna y la funcionalidad antimalware. Los componentes serán instalados en el Edificio Raúl Porras Barrenechea, ubicado en el Jirón Ucayali N.º 337, Cercado de Lima.

Los componentes requeridos deberán ser del tipo NGFW, los cuales se configurarán dos (2) como perimetral externo y dos (2) como interno, configurados en Alta Disponibilidad (Activo/Standby).

La plataforma de NGFW debe demostrar liderazgo en la industria, para ello debe haber alcanzado el nivel de "Strong Performers" o "Leaders" en el reporte (indicador) de Forrester para Enterprise Firewalls del 2022, asimismo debe ser considerado líder en el reporte (indicador) de Gartner para Network Firewalls del 2022.

Los componentes para los Firewalls Externos deberán contar con las siguientes características mínimas:

- NGFW Throughput con todas las funcionalidades definidas por cada fabricante 11 Gbps como mínimo, medido en condiciones reales o con tráfico mixto de aplicaciones.
- Capacidad mínima de sesiones concurrentes de 1.2 millones medidos en HTTP y HTTPS u 8 millones de sesiones concurrentes como mínimo medidos en TCP
- El throughput de prevención de amenazas (Control de aplicaciones, IPS, antivirus y antimalware), deberá ser de 10 Gbps como mínimo, medido con transacciones HTTP de 64K o tráfico mixto o mixto empresarial, presentar carta de fabricante en caso se requiera el sustento
- Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el modo más alto de inspección de seguridad y este deberá estar público en su hoja de datos. Se debe garantizar que el equipo no degrade su rendimiento por debajo de lo requerido al habilitar los módulos de seguridad..
- Inspección SSL throughput de 8 Gbps medidos con la funcionalidad de prevención de amenazas (control de aplicaciones, IPS, antivirus y antimalware) activada simultáneamente, o throughput de inspección SSL de 8 Gbps como mínimo con la funcionalidad de IPS sobre HTTPS habilitada, además esta información deberá estar en la documentación pública del fabricante.
- Capacidad mínima de nuevas sesiones o conexiones por segundo de 140,000 medidos en HTTP
- Cada componente debe soportar IPV4 y IPV6.
- 06 interfaces de red 1G SFP y 06 interfaces RJ45 como mínimo.
- 02 interfaces de red 10G SFP+, incluir sus módulos correspondientes de fibra óptica multimodo.
- Para ahorro en el Datacenter, cada componente debe ocupar como máximo 2 RU de espacio en los racks.
- Cada componente podrá soportar la creación de dominios virtuales (Firewall's independientes dentro de un solo dispositivo) cantidad como mínimo igual a 5.
- Cada componente debe proporcionar mecanismos de seguridad de VLANs embebidos en el mismo equipo.
- Cada componente debe soportar esquemas de operación en modo ruteado y modo transparente.
- Cada componente debe soportar la creación de zonas y conductos para elevar el nivel de seguridad.

- Cada componente debe contar con capacidad para integrar esquemas de red NAT/PAT (Network Address Translation/Port Address Translation).
- Cada componente debe contar con un mecanismo de control basado en técnicas "stateful inspection" u otra tecnología que permita el reconocimiento de aplicaciones en capa 7 del modelo OSI, incluso para los protocolos connection-less como UDP y RPC.
- Cada componente deberá identificar y bloquear tráfico de comunicación HTTPS (SSL/TLS) según su contenido.
- Cada componente debe soportar direccionamiento IPv6 basado: direccionamiento en interfaces; IPv6 lista de acceso; IPv6 rutas estáticas.
- Cada componente debe soportar ser accesado mediante una línea de comando segura HTTPS y CLI (SSH) con la finalidad realizar configuraciones y troubleshooting mediante estos medios.
- Cada componente debe soportar construir políticas basadas en grupos dinámicos.
- Cada componente debe incorporar herramientas para troubleshooting avanzado como la capacidad de visualizar la trazabilidad de los paquetes y realizar capturas de tráfico en tiempo real desde el propio equipo sin la instalación de software o equipamiento adicional.
- La solución deberá complementarse e integrarse con la solución de Sandboxing especificada en este documento.
- La solución debe permitir importar una lista negra de 100,000 URLs como mínimo de manera periódica desde un servicio web local o en la nube a través de HTTP. También se aceptara que las listas negras se encuentren en la nube de inteligencia del fabricante.
- La solución debe soportar balanceo de enlaces basado en SD-WAN, permitiendo definir e intercalar reglas de balanceo y selección de enlaces basado en el desempeño de los enlaces.
- La solución debe contar con la funcionalidad de antivirus.

Los componentes para los Firewalls Externos deberán contar con el Módulo de inspección IDS/IPS de nueva generación. Cumplirá con las acciones de inspección del tráfico y protección frente a intrusiones utilizando técnicas de detección y bloqueo basadas en firmas y reputación.

- El módulo debe contar como mínimo con las siguientes técnicas de análisis de tráfico: identificación del protocolo a través del puerto utilizado; identificación de protocolos que utilizan puertos aleatorios; identificación de protocolos en forma independiente del puerto utilizado.
- Deberá ser capaz de identificar amenazas sobre el tráfico DNS encriptado camuflado sobre HTTPS (DNS over HTTPS – DoH), o también DNS sobre TLS.
- El módulo deberá tener la habilidad de decodificar e inspeccionar todos los protocolos apoyados IPv4 e IPv6.
- El módulo deberá poder crear perfiles de tráfico con reglas específicas para monitorear el tráfico entre dos hosts de la red.
- El módulo deberá permitir una integración a un sistema correlacionador de eventos.
- Con la finalidad de contar con una protección robusta contra amenazas emergentes a nivel mundial, la solución deberá ser capaz de actualizar su base de firmas de malware en tiempo real sin afectar el performance del equipo.
- El módulo deberá generar logs sobre los eventos de filtrado y errores del sistema.
- El módulo deberá soportar la desfragmentación de paquetes IP fragmentados y/o coincidentes.
- El módulo debe soportar geolocalización del origen del tráfico.
- Deberá ser capaz de identificar y bloquear amenazas avanzadas indetectables por firmas o heurística, incluyendo ataques de inyección y command and control realizados por herramientas de hacking sofisticadas.
- La protección antimalware debe estar basada en mecanismos de inteligencia artificial o machine learning o superior, y deberá poder detectar amenazas avanzadas indetectables por firmas o amenazas de día cero

Los componentes que deben tener los dos (2) Firewalls Externos deberán cumplir la siguiente funcionalidad a nivel de VPN Site to Site y las de Client to Site, teniendo las siguientes características:

- Los componentes deberán contar con un SSL-VPN throughput mínima de 4 Gbps.
- Los componentes deberán contar con un IPsec VPN throughput mínima de 10 Gbps.
- Los componentes deberán soportar 2000 túneles VPN IPsec Gateway to Gateway.
- Los componentes deberán soportar 1800 túneles VPN IPsec Client to Gateway.
- Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).
- Soporte para IKEv2 y IKE Configuration Method.
- Soporte de VPNs con algoritmos de cifrado: AES y 3DES.
- Los componentes deberán soportar longitudes de llave para AES de 256 bits como mínimo.
- Los componentes deberán soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14.
- Los componentes deberán soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.
- Posibilidad de crear VPN's entre gateways y clientes con IPSec. Esto es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site.
- La solución debe soportar Fordward Error Correction (FEC) para las VPN sobre IPsec para reducir la pérdida de paquetes durante la transmisión.

Los dos (2) Firewall Internos, deberán cumplir técnicamente las siguientes características:

- NGFW Throughput con todas las funcionalidades definidas por cada fabricante, 17 Gbps sobre NGFW Throughput como mínimo, medido en condiciones reales o con tráfico mixto de aplicaciones.
- El throughput de prevención de amenazas (Control de aplciaciones, IPS, antivirus y antimalware, deberá ser de 15 Gbps como mínimo, medido con transacciones HTTP de 64K o tráfico mixto o mixto empresarial (presentar carta de fabricante, en caso requiera el sustento). Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el modo más alto de inspección de seguridad y este deberá estar público en su hoja de datos. Se debe garantizar que el equipo no degrade su rendimiento por debajo de lo requerido al habilitar los módulos de seguridad
- Capacidad mínima de nuevas sesiones o conexiones por segundo de 260,000 medidos en HTTP o TCP.
- 10 interfaces de red 10G SFP+, incluir sus módulos correspondientes de fibra óptica multimodo.
- 12 interfaces GE RJ45 como mínimo.
- Se deberá incluir 08 transceivers de fibra MMF LC de 10Gbps
- Capacidad mínima de sesiones concurrentes de 5 millones medidos en HTTP o 12 millones medidos con paquetes TCP.
- Se precisa también que se aceptarán equipos que soporten 260 mil conexiones por segundo con transacciones HTTP o 750 mil medido con TCP.
- Inspección SSL throughput de 13 Gbps medidos con la funcionalidad de prevención de amenazas (control de aplicaciones, IPS, antivirus y antimalware) activada simultáneamente o throughput de inspección SSL de 12 Gbps como mínimo con la funcionalidad de IPS sobre HTTPS habilitada.
- Cada componente debe soportar IPV4 y IPV6.
- Para ahorro en el Datacenter, cada componente debe ocupar como máximo 2 RU de espacio en los racks.
- Appliance para la seguridad de navegación web que combine funciones de Proxy Caché, URL Filtering.
- Inspección profunda de contenido de las aplicaciones y monitor de tráfico Layer 4.
- Ofrece gran desempeño y eficacia al combinar una completa y rápida aplicación Proxy y monitor de tráfico L4.
- Los NGFW internos puede ser configurado como un proxy o coexistir con otras proxies
- Debe soportar la configuración de Proxy en Modo Transparente o en Modo Explícito.
- Filtrado de aplicaciones bajo criterios personalizables.

- Debido a que diariamente se crean decenas de miles de nuevas páginas web, la solución deberá ser capaz de analizar en tiempo real si la página web tiene contenido malicioso cuando un usuario intenta acceder.
- Limitar el número y tipos aplicaciones que están autorizadas para funcionar en la red.
- Controlar las aplicaciones en cualquier puerto.
- Cada componente debe detectar como mínimo 2000 aplicaciones y categorizarlas por riesgo y relevancia empresarial, dentro de las cuales están: Adobe Flash, Facebook, Twitter, Skype, Whatsapp, Facetime, LinkedIn, LogMeIn, Anydesk, Netflix, UltraSurf, Gsuit, etc.
- Debe contar con un repositorio en nube del fabricante que permita realizar consultas de URL y recursos DNS no identificados y/o no clasificados al momento de ser registrado en los top level domain, sin necesidad que esa URL o dominio haya pasado por el NGFW (opcional).
- Cada componente debe controlar el uso de las aplicaciones a través de acciones como: Allow, Block/Deny, reset del cliente o del servidor.
- La autenticación integrada a través de los directorios tales como LDAP o Active Directory y capacidad de ejecutar múltiples esquemas de autenticación como NTLM o Básica.
- Cada componente debe permitir la creación de reglas para controlar el uso de aplicaciones a través de las siguientes condiciones: IP, zona, Red, VLAN, Usuarios y Puertos.
- Cada componente debe soportar geolocalización; permitiendo obtener al menos la siguiente información: país, longitud, latitud.
- Cada componente debe permitir bloquear tráfico por geolocalización; ya sea por país o continente.
- Cada componente deberá incluir un sistema de integración con directorio activo.
- Debe permitir crear categorías personalizadas.
- Debe permitir crear política basada en tiempos y días.
- Debe permitir el funcionamiento del IDS/IPS en modo monitoreo y poder alertar tráfico anómalo.
- La solución debe permitir importar una lista negra de 100,000 URLs como mínimo de manera periódica desde un servicio web local o en la nube a través de HTTP. También se aceptará que las listas negras se encuentren en la nube de inteligencia del fabricante
- La solución debe contar con la funcionalidad de antimalware.

Los cuatro (4) Firewalls, tanto externo como interno, deberán cumplir la siguiente funcionalidad a nivel de Prevención de Intrusos y/o Amenazas:

- Cada componente debe contar como mínimo con las siguientes técnicas de análisis de tráfico: identificación del protocolo a través del puerto utilizado, identificación de protocolos que utilizan puertos aleatorios, identificación de protocolos en forma independiente del puerto utilizado.
- Deberá ser capaz de identificar amenazas sobre el tráfico DNS, opcionalmente encriptado camuflado sobre HTTPS (DNS over HTTPS – DoH), o también DNS sobre TLS.
- Cada componente deberá identificar y bloquear tráfico de comunicación HTTPS (SSL/TLS) según su contenido.
- Cada componente debe soportar la creación de firmas customizadas.
- Cada componente debe de soportar la identificación y protección de ataques en protocolos de Voice over IP (VoIP) sobre SIP.
- Cada componente debe permitir tener la flexibilidad de controlar políticas a nivel de dispositivo, puerto, VLAN y direcciones IP.
- Cada componente debe tener la funcionalidad de decodificar e inspeccionar todos los protocolos apoyados IPv4 y IPv6.
- Con la finalidad de contar con una protección robusta contra amenazas emergentes a nivel mundial, la solución deberá ser capaz de actualizar su base de firmas de malware en tiempo real o recurrente sin afectar el performance del equipo.
- Cada componente debe tener la capacidad de ser administrado a través de conexiones SSH, CLI y HTTPS.
- Cada componente debe contar con la funcionalidad Anti-malware.

- Cada componente debe soportar integración a través del directorio activo.
- Cada componente podrá crear reglas de seguridad que permitan proteger al menos los siguientes ataques : ejecución de código, ataques de fuerza bruta, exploit-kits, injección de SQL, ofuscación de código, overflows.
- Cada componente deberá ser capaz de detectar anomalías de tráfico en la red por comportamiento o filtros por categoría de la aplicación "o" el comportamiento de la aplicación.
- Cada componente Debe soportar referencia cruzada como CVE.
- Cada componente debe estar basado en firmas y/o por comportamiento.

Los cuatro (4) Firewalls, tanto externo como interno, deberán cumplir la siguiente funcionalidad a nivel de Protección Avanzada de Malware:

- Detección de amenazas avanzadas de nueva generación, específicamente diseñado para proteger a la institución contra ataques cibernéticos como malware, exploits y amenazas avanzadas persistentes (APT) ó similares.
- La solución debe utilizar una Red de Inteligencia Global que le permita beneficiarse de la información recogida por los esfuerzos de investigación del fabricante.
- La solución debe proteger las comunicaciones desde y hacia los servicios de internet.
- La solución deberá desencriptar el tráfico HTTPS (SSL/TLS) según su contenido.
- La inspección deberá ser realizada en todos los protocolos de red.
- La solución deberá tener la capacidad de detectar y bloquear software malicioso que se aprovecha de vulnerabilidades conocidas y/o sitios web maliciosos.
- La solución debe proporcionar protección contra ataques originados en la web, como descargas de archivos maliciosos y acciones de devolución de llamada (callback) de malware.
- La solución debe detectar la amenaza sin necesidad de conocer la firma, es decir, a través del comportamiento de la propia amenaza o proceso que lo origine.
- La solución debe ser capaz de ejecutar el código sospechoso, acceso URL's y diversos tipos de archivos en un entorno virtual de inspección. Para ello realizará tanto análisis estático (basado en reglas) como dinámico (basado en comportamiento usando diferentes técnicas).
- Cada componente debe soportar la inspección de archivos: documentos de la suite MS Office, documentos PDF, archivos ejecutables, archivos comprimidos, archivos multimedia, Java, Dlls etc.
- La solución debe contar con la capacidad de bloquear, detener o descartar una conexión identificada como maliciosa.
- La herramienta deberá permitir añadir reglas de inspección personalizadas mediante la configuración directa de las mismas o importándolas a través de un archivo.
- La solución debe permitir la identificación de las direcciones IP de origen y destino de los ataques (geolocalización).
- La solución debe proteger a los usuarios internos de manera que prevenga el acceso o descarga a los archivos en tanto estos son analizados en el equipo de emulación, si el archivo es benigno se entrega el archivo original al usuario y si el archivo es maligno se deniega su acceso o descarga.
- La solución debe tener la capacidad de bloquear llamadas a servidores remotos (Callbacks, llamadas de Comando & Control).
- La solución deberá tener la capacidad de conectarse a equipos Sandboxing analizar el comportamiento del malware (análisis dinámico).
- La solución debe poder integrarse de manera nativa con la solución Sandbox solicitada en este pliego, provisto por el mismo fabricante.

Los cuatro (4) Firewalls, tanto externo como interno, deberán cumplir la siguiente funcionalidad (propia o servicio de fábrica) a nivel de Protección del DNS:

- La plataforma deberá ser alimentada por un servicio de inteligencia en nube y en tiempo real, capaz de identificar múltiples amenazas en dominios maliciosos.

- Se aceptará que al menos cuente con una protección contra amenazas sofisticadas basadas en DNS que incluye el bloqueo de dominios de alto riesgo, incluidos dominios maliciosos recién registrados

- El análisis del tráfico DNS se podrá realizar de manera local en el mismo equipo o a través del redireccionamiento del tráfico DNS hacia una plataforma externa (en nube u onpremise) del mismo u otro fabricante.
- En caso de ser una plataforma en nube deberá estar certificado en SOC2 Tipo II de AICPA opcionalmente.
- Deberá ser capaz de prevenir ataques como DNS Tunneling y opcionalmente funcionalidades (tanto de múltiples dominios como consultas a velocidades lentas para evadir los controles) e infiltración y exfiltración de data de DNS
- Deberá ser capaz de prevenir ataques como DGA (Domain Generation Algortihm) y opcionalmente funcionalidades especificas a un fabricante como "Random y de Diccionario, Fast Flux Domains, NXNS Attack, DNS Rebinding, abuso de wildcards, CNAME cloaking
- Deberá soportar el manejo excepciones para poder mitigar los falsos positivos.
- Deberá contar con dashboards mostrando como mínimo la siguiente información: el Dominio, Categoría, Numero de clientes y/o estadísticas sobre la cantidad y tipo de peticiones DNS, clasificación de las amenazas generadas por los dispositivos internos de la entidad.
- Deberá identificar dominios maliciosos inscritos por ciberdelincuentes , desde una lista negra y/o indicadores de compromiso y/o información del fabricante.

Los cuatro (4) Firewalls, tanto externo como interno, deberán contar con una solución centralizada e independiente para la administración de logs y Reportería o por más de un componente del mismo fabricante, la cual deberá cumplir con lo siguiente:

- Deberá ser una solución de tipo appliance del mismo fabricante y deberá poder operar con una capacidad de almacenamiento para logs de eventos como mínimo de 16TB utilizables o después de realizarse el RAID.
- Poseer estadísticas en interfaz gráfica de todo el tráfico que pasa por el equipamiento de seguridad
- Debe gestionar los cuatro (4) firewalls de la entidad para la creación de reglas de seguridad, objetos y actualización de firmas de seguridad como mínimo.
- Resúmenes con la vista correlacionada de aplicaciones amenazas (IPS) URLs y filtro de archivos
- Mostrar las principales aplicaciones por riesgo.
- Mostrar los administradores autenticados, el número de sesiones simultaneas, el estado de las interfaces, mostrar el uso de CPU
- Debe soportar 3000 eventos o log por segundo para garantizar la recepción de absolutamente todos los eventos y políticas de los cuatro (4) firewalls.
- Generación de reportes de:
  -Aplicaciones más utilizadas por usuarios o dirección IP.
  -Utilización de ancho de banda de entrada y salida.
  -Aplicaciones por tasa de transferencia.
  -Hosts por número de amenazas identificadas.
  -Actividades de un usuario específico y grupo de usuarios de AD/LDAP.
  -Reportes personalizados.
  -Reportes programables con envío automático a un correo electrónico.
- Cada componente deberá ser otorgado en calidad de alquiler, formando parte del servicio ofertado.
- En caso la solución centralizada e independiente para la administración de logs y Reportería permita disponer de los logs de las otras soluciones por ser de la misma marca, serán configuradas en coordinación con la OTI del MRE.

El Contratista será responsable del transporte, recepción, instalación, configuración y puesta en operación de los componentes para la seguridad perimetral. Así como también, el Contratista será el responsable del mantenimiento preventivo y correctivo de los componentes cedidos en calidad de alquiler.

d) Seguridad Sandbox.

El Contratista deberá proveer una (1) solución en físico de Sandbox o cloud del propio fabricante, exclusivamente para el análisis de malware avanzado; a través, de la

inspección de archivos y direcciones electrónicas, a fin de detectar malware de día cero, malware polimórfico y otras posibles amenazadas persistentes y avanzadas que existan en la red. Cabe indicar, que en caso se procese datos en la nube del propio fabricante, el contratista deberá de dar cumplimiento a la ley de protección personales o su equivalente vigente en cada país donde esté ubicado el centro de datos de dicha nube. En ese sentido, el Contratista deberá proveer un (01) Appliance o Equipamiento si se propondará una solucion física que permita el óptimo desarrollo de la solución Sandbox. De ser el caso ell componente será instalado en el Edificio Raúl Porras Barrenechea, ubicado en el Jirón Ucayali N.° 337, Cercado de Lima.

Arquitectura y Diseño

- El Contratista en coordinación con la Entidad elegirán las plataformas operativas y el método de implementación idóneos para la institución.
- La solución de Sandbox no deberá presentar conflictos de integración con la Solución de Detección y Respuesta Endpoint (EDR).

Características básicas

- La solución debe analizar por lo menos 4,000 archivos por hora realizando análisis efectivo, es decir con análisis estático y dinámico con prefiltrado habilitado, tambien deberá tener un rendimiento al menos de 350 archivos por hora realizando un analisis dinámico, entiéndase por análisis dinámico aquel que no está basado en firmas, ni prefiltros, sino en emulación y/o ejecución completa del potencial malware para todo el tipo de tráfico que soporta el equipo
- Deberá contar una respuesta del análisis dinámico en un tiempo no mayor a 4 minutos
- Los recursos de sandboxing serán dedicados para el MRE y no un servicio compartido por otras empresas o instituciones
- En caso de que la solución sea física, debe cumplir con lo siguiente
    - Debe contar como mínimo con un throughput de 1 Gbps.
    - Debe tener un disco duro mínimo de 950GB.

- En caso que la solución sea en cloud, se deberá utilizar un sensor para cumplimiento de los mismos requisitos solicitados con su equivalente en físico.
- La solución deberá ser de propósito especifico Sanboxing, La solución se debera integrar a los Firewall Internos y Externos, con el fin de detectar amenzas mediante tecnicas de emulacion
- La extracción del archivo debe escanearse utilizando el laboratorio de virus interno, sin enviar la muestra fuera de la red en caso la solución sea física.
- La emulación deberá dar en sistemas operativos Windows, Linux, Android y (opcional) MacOS.
- Los datos forenses deben almacenarse en el local dentro de la plataforma o nube.
- El Sandbox debe tener la capacidad de escanear y ejecutar los archivos recopilados en un ambiente aislado para un análisis profundo.
- La solución debe detectar malware avanzado, también debe descubrir malware avanzado de día cero, a través de la emulación o ejecución que las soluciones basadas en firmas normalmente no detectan.
- La solución debe poder analizar cualquier tipo de archivo mediante el uso de múltiples aplicaciones y múltiples versiones, que incluyan: exe, dll, pdf, doc, docx, xls, xlsx, swf, arj o wsf, iso, htm o hta, html, upx o aspx, rar, cmd o Shell script, zip, ppt, pptx, rtf, 7z, rar, entre otros.
- La solución debería ser capaz de lidiar con las técnicas de evasión.
- La solución debe tener la capacidad de verificar / ejecutar un análisis en todos los hosts para cualquier nombre de archivo, extensiones ejecutables de archivo, archivo MD5 / SHA1 o IOC provisto.
- La solución debe defender contra ataques avanzados persistentes / de día cero, que incluyen, pero no se limitan a:

    ✓ Malware general.
    ✓ Ataques de día cero.
    ✓ Ransomware.

- ✓ Inyección SQL.
- ✓ Hacktivismo.
- ✓ Clickjacking.
- ✓ Spyware.
- ✓ Ataques de botnet.
- ✓ Rootkits.

- La solución debe detectar malware sin depender de firmas o listas estáticas que requieren actualización constante.
- La solución debe proporcionar una visibilidad rápida a través de múltiples canales de comunicación para identificar amenazas.
- La solución debe ser capaz de detectar el ataque localmente o en un servicio en la nube.
- La solución debe ser capaz de identificar con precisión el malware y mantener una tasa de falsos positivos muy baja, es decir que la que la solución tenga la capacidad de reducir la tasa de falsos positivos a través de distintas técnicas que el fabricante posea. La detección debe incluir protección contra el malware omitido por productos de seguridad existentes. La solución debe ser capaz de identificar con precisión los archivos maliciosos, que incluyen, entre otros, cualquier extensión de archivo o aquellos achivos que requieren la actualización paquetes de contenido para ejecución, archivo (incluidos archivos protegidos con contraseña) u ofuscación.
- La solución debe utilizar una red de inteligencia global para beneficiarse de la información recopilada por los esfuerzos de investigación del proveedor, en la que los suscriptores reciben y opcionalmente comparten inteligencia de malware, como ataques de día zero y destinos de callback.
- La solución debe ser capaz de proporcionar datos forenses detallados del objeto malicioso. Los datos forenses deben incluir, entre otros:
  - ✓ Tráfico de malware activo.
  - ✓ Grabación de video de la VM durante la ejecución del malware o proporcionar una lista de reproducción por reproducción de toda la actividad registrada.
  - ✓ Descarga de captura de paquetes o capturas de pantalla.
- La solución debe (si es necesario) permitir la comunicación de red desde el análisis VM (Máquina Virtual) / Sandbox a Internet. El malware dentro del entorno limitado de VM debe estar permitido (si es necesario) para comunicarse con cualquier C & C o URL en Internet. Precisar que las VMs deberán ser de uso exclusivo para uso en la entidad, y esto deberá sustentarse con documentación pública y/o documentación del fabricante.
- La solución debe proporcionar detección de amenazas desde cualquier fuente, incluidas, entre otras, las siguientes:
  - ✓ A través de descargas web.
  - ✓ A través del contenido copiado de dispositivos de almacenamiento que se ejecuten en cualquiera de las estaciones de trabajo de la entidad, enlaces o archivos adjuntos en correos electrónicos.
  - ✓ Infección entregada a través de contenido encriptado.
- La solución debe tener la capacidad de detección y respuesta para eliminar el enfoque tradicional del equipo de seguridad (detecta, notifica y resuelve manualmente).
- Eliminar y poner en cuarentena malware o archivos temporales en las carpetas de las estaciones de trabajo.

Administración y reportes

- La solución debe tener políticas unificadas, reportes centralizados y análisis forenses procesables dentro de una consola única para la administración centralizada.
- La solución debe analizar URLs en busca de amenazas internas o externas.
- La solución debe proporcionar herramientas para realizar análisis de causa desde la raíz.
- Capacidades de detección y reportes con respecto al usuario que generó el archivo a ser analizado, el dispositivo origen (ip origen) del archivo y el estado del análisis respectivamente.
- La alerta inmediata de incidentes y sistemas que requieran tomar una acción inmediata.

- Proporcionar visibilidad en equipos adicionales en la organización en donde puede existir esta amenaza.
- Visibilidad completa para rastrear y analizar malware.
- Identificar malware avanzado que puede ser único o día cero.
- Debe permitir la exportación de reportes relacionados con malware.
- La solución debe ser capaz de integrarse con SIEM para la administración de logs.
- La solución debe poder enviar notificaciones por correo electrónico.
- Si la solución es física o en ambiente nube, debe permitir, la implementación del agente en un entorno debe ser rápida y automática.
- Fuente de amenazas de terceros y propias que brinde inteligencia de amenazas para identificar ataque de terceros.
- Compartir datos con sistemas de terceros (SIEM, análisis, flujo de trabajo, etc.)
- Si la solución es física debe permitir, la sincronización del tiempo con un servidor NTP local.
- Si la solución es física, debe permitir la creación de cuentas con diferentes roles utilizados para administrar la solución, solo monitorear las alertas o revisar los cambios (opcional).
- Si la solución es física, cada componente deberá ser otorgado en calidad de alquiler, formando parte del servicio ofertado.

El Contratista será responsable del transporte, recepción, instalación, configuración y puesta en operación del componente para la seguridad Sandbox. Así como también, el Contratista será el responsable del mantenimiento preventivo y correctivo del componente cedido en calidad de alquiler.

e) Filtro de Correos Electrónicos

El Contratista deberá proveer un (1) Appliance o Equipamiento de seguridad para filtro de correos. En este componente se habilitarán los filtros de seguridad para el envío de correos de los sistemas internos hacia los usuarios, con el objetivo de tener un filtro de seguridad, gestión y visibilidad de dichos correos que pasen por la herramienta. El componente será instalado en el Edificio Raúl Porras Barrenechea, ubicado en el Jirón Ucayali N.° 337, Cercado de Lima.

La entidad proporcionará la conectividad a nivel de Switches, los equipos serán conectorizados mediante cableado UTP RJ45.

Características de los Componentes

- Mínimo de 4 interfaces de 1Gbps RJ-45.
- Tener al menos 1TB de espacio en disco.
- Permitir configurar por lo menos 5 dominios.
- Deberá procesar al menos 50,000 mensajes por hora.
- Soporte de los protocolos de correo electrónico SMTP y ESMTP.
- Sistema operativo propietario, desarrollado por el fabricante.
- La solución debe contar con un puerto de consola dedicado.
- Incluir actualizaciones periódicas o inmediatas, de nuevas reglas y algoritmos de correo no deseado.
- Distribución diaria de las actualizaciones, el cual debe estar correctamente licenciado hasta el término del servicio, continua y automática contra firmas de ataques.
- Soportar el manejo de colas de envío y recepción de correo en paralelo (por destino), por dominio o dirección IP.
- Soportar manejo de máximas conexiones concurrentes desde una sola IP configurable por dominio o IP origen.
- Soportar manejo de máximos mensajes por conexión configurable por dominio o IP origen.
- Soportar manejo de límite de máximo destinatarios por mensaje configurable por dominio o IP origen.
- Soportar manejo de límite de recepción de correo (rate limit) configurable por dominio o dirección IP origen

- Funcionamiento en modo antirelay.
- Interoperabilidad con MS Exchange Server 2000 o superior.
- Integracion con Microsoft Outlook e IBM Notes.
- Integración con LDAP para Microsoft Active Directory e IBM Notes.
- Soporte para enmascaramiento de dominio, por LDAP en el correo saliente.
- Tecnología de Gateway Virtual para configurar más de una dirección IP sobre una interfase ethernet para el envío o recepción de correos electrónicos
- Servicio de base de datos de filtrado por reputación, desarrollada y mantenido por el fabricante.
- Contar con una cuarentena a la que se puedan dirigir los correos electrónicos dudosos, para su futura revisión.
- Período de almacenamiento en cuarentena configurable.
- Envío de un correo electrónico con resumen del contenido de las casillas de correo individuales para cuarentena a todos los usuarios finales, con mensajes en cuarentena, y al administrador del sistema. El envío será automático y en forma diaria.
- Proporcionar acceso vía Web a los usuarios hacia sus respectivas casillas de cuarentena.
- Herramienta de monitoreo incorporada.
- Administración centralizada e integral del sistema, permitiendo al administrador configurar y ejecutar políticas, y monitorear la efectividad de la protección de filtrado. Dichas políticas comprenderán reglas para usuarios individuales o para grupos de usuarios
- La solución deberá poseer un servicio de detección de amenazas y explotaciones de día 0 (zero day), así como malware polimórfico avanzado (tipo Ransomware).

Requisitos mínimos de funcionalidad

- Solución debe basarse en "appliance" de propósito específico. No se tendrán en cuenta los equipos de uso general (PCs o servidores) en la que se puede instalar y / o ejecutar un sistema operativo regular, como Microsoft Windows, FreeBSD, Solaris de Sun o GNU / Linux.
- La solución debe ser capaz de realizar la inspección del correo saliente.
- La solución debe contar con un Wizard para el fácil y rápido aprovisionamiento de las configuraciones básicas del equipo y de los dominios a proteger.
- La solución se debe conectar en tiempo real con la base de datos del fabricante para descargar actualizaciones.
- La solución debe proporcionar soporte para múltiples dominios de correo electrónico.
- La solución debe ser compatible con la implementación de políticas por destinatario, de dominio, del tráfico saliente.
- La solución debe permitir la creación de perfiles de configuración granular, donde cada perfil puede agregar características de configuración específicos.
- La solución debe ser capaz de funcionar como un gateway SMTP para los servidores de correo existentes.
- La solución debe ser capaz de entregar el correo en función de los usuarios existentes en una base de LDAP.
- La solución debe ser capaz de realizar el almacenamiento de correo electrónico (Archivado/archiving), basado en el envío y recepción de políticas, con el apoyo también de almacenamiento remoto.
- La solución debe ser capaz de mantener la cola de correo (Queue) en caso de fallo en la conexión de salida, retrasos o errores de entrega.
- La solución debe ser capaz de realizar la autenticación SMTP a través de LDAP, RADIUS, POP3 o IMAP.
- La solución debe contar con capacidades de evaluar, retener y/o bloquear correos que cuente con amenazas avanzadas, día zero mediante el análisis de archivos con herramientas de sandboxing.
- La solución debe ser capaz de filtrar y analizar los archivos adjuntos y el contenido del e-mail.
- La solución debe ser capaz de realizar una inspección minuciosa de los encabezados de correo electrónico.

- La solución debe ser capaz de realizar análisis bayesiano para determinar si un correo es spam.
- La solución debe ser capaz de filtrar mensajes de correo electrónico basados en los URI (Uniform Resource Identifier) contenidas en el cuerpo del mensaje.
- La solución debe ser capaz de realizar análisis sobre la base de palabras prohibidas (Banned Words).
- La solución debe ser capaz de soportar las listas negras de terceros (Blacklist).
- La solución debe ser compatible con el enrutamiento en IPv4 y IPv6.
- La solución debe ser compatible con la lista gris para las cuentas de correo electrónico en IPv4 e IPv6.
- La solución debe ser capaz de detectar las direcciones IP falsificadas (Forged IP).
- La solución debe soportar listas blancas y negras (White/Black List) por usuario, por dominio y globalmente para todo el sistema.
- La solución debe ser capaz de ejecutar el análisis antivirus / antispyware en archivos comprimidos como ZIP, PKZIP, LHA, ARJ y RAR.
- La solución debe permitir la sobrescritura, la edición y personalización de los mensajes de notificación de antivirus y anti-spyware.
- La solución debe ser capaz de actuar como gateway, en calidad de MTA (Mail Transfer Agent).
- La solución debe ser capaz de funcionar de una manera transparente, actuando como un proxy transparente para el envío de mensajes a los servidores de correo protegidas.
- La solución debe ser compatible con Sender Policy Framework (SPF).
- La solución debe ser compatible con Domain Keys Identified Mail (DKIM).
- La solución debe ser compatible con Domain Based Message Authentication (DMARC).
- La solución debe poder retrasar el envío de correo sobredimensionados a horarios que sean de menos carga.
- La solución debe poder definir el reenvío de correo (relay) a una IP específica con base a la IP origen del mensaje.
- La solución debe permitir el almacenamiento de correo electrónico y de cuarentena a nivel local o servidor remoto.
- La solución debe permitir su configuración a través del acceso web (HTTP, HTTPS).
- La solución debe ser capaz de permitir la creación de administradores únicos para la administración y configuración de la solución por dominio, siendo también posible restringir el acceso por dirección IP y la máscara de red de origen.
- La solución debe ser capaz de proporcionar al menos dos niveles de gestión de acceso: lectura / escritura (Read/Write) o de sólo lectura (Read Only).
- La solución debe ser capaz de almacenar los registros y eventos a nivel local y también enviarlos a servidores remotos (Syslog).
- La solución debe permitir que se informe de la actividad, el análisis de los archivos de eventos (logs) y presentarlos en formato de tabla o gráfica.
- La solución debe generar reportes por demanda o programados a intervalos de tiempo específicos.
- La solución debe generar y enviar reportes en formato PDF o HTML.
- La solución debe ser capaz de detectar si el correo electrónico es un boletín de noticias (Newsletter).
- La solución debe soportar su implementación en modo de servidor, operando como un servidor de correo MTA independiente con buzones para los usuarios. Debe ser capaz de almacenar localmente mensajes de correo electrónico para su entrega a los usuarios a través de correo Web, POP3 y / o IMAP.
- La solución, estando en server mode, debe poder Sincronizar contactos y calendarios con clientes de correo (MUA).
- En modo server, debe soportar los protocolos WebDAV y CalDAV para la publicación y sincronización de calendarios.
- La solución debe contar con algún mecanismo para la fácil migración de buzones y cuentas desde un servidor a la nueva solución estando en server mode.
- Debe soportar Cifrado de mensajes basado en identidad (IBE- Identity Based Encryption), de tal forma que el destinatario no requiera de un PSK o certificado previamente instalado para su descifrado.

- El cifrado de mensajes con IBE, debe soportar tanto el método push como pull, donde el mensaje cifrado estará almacenado en la plataforma de correo para su acceso remoto autenticado, o bien sea enviado como un adjunto al destinatario.
- En ambos métodos de cifrado con IBE se debe contar con un registro del destinatario en la plataforma de correo, de tal forma que para ver los mensajes cifrados se requiera un proceso de autenticación.
- La solución deberá complementarse e integrarse con la solución de Sandboxing especificada en este documento.
- Cada componente deberá ser otorgado en calidad de alquiler, formando parte del servicio ofertado.

El Contratista será responsable del transporte, recepción, instalación, configuración y puesta en operación de los componentes para la seguridad antispam y antimalware. Así como también, el Contratista será el responsable del mantenimiento preventivo y correctivo de los componentes cedidos en calidad de alquiler.

f) Solución de Detección y Respuesta Endpoint (EDR)

El Contratista deberá proveer una (1) solución en físico o virtual o nube de seguridad endpoint centralizado que permita el óptimo desarrollo de la solución endpoint. En caso se opte por la modalidad virtual, la entidad proveerá el espacio virtual para la solución endpoint en plataformas VMWare, con software base Windows Server, en donde el Contratista deberá considerar al menos 1800 agentes a desplegarse en las diferentes estaciones de la entidad (equipos de cómputo y servidores). El Contratista deberá proveer el licenciamiento para el funcionamiento de la solución.
El componente será instalado en el Edificio Raúl Porras Barrenechea, ubicado en el Jirón Ucayali N.° 337, Cercado de Lima.

Características de la Solución:

- La solución propuesta debe ser compatible con los siguientes sistemas operativos: Windows 7, 8.1 y superior.
- La solución propuesta debe ser compatible con los siguientes sistemas operativos: Windows Server, 2008 R2, 2012, 2012 R2, 2016, 2019 y 2022
- La solución propuesta debe ser compatible con los siguientes sistemas operativos: macOS Versiones: y Catalina (10.15, 4), Big sur 11, Monterey 12 y ventura 13
- La solución propuesta debe ser compatible con los siguientes sistemas operativos: Linux Versiones: RedHat Enterprise Linux y CentOS 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6 y 7.7 y Ubuntu LTS 16.04.5, 16.04.6, 18.04.1 y 18.04.2 server, 64-bit.
- La solución propuesta debe poder ser gestionada on-premise o en nube.
- La solución propuesta debe tener la habilidad de actualizar el Endpoint sin interacción por parte del usuario y sin necesidad de reinicio
- La solución propuesta debe trabajar sin depender de firmas hash locales conocidas para la detección de archivos maliciosos
- La solución propuesta debe poder registrar en tiempo real información del proceso e informaciones adicionales tal como conocer el usuario asociado con los eventos
- La solución propuesta debe contar con la opción de establecer contraseña o token para desinstalar el agente en el endpoint.

Detección de Malware:

- La solución propuesta debe poder funcionar en caso el agente no se encuentre conectado a la red empresarial.
- La solución propuesta debe poder detectar, eliminar y volver a su valor inicial o activar shadow copy y cambios realizados por procesos maliciosos en el registro de las PC.
- La solución propuesta debe poder detectar conexiones de red desde el dispositivo.
- La solución propuesta debe poder incorporar inteligencia de amenazas en el esquema de detección.

- La solución propuesta debe tener la capacidad para realizar la búsqueda de amenazas en las estaciones Windows utilizando indicadores de compromisos (IOC).
- La solución propuesta debe identificar actividad maliciosa conocida.
- La solución propuesta debe tener la capacidad de categorizar los eventos detectados en diferentes categorías.

Prevención de Malware:

- La solución propuesta debe tener la capacidad de prevención de ejecución de archivos maliciosos.
- La solución propuesta debe incorporar un motor de antivirus basado en el kernel con capacidad de "Machine Learning".
- La solución propuesta debe tener capacidad de controlar dispositivos USB
- La solución propuesta debe tener capacidad de crear excepciones a los dispositivos USB basado en: nombre del dispositivo o vendor o número serial.
- La solución propuesta debe poder bloquear tráfico malicioso de exfiltración de datos.
- La solución propuesta debe poder bloquear tráfico malicioso de comunicación hacia C&C (Command & Control).
- La solución propuesta debe poder frenar brechas de seguridad e intentos de ransomware en tiempo real.
- La solución propuesta debe evitar cifrados de disco y/o información causado por ransomware.
- La solución propuesta debe permitir que las políticas en la misma sean modificadas permitiendo varios estados como: Activa, Desactivada o solo crear "logs" para las reglas de seguridad contenidas en estas.
- La solución propuesta debe poder ser configurada en modo de monitoreo, donde no se realice ningún bloqueo, pero toda actividad maliciosa es registrada.
- La solución propuesta debe poder permitir la realización de escaneos periódicos de los archivos contenidos en los dispositivos con el Agente instalado.

Mitigación de Malware:

- La solución propuesta debe permitir el aislamiento automático del tráfico de red de un dispositivo donde se ha encontrado una actividad causada por malware.
- La solución propuesta debe permitir el bloqueo de las actividades realizadas por parte de archivos maliciosos.
- La solución propuesta debe tener la capacidad de creación de excepciones para los procesos basados en la localización del archivo y en el destino del tráfico.
- La solución propuesta debe tener la capacidad de recalificar automáticamente la actividad como falso positivo y evitar que ocurran detecciones similares.
- La solución propuesta debe permitir la creación de excepciones de eventos basados en direcciones IP, o aplicaciones o protocolos.

Respuesta a Incidentes:

- La solución propuesta debe almacenar meta-data generada por los dispositivos para que la misma sea usada en investigaciones forenses.
- La solución propuesta debe permitir la integración con plataformas SIEMs (Security Information and Event Management) a través de syslog u otros.
- La solución propuesta debe tener la capacidad de obtener capturas instantáneas de memoria o "dumps" de memoria que permitan la realización de procesos forenses.
- La solución propuesta debe permitir la integración a través de API donde el mismo tenga la capacidad de entregar información generada en un evento tales como: Dirección IP, nombre de host, usuario, fecha / hora ocurrida, actividad sospechosa, etc.) para permitir la integración vía API.
- La solución propuesta debe tener la capacidad para terminar un proceso basado en la clasificación del mismo o implicado en un proceso malicioso.
- La solución propuesta debe tener la capacidad para eliminar un archivo basado en la clasificación maliciosa del mismo.

- La solución propuesta debe tener la capacidad para aislar dispositivos infectados de la red.
- La solución propuesta debe obtener visibilidad completa de la cadena de ataque y cambios maliciosos.
- La solución propuesta debe permitir la limpieza automática de los dispositivos y revertir los cambios maliciosos mientras mantiene el tiempo de disponibilidad del dispositivo o a través de la habilitación del shadow copy de Windows para restaurar capacidades ante un ataque Esto es de cumplimiento obligatorio del contratista, con la excepción que pueda presentar una solución mejorada, con sustento en documentación técnica de libre disponibilidad o documentación del fabricante.
- La solución propuesta debe permitir la suscripción de servicios opcionales de detección y respuesta a incidentes (Ej.: Servicios gestionados de detección y respuesta)
- La solución propuesta debe permitir el envío de ejecutables para su análisis a un sandbox, con la finalidad de determinar si son maliciosos o inofensivos.
- La solución propuesta debe proporcionar múltiples mecanismos de protección, incluida como la terminación de un proceso, eliminación de un archivo malicioso, el bloqueo de una conexión de red.
- Deberá mostrar una secuencia gráfica del incidente de seguridad que correlacione las alertas individuales con el objetivo de identificar la causa raíz. Esta secuencia gráfica deberá ser construida de manera automática a partir de la inteligencia artificial de la plataforma.
- Deberá de mostrar información de los procesos correlacionados en la secuencia gráfica, entre los que se encuentran ruta de ejecución, nombre de usuario que ejecutó el proceso, entidad que firmó el proceso, valor SHA256 del ejecutable relacionado con el proceso, veredicto del análisis del sandbox y línea de comandos de la ejecución.
- Por cada proceso correlacionado en la secuencia gráfica del incidente o obtener la información desde una vista o sección especializada en realizar investigaciones de cacería de amenazas se deberá mostrar lo siguiente:
    - Fecha, hora, hostname, dirección IP, nombre del usuario, sistema operativo del equipo que generó el proceso o al menos obtener la información del sistema operativo del equipo que generó el proceso desde una segunda vista donde se encuentra la lista de dispositivos gestionados.
    - Alertas relacionadas al proceso analizado con su respectiva descripción, acción tomada sobre la alerta, categoría de la amenaza, ejecutable que lo inicializó, táctica y técnica del ataque según el framework MITRE ATT&CK.
    - Actividad de la red del proceso: IP y puerto origen, IP y puerto destino, resolución del DNS, país destino, indicar si la conexión fue exitosa o fallida.
    - Creación, escritura, lectura, eliminación, renombre, cambio de atributos, hash en SHA256 y MD5 de los archivos relacionados al proceso analizado. En caso del renombre deberá mostrar el nombre anterior y actual para facilitar la investigación del analista o al menos obtener la información desde una segunda vista que permita realizar investigaciones de cacería de amenazas.
    - Creación, apertura, escritura, eliminación, renombre, cambio de atributos de los directorios relacionados al proceso analizado.
    - Actividad sobre la clave y valores de registros, tales como creación, eliminación, carga, apertura, renombre, escritura, del proceso analizado.
    - Mostrar los system calls, rpc calls y procesos inyectados sobre cada proceso analizado o al menos obtener la información desde una segunda vista que permita realizar investigaciones de cacería de amenaza.
    - Deberá contar con un mecanismo inteligente que separe de manera automática los binarios y DLLs no significados de la secuencia gráfica del incidente o al menos que la solución incluya en la investigación la información de los binarios y DLL que tuvieron interacción con el evento investigado.
    - Deberá permitir realizar búsquedas avanzadas sobre la actividad de los endpoints:
    - Actividad de los archivos, identificando las siguientes operaciones: creación, lectura, eliminación, escritura y renombrar.
    - Actividad de red, identificando el tráfico saliente, entrante, IP origen e IP destino, Puerto origen y Puerto destino, protocolo de red o al menos obtener la información desde una segunda vista que permita realizar investigaciones de cacería de amenazas .

- Actividad en el registro Windows, identificando la creación, eliminación, renombrado, definición de valores, eliminación de valores de las llaves de registro.
- Actividad de procesos, identificando si se trata de una ejecución o inyección, ruta desde donde se ejecuta, comando que inicializa el proceso, usuario, hash en SHA256 y MD5 o al menos obtener la información desde una segunda vista que permita realizar investigaciones de cacería de amenazas..
- Actividad en el Log de Eventos de Windows, identificando la descripción, ID del evento, nivel, mensaje, nombre del proveedor y usuario o al menos obtener la información desde una segunda vista que permita realizar investigaciones de cacería de amenazas..
- Actividad de autenticación al endpoint o al menos obtener la información desde una segunda vista que permita realizar investigaciones de cacería de amenazas
- Permitir realizar búsquedas en base a cualquier dato recopilado por la plataforma.
- Permitir seleccionar las columnas y orden de los datos mostrados como resultados de las búsquedas.
- Los resultados de las búsquedas deberán poder ser mostrados en una tabla o una gráfica de tipo pye, columnas, burbuja y área, con la finalidad de facilitar el análisis del investigador o al menos brindar las opciones de tabla o gráficas desde la solución o desde una plataforma del mismo fabricante que permita procesar la información para obtener la presentación en formato de tabla o gráfica.
- Deberá contar con una librería predeterminada de búsquedas habituales realizadas en una labor de threat hunting. Esta librería podrá ser editada según la labor del investigador o al menos obtener la información desde una segunda vista que permita realizar investigaciones de cacería de amenazas.

- Las búsquedas deberán estar disponibles tanto para endpoints en línea y fuera de línea.
- Las búsquedas deberán de poder programarse para ser ejecutadas en un día y hora determinados durante una sola ocasión y también de manera recurrente.
- Todas las opciones de búsqueda anteriormente detalladas deberán poder ser utilizadas para configurar reglas personalizadas de seguridad, que permitan generar una alerta cuando un endpoint en particular genere ese comportamiento.
- Deberá de contar con un dashboard que permita visualizar alertas generadas de distintas fuentes.
- El timeline del ataque deberá mostrar el intento de ataque en diferentes fases de explotación acorde al Framework MITRE ATT&CK, tales como Ejecución, Persistencia, Descubrimiento, Desplazamiento Lateral, Command & Control, Exfiltración o al menos brindar la información de los intentos de ataque con las fases del Framework MITRE ATT&CK desde la solución o desde una plataforma del mismo fabricante que permita procesar la información para obtener la presentación deseada.
- Deberá permitir la personalización de reglas de correlación que permitan configurar casos de uso utilizando los eventos recolectados de las diversas fuentes.

Telemetría y colección de datos:

- El agente deberá poder capturar, como mínimo, las siguientes acciones en equipos Windows:
  - Proceso ejecutado, incluyendo el tiempo de inicio, el tamaño del archivo asociado.
  - Actividades de creación, escritura, renombre, eliminación, modificación de archivos.
  - Archivos DLL: ruta completa, dirección base, id del proceso, tamaño de la imagen, firma, valores hash calculados con los algoritmos MD5 y SHA256 del archivo DLL.
  - Creación y terminación de los procesos, incluyendo los siguientes atributos: nombre del 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.
  - 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) o al menos la identificación del hilo de proceso inyectado, ya que el resto de valores son parte de la información entregada por los procesos regulares.
  - Interacciones de red de cada enpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP), resolución de dominio (hostname), tráfico entrante y saliente, país destino de la IP pública.
  - Estadísticas de red: volumen de tráfico en eventos de subida y descarga de tráfico TCP o brindar la información de consumo de tráfico desde la solución SIEM, la cual pueda procesar los datos para brindar el detalle solicitado..
  - Acciones sobre los registros de Windows: Configuración o eliminación de valores del registro. Creación, modificación, eliminación, adición, restauración y guardar llaves del registro. Con los siguientes parámetros: ruta del registro del valor o llave que fue modificado. Nombre del valor o llave modificado. Datos del valor modificado.
  - 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 o también se aceptará obtener esta información desde los logs de eventos de Windows que procesa la solución.
  - Logs de eventos de Windows.
- El agente deberá poder capturar, como mínimo, las siguientes acciones en equipos MacOS:
  - Actividades de creación, escritura, renombre, eliminación, modificación de archivos.
  - Inicio y detención de procesos, con los siguientes parámetros: PID de proceso del proceso padre, PID 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.
  - Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP).
  - Las siguientes acciones de red: accept, connect, connect failure, disconnect, listen, statistics o como mínimo accept, connect, disconnect y listen.
  - Logs de eventos de autenticación
- El agente deberá poder capturar, como mínimo, las siguientes acciones en equipos 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). Información del copiado o renombrado de 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.
  - Inicio y detención de procesos, con los siguientes parámetros: PID de proceso del proceso padre, PID 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.
  - Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP).
  - Las siguientes acciones de red: accept, connect, connect failure, disconnect, listen, statistics o como mínimo accept, connect, disconnect y listen.
  - Logs de eventos de autenticación.
- Deberá incluir un sensor que realice inspección de la red interna conectada a un puerto espejo del switch. Deberá recolectar eventos como: aplicaciones accedidas por los usuarios y dispositivos, IP origen y destino, Puerto origen y destino, URLs, volumen de

tráfico en bytes y paquetes, región de las conexiones, amenazas internas basadas en feeds (opcional)

Analítica de comportamiento de Usuario:

- Deberá ser capaz de retener los eventos recolectados durante al menos 30 días y aprender una línea base o perfil de comportamiento de cada dispositivo o como mínimo incluya algoritmos de machine learning o aprender una línea base o perfil de comportamiento de cada dispositivo para detectar anomalías de dispositivo.
- Los perfiles de comportamiento deberán de ser generados mediante el uso de algoritmos de aprendizaje de máquina no supervisado.
- El producto deberá de alertar las anomalías en el perfil de comportamiento generado o como mínimo la generación de alertas de anomalías en la sección general de revisión de alertas.
- La alerta deberá de formar parte de los incidentes que se hayan generado.
- A partir del comportamiento aprendido, la solución deberá ser capaz de alertas los siguientes comportamientos inusuales, que estén fuera del perfil base aprendido o como mínimo que se brinde mecanismos de consulta que permiten identificar los comportamientos inusuales, los cuales se indicarán en cada punto:
    - User agent sospechoso o un query para identificar user agent que no sea parte de la lista regular permitida.
    - Cantidad de interacciones de red inusuales o brindar la información de cantidad de interacciones de red inusuales desde la solución SIEM, la cual pueda procesar los datos para brindar el detalle solicitado.
    - Query LDAP inusual o se aceptará realizar un query para identificar queries LDAP que no sean parte de la lista regular permitida
    - Creación de reglas de firewall inusuales o que pueda realizar un query para identificar eventos de creación de reglas de firewall de hosts para investigar si son irregulares
    - Sesión WinRM anómala o realizar un query para identificar sesiones WinRM que no sean parte de la lista regular permitida
    - Servidor Python inicializado o realizar un query para identificar inicio de servicios Python que no sean parte de la lista regular permitida
    - Proceso raro ejecutado en la institución o realizar un query para identificar de servicios nuevos que no sean parte de la lista regular permitida.
    - Elevación de privilegios con usuario SYSTEM de manera anómala o realizar la detección de elevación de privilegios como mínimo
    - Firewall de Linux desactivado de manera anómala o realizar la detección de desactivación de firewall de linux como mínimo.
    - Tarea programada creada de forma inusual o realizar un query para identificar las tareas programadas nuevas que no sean parte de la lista regular permitida.
    - Ejecución de arp.exe anómala o realizar un query para identificar la ejecución de arp.exe desde hosts que no sean parte de la lista regular permitida.
    - Cantidad inusual de screenshots tomados o se aceptará realizar un query para identificar la toma de screenshots y que la solución SIEM del proyecto detecte que es una cantidad de eventos que superan el umbral permitido.
    - Cantidad excesiva y anómala de información subida a internet o también se aceptará como mínimo brindar la información de cantidad de información subida a Internet desde la solución SIEM, donde se puedan definir umbrales para detectar excesos, la cual pueda procesar los datos para brindar el detalle solicitado.
    - Conexión RDP inusual o también se aceptará realizar un query para identificar conexiones RDP desde hosts que no sean parte de la lista regular permitida.
    - Escaneo de puertos sospechoso
    - Creación de una máquina en el dominio o también se aceptará realizar un query para identificar la creación de máquina de dominio.
    - Creación de usuario con permisos de domain admin o también se aceptará como mínimo brindar esta información desde la solución SIEM.
    - Usuario imprime una cantidad inusual de archivos o también se aceptará como mínimo brindar esta información desde la solución SIEM.
    - Conexiones VPN sospechosas o también se aceptará como mínimo brindar la información de cantidad de conexiones VPN y desde orígenes sospechosos

desde la solución SIEM, donde se puedan definir umbrales para detectar excesos, la cual pueda procesar los datos para brindar el detalle solicitado.
  - Logueo VPN desde una cuenta de servicio o también se aceptará que esta detección sea realizada desde la solución SIEM.
  - Uso de aplicación no habitual o también se aceptará realizar un query para identificar el uso de aplicaciones que no sean parte de la lista regular permitida.
  - Cantidad inusual de solicitudes DNS generadas o también se aceptará como mínimo brindar la información de cantidad inusual de solicitudes DNS generadas desde la solución SIEM, donde se puedan definir umbrales para detectar excesos, la cual pueda procesar los datos para brindar el detalle solicitado.
  - Actividad inusual en nube como: borrado de RDS, creación de usuarios, borrado de recursos o también se aceptará como mínimo brindar la información de borrado de RDS, creación de usuarios, borrado de recursos desde la solución SIEM, donde se puedan definir umbrales para detectar excesos, la cual pueda procesar los datos para brindar el detalle solicitado.
- La solución deberá de tener la capacidad de permitir al analista bloquear las direcciones IP destino que hayan sido identificadas en el ataque mediante la modificación del sensor de red. Esta modificación deberá de poder realizarse bajo demanda (opcional).
- Deberá tener más de 200 casos de uso automáticos que puedan ser generados a partir del aprendizaje del comportamiento de la inteligencia artificial o también se aceptará que la solución permita definir consultas para más de 200 caso de uso.
- Deberá ser posible alertar determinados comportamientos de los usuarios y hosts asociados a actividad en archivos, directorios, procesos red, cambios de registro.
- Deberá contar con integración al Active Directory para extraer información contextual del usuario, incluyendo el departamento en el cual labora, número de teléfono, última fecha de autenticación.

Control de Vulnerabilidades y Comunicación:

- La solución propuesta debe proporcionar múltiples mecanismos de protección, incluida como la terminación de un proceso, eliminación de un archivo malicioso, el bloqueo de una conexión de red.
- La solución categoriza aplicaciones que están instaladas en el sistema operativo se estén comunicando a través de la red y que estas representen riesgo al endpoint.
- La solución propuesta debe poder detectar e identificar todas las aplicaciones en los dispositivos que se comunican en la red o se encuentran instaladas en el sistema operativo.
- La solución debe identificar vulnerabilidades asociadas al sistema operativo con su respectivo CVE o también se aceptará gestionar la detección de vulnerabilidades de sistema operativo desde la solución SIEM.
- La solución propuesta debe poder entregar información sobre el uso de aplicaciones en red mostrando información como cuales dispositivos generan tráfico de una aplicación
- La solución propuesta debe poder visualizar y entregar información sobre el uso de aplicaciones en red mostrando información como los IP destinos del tráfico generado por la aplicación.

Consola de Administración:

- La solución propuesta debe cumplir con el estándar GDPR o certificación SOC2 tipo II.
- La consola de administración de la solución propuesta debe permitir la integración con "Active Directory" para garantizar el cumplimiento de los requisitos de la política de contraseñas de la empresa.
- La consola de administración de la solución propuesta debe permitir el uso de autenticación de doble factor (2FA) para acceder a la misma.
- La consola de administración de la solución propuesta debe permitir el uso de roles granulares para los administradores
- La consola de administración de la solución propuesta debe permitir la gestión a través de APIs Full Restful API.
- La solución propuesta debe poder ser gestionada completamente en nube.

- La solución propuesta debe soportar la integración con el laboratorio en nube del mismo vendor para actualización de inteligencia de malware y amenazas.
- La consola de administración de la solución propuesta debe permitir la visualización de los eventos registrados en los dispositivos que requieran atención.
- La consola de administración de la solución propuesta debe permitir la visualización de salud de los agentes instalados.
- La consola de administración de la solución propuesta debe permitir la desactivación/activación remota del agente instalado en los dispositivos.
- La consola de administración de la solución propuesta debe permitir la actualización remota del agente instalado en los dispositivos.
- La consola de administración de la solución propuesta debe permitir la creación de reportes ejecutivo conteniendo un resumen que describe los eventos de seguridad y el estado del sistema.
- Los reportes deben ser personalizables según los criterios de la entidad.
- Debe tener la capacidad de crear reglas de comportamiento según los criterios de la entidad.
- Debe ingestar IoC del mismo fabricante o terceros que automáticamente genere una alerta cuando un evento de seguridad del endpoint involucra la coincidencia con algún IoC ingestado.
- La consola de administración de la solución propuesta debe permitir la creación de grupos organizativos de dispositivos en los cuales cada grupo podrá tener reglas de protección independiente de los demás.
- La consola de administración de la solución propuesta debe permitir la visibilidad de eventos generados por los dispositivos o eventos de acuerdo al proceso ejecutado.
- La consola de administración de la solución propuesta debe el envío de alertas a través de correo electrónico.
- La solución propuesta debe permitir que los servicios en nube recategoricen la clasificación de un evento.
- La solución propuesta debe permitir que los administradores deshabiliten las notificaciones de un evento de detección.
- La solución deberá complementarse e integrarse con la solución de Sandboxing especificada en este documento para que se tome acción y contenga/bloquee un ataque malicioso identificado por el sandboxing.
- Para la implementación de la solución EDR se podrá coordinar entre el Contratista y el MRE para que se puedan desplegar una cantidad de agentes en la etapa de implementación y el resto en la etapa de soporte en caso haya limitantes que impidan un despliegue masivo y rápido desde la consola centralizada y se tenga que realizar la instalación de los agentes de manera manual.
- Cada componente deberá ser otorgado en calidad de alquiler, formando parte del servicio ofertado.

El Contratista será responsable del transporte, recepción, instalación, configuración y puesta en operación del componente para la seguridad endpoint centralizado. Así como también, el Contratista será el responsable del mantenimiento preventivo y correctivo del componente cedido en calidad de alquiler.

g) Sistema de Detección de Amenazas con Inteligencia Artificial

Sistema de Detección de Amenazas

- El servicio debe ser capaz de identificar cualquier amenaza anómala en la red en tiempo real a través del aprendizaje automático e inteligencia artificial.
- Contar con autorización del fabricante o su representante, para comercializar la marca y brindar las soluciones requeridas.
- El oferente y /o contratista deberá entregar un servicio con licenciamiento total de la solución para 4.000 dispositivos por dos años o se aceptará capacidad de rendimiento de 10 Gbps.
- El servicio deberá estar basada en hardware appliance, es decir, un (1) hardware de propósito específico destinado a alojar el sistema de seguridad requerido con las condiciones de endurecimiento propias de un sistema de seguridad.

- El servicio debe basarse en un sistema de seguridad que reciba todo el tráfico de la red desde uno o varios switches, lo analice e identifique las amenazas o incidentes que están ocurriendo en la red
- Después del período de aprendizaje inicial, la tecnología debe proporcionar automáticamente un seguimiento de auditoría completo de todos los dispositivos en el entorno, clasificando previamente al menos el tipo de dispositivo, el nombre de host, la dirección MAC, la primera y la última vez que se detectó el dispositivo en la red
- El servicio debe basarse en el análisis de comportamiento y correlación inteligente pudiendo detectar:
  - ✓ Toda conectividad inusual en la red.
  - ✓ Todas las actividades anómalas en la red.
  - ✓ Ser capaz de hacer un seguimiento detallado del dispositivo, indicando incluso su historial de dirección IP, uso del protocolo DHCP, etc o también se aceptará Amenaza de aplicación de DHCP.
  - ✓ Tener la capacidad de hacer un seguimiento detallado del usuario indicando incluso todos los nombres de host asociados a unas determinadas credenciales o también se aceptará que pueda ser brindada desde la solución SIEM del presente proceso.
  - ✓ Identificar un volumen de conexiones significativamente inusual.
  - ✓ Identificar el nivel de rareza de un dispositivo en la red, así como el nivel de rareza de un acceso a un sitio externo.
- El servicio debe alertar automáticamente sobre todas las actividades inusuales y anómalas en la red.
- La solución debe ser una plataforma de autoaprendizaje y tener un enfoque adaptativo que utilice inteligencia artificial comprobada para aprender sobre el entorno en el que se encuentra, detectar y responder a las desviaciones de la línea de base normal de comportamiento, así:
  - ✓ La línea base de la red debe ser lo suficientemente adaptable y dinámica para adaptarse a cualquier cambio en el comportamiento del entorno
  - ✓ Debe funcionar completamente en función del comportamiento, donde no se permitan las tecnologías que hacen uso de reglas y / o firmas o también se aceptará que se pueda complementar el sistema con el uso de firmas de día cero, para un detección más eficaz.
- La herramienta debe utilizar modelos matemáticos de estimación recursiva bayesiana o similares con el fin de validar los comportamientos anómalos en la red.
- El servicio debe proporcionar visibilidad completa de la red, incluidas las tecnologías tradicionales y no tradicionales
- El servicio debe poder identificar cualquier comportamiento anómalo en el entorno y alertar sobre estos comportamientos en tiempo real
- El servicio debe ser capaz de identificar cualquier dispositivo nuevo en la red
- Capacidad de realizar consultas a los datos capturados y almacenados en el hardware de uso específico (appliance) sin conectarse a la nube.
- Debe basarse en métodos matemáticos probabilísticos, analizando y correlacionando múltiples dimensiones distintas dentro del paquete o también se aceptará considerar análisis dentro del paquete o archivo.
- La solución debe poder realizar una captura de paquetes en tiempo real que permita un análisis exhaustivo del incidente en el momento de su ocurrencia así como ofrecer la opción de analizar el paquete tanto en Wireshark como dentro de su propia interfaz de usuario o también se aceptará considerar análisis dentro del paquete o archivo..
- La solución debe permitir la personalización y adaptación del aprendizaje automático a condiciones y características específicas de la red.
- Ser completamente automatizada, no debe requerirse de reglas o intervención humana para instruir a la solución sobre cómo utilizar los logs y flows recolectados para correlacionar y determinar ataques en tiempo real.
- Debe poder realizar investigaciones autónomas basadas en inteligencia artificial, sea por demanda a través de la interfaz gráfica y/o a través de la integración vía API, esta investigación debe incluso poder realizarse sin intervención humana y generar un reporte donde se evidencia al menos un resumen ejecutivo del incidente, las alertas que fueron investigadas que hacen parte de incidente e información técnica de cada uno de los eventos identificados, asociándolos a la fase del Cyber Kill Chain y a una posible TTP de framework ATT&CK Mitre.

- La Investigación basada en Inteligencia Artificial debe generar un reporte como resultado del proceso investigativo que contenga como mínimo:
  - ✓ Una reconstrucción cronológica de los eventos que hacen parte del Incidente.
  - ✓ Un resumen del incidente con una narrativa basada en procesamiento de lenguaje natural que describa a alto nivel los comportamientos evidenciados durante el incidente.
  - ✓ Detalles técnicos relevantes a la investigación realizada como direcciones Ips, Hostnames, cuentas de usuario involucradas (opcional), saltos de conexión, cantidad de transferencia de datos, destinos externos, rareza de los destinos, rareza de las conexiones y resúmenes de conexiones.
- Debe realizar un análisis completo del tráfico (No análisis parciales de los paquetes p.e: sflow, jflow, netflow, Syslog) o también se aceptará uso de netflow para identificar patrones diferentes de ataques, para un detección más eficaz.
- La solución debe permitir la integración con LDAP o Directorio Activo
- El sistema debe ser OPEN API, que admita integraciones con otros elementos de seguridad al menos en los formatos, CEF, LEEF, JSON, SYSLOG, entre otros o también se aceptará al menos considerar formatos estándares como: STIX, JSON, SYSLOG..
- La tecnología deberá proporcionar la capacidad de realizar procedimientos automatizados por parte del proveedor del servicio para la cacería de amenazas basados en inteligencia artificial con al menos las siguientes capacidades:
  - ✓ Procesos de Threat Hunting basados en anomalías de comportamiento detectadas por la inteligencia artificial o análisis forense de un incidente o amenaza.
  - ✓ El proceso de Threat Hunting "o" análisis forense de un incidente o amenaza deberá poder correlacionar anomalías detectadas dentro de la misma plataforma de IA e identificar si pertenecen o no a un ataque más complejo. Se deben validar con otras fuentes de información que llegan al correlacionador para dar mayor contexto a los hallazgos identificados por la inteligencia Artificial.
  - ✓ Se deberá poder integrar el proceso de Threat Hunting automatizado "o" análisis forense de un incidente o amenaza para que otros servicios vía API puedan solicitar informes de cacería de amenazas de manera automatizada.
  - ✓ Se deben poder solicitar investigaciones autónomas y a demanda a la inteligencia artificial, donde el disparador pueda ser una anomalía ya detectada o una simple investigación a demanda.
  - ✓ El proceso de Threat Hunting deberá proporcionar un informe base entregado por la inteligencia artificial y uno adicional con la información de contexto y otras investigaciones adicionales realizadas por los analistas humanos (opcional).
  - ✓ El proceso deberá tener la capacidad de realizar investigaciones continuas 24/7 y en tiempo real de las anomalías detectadas por la inteligencia artificial
  - ✓ Se deberán proponer los reportes estadísticos del servicio a nivel ejecutivo.
  - ✓ Se deberán acordar los reportes de los Threat Hunting y sus respectiva evidencia con al menos un reporte por cada investigación realizada o al menos considerar considerar Theat Hunting o análisis forense de un incidente o amenaza.
  - ✓ Se deberán realizar procesos de Threat Hunting manuales basados en TTP's mitre de manera recurrente o análisis forense de un incidente o amenaza , identificando qué anomalías detectadas por la plataforma de Inteligencia Artificial hacen parte de las técnicas buscadas para cada ejercicio de Treath Hunting propuesto o análisis forense de un incidente o amenaza .
- La solución debe permitir la personalización avanzada de la tecnología, permitiendo considerar múltiples parámetros de datos al verificar un determinado comportamiento, entre los parámetros debería ser posible tener las siguientes opciones: Conexiones, conexiones externas, conexiones internas, transferencia de datos, datos externos transferencia, conexiones SMB, conexiones de puerto cerrado, difusiones, dispositivos conectados, transferencia de datos (cliente), transferencia de datos (servidor), entre otras métricas relevantes.
- La solución debe utilizar varios algoritmos de inteligencia artificial, así como varias técnicas de Machine Learning como: Deep Learning, Machine Learning supervisado y Machine Learning no supervisado.
- La tecnología de identificación de amenazas de la solución no debe basarse en firmas, ni reglas, ni heurística, ni sandboxing. Debe estar puramente basada en algoritmos

avanzados de Machine Learning e Inteligencia Artificial, también se aceptará que se pueda complementar el sistema con el uso de firmas de día cero, para un detección más eficaz.

- Debe funcionar completamente en función del comportamiento, donde no se permitirán las tecnologías que hacen uso de reglas, firmas y/o Indicadores de Compromiso (IoC's), también se aceptara que se pueda complementar el sistema con el uso de firmas de dia cero, para un detección más eficaz
- La solución debe tener la capacidad de modelar el comportamiento normal a nivel de usuario, dispositivos y red y a partir de estos identificar de forma autónoma las anomalías que corresponden a brechas de seguridad.
- La herramienta debe poder realizar un aprendizaje autónomo del comportamiento normal de la red sin requerir previo conocimiento del historial de comportamiento anómalo, con la posibilidad de identificar amenazas desde el primer día de instalación.
- La tecnología debe tener la capacidad de detectar amenazas internas y externas
- La tecnología debe ser auto-configurable, es decir, debe tener capacidad de adaptarse de forma automática a los cambios del entorno en tiempo real.
- La solución debe tener capacidad de detectar como mínimo los siguientes tipos de brechas de seguridad:
  - ✓ Ataques de tipo botnet
  - ✓ Propagación de gusanos
  - ✓ Ataques de ransomware
  - ✓ Infiltración y exfiltración de datos
  - ✓ Troyanos bancarios
  - ✓ Credenciales comprometidas (opcional)
  - ✓ Minería de bitcoins
  - ✓ Malware
  - ✓ Ataques de DDoS a través de dispositivos IoT
  - ✓ Amenazas avanzadas persistentes (APT)
- La herramienta debe ser on premise, no se aceptan soluciones que necesiten de la nube para hacer los análisis de la información, cualquier configuración remota debe ser consultada y autorizada con la entidad.
- La solución contra amenazas deberá funcionar sin necesidad de tener conexión a una nube de inteligencia de amenazas, sandbox o cualquier consola en general que se encuentre en la nube o deba recolectar información desde la nube pública, también se aceptara que se pueda complementar el sistema con el uso de firmas de día cero, para un detección mas eficaz.
- La herramienta debe ser tipo appliance no se aceptarán equipos que involucren la instalación de agentes en los dispositivos a monitorear (agent-less).
- La solución debe poder reconocer nuevas amenazas que no hayan sido advertidas previamente (Zero Day).

Visualización de red

- La solución debe poseer una interfaz de visualización amigable, que debe ser accesible vía web.
- La interfaz de visualización debe permitir tener visibilidad gráfica de cualquier elemento de la red con gran profundidad en el detalle. Debe poder llegarse a ver gráficamente hasta el nivel de dispositivo y sus conexiones en tiempo real. No deberá necesitar compartir datos con una nube de seguridad global para obtener su inteligencia de seguridad
- La visualización de cualquier elemento en la red debe ser en tiempo real y también debe existir la posibilidad de visualizar actividad histórica de manera gráfica. La solución debe permitir la búsqueda en la hora exacta que se desea ver la actividad histórica, con un nivel de exactitud preciso.
- La solución debe ser capaz de agrupar automáticamente los dispositivos en grupos y/o grupos por su similitud de comportamiento.
- La solución debe tener una barra de búsqueda que permita buscar inmediatamente un dispositivo, IP, subred o host de red.
- La solución debe tener una interfaz de usuario donde se pueda consultar el estado completo del sistema, incluyendo:

- ✓ La versión del software, el espacio en disco utilizado, el consumo de CPU y el consumo de memoria.
- ✓ El detalle de todas las interfaces activas y el tráfico respectivo recibido a través de cada una de ellas
- ✓ El ancho de banda total procesado, el ancho de banda promedio procesado hasta la fecha, el ancho de banda registrado en los últimos periodos de tiempo.
- ✓ Un análisis detallado de todo el tráfico recibido en el dispositivo y la última vez que se identificaron los protocolos principales, entre ellos HTTP, HTTPS, FTP, LDAP, SMTP, SSH, SMB, SSDP, POP3, NTLM, IMAP, Kerberos, etc.

- La solución debe tener visibilidad en tiempo real de los siguientes datos correspondientes a la red:
  - ✓ Cantidad de servidores
  - ✓ Cantidad de estaciones cliente
  - ✓ Cantidad de credenciales de usuario (opcional)
  - ✓ Tráfico de red
- La interfaz de visualización debe poseer una barra de búsqueda que permita identificar de manera rápida cualquier elemento de la red bajo los siguientes criterios:
  - ✓ Dirección IP
  - ✓ Tipo de dispositivo
  - ✓ Función o protocolo conocido.
  - ✓ Tipo de dispositivo
  - ✓ Nombre del dispositivo
- Cuando se hace búsqueda de un dispositivo, la interfaz debe poder mostrar la información de éste en detalle incluyendo: dirección IP, dirección MAC, sistema operativo, logs de eventos, logs de brechas de seguridad identificadas, historial de conexiones, lista de dispositivos similares. Adicionalmente, proporcionar el primer y último vistamiento para cada detección de actividad maliciosa observada.
- La interfaz debe permitir la visualización de todas las subredes, así como todos los dispositivos que las conforman. Debe permitir la visualización de la subred de manera gráfica en tiempo real, mostrando el esquema de conexiones entre los dispositivos, también se aceptará que la solución permita mostrar todos los dispositivos y como estos se comunican a través de diagrama de flujos y/o cuadros estadísticos.
- Las subredes deben poder visualizarse en un mapa global que permita conocer la ubicación real de cada una, también se aceptara que la solución permita mostrar todos los dispositivos y como estos se comunican a través de diagrama de flujos y/o cuadros estadísticos.

Visibilidad de amenazas

- La interfaz debe mostrar las amenazas que se van identificando en la red en tiempo real, con el detalle de eventos de cada amenaza generados por la herramienta, así como vistas gráficas que permitan ver el comportamiento de la amenaza en el tiempo.
- La solución debe proporcionar filtros simples y rápidos para permitir el análisis de eventos informáticos por parte de Usuarios (opcional), Dispositivos y tipo de evento.
- La interfaz debe poder mostrar la amenaza de manera gráfica y en tiempo real.
- Las amenazas identificadas deben tener un nivel de clasificación según su criticidad y debe contar con un código de colores asociado a cada nivel.
- La interfaz debe brindar la posibilidad de investigación de alertas en profundidad en tiempo real, de manera gráfica y mediante eventos.
- La solución debe tener una función que permita el análisis retrospectivo de los registros del incidente, devolviendo la conexión en segundos, minutos, horas o días antes de que se haya identificado una anomalía
- La interfaz debe poseer herramientas o funcionalidades que permitan la investigación forense al mayor nivel de detalle de cualquier amenaza identificada, sin necesidad de uso de herramientas externas.
- La solución debe ser capaz de agrupar las anomalías de manera inteligente y por nivel de criticidad.
- La solución debe contar dentro la su propia interface con herramientas tipo Punycode Convertor, RegEx Tester, Base64 Convertor, JS Beautifie ,Epoch Converter , Facilitando el análisis de los incidentes, también se aceptara que la solución de NDR

podra contar al menos una de las herramientas mencionadas "o" que se podrá integrar a herramientas terceras mediante: STIX, JSON, SYSLOG.

- La interfaz de visualización debe permitir tener visibilidad gráfica en 3D o 2D de cualquier elemento de la red con gran profundidad en el detalle. Debe poder llegarse a ver gráficamente hasta el nivel de dispositivo y sus conexiones en tiempo real, también se aceptará que la solución permita mostrar todos los dispositivos y como estos se comunican a través de diagrama de flujos y/o cuadros estadísticos.
- La visualización de cualquier elemento en la red debe ser en tiempo real y también debe existir la posibilidad de visualizar actividad histórica de manera gráfica. La solución debe permitir la búsqueda en la hora exacta que se desea ver la actividad histórica, con un nivel de exactitud preciso.

Arquitectura de la Solución

- El oferente y/o contratista deberá entregar un (1) equipo como servicio para Monitoreo de Red con Inteligencia Artificial con el objetivo de revisar el tráfico de red y alertar Cyberamenazas que existan en la red de la entidad.
- La solución debe ser centralizada, es decir, debe contar con una única interfaz de administración y visualización, desde la cual se pueda gobernar toda la solución y monitorear todo el entorno.
- El análisis del tráfico mediante los algoritmos de Machine Learning e Inteligencia Artificial debe realizarse de manera centralizada y a la totalidad del tráfico proveniente del datacenter Principal
- El equipo que conforma el servicio debe ser instalado fuera de línea, es decir, la recepción del tráfico de red debe hacerse a través de puertos pasivos (spam port), de tal manera de no causar retardos en el desempeño de la red.
- La solución debe realizar un análisis completo del tráfico.
  - ✓ Se debe considerar los siguientes datos para el dimensionamiento del servicio a ofertar (appliance especifico propio del fabricante):
  - ✓ Cantidad de appliance (uno (1)), doble fuente de suministro eléctrico swipe up como servicio
  - ✓ Conexiones por minuto 50.000 o rendimiento de análisis de malware 160,000 (Archivos por hora)
  - ✓ Troughput: 10 Gbps
  - ✓ Cantidad de dispositivos a analizar: 4.000 o rendimiento de análisis de malware 160,000 (Archivos por hora)
- Tipo de interfaz
  - ✓ La solución debe tener al menos un (1) puerto 10/100/1000 BASE-T de monitoreo y análisis, dos (2) puertos 10Gbe/1Gbe SFP+ de monitoreo y análisis y un (1) puerto 10/100/1000 BASE-T para Gestión.
- La herramienta debe soportar los siguientes modos de implementación: Port mirror (SPAN PORT)

Notificaciones

- La solución debe contar con la capacidad de poder notificar las amenazas a través de correos electrónicos.
- Contar con una interfaz móvil disponible para Android y iOS, activa 7x24 que acelere las tareas de mitigación de riesgos mediante el envío de notificaciones push para dar aviso de amenazas en proceso y la posibilidad de confirmar acciones de respuesta autónoma. Este punto se puede cumplir con herramientas propias del fabricante o con integraciones de terceros, así mismo, se pueda acceder a la plataforma desde un dispositivo móvil a través de la WEB gui, 24x7 con el fin de poder monitorear las alertas generadas.

Administración

- La herramienta debe ser capaz de realizar backup y restore de la configuración, permitiendo al administrador programar la realización de los backups en el momento deseado.

- Los backups deben poder ser transferidos a un repositorio vía SFTP o alguna tecnología de transferencia equivalente, es decir, que considere las medidas de seguridad bajo protocolos aceptados por la industria.

Contención

- La solución debe estar en la capacidad de responder frente a incidentes de forma autónoma, esto es a partir del aprendizaje obtenido la inteligencia artificial debe decidir qué debe bloquear y como debe hacerlo, no debe utilizar configuraciones ni políticas predefinidas para realizar el bloqueo y debe bloquear únicamente el tráfico asociado a la amenaza mientras permite que el tráfico restante (no anómalo) siga fluyendo o al menos la solución NDR debe contar con una arquitecta con la capacidad de responder frente a incidentes y debe bloquear el tráfico de los orígenes/destinos maliciosos detectados a través de ML/IA pudiendo incorporar un dispositivo adicional si su arquitectura lo requiere..
- Permitir integrarse con la infraestructura de seguridad existente, permitiendo optimizar la detección de amenazas y automatizando la mitigación de las mismas.
- Las acciones de bloqueo deben ser generadas con la precisión necesaria para interrumpir exclusivamente el tráfico que corresponde a las acciones maliciosas detectadas, de manera que no se afecte al tráfico de las actividades normales de los dispositivos involucrados.
- Capacidad para bloquear tráfico Norte-Sur y Este-Oeste de forma automática sin la instalación de dispositivos de control adicionales o al menos la solución NDR debe contar con una arquitecta con la capacidad de responder frente a incidentes y debe bloquear el tráfico de los orígenes/destinos maliciosos detectados a través de ML/IA pudiendo incorporar un dispositivo adicional si su arquitectura lo requiere.
- Capacidad de determinar automáticamente como bloquear el tráfico sin causar mayor impacto a la organización utilizando inteligencia artificial. Entre las posibles acciones de bloqueo soportadas se debe tener : Desactivar las credenciales de un usuario o grupo de usuarios (opcional), bloquear conexiones específicas a través del envío de TCP-RST, y generar políticas en el firewall para bloquear una IP externa o aislar una IP interna.
- La solución con la que se prestará el servicio debe poder ser configurada en modo pasivo-monitoreo o modo activo-bloqueo según la configuración predeterminada definida en conjunto con el personal de la entidad
- La automatización a la respuesta a incidentes se deberá realizar utilizando los servicios REST API de forma bidireccional a las plataformas tecnológicas con las cuales se integrará la solución
- Deberá ser gestionable desde una interfaz gráfica (GUI).

Soporte del Fabricante

- El fabricante deberá brindar las actualizaciones de software sin costo adicional durante el periodo de vigencia del contrato.
- En caso de falla del equipo, el fabricante deberá proporcionar los materiales y/o piezas para su reparación o en su defecto un equipo nuevo para el reemplazo sin costo adicional, modalidad RMA.

h) Gestión de Accesos Privilegiados

Arquitectura y Rendimiento

- La solución se utilizará como la única puerta de enlace que conecta la estación de trabajo del usuario con los sistemas administrados para obtener acceso privilegiado.
- La solución iniciará la sesión de inicio de sesión desde la estación de trabajo hacia los sistemas gestionados utilizando un proxy de sesión (a través de un portal de inicio de sesión).
- La solución debe permitir definir perfiles de administradores, de modo que puede segmentar la responsabilidad de los administradores por tareas operativas

- La solución de gestión de identidades deberá integrarse a una autenticación de doble factor
- La solución debe admitir un motor distribuido para la administración de contraseñas y sesiones en diferentes segmentos de red aislados y regiones geográficas, mientras que todos los sistemas y políticas de destino aún se pueden administrar de forma centralizada.
- La solución no requerirá cambios en la topología de la red para garantizar que todas las sesiones privilegiadas estén controladas por la solución.
- La solución se basará en una arquitectura sin agente para la administración de contraseñas y sesiones.
- La solución se entregará en hardware o dispositivo virtual asegurado con estándares reconocidos en el mercado
- La solución admitirá la alta disponibilidad en modo Activo-Pasivo con conmutación por error automática y manualmente dentro del mismo sitio Datacenter o entre datacenters sin necesidad de licencias adicionales.
- La solución ofrecerá opciones de implementación de dispositivos en proveedores de nube pública, incluidos Azure y AWS.
- La solución admitirá no menos de 300 sesiones de grabación concurrentes (RDP) o 600 Sesiones concurrentes SSH para cada nodo y podrá ampliarse para admitir miles de sesiones concurrentes.
- La solución debe utilizar una base de datos no patentada, compatible con las mejores prácticas de seguridad, que estén documentadas y sean públicas. Dicha base de datos debería permitir una alta disponibilidad y mecanismos para la recuperación ante desastres.
- La solución debe entregarse en formato de appliance virtual, virtualizadas bajo las plataformas Hyper-V y/o VMware. Se aceptarán las soluciones entregadas en software, siempre que todos los componentes necesarios para su funcionamiento (como el sistema operativo, la base de datos y las licencias adicionales necesarias) se incluyan en la propuesta y entrega de la solución.
- La solución tendrá la capacidad de almacenar en caché las credenciales seleccionadas externamente. Estas credenciales se pueden usar para conexiones de "aplicación con aplicación" para mitigar la interrupción temporal de la infraestructura PAM.

Manejo de activos y descubrimientos

- La solución tendrá capacidad de carga masiva para importar sistemas administrados, cuentas privilegiadas, usuarios y otros objetos necesarios.
- La solución tendrá la capacidad de registrar la información del sistema para los sistemas administrados, incluidos, entre otros, la dirección IP, la dirección MAC, el nombre DNS, el propietario del sistema, el tipo de plataforma y la versión, listado de cuentas y sus estados en sistemas operativos.
- La solución permitirá al administrador definir atributos personalizados tanto para el sistema administrado como para la cuenta privilegiada.
- La solución tendrá la capacidad de descubrir, inventariar y cambiar credenciales de todas las cuentas privilegiadas y no privilegiadas en sistemas conocidos y desconocidos, incluidos, entre otros:
  - ✓ Windows
  - ✓ Unix / Linux
  - ✓ Mac OS
  - ✓ Directorios (AD / LDAP)
  - ✓ Bases de datos
  - ✓ Dispositivos de red
  - ✓ La solución debe funcionar como un servidor RADIUS (Remote Authentication Dial-In User Server), proporcionando autenticación a dispositivos compatibles con dicho protocolo
  - ✓ La solución La solución debe soportar la integración con el servidor RADIUS remoto
  - ✓ La solución puede funcionar como un servidor LDAP (Lightweight Directory Access Protocol), proporcionando autenticación a dispositivos compatibles con ese protocolo

- ✓ La solución debe tener un servidor LDAP interno que permita su configuración jerárquica, para la correcta administración por grupos o unidades organizativas de usuarios locales.
- ✓ La solución debe soportar la integración con un servidor LDAP remoto (como Microsoft Active Directory)
- ✓ La solución debe soportar la autenticación de usuarios con credenciales de redes sociales como Facebook, Twitter y LinkedIn

- La solución proporcionará la capacidad del motor de descubrimiento distribuido que permite descubrir activos en diferentes segmentos de red aislados y regiones geográficas e informar el resultado del descubrimiento de forma centralizada.
- La solución tendrá la capacidad de descubrir los Servicios de Windows y las Tareas Programadas para que las credenciales privilegiadas que utilizan puedan administrarse automáticamente.
- La solución tendrá la capacidad de descubrir cuentas de dominio de Active Directory y vincular automáticamente las cuentas descubiertas a servidores miembros específicos para que el usuario solicite acceso.
- La solución tendrá la capacidad de descubrir el software que está instalado y los puertos están abiertos en el sistema de destino.
- La solución tendrá la capacidad de agrupar sistemas de destino basados en atributos de sistema definidos descubiertos y personalizados.
- La solución tendrá la capacidad de agrupar sistemas y cuentas en función del resultado de la consulta AD / LDAP.
- La solución tendrá la capacidad de enviar notificaciones por correo electrónico al personal designado al descubrir nuevos sistemas objetivo o sistemas encontrados que ya no son accesibles.
- La solución tendrá la capacidad de descubrir nuevas cuentas privilegiadas y de incorporarlas automáticamente para la gestión de contraseñas.

Gestión de contraseñas

- La solución admitirá la administración de contraseñas para las siguientes plataformas listas para usar:
  - ✓ Sistemas operativos: AIX, HP-UX, AS400, Z / OS, Linux, Mac OS, Solaris, Windows Desktop, Windows Server
  - ✓ Bases de datos: MySQL, Oracle, PostgreSQL, SQL Server.
  - ✓ Directorios: Active Directory, LDAP, RACF
  - ✓ Dispositivos: BIG-IP (F5), Checkpoint, Cisco IOS, Dell iDRAC, Fortinet, espson, HP iLo, Juniper (JunOS), Palo Alto Networks, Impresora Xerox, entre otros.
  - ✓ Aplicaciones: VMware vSphere API, VMware vSphere SSH, Amazon AWS, Office 365
- Además de las plataformas compatibles de fábrica, la solución tendrá la flexibilidad y la interfaz fácil de usar para configurar una plataforma personalizada para administrar la contraseña de la cuenta. La función de plataforma personalizada debe ser fácil de usar y permitir al usuario (el cliente) realizar la configuración sin la participación del proveedor del producto.
- La solución admitirá la definición de múltiples políticas de contraseña y la capacidad de aplicar una política de contraseña para múltiples sistemas administrados y una política de contraseña individual para cada sistema administrado.
- La solución debe permitir la definición de un nivel de complejidad mínima para las contraseñas de todos los usuarios registrados en la base de datos local, permitiendo la definición de un número mínimo de letras minúsculas, mayúsculas, caracteres numéricos, caracteres especiales, entre otros.
- La solución debe permitir la creación de una política de bloqueo automático de usuarios después de una serie de fallas de autenticación, evitando así los ataques de fuerza bruta
- La solución debe permitir la definición de un nivel de complejidad mínima para las contraseñas de todos los usuarios registrados en la base de datos local, permitiendo la definición de un número mínimo de letras minúsculas, mayúsculas, caracteres numéricos, caracteres especiales, etc.

- La solución tendrá la flexibilidad de definir un cronograma para restablecer y aleatorizar las contraseñas por sistema administrado y por cuenta sin conocimiento de las contraseñas existentes.
- La solución tendrá la flexibilidad de restablecer y aleatorizar las contraseñas de las cuentas seleccionadas al momento del check-in para eliminar el riesgo de que las contraseñas se vean comprometidas.
- La solución admitirá la recuperación de la contraseña basada en el tiempo mediante la cual la contraseña solicitada se restablece automáticamente al vencimiento del plazo otorgado.
- La solución tendrá la capacidad de desbloquear la cuenta al cambiar su contraseña.
- La solución tendrá la capacidad de establecer la frecuencia de cambio de contraseña en función de la fecha y la hora.
- La solución debe tener la capacidad de cambiar la contraseña de una vez para sistemas individuales, grupales y administrados en función de criterios específicos.
- La solución debe tener la flexibilidad de admitir el cambio de contraseña manual a pedido por parte de un usuario autorizado.
- La solución tendrá la capacidad de hacer cumplir la integridad de la contraseña restableciendo automáticamente las contraseñas de las cuentas que no verificaron o que ya no se sincronizaron con las contraseñas almacenadas en la solución.
- La solución tendrá la capacidad de cambiar automáticamente la contraseña de inicio de sesión de los Servicios de Windows y las Tareas programadas y, opcionalmente, reiniciar los Servicios cuando la solución cambie la contraseña de la cuenta privilegiada correspondiente.
- La solución tendrá la capacidad de realizar una verificación de contraseña en la cuenta administrada y notificar las contraseñas 'fuera de sincronización'.
- La solución tendrá la capacidad de sincronizar contraseñas para cuentas seleccionadas que residen en múltiples sistemas con diferentes tipos de plataforma.
- La solución mantendrá el historial de contraseñas para cuentas privilegiadas administradas y proporcionará una manera fácil de ver las contraseñas antiguas a través de la interfaz web de la solución.
- La solución permite a los usuarios locales restablecer sus contraseñas de manera segura, sin la intervención de los administradores, por correo electrónico o preguntas de seguridad en portal de autoservicio.
- La solución debe soportar autenticación de dos factores en al menos dos tipos diferentes de tokens, el primero es físico (token) y el segundo lógico como software para dispositivos móviles.
- La solución admitirá la gestión de claves SSH a través del almacenamiento automatizado de claves SSH y la rotación de claves SSH de acuerdo con un cronograma definido.
- La solución admitirá la generación de claves SSH con tipos de clave DSA y RSA y tamaño de clave configurable.
- La solución tendrá la capacidad de cambiar la clave SSH de una sola vez para sistemas individuales, grupales y administrados en función de criterios específicos.
- La solución debe tener la flexibilidad de admitir el cambio de clave SSH manual a pedido por un usuario autorizado.

Gestión de Sesiones

- La solución admitirá la supervisión y el registro del acceso de sesión privilegiado a través de los protocolos estándar RDP y SSH. El inicio de sesión automático sin exponer la contraseña de la cuenta privilegiada debe ser compatible con este tipo de acceso.
- La solución admitirá el monitoreo y la grabación de sesiones privilegiadas para el acceso de cualquier aplicación de cliente para clientes gruesos de Windows, incluidos, entre otros, vSphere Client, Microsoft SQL Management Studio, SQL Developer, SAPGui, Toad, etc. y navegadores web. El inicio de sesión automático sin exponer la contraseña de la cuenta privilegiada debe ser compatible con este tipo de acceso.
- La solución permitirá a los administradores agregar y configurar el acceso de cualquier nueva aplicación cliente con monitoreo de sesión y capacidades de inicio de sesión automático.

- La función de grabación de sesión de la solución admitirá el uso de herramientas de cliente comerciales: Escritorio remoto de Windows para acceso RDP y el cliente SSH preferido del usuario, como PuTTY / SecureCRT para acceso SSH.
- La solución tendrá la capacidad de limitar el número de sesiones que un usuario puede abrir para cierto conjunto de cuentas privilegiadas al mismo tiempo.
- La solución debe permitir la carga / descarga directa y la transferencia de archivos desde los sistemas administrados hacia y desde la estación de trabajo del usuario a través de sesiones RDP y SSH. No habrá archivos residuales en la solución después de que se transfieran los archivos.
- La solución tendrá la capacidad de reproducir sonido en sesiones privilegiadas RDP activas.
- La solución tendrá la capacidad de permitir a los usuarios realizar una conexión directa al sistema administrado a través de sus clientes RDP y SSH favoritos sin la necesidad de iniciar sesión en la interfaz web de la solución. La grabación de la sesión, el inicio de sesión automático y sin exponer las características de contraseña de cuenta privilegiada aún se aplicarán a esta forma de acceso.
- La solución tendrá la capacidad de mostrar mensajes en pantalla con temporizador de cuenta regresiva para notificar al usuario antes de que el acceso aprobado exceda el marco de tiempo solicitado.
- La solución tendrá la opción de configuración para finalizar automáticamente una sesión de acceso remoto solicitada si el acceso aprobado excede el período de tiempo solicitado.
- La solución tendrá la capacidad de registro de pulsaciones de teclas para todo tipo de acceso, incluidos los clientes de aplicaciones basadas en RDP, SSH, Web y GUI. La pulsación de tecla debe poder buscarse.
- La solución tendrá la capacidad de enmascarar la contraseña para la sesión RDP y SSH, incluso si se registra la pulsación de tecla.
- La solución tendrá la capacidad de bloquear la sesión SSH cuando se ejecute un comando en la lista negra y, opcionalmente, enviar una notificación por correo electrónico al personal designado al detectar la ejecución de esos comandos.
- La solución tendrá la capacidad para que el usuario autorizado busque en todos los tipos de grabación por pulsación de tecla, fecha / hora, nombre de usuario, nombre del sistema de destino y nombre de cuenta privilegiada.
- La solución permitirá al usuario autorizado reproducir la grabación seleccionada desde la interfaz web sin la necesidad de instalar software de cliente de terceros.
- La capacidad de reproducción de la sesión debe admitir la reproducción desde un punto en el tiempo en la línea de tiempo y la palabra clave buscada en lugar de reproducirse desde el comienzo de la grabación.
- La capacidad de reproducción de la sesión admitirá la reproducción de avance rápido.
- La solución permitirá al usuario autorizado proporcionar comentarios de revisión mientras reproduce la sesión grabada e indicará que la sesión grabada ha sido revisada.
- La solución admitirá el monitoreo en vivo de sesiones desde la interfaz web sin la necesidad de instalar software de cliente de terceros.
- La solución admitirá la intervención de sesión en tiempo real que permite al usuario autorizado bloquear o finalizar una sesión de forma remota cuando se realiza una actividad sospechosa.
- La solución debe tener la opción de configuración para desactivar la grabación para el acceso a la sesión privilegiada seleccionada, pero aun así proporcionar la función de inicio de sesión automático.
- La solución tendrá la flexibilidad de permitir a los usuarios conectarse de forma segura a sistemas de destino remotos a través de la función de grabación de sesión utilizando cuentas que no son administradas por la solución.
- La solución tendrá la capacidad de archivar sesiones grabadas en el almacenamiento a largo plazo para satisfacer los requisitos de retención a largo plazo.
- La solución tendrá la capacidad de reproducir la sesión archivada utilizando la aplicación en sí sin la intervención del administrador. La sesión archivada debe estar protegida y encriptada para que no se pueda acceder fuera de la solución.
- La solución tendrá la capacidad de garantizar la integridad de las sesiones grabadas para evitar la manipulación.

- La solución admitirá la grabación de sesiones con inicio de sesión automático para el sistema Windows donde el agente de autenticación RSA se implementa para la autenticación de dos factores.
- La solución admitirá sesión privilegiada con inicio de sesión automático para la plataforma Windows donde la autenticación con "smart card" esté habilitada.
- La solución admitirá sesión SSH privilegiada en entornos de acceso de shell restringido.

Administración y flujos de trabajo

- La solución garantizará la segregación adecuada de tareas con la capacidad de Control de acceso basado en roles (RBAC) de modo que los roles y los accesos se definan adecuadamente.
- La solución apoyará mínimamente los roles de solicitante, aprobador y revisor para la segregación de funciones.
- La solución tendrá la capacidad de agrupar dinámicamente cuentas administradas en función de criterios que incluyen, entre otros, el tipo de plataforma, la versión de la plataforma, el nombre de dominio, la dirección IP, el nombre del sistema, el nombre de la cuenta, el privilegio de la cuenta, etc. usuarios apropiados para solicitud.
- La solución admitirá el flujo de trabajo basado en políticas y permitirá una configuración sencilla a través de la interfaz web para enrutar la contraseña y la solicitud de sesión a los aprobadores apropiados.
- La solución tendrá la flexibilidad de especificar cero, uno o múltiples aprobadores para cuentas individuales, grupales o todas administradas para control dual. La solución tendrá la flexibilidad para permitir que esta configuración se aplique a uno o grupos de cuentas administradas.
- La solución tendrá la flexibilidad de permitir que múltiples usuarios soliciten la misma contraseña de cuenta y sesión para el mismo sistema administrado en el mismo período de tiempo.
- La solución tendrá la capacidad de restringir el marco de tiempo y la frecuencia con la que los usuarios pueden solicitar contraseñas y sesiones a los sistemas administrados. La solución tendrá la flexibilidad para permitir que esta configuración se aplique a uno o grupos de cuentas administradas.
- La solución tendrá la capacidad de restringir la dirección IP de la computadora del usuario donde se realizan solicitudes de contraseña y sesión. La solución tendrá la flexibilidad para permitir que esta configuración se aplique a uno o grupos de usuarios.
- La solución tendrá la flexibilidad de permitir que se asignen múltiples políticas de aprobación a una cuenta administrada para el mismo solicitante. Esto es para admitir los casos de uso, como una cuenta privilegiada que no requiere aprobación durante el horario de oficina, pero se requiere aprobación después del horario de oficina.
- La solución debe ser configurable para permitir al usuario autorizado eludir las aprobaciones de una cuenta privilegiada seleccionada para casos de emergencia.
- La solución tendrá la capacidad de enviar notificaciones por correo electrónico a los solicitantes y / o aprobadores cuando se haya solicitado una contraseña o sesión.
- La solución tendrá la capacidad de enviar notificaciones por correo electrónico al solicitante y / o aprobadores cuando el aprobador haya aprobado o rechazado la solicitud.
- La solución tendrá la capacidad de enviar notificaciones por correo electrónico al personal designado para cualquier contraseña o solicitud de sesión, independientemente del requisito de aprobación.
- La solución tendrá la capacidad de enviar notificaciones por correo electrónico al personal designado en caso de falla en el cambio de contraseña.
- La solución tendrá la capacidad de enviar notificaciones por correo electrónico al personal designado en caso de que la contraseña de la solución no coincida con la del sistema administrado.
- La solución tendrá la capacidad de permitir la personalización de plantillas de correo electrónico.

Interfaz de usuario

- La solución proporcionará una única interfaz web HTML5 para que los usuarios realicen actividades relacionadas con una cuenta privilegiada, como solicitud, aprobación, reproducción de sesión y recuperación de seguimiento de auditoría, etc., y administradores para administrar cuentas privilegiadas, perfiles de usuario, grupos, organizaciones, roles y políticas.
- La solución deberá tener una interfaz de autoservicio que permita al usuario ver y buscar cuentas privilegiadas para acceder.
- La solución tendrá una interfaz de autoservicio para que el usuario autorizado recupere las credenciales y solicite una sesión de acceso privilegiado para un acceso de tiempo limitado o único.
- La solución permitirá al usuario especificar la fecha / hora de inicio, la duración y la razón al solicitar una contraseña y sesión de cuenta privilegiada.
- La solución permitirá al usuario ver y buscar solicitudes antiguas, existentes y pendientes.

Auditoría, reportería y analítica

- La solución deberá respaldar la auditoría y la rendición de cuentas donde se registra cada transacción para cada solicitud.
- La solución capturará todos los cambios realizados por los administradores en la pista de auditoría, incluido el nombre de usuario, la marca de tiempo, la actividad realizada, la dirección IP y los valores antiguos / nuevos.
- La solución tendrá la capacidad de generar todos los informes por frecuencia, bajo demanda o como tareas programadas.
- La solución admitirá mínimamente estos formatos de informe: CSV, Excel, PDF, PowerPoint, MHTML, Word, TIFF y XML.
- La solución debe proporcionar los siguientes tipos de informes listos para usar sin ningún componente adicional y sin costo adicional:
  - ✓ Informe de antigüedad de contraseña de cuenta que proporciona la última fecha y fecha de cambio de contraseña para cada cuenta administrada.
  - ✓ Informe de actividades del usuario que proporciona una vista transaccional detallada de las actividades de aprobación y solicitud de sesión y contraseña.
  - ✓ Informe de derechos que detalla quién tiene acceso a qué cuentas.
  - ✓ Informe de actividad de cambio de contraseña que detalla el motivo y el resultado del cambio de contraseña.
  - ✓ Informe de programación de cambio de contraseña que proporciona detalles del próximo cambio de contraseña programado.
  - ✓ Restablecimiento de contraseña al liberar el informe de conciliación que muestra los estados de restablecimiento de finalización de solicitud de contraseñas de cuentas administradas para proporcionar evidencia auditable de que las contraseñas se han restablecido adecuadamente después de ser liberadas.
  - ✓ Informe de inventario de activos que proporciona una lista de todos los sistemas administrados y no administrados, activos de TI descubiertos agrupados por sistema operativo.
  - ✓ Informe de inventario de cuenta que proporciona una lista de todas las cuentas administradas y no administradas.
  - ✓ Informe delta de cuenta que proporciona cambios delta para cuentas agregadas y eliminadas de acuerdo con períodos diarios, semanales y mensuales.
  - ✓ Informe de cuentas administradas vs no administradas que proporciona una lista de cuentas del sistema de destino e indica cuáles están bajo administración de contraseñas.
  - ✓ Informe de uso de la cuenta de servicio que proporciona una lista detallada de qué sistemas están utilizando una cuenta de servicio para iniciar uno o más servicios de Windows.
  - ✓ Informe de cumplimiento normativo que proporciona información sobre los estándares reglamentarios (pero no se limita a): COBIT, GLBA, HIPPA, HITRUST, ISO-27002, ITIL, MASS 201, NERC-FERC, NIST 800, PCI y SOX.
- La solución tendrá la capacidad de entregar informes por correo electrónico o en una carpeta compartida de forma automática según un cronograma predefinido para que el usuario no tenga que generar o recuperar informes manualmente.

- La solución admitirá contenido de informes enriquecido que incluye, entre otros, texto, tabla, gráficos, gráfico, barra, etc.
- La solución tendrá la capacidad de permitir la creación de informes personalizados.
- La solución tendrá una capacidad de análisis de amenazas avanzada que identifica usuarios y sistemas específicos de alto riesgo al correlacionar datos de privilegios, solicitudes anómalas y otras amenazas.

Autenticación, seguridad y cumplimiento

- La solución debe estar acreditada con el certificado Common Criteria.
- La solución no deberá contener credenciales codificadas que no puedan administrarse.
- La solución tendrá la capacidad de integrarse con múltiples métodos de autenticación empresarial, incluidos Active Directory, LDAP, Smart Card, RADIUS y mecanismo de autenticación incorporado.
- La solución admitirá la autenticación nativa mediante segundo factor de autententicación TOTP, sin integración con otros componentes en la red.
- La solución admitirá la autenticación integrada de Windows y SAML para el inicio de sesión único.
- La solución admitirá la aplicación de una autenticación fuerte con RADIUS Two Factor Authentication (2FA).
- La solución tendrá la capacidad de integrarse con varios dominios de directorios AD / LDAP, simultáneamente
- La solución tendrá la capacidad de revocar temporalmente a los usuarios seleccionados para evitar que los usuarios accedan a la solución para realizar una solicitud de acceso con privilegios. Al integrarse con AD / LDAP para la autenticación, revocar al usuario en la solución no deberá deshabilitar ni bloquear la cuenta AD / LDAP.
- La solución tendrá la capacidad de integrarse con el Módulo de seguridad de hardware (HSM) listo para usar utilizando el estándar PKCS # 11.

Administración del sistema y APIs

- La solución tendrá la capacidad de realizar una actualización automática cuando haya disponible una versión más reciente del software.
- La solución tendrá la capacidad de enviar notificaciones por correo electrónico al personal designado cuando haya una nueva versión de los paquetes de software disponibles o se hayan instalado automáticamente.
- La solución tendrá la capacidad de realizar copias de seguridad programadas y ad-hoc programadas en sus configuraciones de estado operativo.
- La solución tendrá la capacidad de restaurar sus configuraciones de estado operativo desde la copia de seguridad.
- La solución tendrá la capacidad de enviar información de salud del sistema basada en umbrales predefinidos a través de syslog.
- La solución tendrá la capacidad de enviar información del estado del sistema en función de umbrales predefinidos a través de la captura SNMP.
- La solución tendrá la capacidad de enviar información de salud del sistema en base a umbrales predefinidos por correo electrónico.
- La solución ofrecerá un Kit de desarrollo de software (SDK) que puede abordar casos de esquina, utilizando API disponibles para prácticamente todas las plataformas para permitir el acceso programático en tiempo real a las contraseñas. El SDK permite que las aplicaciones y las personas accedan al almacén de contraseñas de forma independiente, sin usar la interfaz original del producto.
- La solución ofrecerá un Kit de desarrollo de software (SDK) para permitir la administración de contraseñas de cualquier sistema.
- La solución proporcionará RESTful API con características integrales que permiten la administración de la solución mediante programación, que incluye, entre otros, agregar / modificar / eliminar sistemas / cuentas administradas, actualizar políticas de acceso, agregar / eliminar usuarios, recuperación de credenciales de cuenta privilegiadas, solicitud y lanzamiento privilegiado sesión, etc.

- La solución proporcionará documentación API y programas API de muestra en al menos los siguientes lenguajes de programación: Python, C #, Java, PowerShell, Ruby y Unix Shell Script.
- La solución proporcionará una utilidad de línea de comandos con una capacidad similar a la API. La utilidad de línea de comandos debe ser compatible con las plataformas Windows, Linux, AIX, HP-UX y Solaris.

Integraciones

- Integración SIEM: la solución debe tener una integración nativa con las siguientes soluciones SIEM para reenviar eventos. El tipo de eventos debe incluir, entre otros, umbrales predefinidos basados en el estado del sistema, cambios en la configuración del sistema, inicio / cierre de sesión del usuario, solicitud de acceso privilegiado del usuario, solicitud de aprobación / rechazo del aprobador. (Exabeam, Archsight, Qradar, LogRhythm, McAfee DXL y ESM, NetIQ, Syslog, XML, JSON)
- Integración del sistema de tickets: la solución debe tener una integración nativa con los siguientes sistemas de tickets para la validación de tickets: BMC, CA Service Desk, JIRA, ServiceNow
- Integración ITSM: la solución debe tener una integración nativa con las siguientes soluciones ITSM para exportar información de activos: BMC Remedy, ServiceNow
- Integración de IAM: la solución debe tener una integración nativa con las siguientes soluciones de IAM para el proceso de certificación / certificación de acceso privilegiado y el aprovisionamiento automático de usuarios / grupos para la solución: Sailpoint
- Integración de Vulnerability Management: la solución debe tener una integración nativa con las siguientes soluciones de Vulnerability Management como proveedor de credenciales para el análisis autenticado:Tenable y Qualys
- Integración de Threat Analytics: la solución debe tener una integración nativa con las siguientes soluciones de Threat Analytics: Fireeye, Kenna, STIX, PaloAlto
- Integración en la nube: la solución debe tener una integración nativa con las siguientes plataformas de nube y virtualización para descubrir máquinas virtuales en línea / fuera de línea: AWS, GoGrid, GCP, IBM SmartCloud, Microsoft HyperV, Rackspace, VMWare vCenter

Consideraciones

- Debe permitir gestionar al menos 1,500 usuarios concurrentes y soportar mediante upgrade hasta 3500.
- Debe soportar gestionar 3,000 tokens (físicos o Soft-tokens)
- Debe poder soportar como mínimo 500 clientes Radius
- Debe permitir gestionar 7,500 certificados de usuarios
- Como parte de la implementación el contratista deberá de considerar la integración de 200 servidores entre Windows y Linux.
- El contratista deberá brindar el equipamiento físico en caso ofertar equipamiento on-premise.
- En caso la solución ofertada sea en modalidad virtual, las capacidades de hardware serán brindadas por la entidad, así como el licenciamiento Vmware.
- El contratista deberá de considerar el licenciamiento para el sistema operativo y base de datos.
- De requerir utilizar licencias RDS User CAL estas deberán ser provistas por el contratista.
- La entidad podrá realizar requerimientos durante el periodo del servicio para realizar integraciones adicionales de otros equipos de seguridad o comunicación de propiedad de la entidad.
- El proveedor realizará la revisión de estas integraciones y realizará aquellas que se encuentren soportados o que tengan conectores desarrollados por el fabricante de la solución propuesta.

i) Servicio del Sistema de Analítica, Eventos de Seguridad Informática y correlación (SIEM)

El servicio de monitoreo y correlación de eventos deberá ser provisto como parte del servicio del Centro de Operaciones y Seguridad (SOC), Además, los DC deben contar con mínimo la certificación TIER III; a través, de una plataforma modular (stack)(opcional) que separe funcionalmente las capas de ingesta, almacenamiento y explotación de la data. El servicio de monitoreo y correlación de eventos deberá ser en las instalaciones del MRE o ser cloud (el contratista debe brindar servidores físicos conforme a lo requerido en caso sea necesario), garantizando la confidencialidad, integridad y disponibilidad que es gestionada por este servicio. A su vez, para el encriptado, decodificación y almacenamiento de los logs, en caso de ser necesario el Contratista deberá proveer una (1) solución en físico o virtual que permita asegurar la data del MRE. El Contratista deberá proveer el licenciamiento para el funcionamiento de la solución.

El servicio deberá proveer capacidades integradas de administración personalizable y basada en web, Monitoreo de Seguridad, Investigación basada en metadatos de eventos de seguridad, correlación de eventos e incidentes de seguridad. Debe tener capacidad de recolectar, transformar, correlacionar e indexar, la información enviada por los dispositivos de seguridad contempladas en este servicio solicitado.

La solución deberá estar integrado a una solución de inteligencia de amenazas de diferente fabricante o de propiedad del contratista que ofrezca una combinación única de inteligencia de amenazas impulsada por el aprendizaje automático y el análisis humano que deba correlacionar automáticamente con los incidentes o eventos que se identifiquen en la plataforma.

La solución deberá utilizar algoritmos de big data y procesamiento de lenguaje natural para recopilar, del conjunto más amplio de fuentes, y conectar los puntos entre ellos con la inteligencia relevante de la superficie en tiempo real. Este requerimiento deberá ser sustentado con carta de fabricante (opcional)

La solución deberá identificar adversarios y alertas sobre TTPs con sofisticados algoritmos de aprendizaje automático que emergen y analizan datos de amenazas en tiempo real. Deberá tener una idea completa de lo que se sabe sobre los actores de amenazas, incluidos los kits de vulnerabilidades conocidos, las vulnerabilidades u otros TTPs asociados con ellos o se aceptará que la solución deberá identificar adversarios y alertas sobre TTPs con sofisticados algoritmos de aprendizaje automático que emergen y analizan datos de amenazas en tiempo real, la información de estos TTPs podrá mostrarse mediante un panel de MITRE ATT&CK.

La solución debe mostrar datos de amenazas de alta fidelidad, como los controladores RAT y los servidores de comando y control conocidos. Se deben correlacionar estos datos externos con sus registros internos para comprender mejor las tendencias y las amenazas emergentes.

La solución debe recopilar y analizar grandes cantidades de datos para ofrecer información relevante sobre amenazas cibernéticas en tiempo real. La solución debe agregar esta inteligencia con cualquier otra fuente de datos de amenazas, que permita a los equipos de seguridad colaborar en el análisis y brindar inteligencia donde más se necesite.
El servicio del contratista deberá incluir el envío a la entidad de Boletines de Ciberinteligencia relacionado a vigilancia de Internet de alto valor, para que la entidad se encuentre informada de las nuevas amenazas que circulen por el Internet.

Los equipos por correlacionar serán los descritos en esta propuesta, el Controlador de dominio del MRE (Active Directory - AD) el cual cuenta con tres (3) controladores de dominio (instalando los agentes de ser necesario) y otras soluciones que el MRE disponga, hasta un máximo de 50 dispositivos. Para lo cual se deberán ofertar al menos 3000 eventos por segundo (EPS) o 200 Gb de consumo de eventos por día para la solución.

En la etapa de implementación y/o migración de la solución, se ha de mantener los mismos casos de uso que el MRE pueda contar hasta la fecha, para esto se deberá coordinar con el MRE.

Se deberán configurar los casos de uso que requiera el MRE como parte del servicio con fines de proteger la infraestructura digital, todos estos se deberán coordinar con la OTI del MRE.

En caso realizar una migración de su SIEM actual a la solución ofertada se deberá realizar las migraciones de las configuraciones del SIEM actual a la solución ofertado, manteniendo los mismos casos de uso para este nuevo servicio. Los Logs del SIEM actual serán importados por el proveedor del actual servicio, siendo esta su solución, a un sistema de almacenamiento definido por el MRE. Para esto el MRE brindará el almacenamiento necesario para la migración de los logs.

Se deberán configurar los casos de uso que requiera el MRE como parte del servicio con fines de proteger la infraestructura digital, todos estos se deberán coordinar con la OTI del MRE

Como es de conocimiento técnico, los casos de uso en un SIEM son combinaciones de reglas técnicas o acciones de varias reglas según las necesidades de cada organización, y que sirven de ayuda y soporte a los analistas de seguridad con el objetivo de monitorear amenazas y alertar a los SOC, minimizando los falsos positivos. Los casos de uso en un SIEM son configurados conforme evolucionan las amenazas y deben ser configurados y modificados a requerimiento del MRE, por lo que no se dispone de un número que pueda ser confirmado. Para información de los postores, a la fecha el MRE dispone de 25 casos de uso en producción, y dado que se ha requerido agentes de SIEM para el Controlador de Dominio, definitivamente se necesitará implementar casos de uso asociados al controlador de dominio del MRE. Por lo señalado, con base a la experiencia de la institución, se estima que como máximo se podrían requerir 25 casos de uso adicionales.

El Contratista deberá asegurar que los logs en la consola SIEM se puedan visualizarse en línea de por lo menos 3 meses atrás, y que en caso se requiera se pueda visualizar cualquier archivo de log requerido de como mínimo 1 año atrás, a través de cualquier repositorio de almacenamiento de log que el contratista defina.

El contratista recepcionará, de la entidad, la data histórica al inicio del servicio, esto para cargarla al SIEM en formato csv o texto plano, como mínimo. La cantidad de información a migrar será en promedio de 15 TB.

El contratista deberá poner a disposición toda la data histórica generada por las soluciones de la entidad, para que se gestione su respaldo.

La plataforma, en su conjunto, deberá cumplir como mínimo con las siguientes características:

- Todas las comunicaciones entre módulos deben estar protegidas por HTTPS.
- La plataforma deberá estar licenciada por todo el tiempo de soporte, para cubrir el monitoreo y correlación de todos los equipos de seguridad que forman parte de la solución.
- Deberá incluir un sensor que realice inspección de la red interna conectada a un puerto espejo del switch core, esta tecnología deberá otorgar capacidades de collectores o agentes collectores para recibir eventos por segundos
- El sensor de trafico de la solución debe ser capaz de enviar eventos a la plataforma de correlación (opcional), dichos eventos deberán contener por lo menos la siguiente información:
    - IP y puerto origen y destino, nombre de la aplicación, país origen y destino, usuario origen (cuando el sensor se encuentre integrado al Active Directory), URL accedida, Bytes enviados y recibidos, Paquetes enviados y recibidos.
- Capacidad de recolectar la siguiente información de red:
    - Nombre, tipo, categoría y severidad de la amenaza identificada a nivel de red.
    - Nombre del archivo transferido a través de la red.

  - Tipo, categoría, marca, sistema operativo, fabricante del dispositivo origen y destino que genera tráfico de red; siempre y cuando esta información se encuentre disponible en la red.
  - Información de conexiones VPN, tales como IP asignada, IP Pública, País origen, Duración de la sesión VPN, Método de conexión, Estado del login (fallido, exitoso), nombre del acceso VPN.

- Capacidad de recolectar logs de Firewalls Fortinet, Palo Alto, Cisco, Checkpoint, Sophos, entre otros.
- La solución de correlación deberá ser capaz de recolectar eventos de Google Workspace vía API, tales como: eventos de Google Chrome, acciones administrativas de la consola, Google chat, login, reglas, Google Drive, tokens, cuentas de usuarios, alertas, metadata de correos electrónicos (opcional)
- La solución de correlación deberá ser capaz de recolectar eventos de Office 365 vía API, tales como: auditoría de Office 365, Azure AD, Exchange, Sharepoint, metadata de correos electrónicos
- La solución de correlación deberá ser capaz de recolectar eventos de Active Directory (Window Event Logs), tales como: búsquedas de LDAP, gestión de grupos y usuarios de dominio, gestionar de computadoras del dominio.
- La solución de correlación deberá ser capaz de recolectar eventos de Netflow.
- La solución de correlación deberá ser capaz de recolectar eventos de otras fuentes de diferentes marcas a través del protocolo Syslog, pudiendo soportar al menos los formatos CEF, LEEF (opcional), RAW.
- La plataforma de correlación deberá realizar la colección de fuentes en formato o protocolos: CSV, PSV, TSV, texto plano, Archivos en formato CEF/LEEF, JSON; alojados Servidores FTP/SFTP/FTPS y en carpetas compartidas de equipos Windows y Linux.
- Para los archivos alojados en carpetas compartidas, la solución debe ser capaz de colectar los eventos en línea y/o vía batch definiendo la frecuencia en base a minutos, horas o días (opcional).
- La plataforma de correlación deberá ser capaz de conectarse a bases de datos como MySQL, MSSQL, Oracle y PostgreSQL, para poder colectar información alojada en tablas de bases de datos.
- La solución deberá soportar el uso de agentes para equipos Linux, capaces de recolectar los logs nativos de sistemas Red Hat, Centos, Debian, Ubuntu, así como logs de Nginx de forma opcional.
- La solución deberá soportar el uso de agentes para equipos Windows, capaces de recolectar los logs de DNS, logs de DHCP, logs de servidores IIS y Nginx de forma opcional.
- La solución de correlación deberá ser capaz de configurar un formato, normalizar y tabular (parsing) los eventos recibidos de las diferentes fuentes.
- La plataforma deberá poder almacenar la información recolectada en formato raw log (log crudo) por al menos 90 días para cumplir con la política de gestión de incidentes de la entidad.
- La plataforma debe permitir el indexado de los eventos colectados en un esquema de tablas que permitan la búsqueda y uso de estadísticas/métricas de cada campo normalizado
- La plataforma debe permitir visualizar las métricas de espacio, promedio de ingesta diaria, promedio de ingesta total, fecha de última vez de colección, etc.
- La plataforma debe soportar un mínimo de 8000 datasets o tablas de base de datos, asociados a cada fuente de datos (opcional).
- Deberá permitir enriquecer las reglas de correlación con atributos asociados a Tácticas y Técnicas de Ataque, Tipo de Amenaza, Severidad.
- La plataforma debe contar con al menos 60 casos de uso de analítica, teniendo en cuenta que el contratista deberá de crear los casos de usos de analítica necesarios de acuerdo a lo requerido por la entidad.

- Debe asociar cada alerta e incidente de seguridad descubierto a tácticas y técnicas de MITRE ATT&CK.

- La plataforma debe contemplar al menos los siguientes casos de correlación y detección:
    - Acceso a aplicaciones SaaS y de Red inusuales
    - Subida masiva de información a sitios de storage
    - Conexiones a múltiples puertos
    - Conexiones fallidas sospechosas
    - Sesiones SMTP anómalas
    - Subida de información anómala y excesiva por HTTPS, FTP u otro puerto no estándar.
    - Recurrente acceso a un Dominio y/o IP inusual
    - Acceso no-web a un sitio como Pastebin o similar
    - Proceso no-web accediendo a un website
    - Conexiones a Github desde Powershell
    - Conexión inusual de túnel de red
    - Anomalía de viajero imposible para logueos en VPN, Office 365, AWS, Azure, GCP
    - Logueo VPN con una cuenta de servicio
    - Logueo VPN desde un país inusual
    - Logueo VPN en un horario no habitual.
    - Intento de logueo VPN con un usuario inactivo o cuenta de servicio
    - Múltiples conexiones fallidas de DNS que puedan representar C&C
    - Exportación de múltiples cloud snapshots (opcional)
    - Enumeración de contenedores Kubernetes (opcional)
    - Modificación sospechosa de claves SSH de entornos cloud service provider (opcional)
    - Snnifer de red detectado en entornos cloud service provider (opcional)
    - Inusual modificación/creación de recursos cloud (opcional)
    - Actividad de herramientas de pentesting en entornos cloud (opcional)
    - Excesivo bloqueo de cuentas de dominio
    - Ataques de fuerza bruta
    - Enumeración remota de usuarios
    - Intento de reseteo de password de usuario administrador
    - Login interactivo de una cuenta de servicio
    - Posible pass the hash
    - Habilitación de usuarios por defecto de Windows
    - Creación sospechosa de usuario domain admin
    - Configuraciones anómalas en Office 365 y Google Workspace
- A través de la integración de agentes se deberá correlacionar de manera automática las alertas de seguridad descubiertas por los agentes con los Logs y Eventos recolectados de plataformas terceras. Si se requiere la instalación de agentes para la recopilación de eventos. Se deberá contemplar 1800 agentes como mínimo. El servicio deberá contemplar un crecimiento de 300 agentes adicionales sin representar ningún costo para la entidad.
- A partir del comportamiento aprendido en los endpoints, la solución deberá ser capaz de alertas los siguientes comportamientos inusuales, que estén fuera del perfil base aprendido:
    - Usuario sospechoso
    - Tarea programada creada de forma inusual en el sistema operativo
    - Conexión de escritorio remoto que no se usan normalmente
    - Escaneo de puertos sospechoso
    - Creación de usuario con permisos privilegiados como administrador de dominio.
    - Actividad en el registro Windows, identificando la creación, eliminación, renombrado, definición de valores, eliminación de valores de las llaves de registro. Almacenando esta información en su mayoría en el cache del agente de ser necesario
    - Actividad de procesos, identificando si se trata de una ejecución o inyección, ruta desde donde se ejecuta, comando que inicializa el proceso, usuario, hash en SHA256 y MD5.

- Actividad de los archivos, identificando las siguientes operaciones: creación, lectura, eliminación, escritura y renombrar. Almacenando esta información en su mayoría en el cache del agente de ser necesario

- Uso de aplicativos que no se usan normalmente

- Deberá contar con un lenguaje propio para realizar consultas de cada dataset, que incluya al menos los siguientes criterios: Filtros por cada atributo del dataset con coincidencia total o parcial de cada atributo; uso operadores booleanos (and, or, not); operadores de comparación (igual, no igual, mayor que, menor que, mayor o igual que, menor o igual que); capacidad para especificar un límite de resultados (top 10, 20, 100, 500, 1000, personalización en general); operadores de comparación de datos; operadores matemáticos (promedio, contar, contar-distinto, máximo, mínimo, sumar); combinar búsquedas de dos o más datasets (opcional).
- Deberá contar con una librería predeterminada de búsquedas habituales realizadas en una labor de threat hunting. Esta librería podrá ser editada según la labor del investigador.
- Todas las opciones de búsqueda anteriormente detalladas deberán poder ser utilizadas para configurar reglas personalizadas de seguridad, que permitan generar una alerta cuando exista alguna coincidencia en el log (o logs) recolectados con la regla de búsqueda
- Se deberá poder integrar las diferentes visualizaciones en dashboard globales que permitan un entendimiento general.
- Los dashboards podrán contener enlaces a otros dashboards para ahondar en el análisis.
- Se aceptará que se cuenten con drilldown en los dashboar de la herramienta
- Dashboards configurables en tiempo real
- Disponibilidad de un conjunto de respuestas pre-configuradas o personalizadas ante eventos de seguridad, de manera que se permita no sólo la detección sino también la remediación automatizada ante determinadas amenazas.
- Establecimiento de patrones de comportamiento y
- visualización a través de un dashboard el comportamiento y actividad base de endpoint/servidor/usuario - granularidad de los 24 hora/día de la semana/fin de semana. (Lunes, martes, miércoles, jueves, viernes, sábado y domingo).
- Se deberán poder realizar visualizaciones de relaciones.
- Deberá contar con un módulo de machine learning no supervisado que permita encontrar anomalías en series de tiempo. Se deberá evidenciar el periodo de entrenamiento y de activación por cada caso de uso que se involucre en la solución
- Deberá contar con un módulo de alertas. Se debe poder definir alertas basadas en umbrales, en correlación de eventos, y en anomalías detectadas por machine learning. estas últimas deberán contar con un mecanismo de duplication de datos antes cualquier evento repetitivo para contar con datos significativos
- La solución SIEM deberá contar con reportes y plantillas modificables por el usuario.
- Deberá mostrar los reportes en pantalla antes de solicitar cualquier exportación a formatos externos.
- La plataforma deberá poder contar con paquetes de reportes de cumplimiento a normativas como CIS Bechmark o reportes predefinidos como Inventarios de Activos en Nube, Análisis del Tráfico de Red, Gestión de riesgos, Ingesta de Datos, entre otros
- Deberá exportar reportes en los formatos CVS y/o PDF y/o DOC y/o XML/HTML
- La información almacenada en la base de datos debe estar protegida por organismos internacionales.
- Tambien se aceptará que la solucion de SIEM cuente con técnicas de Machine Learning para detectar comportamientos inusuales de usuarios y entidades (UEBA) sin requerir configurar reglas complejas.

j) Servicio de Respuesta ante Incidentes

- El Contratista deberá ofertar un servicio de respuesta ante incidentes y emergencia de seguridad informática, con el objetivo de apoyar al MRE en la mitigación, contención y solución de las incidencias, así como en la preparación de la respuesta ante dichas emergencias. Este servicio abarcará todas las soluciones ofertadas en este pliego.

- El servicio deber proveer un modelo de anticipación y respuesta frente a crisis derivadas de incidentes graves de seguridad, así como debe diseñar todos los mecanismos necesarios de contención, análisis, respuesta, erradicación y recuperación como parte de la gestión de incidentes de seguridad. Para ello el Contratista debe contar con un equipo de respuesta ante incidentes de seguridad informática CSIRT (Computer Security Incident Response Team). Las instalaciones y el personal que operan el CSIRT del Contratista, deben estar ubicados en la ciudad de Lima, Perú.
- Este servicio se activará bajo demanda (requerido explícitamente por la OTI del MRE) en el transcurso del período del servicio. El servicio asigna una cantidad de 250 horas para la gestión de incidentes para el MRE por cada año que dure el servicio. El resultado del servicio será un informe por ocurrencia del análisis de incidentes, las medidas de contención y respuesta implementadas y el estado de recuperación de los servicios o activos.
- Este servicio se deberá realizar fundamentalmente desde las instalaciones del Contratista con una conexión remota hacia los activos del MRE que han sido afectados por el incidente, excepcionalmente cuando el incidente no pueda ser superado de manera remota, el Contratista deberá coordinar con el MRE para desarrollar la gestión de incidentes de manera presencial en las locaciones donde se encuentran los activos afectados.

- Este servicio debe basarse en las siguientes políticas:

  - Realizar el registro, clasificación y atención de los incidentes de seguridad.
  - Asesorar en la evaluación de los daños ocasionados por los incidentes de seguridad.
  - Asesorar en la etapa de erradicación y recuperación del incidente al MRE.
  - Reportar los resultados de la gestión de incidentes notificados.
  - El servicio debe ser prestado en la modalidad 24x7.
  - El Contratista accederá a la información obtenida y procesada resultante de la gestión de incidentes.
  - Toda la información generada y procesada es propiedad del MRE, siendo además confidencial.
  - El Contratista deberá implementar los mecanismos físicos y lógicos de seguridad para garantizar que la información que produzca este servicio se mantenga confidencial, integra y disponible.
  - Comunicar al MRE cualquier información relevante que permita gestionar de manera adecuada el incidente notificado.
  - El Contratista deberá contar con un equipo multidisciplinario para atender diversos incidentes que pueda presentarse
  - El Contratista durante todas las etapas de tratamiento del incidente, deberá apoyarse no solo de las herramientas que son parte del servicio contratado, sino también de herramientas adicionales (licenciadas o software libre) y dependiendo de la fase en que la investigación se encuentre, por ejemplo: el uso de herramientas de investigación forense, de análisis de malware, de análisis de aplicaciones web, de sniffer de redes, entre otras necesarias
  - El Contratista durante todas las etapas de tratamiento del incidente, deberá contar con capacidades de Ciberinteligencia para informar sobre posible fuga y publicación de información del MRE en la internet, Deepweb y Darkweb
  - Asesorar al MRE en las medidas a tomar respecto de la gestión de incidentes.
  - Elaborar un informe que contenga las actividades realizadas para la gestión de los incidentes notificados.
  - Informar al MRE en cuanto se advierta la ocurrencia de un incidente de Ciberseguridad que presente un impacto significativo adverso significativo verificado o presumible de:

    - Afectación considerable a la Confidencialidad, Disponibilidad e Integridad de la Información, como, por ejemplo: Pérdida o hurto, Inaccesibilidad y alteración de información de la empresa o de clientes
    - Fraude interno o externo.
    - Impacto negativo en la imagen o reputación de la empresa.

- Interrupción de operaciones críticas de negocio.

- El equipo de respuesta antes incidentes del contratista debe estar registrado como miembro de FIRST (Forum of Incident Response and Security Teams).

- El servicio deberá estar compuesto por las siguientes etapas basado en un enfoque CSIRT:

  a. **Presentación del plan de atención de incidentes.** El Contratista deberá definir en el plan lo siguiente:

     - Conocimiento de la infraestructura y de la red del MRE.
     - Clasificación y jerarquía de los activos de acuerdo con el valor del negocio.
     - Roles, responsabilidades y partes interesadas dentro de la organización encargados de los riesgos, activos, así como de la detección de incidentes, la operación, la continuidad y la disponibilidad del servicio. El CONTRATISTA debe considerar la revisión del actual PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DIGITAL EN LAS ENTIDADES PÚBLICAS para la propuesta de la organización del servicio.
     - Definir los incidentes por tipo y niveles de impacto en base al criterio de taxonomía o clasificación que se vaya a utilizar asociado a los activos de información del MRE. En la fase de transición el Contratista deberá coordinar con el MRE la obtención de la clasificación de los activos de información.
     - El servicio debe tener la capacidad de analizar, mediante el uso de Sandboxing u ambientes propios para tal fin, el malware encontrado.

  b. **Reporte y solicitud de apoyo para la atención de incidentes.** El reporte de un incidente de seguridad será notificado a través del proceso o canal establecido entre el Contratista y el MRE, posterior al reporte en caso corresponda que se requiera apoyo en la contención y mitigación del incidente, podrá hacer uso del servicio solicitando el apoyo por cualquier canal de comunicación (telefónico, correo, aplicativo).

     El Contratista cuando lo requiera podrá solicitar el apoyo de las personas involucradas en el incidente reportado con el fin de las validaciones, aprobaciones y correcta ejecución de actividades.

  c. **Apoyo en la contención y mitigación del incidente.** El Contratista deberá hacer las sugerencias y recomendaciones de las actividades que se deben realizar como parte de la respuesta de la atención del incidente reportado siguiendo estos pasos:

     - Realizar una evaluación inicial.
     - Generar recomendaciones para contener el daño y minimizar el riesgo.
     - Identificar el tipo y la gravedad del ataque.
     - Generar recomendaciones para proteger las pruebas en caso de requerir un análisis forense.
     - Notificar a los organismos externos cuando corresponda.
     - Generar recomendaciones para recuperar los sistemas.
     - Apoyar en la compilación y organización de la documentación del incidente.
     - Apoyar en la valoración de los daños del incidente.
     - Revisar las directivas de respuesta y actualización.

- El Contratista deberá garantizar que cuenta con los recursos que permitan ejecutar el servicio solicitado de forma efectiva, para lo cual deberá cumplir con las siguientes responsabilidades:

  - Garantizar la conformación de un equipo multidisciplinario con amplio conocimiento y experiencia para la ejecución del servicio de respuesta a incidentes.
  - Garantizar la calidad de los servicios y equipos considerados en la prestación del servicio.

- Diseñar un modelo de anticipación y respuesta frente a crisis derivadas de incidentes graves de seguridad.
- Diseñar todos los mecanismos necesarios de contención, análisis, remediación y recuperación que se produzcan en los incidentes de seguridad.
- Presentar un informe de la gestión realizada por cada incidente que se produzca que incluya: las medidas de contención y respuesta implementadas y el estado de recuperación de los servicios o activos.

- El MRE deberá cumplir con las siguientes responsabilidades:

  - Designar personal de contacto autorizado para el servicio.
  - Entregar la información requerida.
  - Dar las facilidades de acceso al personal de El Contratista para la atención de incidentes reportados en la sede del MRE, en caso se requiera.
  - Designar a las personas con responsabilidad suficiente, que serán autorizadas para servir como coordinadores para casos de garantía.
  - Garantizar la conectividad para la conexión remota
  - En caso se detecte un incidente ajeno al alcance del presente servicio gestionado al MRE compartirá los logs o pistas de auditoría.
  - Ejecutará las acciones de contención y erradicación solicitadas por el contratista en los plazos definidos y acordados con el contratista
  - Organizar al comité de crisis para tomar decisiones en conjunto

Importante: **El ganador de la buena pro deberá presentar documentación que evidencie que es miembro de FIRST para el perfeccionamiento del contrato.**

k) Servicios Programados

PENTESTING

ALCANCE	FRECUENCIA
Diez (10) dominios externos relacionados a aplicaciones o servicios web, primero en modalidad de caja negra y luego de caja gris por año	Anual (una vez al año)
Cinco (05) dominios internos relacionados a aplicaciones o servicios web, primero en modalidad de caja negra y luego de caja gris por año	Anual (una vez al año)
Quince (15) activos informáticos, los cuales podrían ser servidores u equipos de comunicación	Anual (una vez al año)

La programación se realizará en coordinación entre el Contratista y el MRE.

El contratista deberá brindar un servicio de pentesting que permita identificar de manera proactiva las vulnerabilidades al que podría estar expuesta la Infraestructura TI y activos de información del MRE, frente a la posible materialización de una amenaza. Este servicio será ejecutado de manera presencial y remota, dependiendo sea el caso.
Respecto a la prueba de pentesting, el servicio de Pentesting para sus pruebas de caja negra y caja gris comprende la revisión sobre los activos dentro del presente servicio gestionado. Para ello, en base a la programación establecida, el contratista deberá ejecutar las siguientes actividades:

- Realizará las pruebas automáticas (automatizadas) y/o manuales sobre los servicios para revelar vulnerabilidades y debilidades de seguridad.
- Utilizará las metodologías siguientes:
  - Manual de código abierto para la realización de pruebas de seguridad OSSTM v3
  - Guía de Pruebas OWASP v4 (Proyecto abierto de seguridad de aplicaciones web).
- Basado en la Guía OWASP para los diferentes recursos de cada activo se deberá verificar las pruebas de 89 controles los mismos que son listados a continuación;

asimismo bajo el supuesto que se indisponga los activos y servicios asociados, estas actividades se deben realizar previa coordinación con el personal encargado del MRE.

Lista de controles de la guía de Pruebas OWASP:

N°	DESCRIPCIÓN DEL CONTROL	CÓDIGO DEL CONTROL
Recopilación de Información		
1	Conducir motor de búsqueda para el descubrimiento y reconocimiento de fugas de información	OTG-INFO-001
2	Huellas digitales servidor WEB	OTG-INFO-002
3	Revisión de los meta-archivos del servidor web en busca de fugas de información	OTG-INFO-003
4	Enumere las aplicaciones en el servidor WEB	OTG-INFO-004
5	Revisión de los comentarios del sitio web y los metadatos en busca de fujas de información	OTG-INFO-005
6	Identificar puntos de entrada de la aplicación	OTG-INFO-006
7	Creación de mapas de rutas de ejecución a través de la aplicación	OTGINFO-007
8	Marco referencial para el uso de huellas digitales en aplicaciones WEB	OTG-INFO-008
9	Huellas digitales aplicaciones WEB	OTG-INFO-009
10	Mapa de arquitectura de la aplicación	OTG-INFO-010
Pruebas para gestionar la configuración y la implementación		
11	Prueba configuración Red/Infraestructura	OTG-CONFIG-001
12	Prueba de la configuración de la plataforma de aplicaciones	OTG-CONFIG-002
13	Prueba manejo de archivos de extensiones en busca información sensible	OTG-CONFIG-003
14	Revisión archivos viejos	OTG-CONFIG-004
15	Enumeración Infraestructura y de Interfaces de administración de aplicaciones	OTG-CONFIG-005
16	Prueba métodos HTTP	OTG-CONFIG-006
17	Prueba HTTP Strict Transport Security	OTG-CONFIG-007
18	Prueba política de dominio cruzado RIA	OTG-CONFIG-008
Pruebas de Administración de Identidad		
19	Prueba de definición de roles	OTG-IDENT-001
20	Prueba proceso de registro de usuarios	OTG-IDENT-002
21	Prueba proceso de provisión de cuentas	OTG-IDENT-003
22	Pruebas para enumeración de cuentas y cuentas de usuario adivinables	OTG-IDENT-004
23	Pruebas para política de nombre de usuarios débiles o sin fuerza	OTG-IDENT-005
24	Pruebas para enumeración de cuentas y cuentas de usuario adivinables	OTG-IDENT-004
25	Pruebas para política de nombre de usuarios débiles o sin fuerza	OTG-IDENT-005
Pruebas de autenticación		
26	Pruebas para credenciales transportadas sobre canales encriptados	OTG-AUTHN-001

27	Pruebas credenciales por defecto	OTG-AUTHN-002
28	Pruebas para mecanismos de seguridad débiles	OTG-AUTHN-003
29	Pruebas para eludir el esquema de autenticación	OTG-AUTHN-004
30	Prueba funcionalidad recordatorio de clave	OTG-AUTHN-005
31	Prueba para debilidades en la memoria del navegador	OTG-AUTHN-006
32	Prueba para política de clave débil	OTG-AUTHN-007
33	Prueba para seguridad pregunta/respuesta débil	OTG-AUTHN-008
34	Prueba para cambios de clave débil o funcionalidades de reinicio.	OTG-AUTHN-009
35	Prueba para autenticación débil en canal alternativo	OTG-AUTHN-010
Pruebas de autorización		
36	Prueba de inclusión archivos de directorio de circulación	OTG-AUTHZ-001
37	Prueba para evadir el esquema de autorización	OTG-AUTHZ-002
38	Prueba para escalación de privilegios	OTG-AUTHZ-003
39	Prueba de la referencia de objetos directos inseguros	OTG-AUTHZ-004
Pruebas de administración y sesión		
40	Prueba para evadir el esquema de administración de sesión	OTG-SESS-001
41	Prueba para atributos de cookies	OTG-SESS-002
42	Prueba de fijación de sesión	OTG-SESS-003
43	Prueba de exposición de variables de sesión	OTG-SESS-004
44	Prueba para falsificación de petición de sitio cruzado	OTG-SESS-005
45	Pruebas funcionalidad cierre de sesión	OTG-SESS-006
46	Pruebas del tiempo cierre de sesión	OTG-SESS-007
47	Prueba para sobrecarga de variables	OTG-SESS-008
	Pruebas de validación de entradas	
48	Pruebas para la reflexión de Cross Site scripting	OTG-INPVAL-001
49	Pruebas de Cross Site Scripting almacenados	OTG-INPVAL-002
50	Pruebas de manipulación de verbos en HTTP	OTG-INPVAL-003
51	Pruebas de contaminación de parámetros HTTP	OTG-INPVAL-004
52	Pruebas de Inyecciones de SQL	OTG-INPVAL-005
	Pruebas de inyección NoSQL	
53	Pruebas de inyección LDAP	OTG-INPVAL-006
54	Pruebas de inyección de ORM	OTG-INPVAL-007
55	Pruebas de inyección de XML	OTG-INPVAL-008
56	Pruebas de inyección SSI	OTG-INPVAL-009
57	Pruebas de inyección XPath	OTG-INPVAL-010
58	Pruebas de inyección de IMAP/SMTP	OTG-INPVAL-011
59	Pruebas de inyección de código	OTG-INPVAL-012
	Pruebas para determinar la inclusión de documentos locales	
	Pruebas para la inclusión remota de archivos	
60	Pruebas de inyección de comandos	OTG-INPVAL-013
61	Pruebe la saturación del Búfer	OTG-INPVAL-014
62	Pruebas de las vulnerabilidades incubadas	OTG-INPVAL-015
63	Pruebas para verificar la separación/contrabando de HTTP	OTG-INPVAL-016
	Pruebas de manejo de errores	
64	Pruebas de errores de código	OTG-ERR-001

65	Pruebas para determinar los rastros de pila de datos	OTG-ERR-002
	Pruebas para Criptografía débil	
66	Pruebas de codificadores SSL/TLS débiles	OTG-CRYPST-001
67	Prueba del Padding Oracle	OTG-CRYPST-002
68	Pruebas para el envío de información sensible por canales sin encriptar	OTG-CRYPST-003
	Prueba de la lógica del negocio	
69	Pruebas de la validación de datos de la lógica del negocio	OTG-BUSLOGIC-001
70	Prueba de la habilidad para manipular consultas	OTG-BUSLOGIC-002
71	Prueba de comprobación de integridad	OTG-BUSLOGIC-003
72	Pruebas del tiempo de procesamiento	OTG-BUSLOGIC-004
73	Prueba del número de veces que limita el uso de una función	OTG-BUSLOGIC-005
74	Pruebas para la evasión de los flujos de trabajo	OTG-BUSLOGIC-006
75	Prueba de las defensas contra el mal uso de la aplicación	OTG-BUSLOGIC-007
76	Prueba de la posibilidad de carga de tipos de archivos inesperados	OTG-BUSLOGIC-008
77	Prueba de la posibilidad de carga de archivos maliciosos	OTG-BUSLOGIC-009
	Pruebas en el lado del cliente	
78	Prueba del Cross Site Scripting basado en DOM	OTG-CLIENT-001
79	Prueba de la ejecución de JavaScript	OTG-CLIENT-002
80	Prueba de inyección de HTML	OTG-CLIENT-003
81	Pruebas de redireccionamiento de la URL del lado del cliente	OTG-CLIENT-004
82	Pruebas de inyección de CSS	OTG-CLIENT-005
83	Pruebas de la manipulación de recursos del lado del cliente	OTG-CLIENT-006
84	Pruebas para el Intercambio de recursos de origen cruzado	OTG-CLIENT-007
85	Pruebas de Cross Site Flashing	OTG-CLIENT-008
86	Pruebas de Clickjacking	OTG-CLIENT-009
87	Pruebas de WebSockets	OTG-CLIENT-010
88	Prueba de mensajería web	OTG-CLIENT-011
89	Prueba de Almacenamiento Local	OTG-CLIENT-012

- Orientado a los equipos de comunicación

  - Levantamiento de información de la red del cliente
  - Mapeo de la red y equipos
  - Escaneo de las vulnerabilidades de la red
  - Explotación de vulnerabilidades
  - Reporte del análisis

- Orientado a los servidores

  - Identificación de los servidores
  - Mapeo de los servicios implementados en los servidores
  - Escaneo de las vulnerabilidades en los servidores
  - Explotación de vulnerabilidades

- Reporte del análisis

- Posteriormente a la evaluación de vulnerabilidades, el contratista deberá realizar acciones de penetración (incluye explotación) previa coordinación con el personal encargado del MRE. Estas acciones sumadas a la identificación de vulnerabilidades formarán parte de una prueba de concepto (POC) que evidencia el hallazgo de la vulnerabilidad, la trazabilidad y la explotación de esta.
- Las acciones que deriven del servicio no deberán causar daño alguno en el funcionamiento de los sistemas o en el desempeño de la red de la Institución.
- Se identificará cualquier deficiencia asociada a la seguridad en el diseño y la estructura de las aplicaciones, evaluando los niveles de seguridad existentes, incluyendo normas básicas de diseño y desarrollo de aplicaciones.
- Se deberán realizar la ejecución de análisis de vulnerabilidades, el cual deberá comprender el uso de herramientas comerciales, comunitarias y open source de ser el caso, sin embargo, se requiere que para el caso de la herramienta para escaneo de vulnerabilidades automatizada se deberá considerar una herramienta comercial que incluya una base de datos actualizada de CVEs, así como la información para la mitigación del servicio vulnerable. Se deberá mostrar la evidencia del uso de esta herramienta comercial.
- Asimismo, en caso se utilice herramientas gratuitas que sean parte de la POC, estas, deberán ser compartidas con la entidad como parte de la transferencia metodológica y posibilidad de replicación que ayude a la mitigación.
- Se deberán combinar técnicas avanzadas de ataque como la simulación de adversarios, emulando un ataque real y en profundidad contra los activos que forman parte del alcance del servicio con el fin de verificar posibles vectores de ataque, así como comprobar y testear los controles de seguridad que tiene desplegados y hasta dónde podría llegar un eventual atacante.
- La transferencia de conocimiento y las reuniones ejecutivas deberán ser realizadas de manera remota y serán grabadas, las cuales serán compartidas finalizando la etapa de Pentesting
- La Metodología y buenas prácticas implementadas durante el desarrollo del servicio deben ser transferidas hacia el MRE (de tal forma que el personal de del MRE pueda observar las tareas que se ejecuten como parte de la transferencia de conocimiento por parte del contratista)
- El informe de Pentesting debe considerar mínimamente el siguiente contenido

    - Descripción de las pruebas realizadas
    - Elemento evaluado
    - Puertos y servicios habilitados
    - Listado de vulnerabilidades encontradas en los elementos de la plataforma tecnológica
    - Descripción de la vulnerabilidad
    - Nivel de criticidad (Extremo, Alto, Medio, Bajo), utilizar una metodología para este aspecto.
    - Riesgo asociado
    - Recomendación.
    - Procedimientos para eliminar las vulnerabilidades internas y externas encontradas.

Respecto a la reevaluación de Vulnerabilidades, Al tercer mes de finalizado las pruebas (previa comunicación con el MRE), el contratista deberá realizar una reevaluación de las vulnerabilidades reportadas en las pruebas de pentesting a fin de validar si fueron implementadas las recomendaciones adecuadamente. Al término de la ejecución de esta fase se deberán actualizar los entregables de las pruebas de pentesting

1.2. Consideraciones Adicionales del Servicio

Las siguientes consideraciones aplican a todo el servicio solicitado:

- El ganador de la buena pro deberá proporcionar la información necesaria que sustente las especificaciones técnicas de los equipos requeridos para todas las soluciones de

seguridad, para ello deberá adjuntar la ficha técnica del fabricante, en donde señale la marca y modelo (en caso de software, se podrá colocar el nombre de la solución o software) de los appliance o componentes ofrecidos en calidad de alquiler, acompañado de la información técnica del fabricante y/o documento del mismo, donde se detalle las características técnicas mínimas solicitadas, en idioma español o en su defecto acompañado de la traducción respectiva, emitido por traductor público juramentado o traductor colegiado certificado, según corresponda (*)

***Importante**: El ganador de la buena pro deberá presentar para la suscripción del contrato las fichas técnicas antes descritas con la información solicitada.*

(*) Se precisa que las especificaciones técnicas de las soluciones serán evidenciadas con Documentación del Fabricante. Cuando existan características técnicas que no se encuentren en la documentación del fabricante podrá acreditarse mediante una carta del fabricante.

- El Contratista será responsable del levantamiento de la información (actuales políticas y reglas de seguridad) y traslado o adaptación de políticas del equipamiento existente, y en caso aplique proponer mejoras previa evaluación de la Oficina de Tecnologías de la Información.
- El Contratista deberá garantizar la infraestructura y configuraciones necesarias para el uso ininterrumpido, a través de redes privadas virtuales (VPN) sobre Internet, de los sistemas de información corporativa que se encuentren en producción al momento de la migración.
- El Ministerio de Relaciones Exteriores podrá solicitar información histórica del servicio con una antigüedad máxima de un (01) año, Esto hace referencia a la información que se almacenará en el Sistema de Gestión de Información y eventos de Seguridad informática.
- El Ministerio de Relaciones Exteriores podrá solicitar que se generen los reportes personalizados de cada solución, y estos se remitan de manera periódica a cuentas de correo electrónico que defina la OTI del MRE.
- El Contratista deberá contar para todos los componentes o appliance para la ejecución del servicio con las licencias y soporte respectivo de los fabricantes durante toda la vigencia del contrato.
- Los appliance o componentes ofrecidos, en calidad de alquiler para la ejecución del servicio requerido, deberán posicionarse dentro de la familia de equipos con tecnologías de última generación, que se encuentren publicadas por el fabricante, lo que significa que no deberán estar descontinuados (end-of-life) durante el periodo de garantía.

4.1.3. Instalación y Configuración

- El Contratista deberá brindar las garantías y soporte de todo el equipamiento a instalar en la Entidad, durante todo el período de ejecución del servicio, que incluya el cambio inmediato en caso de falla, para lo cual el Contratista deberá presentar una declaración jurada o carta de compromiso.
  ***Importante**: La declaración jurada o carta de compromiso deberá ser presentada como requisito para perfeccionar el contrato.*

- Para la realización de trabajos de implementación del servicio, la Entidad brindará al Contratista las facilidades y accesos necesarios de las instalaciones involucradas para la presente contratación. En ese sentido; el Contratista deberá coordinar con la Entidad los horarios de accesos y trabajos de migración.
- El Contratista es responsable de efectuar los estudios de ingeniería respectivos que le permitan cumplir con el servicio, en esa medida, si fuera necesario realizar obras civiles dentro o fuera del local o locales de Ministerio de Relaciones Exteriores, para la instalación de los servicios propuestos, estos deberán ser realizados por el Contratista, quien asumirá los costos que puedan involucrar.
- La implementación se realizará en forma paralela al actual servicio para mantener así su continuidad, para dicho fin la Entidad brindará al contratista las facilidades técnicas. Asimismo; el Contratista realizará las configuraciones necesarias en los equipos

propuestos a fin de mantener o mejorar el nivel de seguridad existente, con el menor impacto posible.

- El Contratista será responsable de la migración, instalación, configuración y puesta en marcha de las soluciones solicitadas; así mismo, el Contratista deberá asegurar que los equipos a proveer sean compatibles entre sí.
- El Contratista debe considerar las características del equipamiento de red interna (LAN) y externa (WAN) existente en la Entidad, a fin de que pueda ser integrado; y de esa manera el equipamiento proveído por el Contratista, en calidad de alquiler, cumpla con el servicio solicitado. Cualquier equipo, insumo, adaptador, cableado, accesorio, configuración o licencia que se requiera adicionalmente y que son necesarios para la integración de los equipos o componentes ofertados, los mismos que serán instalados dentro de la infraestructura y deben cumplir con los requerimientos del Ministerio de Relaciones Exteriores para este servicio, los mismos que serán asumidos por el Contratista, a fin de mantener operativa la prestación del servicio.
- Los servicios y appliance o componentes serán instalados y configurados en su totalidad en la sede del MRE, ubicado en el centro de datos Edificio Raúl Porras Barrenechea, ubicado en el Jirón Ucayali N.° 337 - Cercado de Lima. La configuración será diseñada en coordinación con la Oficina de Tecnologías de la Información.
- Todos los componentes o equipos, con sus respectivos accesorios, proveídos por el Contratista deberán ser otorgados en calidad de alquiler, formando parte del servicio ofertado durante el tiempo de vigencia del contrato.
- El equipamiento ofertado por el ganador de la buena pro, será ubicado en el Centro de Datos del MRE, procurando la proximidad entre dicho equipamiento.

Nota:

- ***En caso se presente alguna falla generada por el ambiente virtual, el equipamiento físico o el software provisto por la entidad, y este perjudique la ejecución o funcionamiento del software o equipamiento ofertado; eximirá de toda responsabilidad al contratista de las soluciones ofertadas, y solo el contratista podrá restablecer el servicio cuando la entidad resuelva cualquier problema con sus componentes.***
- ***Si los servidores físicos y el ambiente virtualizado que brindará la entidad para la ejecución del software serán exclusivamente para la solución ofertada con los recursos necesarios en el periodo de 2 años.***
- ***La entidad brindará al contratista toda la información necesaria para realizar las configuraciones de red, perfiles de seguridad, reglas u objetos en general, para poder implementar correctamente la solución ofertada.***
- ***La entidad asegurará las conexiones eléctricas de todos los equipamientos que se instalen en el Data Center del MRE, contando con tomas de energía de tipo C14 para PDU, entre otras.***
- ***La entidad será responsable de la supervisión, control y custodia de los equipamientos físicos y ambientes virtuales, que provea para la ejecución y funcionamiento de las soluciones de seguridad ofertadas por el contratista.***
- ***La entidad brindará toda información técnica y necesaria para la ejecución y/o implementación de las soluciones de seguridad ofertadas por el contratista.***

4.1.4. Operación del Servicio

- El Contratista efectuará las siguientes actividades durante el servicio gestionado:

  - Trabajos preventivos, correctivos y bajo demanda las 24 horas del día y los 7 días a la semana, el mismo que consistirá en lo siguiente:
    - ✓ Configuraciones a nivel de red.
    - ✓ Configuraciones en las funcionalidades de seguridad.
    - ✓ Configuraciones a nivel de seguridad
    - ✓ Actualizaciones de Firmware de los equipos propuestos. Las actualizaciones no deberán generar un costo adicional al Ministerio de Relaciones Exteriores y deberán realizarse en coordinación con la Oficina de Tecnologías de la Información.

- El Contratista deberá efectuar los Mantenimientos Preventivos que estime conveniente a fin de garantizar el correcto funcionamiento de cada equipo o componente que permita el óptimo desarrollo del servicio requerido.

- Adicionalmente, el contratista dispondrá de un técnico ON-SITE dedicado para el MRE, el mismo que debe participar desde el diseño e implementación del servicio, además prestará servicio posterior a la implementación asistiendo de manera presencial a las instalaciones del MRE de lunes a viernes, previa coordinación con la OTI del MRE, desde las 08:30 hasta las 17:30 horas.

- En caso de requerirse actividades presenciales fines de semana u otros días, el contratista deberá asegurar el soporte presencial, para actividades como atención y soporte para monitoreo de red frente a amenazas en eventos extraordinarios programados por el MRE, apagado o encendido de equipos de la solución, pruebas de alta disponibilidad, upgrades de firmware de equipos de la solución, reemplazo de equipos con fallas u otros de similar naturaleza.

- El Contratista deberá contar con equipos a modo de "spare" en los casos que el equipamiento instalado en la entidad no cuente con alta disponibilidad, para su reposición en caso de que se determine una falla que imposibilite su operación. El plazo final para devolver la operatividad con un equipo de reemplazo no deberá exceder las treinta y seis (36) horas de notificada la avería.
- Si uno de los equipos de la solución que se encuentra en alta disponibilidad presenta una avería que imposibilite su operación, el Contratista deberá considerar una reposición en un plazo máximo de 60 días calendario, en caso de que se presente una situación externa fuera del alcance del Contratista que imposibilite la entrega del equipo en el periodo indicado, esto se deberá justificar con un sustento del fabricante o del mayorista indicando el nuevo plazo de entrega, además, el contratista deberá en un plazo máximo de 4 horas, implementar un equipamiento temporal de igual o superior característica.
- De ser el caso, y durante la etapa de operación del servicio, el Contratista deberá remitir a la Oficina de Tecnologías de la Información una relación del personal técnico o profesional autorizado, para realizar labores de reparación de las appliance o componentes en calidad de alquiler, así como de sus conexiones, instalaciones y configuraciones. La relación del personal antes mencionado deberá ser actualizada cuando se produzcan cambios.
- De ser el caso; ante la posibilidad incrementada de ataques, tales como reuniones diplomáticas a nivel de países, amenazas anunciadas por organismos de hackeo internacional y otros, el Contratista deberá apoyar al Ministerio de Relaciones Exteriores con la presencia de un personal técnico especializado, quien deberá encontrarse en las instalaciones del Ministerio, con el único fin de monitorear efectivamente todos los equipos que constituyen la solución propuesta, para garantizar que se repelen efectivamente los ataques contra el Ministerio. Se precisa que en caso de requerirse al personal técnico especializado On-site para este tipo de situaciones, el tiempo estimado será de 96 horas como máximo dentro del plazo del servicio.

4.1.5. Supervisión

- El servicio estará bajo la supervisión de los coordinadores que designe la Oficina de Tecnologías de la Información, en su calidad de área usuaria y técnica.
- El Contratista mantendrá el control y supervisión permanente de todos los aspectos relacionados al servicio.
- La gestión del equipamiento de seguridad deberá ser compartida, para lo cual el personal del Ministerio de Relaciones Exteriores deberá contar con credenciales de visualización y administración. Los procedimientos para la gestión compartida deberán ser preparados por el Contratista para la aprobación y control de cambios por parte de los coordinadores de la Oficina de Tecnologías de la Información.
- Toda actividad o provisión de bienes que tenga que ejecutar el Contratista para subsanar una avería (interrupción parcial o total del servicio, así como un decremento en la calidad del mismo) serán sin costo alguno para la Entidad.

4.1.6. Calidad del Servicio

- El Contratista deberá contar con un Centro de Operaciones y Seguridad (SOC), donde se encuentren monitoreando las 24 horas del día, los 7 días a la semana y los 365 los días del año durante la vigencia del contrato, este Centro de Operaciones y Seguridad deberá estar dentro del territorio nacional, el cual deberá contar con alta disponibilidad; (el ganador de la buena pro deberá acreditar fehacientemente la pertenencia de este para disponibilidad del Ministerio de Relaciones Exteriores del Centro de Operaciones y Seguridad (SOC). Así mismo el Centro de Operaciones y Seguridad (SOC) deberá contar con un sistema de gestión ON LINE el cual mediante un Dashboard personalizable (el cual se podrá mostrar en un Pc, laptop, u teléfono inteligente) permitirá al Ministerio de Relaciones Exteriores hacer un seguimiento de los eventos, indicadores de gestión para cumplimiento del SLA, reportes de fallas, atención a nuevas solicitudes o tratamiento de reclamos, así como también la atención y solución de averías, y solicitudes derivadas del servicio sin necesidad de cursar comunicación al proveedor. El MRE deberá contar con acceso para al menos cuatro (4) usuarios al sistema de gestión ON LINE.

  Importante: El ganador de la buena pro deberá presentar una Declaración jurada de poseer un Centro de Operaciones y Seguridad (SOC) propio, para el perfeccionamiento del contrato.

- Asimismo, el contratista será responsable de la actualización oportuna de parches y de hacer las copias de respaldo de la configuración y políticas de los productos propuestos, para esto deberá demostrar que el Centro de Operaciones y Seguridad (SOC) cuenta con procedimientos que han logrado un nivel de madurez de nivel 3 de un total de 5, los cual deberá acreditar con documento emitido por una entidad auditora internacional.

  Importante: El ganador de la buena pro deberá presentar el certificado o constancia del nivel de madurez del Centro de Operaciones y Seguridad (SOC) para el perfeccionamiento del contrato.

- El Centro de Operación y Seguridad (SOC) deberá operar bajo las mejores prácticas y estándares en seguridad de la información y/o ciberseguridad, a su vez deberán poder operar bajo el concepto de resiliencia tecnológica, para esto el ganador de la buena pro deberá acreditar que el Centro de Operación y Seguridad (SOC) ha logrado obtener una certificación de estándares internacionales que cubra el alcance como "Centro de Operaciones de Seguridad (SOC o CYBERSOC)" en el territorio nacional.

- El Centro de Operación y Seguridad (SOC) deberá operar bajo las mejores prácticas y estándares en seguridad de la información y/o ciberseguridad, a su vez deberán poder operar bajo el concepto de resiliencia tecnológica, para esto el ganador de la buena pro deberá acreditar que el Centro de Operación y Seguridad (SOC) ha logrado obtener una certificación de estándares internacionales que cubra el alcance como "Centro de Operaciones de Seguridad (SOC o CYBERSOC)" en el territorio nacional. También se aceptará el documento emitido por entidad auditora internacional o que el SOC cuenta con certificación internacional ISO 27001.

  Importante: El ganador de la buena pro deberá presentar el certificado o constancia de ISO/IEC 27001:2013 del Centro de Operaciones y Seguridad (SOC) o en los servicios relacionados a Servicios de Seguridad para clientes, para el perfeccionamiento del contrato.

- El Centro de Operaciones y Seguridad (SOC) deberá tener la capacidad de escalamiento interno a otros niveles de servicio sin la necesidad de que el Ministerio de Relaciones Exteriores informe sobre la demora o falta de atención de un evento o incidente informado por cualquier canal de atención (atención telefónica, correo electrónico, etc.).

- El Contratista deberá ofrecer un centro de atención mediante vía telefónica, utilizando un número (0800 o similar), correo electrónico y un teléfono fijo para los escalamientos a nivel nacional, a fin de reportar cualquier incidencia que pueda presentarse durante la ejecución del servicio. El servicio del centro de atención debe estar alineado a ITIL v3 y deberá contar con personal especializado. La atención será las 24 horas del día, los 7 días a la semana y los 365 los días del año, y deberá incluir los siguientes servicios:

  - ✓ La atención de las incidencias de avería de manera remota y/o en sitio (Gestión de Incidentes).
  - ✓ La atención de los cambios en sitio y/o remoto (Gestión de Cambios).
  - ✓ La atención e identificación de incidentes repetitivos (Gestión de Problemas).
  - ✓ La atención de reportes bajo demanda de la Entidad.
- Ante una contingencia (interrupción parcial o total del servicio, así como a un decremento en la calidad del mismo) comunicada por la Entidad, el tiempo de respuesta por parte del Contratista deberá ser no mayor a treinta (30) minutos de lunes a viernes, las 24 horas del día y no mayor de cuarenta y cinco (45) minutos en los días no laborables, ello no exceptúa que el inicio de plazo para la solución de la contingencia o avería se establece a partir de la comunicación vía telefónica por parte de la Entidad.
- El tiempo máximo de subsanación de un evento o incidente, y que corresponde al tiempo transcurrido desde que el Ministerio de Relaciones Exteriores reporta la incidencia al Centro de Operaciones y Seguridad (SOC), que parte desde la asignación un ticket de atención a la Entidad, hasta la subsanación del evento a satisfacción del Ministerio de Relaciones Exteriores, será de cuatro (4) horas.
- El tiempo máximo de subsanación de un incidente que haya sido elevado al fabricante o marca mediante un ticket, será de la siguiente manera:

Escalas de impacto de tickets escalados al fabricante		
Tipo de Impacto	**Descripción**	**Plazo máximo respuesta**
Bajo	Afectación mínima a la confidencialidad integridad y disponibilidad de la información y servicios críticos, que permita operar a la entidad con normalidad, por ejemplo: • Desconfiguraciones en las soluciones de seguridad ofertadas que requieren mayor investigación. • Actualización de Parches de seguridad y cierre de brechas de seguridad en las soluciones ofertadas.	Diez (10) días
Medio	Afectación media a la confidencialidad integridad y disponibilidad de la información y servicios críticos, que permita trabajar de manera monitorizada y condicionada, por ejemplo: • Alerta sobre exceso de Umbrales de las soluciones de seguridad ofertadas. • Ataques masivos que generen muchas alertas y requieran mayor investigación por parte del Fabricante	Veinticuatro (24) horas
Alto	Afectación alta a la confidencialidad integridad y disponibilidad de la información y Servicios críticos, por ejemplo:	Cuatro (4) horas.

	• Pérdida total de las comunicaciones internas y externas. • Pérdida total de la operatividad de los controles de seguridad asociadas a las soluciones de seguridad ofertadas • Afectación total al acceso de la información y servicios de la institución, debido a una configuración errónea o mal dimensionamiento de las soluciones de seguridad ofertadas	

- El Contratista deberá designar un gestor de Mejora Continua del Servicio de Atención, para una mejor comunicación de requerimientos y atención de incidencias o averías.
- En caso del incumplimiento en los tiempos de respuesta para el registro de una avería o solicitud, así como el tiempo de subsanación de una avería, se aplicará la penalidad resultante señalado en el numeral 4.17. del presente Término de Referencia.

4.2. CAPACITACIÓN

El Contratista se compromete a realizar capacitaciones, según el siguiente detalle:

4.2.1. Capacitación de Entrenamiento:

El Contratista brindará una capacitación de entrenamiento que siga el currículo y estructura temática oficial en la solución propuesta en seguridad gestionada. El entrenamiento debe tener como mínimo ocho (8) horas por solución de seguridad propuesta, para un mínimo cuatro (4) personas, las mismas que designará la Oficina de Tecnologías de la Información, en su calidad de área usuaria y técnica.

El lugar a dictarse la capacitación y/o modalidad (presencial o virtual), las fechas y el horario de la capacitación será previa coordinación con la Oficina de Tecnologías de la Información.

4.2.2. Capacitación Oficial:

La Capacitación Oficial de la solución de seguridad debe ser en las siguientes dos (2) soluciones:

- ✓ **Solución Firewall de Aplicaciones Web (WAF)**
- ✓ **Solución de Endpoint Detection and Response (EDR)**
- ✓ **Solución Firewalls**

Ambas, propuesto por el Contratista.
La capacitación deberá ser impartida para un mínimo de dos (2) personas, las mismas que serán designadas por la Oficina de Tecnologías de la Información, en su calidad de área usuaria y técnica.

La capacitación oficial será dictada con el currículo oficial, en una institución reconocida, que cuente con los instructores certificados. El lugar a dictarse la capacitación y/o modalidad (presencial o virtual), las fechas y el horario de la capacitación será previa coordinación con la Oficina de Tecnologías de la Información.

Importante:

- ✓ ***La capacitación de Entrenamiento deberá ser impartida desde el día siguiente de suscrita el Acta de Implementación del Servicio hasta un plazo máximo de cuatro (4) meses posteriores de haberse firmado el acta de inicio del servicio.***
- ✓ ***La capacitación Oficial deberá ser impartida hasta un plazo máximo de doce (12) meses posteriores de haberse firmado el Acta de Inicio del Servicio.***
- ✓ ***El Contratista deberá entregar a cada participante, los manuales de la capacitación, en físico o en medios electrónicos, por cada una de las capacitaciones.***
- ✓ ***Finalizada cada una de las capacitaciones se suscribirá un Acta de Asistencia entre el Contratista y cada uno de los participantes, acreditando la capacitación impartida.***
- ✓ ***En caso de que las capacitaciones de entrenamiento, así como la capacitación oficial se dicten de manera virtual, deberán ser grabadas y dichas grabaciones serán compartidas digitalmente***
- ✓ ***Al término de todas las capacitaciones, el Contratista deberá entregar las constancias a cada uno de los participantes, vía mesa de partes del Ministerio de Relaciones Exteriores, en donde acredite la capacitación impartida.***

Mesa de partes del Ministerio de Relaciones Exteriores, se encuentra ubicada en el Jirón Lampa N.° 545, sótano 1, en el distrito de Cercado de Lima, y el horario de atención es de lunes a viernes de 8:30 am a 4:30 pm; o ser el caso las constancias serán remitidos en formato digital vía Mesa de Partes Digital de la entidad, mientras dure la emergencia sanitaria de nuestro país.

4.3. PLAN DE TRABAJO

El Contratista deberá presentar un Plan de Trabajo y el cronograma de actividades que se desarrollarán durante la ejecución del servicio de seguridad gestionada, el mismo que deberá contener lo siguiente:

- Diseño, la metodología y el cronograma detallado de las actividades que se realizarán para la implantación del servicio. El Contratista podrá realizar visitas técnicas in-situ antes de la presentación del diseño; las fechas y el horario para la visita in-situ será previa coordinación con la Oficina de Tecnologías de la Información.

- El Contratista deberá describir el detalle de las labores y procesos que empleará en la implementación, configuración, programación y puesta en marcha del servicio de seguridad gestionada. Así como también; el plan de trabajo deberá incluir la relación del personal técnico o profesional autorizado, la misma que de ser el caso deberá ser actualizada cuando se produzcan cambios y comunicada a la Entidad. Asimismo; el horario de labores en las instalaciones del Ministerio de Relaciones Exteriores será previa coordinación con la Oficina de Tecnologías de la Información.

- El Plan de Trabajo deberá ser remitido en un plazo máximo de diez (10) días calendario, contabilizados a partir del día siguiente de suscrita el **Acta de Implementación del Servicio**. El Plan de Trabajo será aprobado por la Oficina de Tecnologías de la Información en un plazo máximo de cinco (5) días calendario, que será contabilizado a partir del día siguiente de haber sido recepcionado el plan de trabajo vía mesa de partes.

Importante: Mesa de partes del Ministerio de Relaciones Exteriores, se encuentra ubicado en el Jirón Lampa N.° 545, Sótano 1, en el distrito de Cercado de Lima, y el horario de atención es de lunes a viernes de 8:30 am a 4:30 pm, o ser el caso el Plan de Trabajo será remitido en formato digital vía Mesa de Partes Digital de la entidad.
***(*) El ingreso a la Mesa de Partes Digital es a través de* www.gob.pe/rree**

4.4. INFORMES TÉCNICOS

4.4.1. Informes de Implementación del Servicio

- El contratista deberá remitir tres (3) informes técnicos de implementación del servicio, cada treinta (30) días calendario, a mesa de partes del Ministerio de Relaciones Exteriores, dirigido a la Oficina de Tecnologías de la Información. El cual será contabilizado a partir del día siguiente de suscrita el **Acta de Implementación del Servicio**.

- **El Primer y el Segundo Informe** deberán contener los avances respectivos de las actividades relacionadas a la implementación del servicio. Es importante mencionar que; el **Primer Informe** deberá contener el levantamiento de la información inicial, el cual contendrá la arquitectura inicial, el inventario actualizado, los backups y/o snapshot de las configuraciones realizadas de las soluciones de seguridad del Ministerio de Relaciones Exteriores, la cual deberá ser entregada en formato impreso y/o digital.

- El **Tercer Informe** deberá contener el detalle final de los trabajos de diseño, instalación, configuración, incluyendo el sistema de atención y escalamiento de comunicaciones, así como también la puesta en marcha del servicio de seguridad gestionada, con la descripción del funcionamiento y consideraciones para la operatividad de los componentes y equipamiento de seguridad que forma parte de la contratación.

- Los informes técnicos de la implementación del servicio deberán ser remitidos en un plazo máximo de cinco (5) días calendario, una vez concluido el plazo para cada informe técnico de implementación (treinta (30) días calendario).

4.4.2. Informe Mensual

- El Contratista deberá remitir un (1) informe mensual del servicio vía mesa de partes del Ministerio de Relaciones Exteriores, dirigido a la Oficina de Tecnologías de la Información.
- Los informes mensuales del servicio de seguridad gestionada, deberá incluir como mínimo lo siguiente:

  - ✓ Presentación del consolidado del mes de eventos, incidentes y requerimientos del servicio de seguridad gestionada.
  - ✓ Presentación de la disponibilidad del servicio de seguridad gestionada durante el mes.
  - ✓ Presentación de los Top o Ranking de los diez (10) mayores ataques satisfactorios e intentos de ataques, mostrar las fuentes de ataque (dependiendo de la solución), como, por ejemplo: IP, País, firma, tipos de malware, tipos de ataques a aplicaciones web, direcciones de correos electrónicos sospechosos.
  - ✓ Presentación de los Top o Ranking de los diez (10) mayores consumos de internet a nivel usuarios, top de aplicaciones visitadas, hits de reglas de firewall (mayor interacción o mayor tráfico), Top o Ranking de los correos electrónicos SPAM y correos electrónicos infectados con malware, Top o Ranking de correos electrónicos entrantes y salientes, Top o Ranking de acciones en los hosts (bloqueo, análisis, paso a cuarentena, etc.)
  - ✓ Presentación de incidentes y eventos, con la respectiva solución efectuada de todos los equipos que contempla el servicio de seguridad gestionada durante el mes.
  - ✓ Presentación en los informes mensuales sobre los respaldos realizados a las soluciones ofertadas.
  - ✓ Detalles de cambios en las configuraciones y políticas de los equipos efectuados en el mes.
  - ✓ Cualquier otro aspecto relacionado al servicio que sea solicitado por el Ministerio de Relaciones Exteriores.
  - ✓ Seguimiento y estado de las recomendaciones del informe del mes anterior.
  - ✓ Conclusiones y Recomendaciones.

- Previa coordinación con la Oficina de Tecnologías de la Información, se efectuará una reunión mensual de revisión del informe mensual, entre el Contratista y personal de la OTI.
- En caso de que el área usuaria solicite documentación adicional a los informes mensuales, el Contratista deberá remitir:

- ✓ Información estadística de rendimiento de la atención de las solicitudes de cambios, las incidencias de averías y de la capacidad, el cual deberá ser entregado a solicitud del área usuaria.
- ✓ Informe Anual completo del Servicio Integral.
- ✓ Cualquier otro aspecto relacionado al servicio que sea solicitado por el área usuaria.

- Los informes técnicos mensuales, deberán ser remitidos en un plazo máximo de diez (10) días calendario, una vez finalizado el mes.
- Reunión mensual de seguimiento al servicio.

4.4.3. Informe de Incidencias

En caso de que el área usuaria solicite de forma particular un informe de incidencia, este deberá contener lo siguiente:

- Reportes de incidencias, ataques y fallas de la solución. Estos reportes deberán ser a nivel técnico y también a nivel ejecutivo.
- Reporte de la gestión realizada por cada incidente que se produzca que incluya: las medidas de contención y respuesta implementadas y el estado de recuperación de los servicios o activos.
- Reporte de análisis forense del incidente significativo adverso que identifique las causas y las medidas para su gestión si este fuera necesario.
- Al momento de la solución de una incidencia o avería, el Contratista deberá presentar un reporte preliminar, en un plazo máximo de cuatro (4) horas de ocurrido el incidente. El reporte preliminar deberá especificar el motivo que causó la avería y la solución ejecutada. El reporte preliminar será enviado vía correo electrónico al responsable de las coordinaciones, y deberá ser incluido en el informe mensual del servicio. Posterior a ello, y de ser solicitado por el área usuaria, el Contratista deberá presentar un informe detallado de la avería vía mesa de partes, el cual no deberá exceder las noventa y seis (96) horas luego de remitida la solicitud.

***Importante**: Mesa de partes del Ministerio de Relaciones Exteriores, se encuentra ubicado en el Jirón Lampa N° 545, Sótano 1, en el distrito de Cercado de Lima, y el horario de atención es de lunes a viernes de 8:30 am a 4:30 pm. Asimismo; todos los Informes Técnicos deberán ser remitidos en versión de formato digital (CD/DVD), en formato impreso en físico y en formato digital (pdf) mediante correo electrónico de manera comprimida y con contraseña. O ser el caso los informes serán remitidos en formato digital vía Mesa de Partes Digital de la entidad. (*) El ingreso a la Mesa de Partes Digital es a través de* **www.gob.pe/rree.**

4.4.4. Reporte Semanal y Mensual de estado de salud de los equipos de las soluciones

- El Contratista deberá remitir un (1) reporte semanal (lunes) y un reporte mensual (día 10 de cada mes) vía mensaje de correo electrónico a una cuenta que proporcione la Oficina de Tecnologías de la Información.
- El reporte semanal y mensual debe ser del monitoreo SNMP de las soluciones ofertadas.

4.4.5. Informe de estado de copias de respaldo y logs de las soluciones

- El Contratista deberá contar con una copia de respaldo de la configuración de todos los equipos, así como de los logs en su infraestructura, con una antigüedad mínima de quince (15) días calendarios, a fin de utilizarlos en caso de contingencia, e informar mensualmente el estado de las copias de las dos quincenas anteriores, vía mensaje de correo electrónico a una cuenta que proporcione la Oficina de Tecnologías de la Información.

4.5. OBLIGACIONES DEL CONTRATISTA

El Contratista es el único responsable ante el Ministerio de Relaciones Exteriores de cumplir con la contratación, no pudiendo transferir esa responsabilidad a otras entidades ni terceros en general.

Solo se permitirá la subcontratación en actividades no esenciales como el mantenimiento preventivo y correctivo de los appliance o componentes que serán proporcionados por el Contratista en calidad de alquiler.

4.5.1. OBLIGACIONES DEL CONTRATISTA RESPECTO A LOS PROTOCOLOS DE SANIDAD

El CONTRATISTA y su PERSONAL deberán cumplir y observar lo establecido en todas las disposiciones legales vinculadas a eventos epidémicos y pandémicos emitidas por el Gobierno o la autoridad competente; durante la ejecución de las prestaciones a su cargo.

4.6. LUGAR DE EJECUCIÓN

La ejecución del servicio será en las instalaciones del Edificio Raúl Porras Barrenechea, perteneciente al Ministerio de Relaciones Exteriores, que se encuentra ubicado en el Jirón Ucayali N.° 337 – Sótano. Asimismo; los componentes que forman parte del servicio ofertado, que se encuentran en calidad de alquiler, serán recepcionados e instalados en la Unidad de Redes e Infraestructura de la Oficina de Tecnologías de la Información, que se encuentra ubicado en el Jirón Ucayali N.° 337 – Sótano, en el horario de las 09:00 horas hasta las 17:00 horas.

4.7. SISTEMA DE CONTRATACIÓN

La presente contratación se realizará por el sistema de contratación SUMA ALZADA.

4.8. PLAZO DE EJECUCIÓN

4.8.1. Implementación del Servicio

El plazo máximo para la implementación del servicio será de noventa (90) días calendario, contabilizados a partir del día siguiente de la firma del **Acta de Implementación del Servicio**, previa suscripción del Contrato. Dicha Acta será suscrita entre un (1) representante propuesto por el Contratista y un (1) representante de la Oficina de Tecnologías de la Información.

4.8.2. Ejecución del Servicio

El plazo de ejecución del servicio será por veinticuatro (24) meses, contabilizados a partir del día siguiente de finalizados los trabajos de la implementación del servicio, para lo cual se firmará el **Acta de Inicio del Servicio**, el mismo que será suscrito entre un (1) representante propuesto por el Contratista y un (1) representante de la Oficina de Tecnologías de la Información.

4.9. VIGENCIA

Desde el día siguiente de la suscripción del contrato y hasta que el funcionario responsable emita la conformidad final del servicio y se efectué el pago correspondiente.

4.10. RESPONSABLE DE LAS COORDINACIONES

El personal responsable para las coordinaciones respectivas será designado por la Oficina de Tecnologías de la Información, en su calidad de área usuaria y técnica.

Para tal efecto; la Oficina de Tecnologías de la Información nombrará un/las/los supervisores (res) quien(es) se encargará(n) de efectuar todas las coordinaciones necesarias para los accesos, así como también para liderar reuniones técnicas con el objetivo de implementar y ejecutar el servicio.

4.11. CONFORMIDAD DE LA PRESTACIÓN DEL SERVICIO

La conformidad de las prestaciones se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley N° 30225, Ley de Contrataciones del Estado. La conformidad será emitida por la Oficina de Tecnologías de la Información, previos informes técnicos de la Unidad de Redes e Infraestructura y del Oficial Técnico en Seguridad de la Información o el Experto en Seguridad Informática; en el plazo máximo de siete (7) días de producida la recepción.

Importante:

- ✓ ***Para la conformidad de la primera armada mensual, el Contratista deberá haber cumplido con remitir los Informes de Implementación del Servicio en los plazos establecidos en el numeral 4.4.1. Asimismo, en caso las capacitaciones se hayan impartido, el contratista debe haber remitido las constancias de la capacitación en los plazos establecidos en los numerales 4.2 de los Términos de Referencia.***

- ✓ ***Para el pago mensual de las veinticuatro (24) armadas, el Contratista deberá remitir el informe mensual respectivo, en los plazos establecidos en el numeral 4.4.2 de los Términos de Referencia.***

- ✓ ***En caso las capacitaciones requeridas aún no hayan sido impartidas, el Contratista deberá incluir una carta de compromiso indicando la fecha programada para dicha capacitación.***

4.12. FORMA DE PAGO

El pago de las prestaciones del servicio se regula por lo dispuesto en el artículo 171 del Reglamento de la Ley N° 30225, Ley de Contrataciones del Estado. La forma de pago se efectuará en veinticuatro (24) armadas mensuales iguales, previa presentación del comprobante de pago por parte del Contratista y conformidad emitida por la Oficina de Tecnologías de la Información, previos informes técnicos de la Unidad de Redes e Infraestructura y del Oficial Técnico en Seguridad de la Información o el Experto en Seguridad Informática

El pago se efectuará en moneda nacional, mediante el respectivo abono en la cuenta bancaria, dentro de los diez (10) días calendario de encontrarse completo el expediente de pago, sea a través del Banco de la Nación o de cualquier otra institución bancaria del Sistema Financiero Nacional, para cuyo efecto El Contratista comunicará su Código de Cuenta Interbancario (CCI).

4.13. CONFIDENCIALIDAD DE LA INFORMACIÓN

- El Contratista y su personal se obligan a mantener y guardar estricta reserva y absoluta confidencialidad sobre todos los documentos e informaciones del Ministerio de Relaciones Exteriores a los que tenga acceso durante y al término de la ejecución de presente contratación. En tal sentido, el Contratista y su personal deberán abstenerse de divulgar tales documentos e informaciones, sean en forma directa o indirecta, a personas naturales o jurídicas, salvo autorización expresa y por escrito del Ministerio de Relaciones Exteriores. Asimismo, el Contratista y su personal convienen en que toda la información en virtud de la presente contratación es confidencial y de propiedad del Ministerio de Relaciones Exteriores, no pudiendo el Contratista y su personal usar dicha información para uso propio o para dar cumplimiento a otras obligaciones ajenas establecidas en el presente requerimiento.

- El Contratista se compromete a cumplir con lo indicado en la Ley Nº 29733, Ley de Protección de Datos Personales. Los datos de carácter personal entregados por el Ministerio de Relaciones Exteriores al Contratista y su personal, y obtenidos por estos durante la ejecución del servicio, única y exclusivamente podrán ser aplicados o utilizados para el cumplimiento de los fines del documento contractual.

- El Contratista que tenga acceso a información durante la ejecución del servicio, deberá mantener y guardar estricta reserva y absoluta confidencialidad de la misma, bajo responsabilidad de las acciones legales pertinentes por parte de la Entidad. La utilización, divulgación o modificación no autorizada, así como la adulteración de la información, genera responsabilidad administrativa, sin perjuicio de las responsabilidades civiles y/o penales a que hubiera lugar. Asimismo; el Contratista y su personal se hacen responsables por la divulgación de información que se pueda producir, asumiendo el pago de indemnización por daños y perjuicios que la autoridad competente determine.

- El Contratista deberá adoptar las medidas de índole técnica y organizativa necesaria para que sus trabajadores, directores, accionistas, proveedores y/o cualquier persona que tenga relación con el Contratista no divulgue a ningún tercero los documentos e informaciones a los que tenga acceso, sin autorización expresa y por escrito del Ministerio de Relaciones Exteriores, garantizando la seguridad de los datos de carácter personal y evitar alteraciones.

- El Contratista deberá presentar una declaración jurada comprometiéndose a guardar la adecuada reserva de la contratación realizada.

  Importante: La declaración jurada deberá ser presentada como requisito para perfeccionar el contrato.

4.14. SEGURIDAD DE LA INFORMACIÓN

- Previo requerimiento, evaluación y conformidad el Ministerio de Relaciones Exteriores autorizará los accesos a los recursos y herramientas de la entidad que son requeridos por El Contratista y su personal para la prestación del servicio, finalizada dicha contratación, todos los accesos serán retirados.
- El Contratista y su personal deben tomar medidas de protección de la información del Ministerio de Relaciones Exteriores almacenadas en cualquier soporte y que requiera mantenimiento o atención fuera de las instalaciones del Ministerio de Relaciones Exteriores.
- El Contratista y su personal deben reportar oportunamente eventos, incidentes u otro riesgo potencial que afecte la Seguridad de la Información del Ministerio de Relaciones Exteriores con fines de realizar la investigación que corresponda.
- El Contratista y su personal se comprometen a brindar las facilidades necesarias para que el Ministerio de Relaciones Exteriores audite y/o monitoree los aspectos relacionados a la seguridad de la información que se correspondan con el objeto de la contratación del servicio.
- El Ministerio de Relaciones Exteriores, sus empleados y funcionarios en cualquier modalidad contractual, se exime de toda responsabilidad por las acciones legales, litigios, procedimientos administrativos, reclamaciones o demanda que pudiera derivarse de trasgresiones o supuestas trasgresiones que corresponda a cualquier patente, marca registrada, uso de modelo, diseño registrado, derechos de autor o cualquier otro derecho de propiedad intelectual que estuviese registrado o de alguna otra forma existente a la fecha del contrato, debido a la instalación del bien por parte de El Contratista o su personal o el uso de los mismos por parte del Ministerio de Relaciones Exteriores, siendo esto responsabilidad del Contratista.
- El Contratista y su personal garantizarán al Ministerio de Relaciones Exteriores que, durante la ejecución del servicio, respetará todos los derechos de propiedad intelectual referidos en el Decreto Legislativo N° 822 – Ley sobre el Derecho de Autor, sus modificatorias y complementarias, por lo que se compromete a garantizar que todo el software y las herramientas utilizadas no vulneran ninguna normativa, contrato, derecho, interés, patentes, legalidad o propiedad de terceros referidos en el dispositivo legal en mención.

4.15. RESPONSABILIDAD DEL CONTRATISTA

El Contratista es responsable por la calidad ofrecida y por los vicios ocultos de los servicios ofertados por un plazo de dos (02) años contado a partir de la conformidad otorgada, de acuerdo a lo dispuesto en el artículo 40 del TUO de la Ley N° 30225, Ley de Contrataciones del Estado, y el artículo 173 de su Reglamento.

4.16. PENALIDADES

En caso de retraso injustificado del Contratista en la ejecución del servicio objeto del Contrato, el Ministerio de Relaciones Exteriores aplicará penalidad por mora por cada día de retraso, de conformidad con lo dispuesto en el artículo 162 del Reglamento de la Ley N° 30225, Ley de Contrataciones del Estado.

4.17. DE LAS OTRAS PENALIDADES

Adicionalmente a la penalidad por mora se aplicará las siguientes penalidades de acuerdo con el artículo 163 del Reglamento de la Ley N° 30225, Ley de Contrataciones del Estado:

Otras penalidades			
N.º	**Supuestos de aplicación de penalidad**	**Forma de cálculo**	**Procedimiento**
1	El Contratista cambie al personal clave sin contar con la autorización previa de la Entidad.	2% de una (1) UIT por cada día de ausencia del personal clave.	Según informe del responsable de las coordinaciones designado por la Oficina de Tecnologías de la Información en su calidad de área usuaria.
2	El Contratista no cumpla con el tiempo fijado para la reposición de equipo ante falla, en caso de que no se tenga alta disponibilidad del mismo. Según numeral 4.1.4 de los Términos de Referencia.	20% de una (1) UIT (la penalidad se aplicará por ocurrencia).	
3	El Contratista no responda una solicitud de incidencia en los tiempos asignados, en el numeral 4.1.6 de los Términos de Referencia.	10% de una (1) UIT (la penalidad se aplicará por ocurrencia).	
4	El Contratista, no cumpla con los tiempos definidos en la tabla de Escalas de impacto de tickets escalados al fabricante	10% de una (1) UIT (la penalidad se aplicará por ocurrencia).	
5	El Contratista no cumpla con subsanar la atención al evento o incidente en los tiempos designados, en el numeral 4.1.6 de los Términos de Referencia.	10% de una (1) UIT (la penalidad se aplicará por ocurrencia).	
6	El contratista no remite el informe de implementación del servicio en el plazo establecido.	10% de una (1) UIT (la penalidad se aplicará por cada día de retraso).	
7	El contratista remita el informe fuera de tiempo o remita información errónea sobre algún evento o incidente que impacten en las operaciones críticas del MRE	10% de una (1) UIT (la penalidad se aplicará por ocurrencia).	
8	El contratista no informe sobre algún evento o incidente que impacten en las operaciones críticas del MRE	10% de una (1) UIT (la penalidad se aplicará por ocurrencia).	

Otras penalidades			
N.º	**Supuestos de aplicación de penalidad**	**Forma de cálculo**	**Procedimiento**
9	El contratista no cumple con remitir el informe mensual en el plazo establecido.	10% de una (1) UIT (la penalidad se aplicará por cada día de retraso).	
10	El contratista no cumple con remitir el Reporte Semanal y Mensual de estado de salud de los equipos de las soluciones.	10% de una (1) UIT (la penalidad se aplicará por cada día de retraso).	
11	El contratista no cumple con remitir el Informe de estado de copias de respaldo y logs de las soluciones.	10% de una (1) UIT (la penalidad se aplicará por cada día de retraso).	
12	El contratista no remite el informe de incidencias en el plazo establecido.	10% de una (1) UIT (la penalidad se aplicará por cada día de retraso).	
13	El contratista realiza modificaciones en las soluciones de seguridad sin aprobación del MRE	20% de una (1) UIT (la penalidad se aplicará por ocurrencia).	

UIT (Unidad impositiva tributaria)

5. CONSIDERACIONES ESPECÍFICAS

5.1. DEL PERSONAL CLAVE

El personal clave que se requiere para la implementación y ejecución del servicio son los siguientes:

5.1.1. Un (1) Jefe del Proyecto

La formación académica y experiencia del personal clave como Jefe de Proyecto, se encuentran detallados en los requisitos de calificación que forman parte integrante del requerimiento.

El Jefe de Proyecto deberá estar colegiado y habilitado, por lo cual, el Contratista deberá presentar la colegiatura y habilitación del Jefe del Proyecto para el inicio de su participación efectiva en el servicio. El mismo que deberá ser presentado para la firma del Acta de Implementación del Servicio.

Importante: La experiencia del Jefe de Proyecto, será contabilizada desde la obtención de la colegiatura.

Certificaciones:

El Jefe de Proyecto deberá contar con certificación de Project Management Professional (PMP) vigente e ITIL.

Importante: El ganador de la buena pro deberá presentar para la suscripción del contrato la certificación Project Management Professional (PMP) e ITIL en idioma español, o en su defecto acompañado de la traducción respectiva, emitido por traductor público juramentado o traductor colegiado certificado, según corresponda.

Actividades por Desarrollar: Encargado de liderar, planificar, dirigir y realizar un seguimiento integral de los trabajos y actividades relacionadas a la implementación del servicio. El Jefe del Proyecto deberá representar al Contratista durante las coordinaciones correspondientes en la etapa de implementación. Será el encargado de la elaboración de los informes de Implementación del Servicio.

5.1.2. Un (1) Líder del Servicio

La formación académica y experiencia del personal clave como Líder de Servicio, se encuentran detallados en los requisitos de calificación que forman parte integrante del requerimiento.

Certificaciones:

El Líder del Servicio deberá contar con certificación de ISO/IEC 27032 Lead Cybersecurity Manager vigente o Certificación Certified Information Systems Security Professional - CISSP vigente.

Importante: El ganador de la buena pro deberá presentar para la suscripción del contrato la certificación de Lead Cybersecurity Manager en idioma español, o en su defecto acompañado de la traducción respectiva, emitido por traductor público juramentado o traductor colegiado certificado, según corresponda.

Actividades por Desarrollar: Encargado de realizar la programación y el control del servicio, cumpliendo con los plazos y calidad, así como velar por el correcto cumplimiento de la planificación y ejecución de los trabajos diarios encomendados, supervisando y controlando el desempeño del personal, la calidad de los materiales y herramientas utilizados. El Líder del Servicio deberá representar al Contratista durante la ejecución del servicio y; será el encargado de la elaboración del Informe Mensual, Informe de Incidencias, Reporte Semanal y Mensual de estado de salud de los equipos de las soluciones y del Informe de estado de copias de respaldo y logs de las soluciones.

5.1.3. Un (1) Especialista en Seguridad Gestionada (Técnico On-site)

La formación académica, experiencia y capacitación del personal clave como Especialista en Seguridad Gestionada (Técnico On-site), se encuentran detallados en los requisitos de calificación que forman parte integrante del requerimiento.

Certificaciones:

El personal requerido como Especialista en Seguridad Gestionada (Técnico On-Site) deberá contar con tres (3) certificaciones vigentes como mínimo de las soluciones de seguridad ofertadas, las mismas que formaran parte de lo ofertado por el Contratista.

Importante: El ganador de la buena pro deberá presentar para la suscripción del contrato copia de las certificaciones vigentes en idioma español, o en su defecto acompañado de la traducción respectiva, emitido por traductor público juramentado o traductor colegiado certificado, según corresponda.

Actividades por Desarrollar: Participar desde el diseño del servicio. Responsable técnico de la implementación del servicio en representación del Contratista. Asimismo, tomará nota de los requerimientos técnicos que se encuentren vinculados a la solución de seguridad (Hardware, Software y funcionalidades) y que sean planteados por parte del personal técnico designado por la Oficina de Tecnologías de la Información; evaluando su viabilidad técnica, definiendo los parámetros y alcances de las configuraciones requeridas que proporcionen la funcionalidad deseada. Durante la implementación e instalación de los servicios, será el responsable de los avances, así como de realizar las pruebas pertinentes para asegurar la alta disponibilidad y tolerancia a fallos.

Importante:

- ***En caso de ausencia del personal clave por vacaciones, descanso médico o fuerza mayor, que imposibilite la continuidad de sus labores o a solicitud del Ministerio de Relaciones Exteriores, el contratista deberá garantizar que el personal reemplazante tenga el mismo o mayor nivel de estudios, preparación, conocimientos requeridos. La designación del nuevo personal***

técnico estará sujeta a la previa aceptación por parte de la Oficina de Tecnologías de la Información del Ministerio.

- ***De requerir el contratista de personal adicional al requerido como Personal Clave, podrá contemplar personal complementario sin que esto signifique costos adicionales al Ministerio de Relaciones Exteriores.***

- ***El personal clave y complementario, deberá contar con Seguro Complementario de Trabajo de Riesgo, el mismo que deberá ser presentado para la prestación efectiva del servicio.***

6. **RESOLUCIÓN DEL CONTRATO** ***(artículo 8 de la Ley N° 31564, Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio Público).***

Son causales de resolución del contrato la presentación con información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público. Asimismo, en caso se incumpla con los impedimentos señalados en el artículo 5 de dicha ley se aplicará la inhabilitación por cinco años para contratar o prestar servicios al Estado, bajo cualquier modalidad.

Nota: se deberá presentar una declaración jurada de prohibiciones e incompatibilidades como requisito para perfeccionar el contrato.

II. REQUISITOS DE CALIFICACIÓN

B	**CAPACIDAD TÉCNICA Y PROFESIONAL**
B.3	**CALIFICACIONES DEL PERSONAL CLAVE**
B.3.1	**FORMACIÓN ACADÉMICA**
	Requisitos: **Un (1) Jefe del Proyecto** Título Profesional en Ingeniería Electrónica o Ingeniería de Sistemas o en Tecnologías de la Información o en Ingeniería de Cómputo y Sistemas o Ingeniería Informática o Ingeniería de Sistemas de Información o Ingeniería de Software o Ingeniería de TI y Sistemas o Ingeniería de Sistemas e Informática o ingeniería de las Telecomunicaciones e Ingeniería Electrónica, del personal clave requerido como Jefe de Proyecto. **Un (1) Líder de Servicio** Título Profesional o Grado de Bachiller en Ingeniería Electrónica o Ingeniería de Sistemas o en Tecnologías de la Información o en Ingeniería de Cómputo y Sistemas o Ingeniería Informática o Ingeniería de Sistemas de Información o Ingeniería de Software o Ingeniería de TI y Sistemas, del personal clave requerido como Líder de Servicio. **Un (1) Especialista en Seguridad Gestionada (Técnico On-site)** Grado de Bachiller en Ingeniería Electrónica o en Telecomunicaciones o en Redes y Comunicaciones o Sistemas o en Tecnologías de la Información o en Cómputo y Sistemas o Informática o de Sistemas de Información o en TI y Sistemas o Ingeniería de Seguridad o Redes y Seguridad Informática, del personal clave requerido como Especialista en Seguridad Gestionada (Técnico On-site). Acreditación: El grado de bachiller y títulos profesionales serán verificados por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: *https://enlinea.sunedu.gob.pe/* o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: *https://titulosinstitutos.minedu.gob.pe/*, según corresponda. En caso de que el grado de bachiller o títulos profesionales no se encuentren inscritos en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.
B.3.2	**CAPACITACIÓN**
	Requisitos: **Un (1) Especialista en Seguridad Gestionada (Técnico On-site)** Cuarenta (40) horas lectivas en Seguridad Informática o Seguridad de la Información o Ciberseguridad o Seguridad de Redes, del personal clave requerido como Especialista en Seguridad Gestionada (Técnico On-site). Acreditación: Se acreditará con copia simple de constancias, certificados u otros documentos, según corresponda.

Importante

Se podrá acreditar la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas lectivas, según la normativa de la materia.

B.4 EXPERIENCIA DEL PERSONAL CLAVE

Requisitos:

Un (1) Jefe del Proyecto

Deberá contar con experiencia mínima de cuatro (4) años en Gestión de Proyectos de TI y/o Seguridad Perimetral, como Jefe o Gestor o Coordinador o Encargado del personal requerido como Jefe del Proyecto.

Un (1) Líder de Servicio

Deberá contar con experiencia mínima de cuatro (4) años en proyectos de plataformas de Seguridad, CyberSOC o Ciberseguridad, como Jefe o Líder o Coordinador del personal requerido como Líder del Servicio.

Un (1) Especialista en Seguridad Gestionada (Técnico On-site)

Deberá contar con experiencia mínima de cuatro (4) años en servicios especializados en configuración y administración de Seguridad Informática o ciberseguridad o seguridad en redes como Especialista o Analista Técnico o Ingeniero en Seguridad o ciberseguridad, del personal requerido como Especialista en Seguridad Gestionada (Técnico On-site).

De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.

Acreditación:

La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

Importante

- *Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.*
- *En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.*
- *Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.*
- *Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.*

C	**EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD**
	Requisitos: El proveedor debe acreditar un monto facturado acumulado equivalente a S/ 5'000,000.00 (Cinco Millones con 00/100 Soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. Se consideran servicios similares a los siguientes: • Servicio de Licencias y/o • Servicio de CYBERSOC y/o • Servicio de Administración y Monitoreo de Plataformas de Seguridad y Correlación Inteligente de Eventos de Seguridad y/o soluciones de ciberseguridad y/o • Servicio de soporte de mantenimiento, monitoreo y administración de plataformas de seguridad TI y/o • Servicio de monitoreo de eventos de seguridad (SOC) y/o • Servicio de CyberSOC y/o • Servicio de Red Team y/o • Servicio de monitoreo de equipamiento de seguridad y/o • Servicio de seguridad Gestionada y/o • Solución Integral Tecnológica de Ciberseguridad -SIEM y/o • Servicio de soporte de plataforma de seguridad y correlación y/o • Servicio de gestión, monitoreo, soporte y mantenimiento de seguridad perimetral y/o • Servicio de soporte, gestión, mantenimiento y monitoreo de las plataformas de seguridad de la información – Cybersoc y/o • Servicio de Cyber Defense Center y/o • Servicio gestionado de seguridad – SOC. • Servicio y/o Solución monitoreo de eventos de SIEM y/o • Servicio de centro de datos y comunicaciones Acreditación: La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago[1], correspondientes a un máximo de veinte (20) contrataciones. En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo

[1] Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

"... el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado"
(...)
"Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término "cancelado" o "pagado"] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia".

se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el **Anexo Nº 8** referido a la Experiencia del Postor en la Especialidad.

En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.

En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.

Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.

Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 9.**

Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicios o de cancelación del comprobante de pago, según corresponda.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo Nº 8** referido a la Experiencia del Postor en la Especialidad.

Importante

- *Al calificar la experiencia del postor, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del objeto contractual no coincida literalmente con el previsto en las bases, se deberá validar la experiencia si las actividades que ejecutó el postor corresponden a la experiencia requerida.*

- *En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que se hayan comprometido, según la promesa de consorcio, a ejecutar el objeto materia de la convocatoria, conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".*

ESTRUCTURA DE COSTOS

DESCRIPCIÓN	CANTIDAD	UNIDAD DE MEDIDA	PRECIO S/
SEGURIDAD GESTIONADA			
a) Solución Firewall de Aplicaciones Web	2	Servicio	
b) Solución Anti-DDoS	1	Servicio	
c) Seguridad Perimetral	5	Servicio	
d) Seguridad Sandbox	1	Servicio	
e) Filtro de Correos Electrónicos.	1	Servicio	
f) Solución de Detección y Respuesta Endpoint (EDR)	1	Servicio	
g) Sistema de Detección de Amenazas con Inteligencia Artificial	1	Servicio	
h) Gestión de Accesos Privilegiados	1	Servicio	
i) Servicio del Sistema de Analítica, Eventos de Seguridad Informática y correlación (SIEM)	1	Servicio	
j) Servicio de Respuesta ante Incidentes.	1	Servicio	
k) Servicios Programados.	1	Servicio	
l) Diseño, Instalación, Configuración, Soporte 24x7, administración remota y monitoreo por 2 años.	1	Servicio	
ll) Capacitación.	1	Servicio	
MONTO TOTAL DEL SERVICIO X 24 MESES (INC. IMPUESTOS DE LEY E IGV 18%)			

Nota: El ganador de la buena pro deberá presentar la estructura de costos como requisito para la suscripción del Contrato.