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, de acuerdo con el siguiente detalle:

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

4. CONSIDERACIONES GENERALES

4.1. CARACTERÍSTICAS DEL SERVICIO

4.1.1. Seguridad Gestionada

La administración de los equipos de seguridad en su totalidad será administrada por el proveedor 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 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 (tráfico que se efectúa por el servicio de correo electrónico corporativo).
- Protección a nivel de endpoint centralizado (tráfico efectuado a través de los equipos de cómputo).
- Sistema de Gestión de Eventos de Seguridad.
- Analizar el tráfico de las redes privadas virtuales (VPN) con las misiones.
- Permitir la verificación del tráfico protocolo para cifrar navegación de páginas web (https)
- 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.

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. Los componentes serán instalados en el centro de datos, ubicado en el Edificio Raúl Porras Barrenechea, ubicado en el Jirón Ucayali N.º 337, Cercado de Lima y ser de tecnología vigente. 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 2TB.
  ✓ 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 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 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 acelera ración 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.
- La solución debe ser capaz de realizar parches virtuales, mediante la integración de escáneres de terceros, para mitigar vulnerabilidades criticas 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, 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.º 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 500Mbps de throughput con crecimiento mínimo a 40Gbps 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.

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.
- 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.
- 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.
- 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.
- Mitigación de ataques basados en aplicación / Web Servers – HTTP: incorporar firmas, expresión regular de carga útil.
- Protección contra hacktivistas y anti-suplantación.
- Mitigación de ataques basados en aplicación / Servidores SIP: SIP malformado, requerimiento de límite de velocidad SIP.
- 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.
- 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 mitigación de ataques en la capa 7 en contra de grandes volúmenes de tráfico (inundación), validando solicitudes SIP.
- 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.

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, 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.

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. 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 2020, asimismo debe ser considerado líder en el reporte (indicador) de Gartner para Network Firewalls del 2021.

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

- NGFW Throughput (Firewall con control de aplicaciones más IPS activos), 7 Gbps como mínimo, medido en condiciones reales o con tráfico mixto.

- Capacidad mínima de sesiones concurrentes de 5 millones.
- Throughput de prevención de amenazas (Control de aplicaciones, IPS, antivirus y antimalware) activos a la vez con todas las firmas que el fabricante posee por defecto, 6 Gbps como mínimo, con tráfico medido en condiciones reales o con tráfico mixto.
- Inspección SSL throughput de 5 Gbps
- Capacidad mínima de nuevas sesiones o conexiones por segundo de 300,000
- 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 deberá 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 soportar los siguientes niveles de inspección: de control de estado SPI (Stateful packet inspection), control de aplicación AIC (Application Inspection and Control) y de IPS.
- 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 URLs de manera periódica desde un servicio web local o en la nube a través de HTTP.
- 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.
- 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.
- 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.

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 1.5 Gbps.
- Los componentes deberán contar con un IPsec VPN throughput mínima de 15 Gbps.
- Los componentes deberán soportar 1900 túneles VPN IPsec Gateway to Gateway.
- Los componentes deberán soportar 10000 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, DES, 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 (Firewall con control de aplicaciones más IPS activos), 9 Gbps como mínimo, medido en condiciones reales o con tráfico mixto.
- Throughput de prevención de amenazas (Control de aplicaciones, IPS, antivirus y antimalware) activos a la vez con todas las firmas que el fabricante posee por defecto, 7 Gbps como mínimo, con tráfico medido en condiciones reales o con tráfico mixto.
- Capacidad mínima de nuevas sesiones o conexiones por segundo de 400,000.
- 04 interfaces de red 10G SFP+, incluir sus módulos correspondientes de fibra óptica multimodo.
- 02 interfaces de red 40G QSFP+, incluir sus módulos correspondientes de fibra óptica multimodo.
- 08 interfaces de red 1G SFP y 12 interfaces RJ45 como mínimo.
- Capacidad mínima de sesiones concurrentes de 8 millones.
- Inspección SSL throughput de 7 Gbps
- 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.
- 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, Netflix, UltraSurf, Gsuit, etc.
- 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, zona horaria.
- 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 URLs de manera periódica desde un servicio web local o en la nube a través de HTTP.
- La solución debe contar con la funcionalidad de antivirus.

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.
- 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.
- 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 debe contar con al menos las siguientes categorías de reglas: 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.
- 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 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 contar con una solución centralizada e independiente para la administración de logs y Reportería, 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 4TB.
- Poseer estadísticas en interfaz gráfica de todo el tráfico que pasa por el equipamiento de seguridad
- 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
- 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, 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. En ese sentido, el Contratista deberá proveer un (01) Appliance o Equipamiento que permita el óptimo desarrollo de la solución Sandbox. El componente será instalado en el Edificio Raúl Porras Barrenechea, ubicado en el Jirón Ucayali N.º 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 con la Solución de Detección y Respuesta Endpoint (EDR).

Características básicas

- La solución debe analizar por lo menos 1200 archivos por hora para tráfico web y de correos.
- Debe contar como mínimo con un throughput de 1 Gbps.
- Debe tener un disco duro mínimo de 2 TB.
- La extracción del archivo debe escanearse utilizando el laboratorio de virus interno, sin enviar la muestra fuera de la red.
- Los datos forenses deben almacenarse en el local dentro de la plataforma.
- 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 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, iso, htm, html, upx, rar, cmd, 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, extensión de archivo, archivo MD5 / SHA1 o IOC provisto.
- La solución debe defenderse 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, sin depender de 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. 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, 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.
  - ✓ 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.
- 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, 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 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 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.
- Debe permitir la exportación de reportes relacionados con malware.
- Debe tener la capacidad de crear reportes: reportes ejecutivos diarios, semanales y mensuales para la administración.
- La solución debe ser capaz de integrarse con SIEM para la administración de logs.
- La solución debe poder enviar notificaciones por correo electrónico.
- 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.)
- La solución debe permitir la sincronización del tiempo con un servidor NTP local.
- La solución debe permitir la creación de cuentas con diferentes roles utilizados para administrar la solución, solo monitorear las alertas o revisar los cambios.
- 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.º 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, incluyendo la actualización gratuita, 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 1500 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.º 337, Cercado de Lima.

Características de la Solución:

- La solución propuesta debe ser compatible con los siguientes sistemas operativos: Windows (32-bit & 64-bit versiones) XP SP2/SP3, 7, 8, 8.1 y 10.
- La solución propuesta debe ser compatible con los siguientes sistemas operativos: Windows Server 2003 R2 SP2, 2008 R1 SP2, 2008 R2, 2012, 2012 R2, 2016 y 2019
- La solución propuesta debe ser compatible con los siguientes sistemas operativos: macOS Versiones: Yosemite (10.10), El Capitan (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14) y Catalina (10.15).
- 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 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 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, aplicaciones y 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.
- La solución propuesta debe tener la capacidad para eliminar un archivo basado en la clasificación 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.
- 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.

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 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.
- 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.
- 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 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.
- 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 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) Servicio del Sistema de Gestión de Información y Eventos de Seguridad Informática (SIEM)

El servicio de monitoreo y correlación de eventos deberá ser provisto como parte del servicio del Centro de Operaciones y Seguridad (SOC); a través, de una plataforma modular (stack) 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 (el contratista debe brindar servidores físicos conforme a lo requerido), garantizando la confidencialidad, integridad y disponibilidad que es gestionada por este servicio. A su vez, para el encriptado, decodificación y almacenamiento de los logs, el Contratista deberá proveer una (1) solución en físico o virtual de SIEM 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.

El SIEM 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.

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.

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.

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) para el SIEM.

En la etapa de implementación y/o migración del SIEM, 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.

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.
- 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.
- Dashboards configurables en tiempo real, con desplazamiento "Slide-Show" para mostrar KPIs.
- Disponibilidad de un conjunto de respuestas pre-configuradas 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 base de endpoint/servidor/usuario - granularidad de la hora/día de la semana/fin de semana.
- 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 (opcional)
- Deberá contar con un módulo de alertas. Se debe poder definir alertas basadas en umbrales, en correlación de eventos, o en anomalías detectadas por machine learning.
- La solución SIEM deberá contar con reportes de estándares y plantillas modificables por el usuario de categorías.
- Deberá mostrar los reportes en pantalla antes de solicitar cualquier exportación a formatos externos.
- Deberá contar con informes predefinidos listos para ser utilizados, que soporten una amplia gama de necesidades de auditoría y cumplimiento normativo, incluyendo: PCI-DSS, HIPAA, SOX, ISO, GLBA y SANS Critical Controls.
- 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 deberá estar cifrada y comprimida.

h) 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.
- En caso el Contratista disponga formalmente y oficialmente con un 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 punto será considerado como opcional.
- 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 80 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.
  - 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:

    - Pérdida o hurto 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.

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

- El servicio deberá estar compuesto por las siguientes etapas:

  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 gestión remota.

<u>Importante</u>: En caso de que el postor sea miembro del FIRST deberá presentar la documentación correspondiente que evidencie lo indicado.

4.1.2. <u>Consideraciones Adicionales del Servicio</u>

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 original (*).

***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.º 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.

<u>Nota</u>:

- ***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 proveedor 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. <u>Operación del Servicio</u>

- 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 dos (2) días a la semana previamente coordinado con la OTI del MRE, desde las 08:30 hasta las 17:30 horas; el resto de los días laborables debe brindar el soporte virtual en el mismo horario de oficina.

- 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. <u>Supervisión</u>

- El servicio estará bajo la supervisión de 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 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) 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 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. <u>Capacitación de Entrenamiento:</u>

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 una duración de ocho (8) horas por cada solución de seguridad propuesta, para como mínimo cuatro (4) personas, las mismas que serán designadas por 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. <u>Capacitación Oficial:</u>

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

- ✓ **Solución Firewall de Aplicaciones Web (WAF)**
- ✓ **Servicio del Sistema de Gestión de Información y Eventos de Seguridad Informática (SIEM)**

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 en 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.***
- ✓ ***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.º 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 de 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, 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 en mesa de partes.

Importante: Mesa de partes del Ministerio de Relaciones Exteriores, se encuentra ubicado en el Jirón Lampa N.º 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 de ser el caso el Plan de Trabajo será remitido en formato digital vía Mesa de Partes Digital de la entidad, mientras dure la emergencia sanitaria de nuestro país.

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 de ser el caso los informes serán remitidos en formato digital vía Mesa de Partes Digital de la entidad, mientras dure la emergencia sanitaria de nuestro país.**

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 será proveídos por el Contratista en calidad de alquiler.

4.5.1. OBLIGACIONES DEL CONTRATISTA RESPECTO A LOS PROTOCOLOS DE SANIDAD EN EL MARCO DEL COVID-19

PROTOCOLO DE SANIDAD

El CONTRATISTA se compromete a cumplir lo establecido en todas las disposiciones legales **vigentes**, vinculadas a eventos epidémicos y pandémicos durante la ejecución de las prestaciones a su cargo.

EL CONTRATISTA debe entregar a **LA ENTIDAD**, un protocolo sanitario que debe cumplir el personal a su cargo en las diversas actividades que desarrollaran en la institución durante la vigencia del contrato, el cumplimiento de este **será supervisado durante la ejecución del requerimiento y/o entrega de bienes a la institución.**

CONSIDERACIÓN IMPORTANTE:

En la etapa de **PERFECCIÓNAMIENTO DE CONTRATO** el ganador de la Buena Pro presentará su protocolo sanitario vigente en contra de la propagación del COVID-19, que guarde relación con el objeto de contratación.

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.º 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.º 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 supervisor (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

La conformidad de las prestaciones se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones, aprobado por el Decreto Supremo N.º 344-2018-EF (La referida norma incluye su respectiva modificación de ser el caso). 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 de Contrataciones del Estado aprobado por el Decreto Supremo N.º 344-2018-EF (La referida norma incluye su respectiva modificación de ser el caso). 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 N.º 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.

  <u>Importante</u>: 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

La conformidad por parte de La Entidad no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto en el numeral 40.2 del Artículo 40 del TUO de la Ley N° 30225, Ley de Contrataciones del Estado aprobado mediante Decreto Supremo N° 082-2019-EF y en el numeral 173 de su Reglamento.

El plazo máximo de responsabilidad del Contratista es de dos (2) años contado a partir de la conformidad emitida por la Entidad.

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 de Contrataciones del Estado, aprobado por el Decreto Supremo N.º 344-2018-EF. (La referida norma incluye su respectiva modificación de ser el caso).

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 de Contrataciones del Estado, aprobado por el Decreto Supremo N.º 344-2018-EF (Las referidas normas incluyen sus respectivas modificatorias, de ser el caso)

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 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 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).	
5	El contratista no remite el informe de implementación del servicio en el plazo establecido.	10% de una (1) UIT (la penalidad se aplicará por ocurrencia).	
6	El contratista no cumple con remitir el informe mensual en el plazo establecido.	10% de una (1) UIT (la penalidad se aplicará por ocurrencia).	
7	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 ocurrencia).	

Otras penalidades			
N.º	**Supuestos de aplicación de penalidad**	**Forma de cálculo**	**Procedimiento**
8	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 ocurrencia).	
9	El contratista no remite el informe de incidencias en el plazo establecido.	10% de una (1) UIT (la penalidad se aplicará por ocurrencia).	
10	El contratista realiza modificaciones en las soluciones de seguridad sin aprobación del MRE	20% de una (1) UIT (la penalidad se aplicará por ocurrencia).	

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.

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 a 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.

<u>Importante</u>: 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 a 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.

<u>Certificaciones:</u>

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.

<u>Importante</u>: 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 a 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.

- ***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.***

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

Un (1) Profesional titulado 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 Jefe de Proyecto.

Un (1) Líder de Servicio

Un (1) Profesional titulado 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)

Un (1) 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 título profesional o grado de bachiller requerido será verificado 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: http://www.titulosinstitutos.pe/, según corresponda.

En caso el título profesional o grado de bachiller requerido no se encuentre inscrito 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 y 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, 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: servicios de implementación y soporte en soluciones de seguridad informática, perimetral, NGFW, firewall de aplicaciones web (WAF), Antiddos, Seguridad de usuarios finales (EDR), Seguridad de acceso a la red (NAC), Seguridad de correo electrónico (Antispam) e IDS/IPS, Servicio de Licencias o Servicio de CYBERSOC o Administración y Monitoreo de Plataformas de Seguridad y Correlación Inteligente de Eventos de Seguridad, Servicio de soporte de mantenimiento, monitoreo y administración de plataformas de seguridad TI, Servicio de monitoreo de eventos de seguridad (SOC), Servicio de CyberSOC, Servicio de Red Team, Servicio de monitoreo de equipamiento de seguridad, Servicio de seguridad Gestionada, Solución Integral Tecnológica de Ciberseguridad -SIEM, Servicio de soporte de plataforma de seguridad y correlación 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 se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el **Anexo N.º 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.**

[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".

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 N.º 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	GLOBAL	
b) Solución Anti-DDoS	1	GLOBAL	
c) Seguridad Perimetral	5	GLOBAL	
d) Seguridad Sandbox	1	GLOBAL	
e) Filtro de correos electrónicos.	1	GLOBAL	
f) Solución de Detección y Respuesta Endpoint.	1	GLOBAL	
g) Servicio del Sistema de Gestión de Información y Eventos de Seguridad Informática.	1	GLOBAL	
h) Servicio de Respuesta ante Incidentes	1	GLOBAL	
Diseño, Instalación, Configuración, Soporte 24x7, administración remota y monitoreo por 2 años.	1	GLOBAL	
Capacitación	1	GLOBAL	
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.