PERÚ | Ministerio de Relaciones Exteriores

MRE

TÉRMINOS DE REFERENCIA PARA CONTRATOS MENORES PARA SERVICIOS EN GENERAL

FECHA: Lima, 19 de mayo de 2026	
Unidad de Organización	Oficina de Arquitectura y Seguridad Digital
Código Tarea / Actividad Operativa	AOI00004501974: Gestión de la Seguridad Digital
Meta Presupuestaria	379
Objeto de la contratación	Contratación del servicio de suscripción de licencias de software de detección y respuesta extendida para los servidores virtuales del Ministerio de Relaciones Exteriores

I. MARCO LEGAL

El marco legal comprende la Ley N° 32069, Ley General de Contrataciones Públicas, en adelante la Ley, y su Reglamento, aprobado por Decreto Supremo N° 009-2025-EF y modificatorias, en adelante el Reglamento, las directivas que emita la Dirección General de Abastecimiento del Ministerio de Economía y Finanzas, así como el OECE y demás normativa especial que resulte aplicable.

II. INCLUSIÓN EN EL CMN

- Solicitud de Modificación del CMN N° 016
- Aprobación de Modificaciones al CMN N° 0001

III. FINALIDAD PÚBLICA DE LA CONTRATACIÓN

Garantizar la protección de la información almacenada en los servidores del Ministerio de Relaciones Exteriores frente a amenazas externas, como malware o virus, mediante el uso de soluciones **de detección y respuesta extendida (XDR)**, las cuales permiten una visibilidad completa y respuesta automática ante posibles amenazas de malware y/o virus en los sistemas de información gestionados desde el Centro de Datos de la institución.

IV. OBJETIVO DE LA CONTRATACIÓN

Objetivo General:

- El objetivo de contratar una solución de detección y respuesta extendida (XDR) para la protección de los servidores del Ministerio de Relaciones Exteriores es fortalecer de manera significativa la capacidad de detección, contención y recuperación ante amenazas cibernéticas avanzadas, especialmente aquellas asociadas a ransomware y ataques destructivos.
- Además de mejorar la visibilidad y el análisis de comportamientos sospechosos en tiempo real, la solución deberá incorporar capacidades avanzadas de remediación automática, incluyendo la reversión o restauración de cambios maliciosos realizados por software dañino en los sistemas comprometidos.

Objetivos específicos:

Esta funcionalidad permite que, ante la detección de un ataque que cifre archivos, modifique configuraciones o altere procesos críticos, el sistema pueda:

- Detener automáticamente la amenaza en ejecución.
- Aislar el servidor afectado para evitar propagación lateral.
- Revertir los cambios maliciosos realizados durante el incidente.
- Restaurar archivos y configuraciones a su estado previo al ataque.
- Con ello, no solo se mejora la capacidad de respuesta inmediata, sino que se reduce significativamente el impacto operativo y el tiempo de recuperación ante incidentes, evitando

REPÚBLICA DEL PERÚ · Oficina de Arquitectura y Seguridad Digital · Ministerio de Relaciones Exteriores · Y.E.G.G.

REPÚBLICA DEL PERÚ · Oficina de Seguridad y Confianza Digital · R.B.B.

REPÚBLICA DEL PERÚ · Oficina de Arquitectura y Seguridad Digital · Ministerio de Relaciones Exteriores · T.C.S.C.

REPÚBLICA DEL PERÚ · Oficina de Arquitectura y Seguridad Digital · Ministerio de Relaciones Exteriores · E.M.M.V.

interrupciones prolongadas en los servicios institucionales.

- La incorporación de esta capacidad de restauración fortalece la resiliencia tecnológica del Ministerio, asegurando la continuidad de las operaciones críticas y la protección de información sensible, incluyendo datos diplomáticos y estratégicos, frente a amenazas que buscan generar indisponibilidad o daño permanente.
- En consecuencia, la solución no solo debe detectar y alertar, sino también contar con mecanismos automáticos de contención y recuperación que permitan restablecer el entorno afectado de forma rápida, segura y verificable.

V. JUSTIFICACIÓN DE LA NECESIDAD DE LA CONTRATACIÓN

La contratación de una solución XDR para los servidores de la Cancillería es una medida estratégica indispensable para proteger información diplomática y datos personales de ciudadanos frente a amenazas avanzadas como ransomware, explotación de vulnerabilidades y robo de credenciales. Un incidente exitoso no solo podría comprometer información sensible, sino también interrumpir servicios esenciales al ciudadano y generar un impacto reputacional significativo a nivel nacional e internacional. Implementar capacidades avanzadas de detección, contención y recuperación automática permite reducir el riesgo de brechas de seguridad, minimizar tiempos de interrupción y fortalecer la resiliencia institucional, garantizando continuidad operativa y protección efectiva del interés público.

VI. DESCRIPCIÓN GENERAL DEL REQUERIMIENTO

6.1. DESCRIPCIÓN GENERAL

Consta del soporte, mantenimiento y licenciamiento de una solución de detección y respuesta extendida (XDR) implementada en doscientas (200) servidores del Ministerio de Relaciones Exteriores, entre plataformas Linux y Windows Server, que conforman la infraestructura crítica del Centro de Datos, con el objetivo de garantizar protección avanzada contra amenazas, monitoreo continuo, contención automática de incidentes y recuperación ante ataques que puedan afectar la disponibilidad, integridad y confidencialidad de la información institucional.

ITEM	DESCRIPCIÓN	CANTIDAD	MEDIDA
1	**Servicio de suscripción de Licencias de Software de Detección y Respuesta Extendida para los Servidores Virtuales del Ministerio De Relaciones Exteriores**	200	Unidad

6.2 DESCRIPCIÓN DE SERVICIO (ACTIVIDADES A REALIZAR)

6.2.1. ALCANCE DE LA CONTRATACIÓN

La presente contratación comprende el servicio de suscripción de doscientas (200) licencias de una solución de Detección y Respuesta Extendida (XDR) para servidores Windows y Linux que forman parte de la infraestructura crítica institucional.
La solución deberá encontrarse en su versión más reciente liberada por el fabricante e incluir todas las capacidades avanzadas de detección, visibilidad, investigación, automatización, remediación y recuperación sin requerir módulos adicionales ni costos complementarios.

6.2.2. CARACTERÍSTICAS TÉCNICAS MÍNIMAS

6.2.2.1. **Consola Centralizada en la Nube**

a. **Arquitectura y Administración Centralizada**
La solución deberá basarse en una arquitectura de **Agente Único e Inteligente** con consola de administración 100% nativa en la nube (SaaS), garantizando:

- **Gestión Unificada:** Control total de los 200 servidores desde una interfaz web única con comunicación cifrada mediante TLS 1.2 o superior.
- **Autonomía del Agente:** El agente debe ser capaz de detectar, bloquear y remediar amenazas (incluyendo el proceso de restauracion) de forma autónoma, incluso si el servidor se encuentra **desconectado de la red o de la consola**.
- **Seguridad Operativa:** Implementación de control de acceso basado en roles (RBAC), autenticación multifactor (MFA) y registro inalterable de auditoría de todas las acciones administrativas.
- **Protección del Agente:** Mecanismos *anti-tampering* nativos para evitar que procesos maliciosos o usuarios locales detengan, modifiquen o desinstalen la protección.

b. **Visibilidad de Activos e Higiene de Seguridad (Nativo)**
Sin requerir despliegues adicionales, módulos extra o costos por "Add-ons", la plataforma debe proveer:

- **Inventario Automático de Aplicaciones:** Identificación en tiempo real de todo el software instalado, versiones exactas y detección de software no autorizado.
- **Gestión de Vulnerabilidades Pasiva:** Correlación automática y continua de las aplicaciones instaladas con bases de datos de vulnerabilidades (CVE), sin realizar escaneos de red intrusivos.
- **Priorización de Riesgo:** Clasificación de servidores basada en la severidad de las vulnerabilidades detectadas, nivel de exposición real y probabilidad de explotación activa.

c. **Motor de Detección Basado en IA Autónoma**
La solución debe prescindir del uso exclusivo de firmas tradicionales, incorporando motores de inteligencia artificial que operen en tiempo real:

- **IA Estática (Pre-ejecución):** Análisis profundo de archivos antes de su ejecución para identificar malware conocido y desconocido (Zero-day).
- **IA Conductual (En ejecución):** Monitoreo continuo de procesos en memoria para identificar comportamientos anómalos, técnicas de inyección, ataques *fileless* y abuso de herramientas legítimas (*Living off the Land*).
- **Mapeo MITRE ATT&CK:** Clasificación automática de cada alerta dentro de las tácticas y técnicas de la matriz MITRE para facilitar la interpretación técnica inmediata.

d. **Respuesta Automatizada y Tecnología de Restauracion Sistémica**
Capacidad crítica de recuperación ante incidentes de Ransomware. El mecanismo de reversión debe cumplir estrictamente con:

- **Restauracion Integral del Sistema:** Capacidad de revertir no solo archivos cifrados, sino también cambios en el registro del sistema, eliminación de servicios, creación de tareas programadas y persistencias creadas por el atacante.
- **Gestión y Protección Activa de VSS:** El agente debe tomar control y proteger activamente los *Volume Shadow Copies* (VSS) del sistema operativo, impidiendo que cualquier proceso malicioso intente eliminarlos o desactivarlos.
- **Independencia de Repositorios de Cuarentena:** La tecnología de reversión debe basarse en el diario de operaciones del sistema de archivos y snapshots protegidos, sin depender del copiado de archivos a carpetas ocultas o "SafeStores" que saturen el almacenamiento local.
- **Operación de "Un Solo Clic":** La restauración debe poder ejecutarse de forma masiva desde la consola, sin requerir herramientas externas ni depender de soluciones de backup tradicionales para la reversión inmediata.
- **Evidencia Verificable:** Generación de un registro detallado de los archivos afectados y restaurados, asegurando la integridad del estado previo al incidente.

e. **Investigación Forense y Telemetría EDR**

Capacidad avanzada de análisis y "Caza de Amenazas" (Threat Hunting):

- **Visualización de la Cadena de Ataque:** Gráfico interactivo que muestre el proceso raíz (Root Cause), conexiones de red, archivos modificados y visualización de intentos de movimiento lateral.
- **Telemetría Completa:** Registro detallado de procesos, hilos de ejecución, actividad de red y eventos del sistema para análisis post-mortem.
- **Correlación Automática:** Agrupación inteligente de eventos relacionados en un solo incidente para reducir la fatiga de alertas.

f. **Reportes Detallados en español**

La consola deberá permitir la generación nativa de reportes técnicos y ejecutivos en idioma español, incluyendo:

- **Análisis de Incidentes:** Detalle técnico completo de ataques bloqueados y acciones de remediación.
- **Reporte de Higiene:** Resumen de vulnerabilidades detectadas por servidor y por criticidad.
- **Actividad de Ransomware:** Métricas específicas sobre intentos de cifrado y efectividad de los procesos de restauracion ejecutados.
- **Exportación:** Los informes deberán poder exportarse en formatos PDF y CSV, con gráficos y métricas listos para auditoría.

g. **Optimización y Rendimiento**

- **Bajo Impacto:** El agente debe estar optimizado para entornos de servidores productivos críticos, con un consumo de recursos que no exceda el 1-3% de CPU en condiciones de operación normal.
- **Licenciamiento Todo Incluido:** Todas las capacidades descritas (Visibilidad, Vulnerabilidades, EDR, restauración y Reportes) deberán estar incluidas en la licencia base para los 200 servidores, sin requerir módulos o servicios de suscripción adicionales.

6.2.2.2. **Soporte Técnico y Acuerdos de Nivel de Servicio (SLA)**

- El contratista deberá brindar soporte técnico especializado por un período de trescientos sesenta y cinco (365) días calendario correspondiente a la vigencia de la suscripción de las licencias contratadas para los 200 servidores.
- El soporte deberá ser brindado directamente por el fabricante o por un partner autorizado y deberá cumplir con las siguientes condiciones mínimas:
  - Disponibilidad de soporte en modalidad 24x7 para incidentes críticos y de alta severidad.
  - Atención de incidentes relacionados con la operatividad de la solución, fallas del sistema, eventos de seguridad, configuraciones y actualizaciones, a través de una línea telefónica 0800 disponible las 24 horas del día, los 7 días de la semana.
  - Disponibilidad de soporte a través de sistema de tickets vía web, teléfono y/o correo electrónico, los cuales constituirán los medios oficiales de comunicación para el registro y seguimiento de requerimientos.
  - El contratista deberá priorizar la atención y solución de los requerimientos reportados por el Ministerio de Relaciones Exteriores, garantizando continuidad operativa.
  - El tiempo máximo de resolución de incidentes relacionados con la operatividad de la solución no deberá exceder las cuarenta y ocho (48) horas, contabilizadas a partir del momento en que el Ministerio de Relaciones Exteriores registre formalmente la incidencia a través de los canales oficiales.
  - El soporte deberá ser brindado por personal técnico debidamente certificado por el

fabricante, con acreditación vigente.

- El servicio deberá incluir asistencia en análisis técnico de incidentes, acompañamiento en respuesta ante amenazas, asesoría especializada y acceso a expertos del fabricante cuando el caso lo amerite.

6.2.2.2.1. Niveles de Severidad y Tiempos de Respuesta

a. Severidad 1 – Crítico
Incidente que afecte la disponibilidad del servidor, presencia confirmada de ransomware activo o compromiso en curso.
- Tiempo máximo de respuesta inicial: hasta 4 horas.
- Tiempo máximo de resolución: hasta 48 horas.

b. Severidad 2 – Alta
Incidente con impacto parcial en la seguridad del servidor o amenaza confirmada sin afectación total del servicio.
- Tiempo máximo de respuesta inicial: hasta 8 horas.
- Tiempo máximo de resolución: hasta 48 horas.

c. Severidad 3 – Media
Alertas investigativas o eventos sin impacto operativo inmediato.
- Tiempo máximo de respuesta inicial: hasta 24 horas hábiles.
- Tiempo máximo de resolución: hasta 3 días hábiles.

d. Severidad 4 – Baja
Consultas administrativas o solicitudes de configuración.
- Tiempo máximo de respuesta inicial: hasta 2 días hábiles.
- Tiempo máximo de resolución: hasta 5 días hábiles.

El soporte deberá incluir acceso a actualizaciones de la plataforma, mejoras del motor de detección, inteligencia de amenazas y parches de seguridad durante toda la vigencia contractual, sin generar costos adicionales para la Entidad.

6.2.2.3. Otras condiciones adicionales

- El contratista deberá cumplir con lo indicado en el Termino de Referencia. *Para tal caso,* ***las caracteristicas técnicas de la licencia de software de Detección y Respuesta Extendida ofertada bajo suscripción, deberá ser acreditado junto a su cotización, mediante brochure y/o información técnica oficial publicado en página web del fabricante.***

  EL contratista hará entrega de una carta en el plazo de siete (07) días contabilizados a partir del día siguiente de notificada la Orden de Servicio y/o suscrito el Contrato, donde indique claramente los medios de comunicación, a través del cual se reportarán los requerimientos (teléfonos, correo electrónico y sistema de atención de tickets), además la relación de contactos para la atención de requerimientos.

Condición Expresa

Todas las capacidades descritas —incluyendo inteligencia artificial, detección conductual, visibilidad de aplicaciones instaladas, identificación de vulnerabilidades, análisis forense avanzado, reportes detallados en español y funcionalidad completa de restauración ante ransomware— deberán encontrarse incluidas en la licencia contratada para los 200 servidores, sin requerir módulos adicionales, addons ni costos extra durante la vigencia del servicio.

6.2.2.4. **Transferencia de conocimiento al personal (Capacitación)**

El contratista deberá brindar capacitación a 2 personas designadas por el equipo de Seguridad Digital, con el fin de garantizar que puedan operar, administrar y mantener la solución de manera eficiente. Se debe contemplar el siguiente temario:

- **Formación fundamental y del producto**
- **Formación en implementación y resolución de problemas**
- **Formación en caza de amenazas y respuesta a incidentes**

Requisitos Mínimos de Cada Capacitación:

- **Duración: La duración deberá ser de 16 horas por temario indicado líneas arriba, incluyendo los laboratorios precisados.**
  La capacitación deberá ser dictada de forma virtual en los horarios coordinados con la oficina de OAS.
- **Material y Documentación:** Cada capacitación deberá incluir documentación detallada de los temas impartidos, así como guías de referencia rápida y manuales de procedimientos.
- **Formación Práctica:** Será obligatoria la inclusión de laboratorios prácticos y ejercicios que simulen escenarios reales de operación, ataque y respuesta, permitiendo a los participantes interactuar directamente con la solución. Estos laboratorios deberán ceñirse estrictamente al material
- Se deberá contar con acceso al portal E-LEARNING de la marca ofertada proporcionado por el fabricante durante la duración de la OS.
- La capacitación será proporcionada por el personal clave del contratista.

6.3. Requisitos según leyes, reglamentos, normas metrológicas y normas técnicas de naturaleza obligatoria vinculadas al objeto de la contratación.

No corresponde

6.4. Impacto ambiental.

No corresponde

6.5. Condición de operación.

No corresponde

6.6. Transporte.

No corresponde

6.7. Seguros.

No corresponde

6.8. Garantía comercial.

No corresponde

VII. CRONOGRAMA DEL SERVICIO

No aplica

VIII. REQUISITOS DEL PROVEEDOR

8.1. Del proveedor

Requisitos:

- El postor debe acreditar un monto facturado acumulado equivalente a S/. 30,000.00 (treinta mil con 00/100 soles), por la contratación de servicios iguales o similares al objeto de la convocatoria
- Contar con Registro Nacional de Proveedores (RNP) vigente en el rubro de servicios.
- Contar con Registro Único de Contribuyentes (RUC) activo y habido.
- El Proveedor deberá ser distribuidor autorizado por el fabricante del software de Detección y Respuesta Extendida, para la comercialización y/o proveer soporte para la licencia de software De Detección Y Respuesta Extendida ofertada en el Perú.

Se consideran servicios similares a los siguientes: suscripción de soluciones de antivirus y/o suscripción de software de detección y respuesta extendida y/o suscripción de software antispyware y/o implementación de soluciones de antivirus y/o implementación de software de detección y respuesta extendida y/o implementación de software antispyware.

Acreditación:

- La experiencia se acreditará con copia simple de (i) contratos u órdenes de servicios y su respectiva conformidad o captura de la consulta amigable del aplicativo del Ministerio de Economía y Finanzas (MEF) donde acredite el abono o cancelación del mismo; o (ii) constancia de prestación; o (iii) certificados; o (iv) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con constancia 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.
- **Distribuidor autorizado:** Copia simple la Certificación y/o carta expedida por el Fabricante de la Licencia de software de Detección y Respuesta Extendida ofertada.

8.2. Personal clave: Un (01) Consultor en Ciberseguridad

Requisitos:

a) Formación académica

Título Profesional o Grado de Bachiller en ingeniería de las siguientes especialidades: Informática y/o Sistemas y/o Redes y Comunicaciones y/o Telecomunicaciones y/o Electrónica.

b) Experiencia

Experiencia de tres (03) años como especialista y/o jefe y/o supervisor en servicios de implementación y/o puesta en funcionamiento en licencias de software de detección y respuesta extendida y/o antispyware y/o antivirus endpoint.

c) Certificación

Deberá contar con certificación técnica emitida por la marca del software de detección y respuesta extendida ofertado.

Acreditación de personal clave:

- **Experiencia:** con cualquiera de los siguientes documentos: (i) copia simple de contratos y/o orden y su respectiva conformidad o (ii) constancias o (iii) certificados o iv) Resolución de designación y cese. Los documentos que acreditan la experiencia deben incluir los nombres y apellidos, el cargo desempeñado, el plazo de la prestación, el nombre de la entidad o empresa

que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.

- **Nivel académico:** copia simple de grado de bachiller o título profesional
- **Certificación:** con copia simple de certificado y/o constancia.

La documentación que acredite los requisitos del proveedor y del personal clave (formación académica, experiencia y certificación) será presentada como requisito para la presentación de cotizaciones.

IX. OTRAS CONSIDERACIONES PARA LA EJECUCIÓN DE LA PRESTACIÓN

9.1. Confidencialidad

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 del presente requerimiento. 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 este presente requerimiento 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° 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 presente documento contractual, así mismo, como el cumplimiento del derecho al secreto e inviolabilidad de las comunicaciones (articulo2, inciso 10 de la Constitución Política), salvo excepciones legales de intervención por un mandato judicial motivado.

El contratista que tenga acceso a información durante la ejecución del servicio deberá mantener y guardar estricta reserva y absoluta confidencialidad de esta, 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 de los bienes a producir, 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 indole 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.

9.2. Anticorrupción y antisoborno

EL PROVEEDOR declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación y/o cualquier servidor de la entidad contratante.

Asimismo, EL CONTRATISTA se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente.

Aunado a ello, EL CONTRATISTA se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación y/o cualquier servidor de la entidad contratante, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito. En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados.

Adicionalmente, EL CONTRATISTA se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con LA ENTIDAD CONTRATANTE.

Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o cualquier persona vinculada a la persona jurídica que representa; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud del contrato.

Finalmente, el incumplimiento de estas obligaciones, durante la ejecución contractual, otorga a LA ENTIDAD CONTRATANTE el derecho de resolver total o parcialmente el contrato. Cuando lo anterior se produzca por parte de un proveedor adjudicatario de los catálogos electrónicos de acuerdo marco, este incumplimiento conllevará que sea excluido de los Catálogos Electrónicos de Acuerdo Marco. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar.

9.3. Conflicto de intereses (Ley N° 31564)

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

9.4. Propiedad intelectual

La Entidad tendrá todos los derechos de propiedad intelectual incluidos, sin limitación, así como las patentes, derechos de autor, nombres comerciales y marcas registradas respecto a los productos o documentos y otros materiales que guarden una relación directa con la ejecución de la prestación o que se hubiere creado o producido como consecuencia o en el desarrollo de la ejecución de la prestación.

9.5. Recursos y facilidades a ser provistas por la entidad

La entidad a través de la Oficina de Arquitectura y Seguridad Digital brindará los accesos y/o facilidades para la ejecución del servicio.

9.6. Responsabilidad por defectos o vicios ocultos

La recepción conforme de la prestación por parte de LA ENTIDAD no obsta su derecho a reclamar posteriormente por defectos o vicios ocultos, de acuerdo con lo dispuesto en el literal c) del numeral 69.2 del artículo 69 de la Ley.

El plazo máximo de responsabilidad del CONTRATISTA es de un (1) año contado a partir de la conformidad otorgada por LA ENTIDAD.

9.7. Gestión de riesgos las partes

REPÚBLICA DEL PERÚ - Oficina de Arquitectura y Seguridad Digital - Ministerio de Relaciones Exteriores — V.E.G.G.

REPÚBLICA DEL PERÚ - Oficina de Arquitectura y Seguridad Digital - Ministerio de Relaciones Exteriores — R.R.B.

REPÚBLICA DEL PERÚ - Unidad Ejecutora de Infraestructura - Ministerio de Relaciones Exteriores

REPÚBLICA DEL PERÚ - Oficina de Arquitectura y Seguridad Digital - Ministerio de Relaciones Exteriores — E.M.S.

LAS PARTES realizan la gestión de riesgos de acuerdo con lo establecido en la presente contratación y los documentos que lo conforman, a fin de tomar decisiones informadas, aprovechando el impacto de riesgos positivos y disminuyendo la probabilidad de los riesgos negativos y su impacto durante la ejecución contractual, considerando la finalidad pública de la contratación.

9.8. Otras obligaciones de la Entidad
No corresponde

9.9. Otras condiciones para la contratación
No corresponde

9.10. Medidas de control durante la ejecución contractual

a) **Áreas que coordinarán con el proveedor:** Oficina de Arquitectura y Seguridad Digital a través del personal de Seguridad Digital, la Oficina de Logística.

b) **Área responsable de las medidas de control:** Oficina de Arquitectura y Seguridad Digital a través del personal de Seguridad Digital, la Oficina de Logística.

9.11. Modalidad de pago

Suma alzada

X. GARANTÍA POR PAGO ANTICIPADO

Cuando sea condición de mercado para la ejecución de las obligaciones a cargo del proveedor para la prestación de servicios, que el pago se realice íntegra o parcialmente al inicio del contrato (pago anticipado), éste se realiza previo otorgamiento de la correspondiente garantía por el mismo monto.

Para tales efectos, se debe contemplar lo señalado en la Ley y su Reglamento.

XI. LUGAR Y PLAZO DE PRESTACIÓN DEL SERVICIO

11.1. Lugar de prestación del servicio:
La ejecución del servicio se realizará en la sede de Raúl Porras Barrenechea del MRE, Jr. Ucayali N° 337- Cercado de Lima

11.2. Plazo de prestación del servicio:

- **Plazo de instalación, implementación y configuración.**
  La instalación, implementación y configuración de las licencias de software de Detección y Respuesta Extendida deberá realizarse en el plazo de sesenta (60) días calendario contabilizados a partir del día siguiente de notificada la Orden de Servicio y/o suscrito el Contrato.

- **Del plazo de ejecución del servicio**
  El plazo de ejecución del servicio relativo a la suscripción de las licencias, tendrán una vigencia de **doce (12) meses, contabilizados a partir de la suscripción del Acta de Activación de las Licencias de software de Detección y Respuesta Extendida**, entre un representante del Contratista y un representante de la Oficina de Arquitectura y Seguridad Digital.

- **Del plazo para la transferencia de conocimiento (Capacitación)**
  Deberá realizarse en el plazo de noventa (90) días calendario, contabilizados a partir del día siguiente de notificada la Orden de Servicio y/o suscrito el Contrato.

XII. ENTREGABLE

12.1. Informe de instalación, implementación y configuración de la solución:

El contratista deberá presentar vía Mesa de Partes del Ministerio de Relaciones Exteriores, un (1) Informe Técnico dirigido a la Oficina de Arquitectura y Seguridad Digital, en el plazo de siete (07) días calendario, contabilizados a partir del día siguiente de ejecutada la instalación, implementación, configuración de las licencias de software ofertado, que acredite la correcta puesta en producción de la solución XDR en los 200 servidores institucionales, detallando de manera estructurada las actividades ejecutadas durante las fases de instalación, implementación y configuración.

- Alcance del proyecto, indicando cantidad de servidores instalados (Windows y Linux), fechas de despliegue y responsables técnicos.
- Evidencia de instalación de los agentes en cada servidor, incluyendo versión instalada y estado operativo.
- Detalle de la configuración aplicada en la consola centralizada, incluyendo políticas de seguridad, perfiles de protección, reglas de respuesta automatizada y configuración de restauración.
- Configuración de visibilidad de aplicaciones instaladas y módulo de identificación de vulnerabilidades.
- Parametrización de alertas, notificaciones y generación de reportes en español.
- Validación de comunicación segura entre agentes y consola en la nube.
- Pruebas funcionales realizadas (detección de amenazas, aislamiento de servidor, simulación de incidente y verificación de restauración).
- Estado final de la plataforma, indicando que se encuentra operativa y en producción.
- El informe deberá adjuntar capturas de pantalla, evidencias técnicas y conclusiones, certificando que la solución se encuentra correctamente implementada conforme a los requisitos establecidos en el TDR.

12.2. Informe de la Transferencia de Conocimiento (Capacitación)

El contratista deberá presentar vía Mesa de Partes del Ministerio de Relaciones Exteriores, un (1) Informe Técnico dirigido a la Oficina de Arquitectura y Seguridad Digital, en el plazo de siete (07) días calendario, contabilizados a partir del día siguiente de culminada la capacitación que incluya:

El entregable deberá considerar lo siguiente:

Informe de Transferencia de Conocimiento: Se documenta la realización de la capacitación al personal señalado en el apartado términos de referencia incluyendo los temas impartidos, las horas comprendidas y el temario al que hace referencia.

***Importante:* Los entregables detallados en el presente numeral, serán remitidos vía Mesa de parte del Ministerio de Relaciones Exteriores, dirigidos a la Oficina de Arquitectura y Seguridad Digital.**

Mesa de parte del Ministerio de Relaciones Exteriores encuentra ubicada en el Jirón Lampa N° 545, Sótano 1, en el distrito de Cercado de Lima, y el horario de atención es de lunes a viernes de 8:30 a 16:30 horas.

Así también se cuenta con Mesa de Partes Digital el cual es a través del siguiente enlace https://www.gob.pe/20416-acceder-a-mesa-de-partes?child=27623. Respecto a la mesa de partes digital; será habilitado las 24 horas del día, los 7 días de la semana, el cual registra de manera automática la fecha y hora exacta de ingreso de los documentos.

Los escritos, solicitudes y documentos que hayan sido presentados desde las 00:00 horas hasta las 23.59 horas de cualquier día de la semana ya sea día hábil o inhábil, se considerarán presentados el mismo día.

XIII. CONFORMIDAD DE LA PRESTACIÓN

La conformidad de la prestación del servicio se regula por lo dispuesto en el artículo 144 del Reglamento de la Ley General de Contrataciones Públicas. La conformidad es otorgada por la Oficina de Arquitectura y Seguridad Digital previo informe de visto bueno del personal de Seguridad Digital

con el VB de la Unidad Funcional de Redes e Infraestructura Tecnológica en el plazo máximo de siete (7) días computados desde el día siguiente de recibido el entregable.

De existir observaciones, la ENTIDAD las comunica al CONTRATISTA, indicando claramente el sentido de estas, otorgándole un plazo para subsanar el cual no debe ser mayor al 30% del plazo del entregable[1] correspondiente, dependiendo de la complejidad o sofisticación de las subsanaciones a realizar. Si pese al plazo otorgado, EL CONTRATISTA no cumpliese a cabalidad con la subsanación, la ENTIDAD puede otorgar al CONTRATISTA periodos adicionales para las correcciones pertinentes, conforme a lo señalado en el numeral 144.4. del Reglamento, u optar con resolver el contrato, de acuerdo con el supuesto de resolución establecido en el literal b) del numeral 68.1 del artículo 68 de la Ley. En caso se otorgue periodos adicionales corresponde aplicar la penalidad por mora desde el vencimiento del plazo inicial para subsanar, sin considerar los días en los que pudiera incurrir la ENTIDAD para efectuar las revisiones y notificar las observaciones correspondientes.

Este procedimiento no resulta aplicable cuando los servicios manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso LA ENTIDAD no efectúa la recepción o no otorga la conformidad, según corresponda, debiendo considerarse como no ejecutada la prestación, aplicándose la penalidad que corresponda por cada día de atraso.

XIV. FORMULA DE REAJUSTE

No corresponde

XV. FORMA Y CONDICIONES DE PAGO

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en Soles, en **PAGO ÚNICO,** luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

Para tal efecto, el responsable de otorgar la conformidad de la prestación deberá hacerlo en un plazo que no excederá de los siete (7) días del día siguiente de recibido el entregable, salvo que se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación, en cuyo caso la conformidad se emite en un plazo máximo de veinte (20) días, bajo responsabilidad de dicho servidor.

Le Entidad efectúa el pago en un plazo máximo de diez (10) días hábiles siguientes de otorgada la conformidad de los servicios, siempre que se verifiquen las condiciones establecidas en el contrato para ello.

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- Documento del funcionario responsable de la Oficina de Arquitectura y Seguridad Digital previo informe de visto bueno del personal de Seguridad Digital con el VB de la Unidad Funcional de Redes e Infraestructura Tecnológica, emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.
- Código de cuenta interbancaria (CCI) o, en el caso de proveedores no domiciliados, el número de cuenta bancaria y nombre de la entidad bancaria en el exterior.
- Entregables del servicio de acuerdo con lo señalado en el numeral XII.

Salvo los documentos de conformidad, el contratista debe presentar la documentación restante en la mesa de partes del Ministerio de Relaciones Exteriores, se encuentra ubicada en el Jirón Lampa N° 545, Sótano 1, en el distrito de Cercado de Lima, y el horario de atención es de lunes a viernes de 8:30 a 16:30 horas.

[1] En caso de que el plazo obtenido como resultado de la aplicación del porcentaje sea una cifra decimal, corresponde que la entidad efectúe el redondeo a favor del contratista, computándose como un día completo adicional en dicho supuesto.

Así también se cuenta con Mesa de Partes Digital el cual es a través del siguiente enlace https://www.gob.pe/20416-acceder-a-mesa-de-partes?child=27623. Respecto a la mesa de partes digital; será habilitado las 24 horas del día, los 7 días de la semana, el cual registra de manera automática la fecha y hora exacta de ingreso de los documentos.

Los escritos, solicitudes y documentos que hayan sido presentados desde las 00:00 horas hasta las 23.59 horas de cualquier día de la semana ya sea día hábil o inhábil, se considerarán presentados el mismo día.

XVI. RESOLUCIÓN CONTRACTUAL

Cualquiera de las partes puede resolver el contrato, de conformidad con el literal b)[2] del numeral 68.1 del artículo 68 de la Ley N° 32069, Ley General de Contrataciones Públicas. De encontrarse en el citado supuesto de resolución del contrato, LAS PARTES proceden de acuerdo a lo establecido en el artículo 122 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

Asimismo, se puede efectuar la resolución contractual, en los siguientes casos:

a) Caso fortuito o fuerza mayor que imposibilite la continuación del contrato.
b) Incumplimiento de obligaciones contractuales, por causa atribuible a la parte que incumple.
c) Hecho sobreviniente al perfeccionamiento del contrato, de supuesto distinto al caso fortuito o fuerza mayor, no imputable a ninguna de las partes, que imposibilite la continuación del contrato.
d) Por incumplimiento de la cláusula anticorrupción.
e) Por la presentación de documentación falsa o inexacta durante la ejecución contractual.
f) Asimismo, puede resolverse de forma total o parcial la Orden de servicio y/o contrato por mutuo acuerdo entre las partes, previa opinión del área usuaria.

XVII. SOLUCION DE CONTROVERSIAS

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante CONCILIACIÓN, conforme con lo establecido en la Ley N° 32069, Ley General de Contrataciones Públicas y su Reglamento.

XVIII. PENALIDADES

La suma de la aplicación de las penalidades por mora y de otras penalidades no puede exceder el 10% del monto del entregable correspondiente.

18.1 Penalidad por mora en la ejecución de la prestación

18.1.1 En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto de la contratación, la entidad contratante le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable. La penalidad se aplica automáticamente y se calcula de acuerdo con la siguiente fórmula:

$$\text{Penalidad diaria} = \frac{0.10 \times \text{monto}}{F \times \text{plazo}}$$

- Donde F tiene los siguientes valores:

[2] b) Incumplimiento de obligaciones contractuales, por causa atribuible a la parte que incumple.

Para servicios: F = 0.40

- Para consultorías de obras:

  a) Para plazos menores o iguales a sesenta días: F = 0.40.

  b) Para plazos mayores a sesenta días: F = 0.25.

18.1.2 Tanto el monto como el plazo se refieren, al monto y plazo del entregable que fuera materia de retraso.

18.1.3 El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobada. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando el contratista acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En este último caso, la calificación del retraso como justificado por parte de la entidad contratante no da lugar al pago de gastos generales ni costos directos de ningún tipo.

18.2 Otras penalidades

OTRAS PENALIDADES			
N°	**UPUESTO DE APLICACIÓN DE PENALIDAD**	**FORMA DE CÁLCULO**	**PROCEDIMIENTO DE VERIFICACIÓN**
1	El Contratista no presente los entregables definidos en el numeral XII. en los plazos definidos	Se aplicará el 1 % de una (01) UIT (penalidad por cada día de retraso). *(*) UIT (Unidad Impositiva Tributaria)*	Según informe y/o reporte del equipo de Seguridad Digital de la Oficina de Arquitectura y Seguridad Digital (OAS)

(Firma digital o manuscrita)

ÁREA USUARIA
OFICINA DE ARQUITECTURA Y SEGURIDAD DIGITAL

Erick Manuel Bocanegra Villanueva
Jefe (e) de la Oficina de Arquitectura y Seguridad Digital.

REPÚBLICA DEL PERÚ - Oficina de Seguridad y Continuidad - Oficina de Arquitectura y Seguridad Digital - Ministerio de Relaciones Exteriores - Y.E.G.G.

REPÚBLICA DEL PERÚ - Oficina de Seguridad y Continuidad - Oficina de Arquitectura y Seguridad Digital - Ministerio de Relaciones Exteriores - R.R.B.

REPÚBLICA DEL PERÚ - Oficina de Seguridad y Continuidad - Oficina de Arquitectura y Seguridad Digital - Ministerio de Relaciones Exteriores - S.C.

SUSTENTO TÉCNICO PARA LA CONTRATACION DEL SERVICIO DE SUSCRIPCION DE LICENCIAS DE SOFTWARE DE DETECCION Y RESPUESTA EXTENDIDA PARA ENDPOINTS

1. **NOMBRE DEL ÁREA**
   Oficina de Arquitectura y Seguridad Digital

2. **RESPONSABLE DE LA EVALUACIÓN**
   Ing. Erick Bocanegra Villanueva
   Jefe (e) de la Oficina de Arquitectura y Seguridad Digital

   Ing., Yoel Godofredo Salinas Castro
   Jefe de la Unidad de Redes e Infraestructura

   Ronald Ramirez Blanco
   Oficial de Seguridad y Confianza Digital

   Ing. Yordi Gabino Guere
   Especialista en Seguridad Informática

3. **FECHA**

   08/05/2026

4. **JUSTIFICACIÓN**

   El Ministerio de Relaciones Exteriores, con el objetivo de optimizar la seguridad de sus sistemas informáticos y reducir las brechas de vulnerabilidad frente a ciberamenazas avanzadas, requiere herramientas de XDR (Extended Detection and Response). Estas herramientas permiten una gestión integral y un monitoreo constante de los posibles vectores de ataques avanzados dentro de la infraestructura tecnológica de la institución, abarcando desde los endpoints hasta las aplicaciones web y redes corporativas.
   El XDR proporcionará una solución centralizada y escalable para detectar, investigar y responder a incidentes de seguridad, asegurando que se minimicen los riesgos de brechas informáticas, lo que contribuirá a la protección de la información y la continuidad operativa de las actividades institucionales.

   En tanto, la Oficina de Arquitectura y Seguridad Digital tiene entre sus funciones las siguientes:

   - Formular y proponer planes, políticas, normas técnicas y estándares para la implementación, desarrollo, operación, mantenimiento y evaluación de los sistemas de información y telecomunicaciones;

- Administrar y supervisar la gestión técnica y operativa de las redes locales y/o remotas, así como de los equipos periféricos;
- Garantizar la continuidad de las operaciones de todos los sistemas informáticos de la Entidad.
- Asegurar todos los sistemas previos a su publicación, realizar pruebas de análisis de vulnerabilidades, con el fin de encontrar brechas de seguridad y subsanarlas antes de pasar a la fase de producción.
- Dirigir y supervisar el diseño, desarrollo, documentación e implementación de los sistemas de tecnologías de información de acuerdo a las normas establecidas;

Al respecto, corresponde señalar que la Ley N° 28612, ley que norma el uso, adquisición y adecuación del software en la administración pública, tiene por objeto establecer las medidas que permitan a la administración pública la contratación de licencias de software y servicios informáticos en condiciones de neutralidad, vigencia tecnológica, libre concurrencia y trato justo e igualitario de proveedores.

Por su parte, en el artículo 6 de dicha Ley, se indica que el uso o adquisición de licencias de software en la administración pública requiere del Informe Previo de Evaluación de la Oficina de Informática o la que haga sus veces, de la institución, que determine el tipo de licencia de software que resulte más conveniente para atender el requerimiento formulado.

5. ALTERNATIVAS

Considerando la justificación del software, se ha procedido a realizar un análisis de evaluación con productos de funcionalidades similares, es decir con características técnicas y requerimientos de instalación semejantes.

De acuerdo a la necesidad expuesta se evalúan las siguientes alternativas del mercado:

Producto
Sentinel One
CrowdStrike Falcon

6. ANÁLISIS COMPARATIVO TÉCNICO

El análisis técnico se ha realizado de conformidad con la metodología establecida en la "Guía Técnica sobre evaluación de software en la administración pública, aprobada por Resolución Ministerial N° 139-2004-PCM, de acuerdo a lo establecido por la Ley N° 28612.

a) Propósito de la Evaluación:
Validar que las alternativas seleccionadas sean las más convenientes técnicamente para gestionar la seguridad en los equipos de cómputo del Ministerio de Relaciones Exteriores.

Exteriores.

b) Identificar el tipo de producto:
Software de prevención, detección y respuesta ante amenazas avanzadas.

c) Especificación del Modelo de Calidad:
Se aplica el Modelo de Calidad de Software descrito y aprobado por Resolución Ministerial No. 139-2004-PCM[1]

d) Selección de Métricas:
Las métricas fueron seleccionadas en base al análisis de información técnica y a los antecedentes previos de evaluación para este tipo de software en el sector público peruano.

Se aplicó el modelo de calidad externa e interna, de acuerdo con la escala de calificación detallado en el cuadro de características, en base a la metodología establecida en la "Guía Técnica sobre Evaluación de Software para la Administración Pública" aprobada por Resolución Ministerial de la Presidencia del Consejo de Ministros, N° 139-2004-PCM, tomando en cuenta los siguientes aspectos:

Cuadro Nº 1: Comparación de Características y Atributos versus Alternativas de Software.

ITEM	ATRIBUTO	DESCRIPCIÓN	Puntaje Máximo	Puntaje mínimo	Sentinel One	CrowdStrike Falcon
FUNCIONALIDAD			70	63	69	61
1	Recuperación	Capacidad de restaurar en su totalidad los archivos y claves de registro afectados por un ransomware	10	9	10	8
2	Interoperabilidad	Capacidad de integrarse con soluciones de seguridad especializadas	10	9	10	9

[1] http://www.gobiernodigital.gob.pe/Bancos/Banco_Normas/archivos/Guia-Evaluacion-SW.pdf.

ITEM	ATRIBUTO	DESCRIPCIÓN	Puntaje Máximo	Puntaje mínimo	Sentinel One	CrowdStrike Falcon
3	Exactitud	Utiliza machine learning para prevenir amenazas desconocidas y protecciones basadas en comportamiento	10	9	10	9
4	Seguridad	Proporciona una profunda visibilidad y prevención de amenazas para endpoints y servidores correlacionando automáticamente los datos en varias capas de seguridad para una detección más rápida	10	9	10	9
5	Estabilidad	Funcionamiento no invasivo en el rendimiento o desempeño del equipo	10	9	9	8
6	Adaptabilidad	Detecta malware, comando y control, movimiento lateral y exfiltración al perfilar el comportamiento e identificar cambios en el comportamiento que indiquen un ataque	10	9	10	9

REPÚBLICA DEL PERÚ - Ofic. de Seguridad y Confianza Digital - Ofic. de Arquitectura y Seguridad Digital - Ministerio de Relaciones Exteriores - Y.E.G.G.

REPÚBLICA DEL PERÚ - Ofic. de Seguridad y Confianza Digital - Ministerio de Relaciones Exteriores - R.R.B.

REPÚBLICA DEL PERÚ - Ofic. de Redes e Infraestructuras Tecnológicas - OAS - Ministerio de Relaciones Exteriores - Y.G.R.C.

REPÚBLICA DEL PERÚ - Ofic. de Arquitectura y Seguridad Digital - Ministerio de Relaciones Exteriores - E.M.B.V.

ITEM	ATRIBUTO	DESCRIPCIÓN	Puntaje Máximo	Puntaje mínimo	Sentinel One	CrowdStrike Falcon
7	Instalación	Capacidad de instalación en modo silencioso y sin necesidad de reiniciar la estación de trabajo o servidor	10	9	10	9
USABILIDAD			**30**	**25**	**28**	**28**
1	Entendimiento	Capacidad del software de advertir las amenazas detectadas al administrador de seguridad para el análisis, trazabilidad y forense correspondiente	10	8	10	8
2	Interfaz Usuario	Contar con una interfaz amigable e intuitiva que permita al usuario la asimilación manejo y adaptabilidad de la herramienta en el menor tiempo posible	10	9	9	10
3	Aprendizaje	Conceptualización de los recursos y funcionalidades de fácil comprensión para una adecuada gestión	10	8	9	10
PUNTAJE TOTAL			**100**	**88**	**97**	**89**

7. ANÁLISIS COMPARATIVO DE COSTO - BENEFICIO

En el análisis costo beneficio se ha tomado en cuenta los criterios establecidos en el punto 8 del Reglamento de la Ley N° 28612, siendo que, en el presente informe técnico previo de

evaluación de software, dos (2 alternativas evaluadas alcanzaron la puntuación mayor e igual al puntaje mínimo, por lo que el análisis costo beneficio debe ser realizado considerando las 2 alternativas.

- Sentinel One: 97 puntos
- CrowdStrike Falcon: 89 puntos

a. Licenciamiento

Producto	Cantidad Mínima de Objetivos (**)	Costo Anual S/.	Puntaje de Análisis Comparativo - Técnico	Beneficio / Costo
Sentinel One	200 objetivos	S/ 42,000.00	97 puntos (*)	**0.97**
CrowdStrike Falcon	200 objetivos	S/ 64.146,33	89 puntos (*)	**0.89**

(*) El total en puntos de beneficio son extraídos del Cuadro N° 1 indicado en el punto 6. Análisis Comparativo Técnico.

(**) Objetivos; se refiere a la cantidad de servidores o endpoints que la herramienta XDR protegerá.

Los precios señalados en el análisis comparativo de costo - beneficio están basados en las cotizaciones que diferentes proveedores han remitido, dichas cotizaciones tienen una validez de 60 días, dicha información se encuentra en la sección de **ANEXOS**

b. Hardware necesario para su funcionamiento de las alternativas:
Las dos (2) alternativas que superaron el puntaje mínimo son normalmente en modalidad software, las cuales pueden ser instaladas en nuestra arquitectura de servidores sin consumir demasiado espacio lógico (disco, memoria y CPU).

c. Soporte y mantenimiento externo
Se requiere gastos adicionales con respecto a este componente, ya que cada una de las alternativas evaluadas requiere el soporte para sus productos.

d. Personal y mantenimiento interno

La Entidad no cuenta con los profesionales idóneos para administrar dicho software.

REPÚBLICA DEL PERÚ - Oficina de Seguridad y Confianza Digital - Ministerio de Relaciones Exteriores - Y.E.G.G.

REPÚBLICA DEL PERÚ - Oficina de Seguridad y Confianza Digital - Ministerio de Relaciones Exteriores - R.R.R.

REPÚBLICA DEL PERÚ - Jefa de la Oficina Funcional de Redes e Infraestructura Tecnológica - Ministerio de Relaciones Exteriores - K.P.C.

REPÚBLICA DEL PERÚ - Oficina de Arquitectura y Seguridad - Ministerio de Relaciones Exteriores - E.M.B.V.

e. **Capacitación.**

Para las dos (2) alternativas que superaron el puntaje mínimo, es necesario considerar transferencia de conocimiento para el personal técnico del Ministerio de relaciones Exteriores, puesto que no poseen conocimientos en el manejo de estos productos.

8. CONCLUSIONES.

- Se determinó los atributos o características técnicas mínimas que deben ser considerados para la evaluación del "**SOFTWARE DE DETECCION Y RESPUESTA EXTENDIDA PARA ENDPOINTS**".
- Los precios obtenidos de cada solución están sujetos a distintas variables que el mercado cambiante, sin embargo, en la sección Anexos, se muestra cotizaciones de las soluciones que se están considerando para lo requerido.
- De las dos (2) alternativas evaluadas, las dos (2) de ellas superaron el puntaje mínimo requerido (88 puntos) en la descripción de los atributos, los mismos que pasaron para el análisis costo beneficio.
- En la evaluación de Costo / Beneficio, podemos observar que el software Sentinel One alcanza el mayor factor Costo / Beneficio de los productos evaluados, por lo que representa la opción más adecuada en la presente evaluación.
- El personal del Ministerio de relaciones deberá ser capacitado, en cualquiera de las, Las dos (2) alternativas que superaron el puntaje mínimo, con el fin de que administren la herramienta de protección de forma adecuada, es de vital importancia para el uso adecuado de la misma.
- De las dos (2) alternativas evaluadas, las dos (2) alternativas superaron el puntaje mínimo, por lo tanto, se recomienda realizar una contratación en el que participen estas herramientas además de cualquier otra que satisfaga los requerimientos mínimos, considerando los aspectos funcionales y técnicos evaluados en el presente informe; seleccionando la alternativa que se estime conveniente, luego de la indagación de mercado efectuada por la Oficina de Logística.

REPÚBLICA DEL PERÚ - Ofic. de Seguridad y Confianza Digital - Ministerio de Relaciones Exteriores - Y.E.G.G.

REPÚBLICA DEL PERÚ - Ofic. de Seguridad y Confianza Digital - Ministerio de Relaciones Exteriores - R.R.P.

REPÚBLICA DEL PERÚ - Ofic. de Redes e Infraestructuras Tecnológicas - Ministerio de Relaciones Exteriores

REPÚBLICA DEL PERÚ - Ofic. de Arquitectura y Seguridad - Ministerio de Relaciones Exteriores - E.M.B.V.

9. FIRMAS.

Ing. Ronald Rudy Ramírez Blanco
Oficial de Seguridad y Confianza Digital
Oficina de Arquitectura y Seguridad Digital
Oficina General de Transformación Digital Institucional

Ing., Erick Manuel Bocanegra Villanueva
Jefe (e) de la Oficina de Arquitectura y Seguridad Digital
Oficina General de Transformación Digital Institucional

Ing. Yordi Gabino Guere
Especialista de Seguridad Informatica
Oficina de Arquitectura y Seguridad Digital
Oficina General de Transformación Digital Institucional

Ing., Yoel Godofredo Salinas Castro
Jefe de la Unidad Funciona de Redes e Infraestructura Tecnológica
Oficina de Arquitectura y Seguridad Digital
Oficina General de Transformación Digital Institucional

ANEXOS

A) **SENTINEL ONE**

HardSecur EIRL SentinelOne

Lima, 24 de Marzo de 2026
COTIZACION CR0000106-03/26

MINISTERIO DE
RELACIONES
EXTERIORES
Ciudad.-

CONFIDENCIAL

HardSecur EIRL
Calle German Schreiber Nro 276
San Isidro - Lima - Peru
Central : +51 - 1 - 4400694
www.hardsecur.net
hardsecur@hardsecur.net

Imagen N° 01

HardSecur EIRL SentinelOne

DESCRIPCIÓN GENERAL DE PROPUESTA ECONOMICA

SENTINELONE COMPLETE				
ITEM	CANTIDAD	DESCRIPCION	VALOR UNITARIO S/.	VALOR TOTAL S/.
01	200	MSSP Annual Subscription includes Endpoint Protection Platform COMPLETE Capabilities, Enterprise (Standard 24x7, email/web/phone) Support Plan, Platform Updates and Upgrades. Codigo : S1 CMPEN-T2-CA Pago Anual	210	42 000.00

CONDICIONES COMERCIALES

- **Sirvanse Girar Orden a nombre de HardSecur eirl**
- **Forma de Pago : Contado**
- **Sujeto a Detraccion 12%**
- **Validez de la Oferta : 05 Dias**

Imagen N° 02

B) CRONSTRIKE FALCON

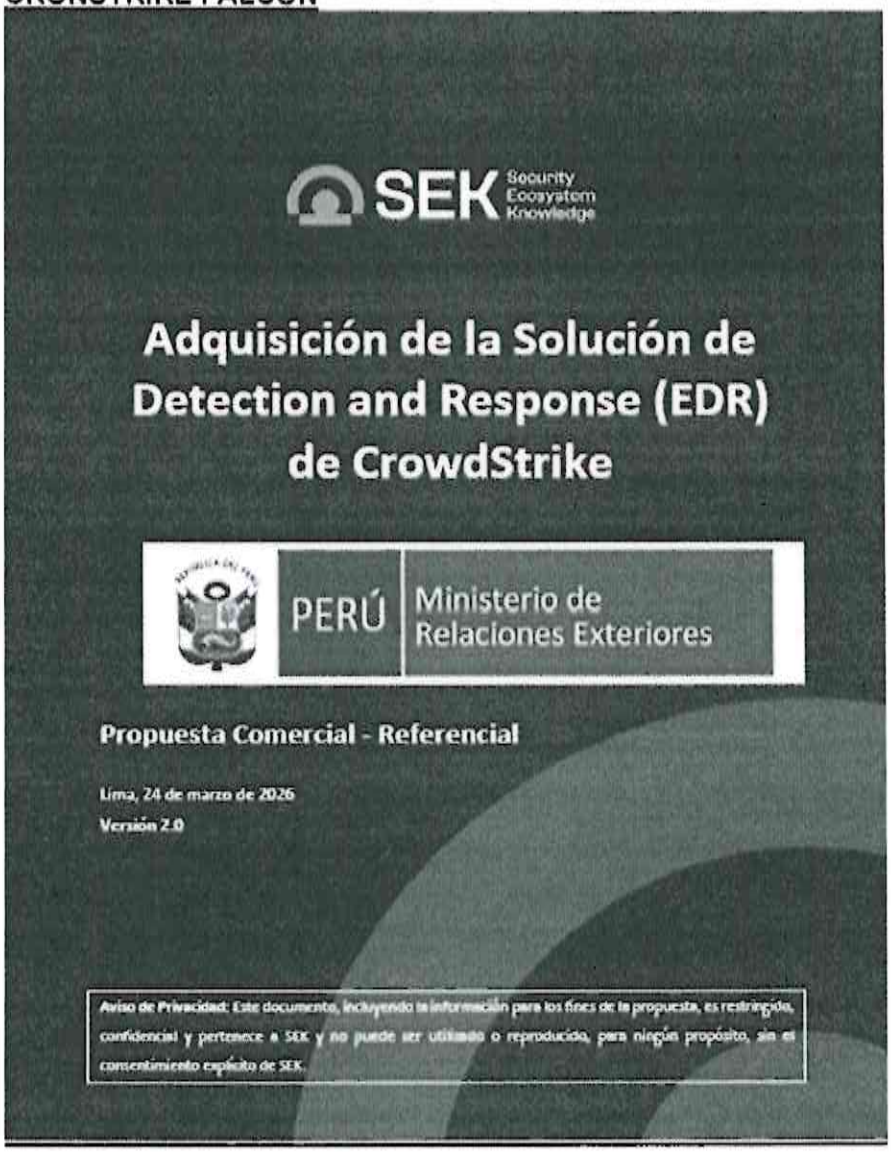

Imagen N° 03

SEK Security Ecosystem Knowledge — Propuesta Comercial - Referencial

1 Propuesta Económica

1.1 Equipamiento, Licencias

En este punto se muestra el equipamiento (solo licencias) propuestos por el periodo de 12 meses:

MARCA			PRECIO VENTA (USD)	
Descripción	Términos	Cantidad	Precio Unitario	Precio Total
Falcon MSSP Defend	12 meses	200	$70.50	$14,100.00
Threat Graph Standard	12 meses	200	$0.00	$0.00
Insight	12 meses	200	$0.00	$0.00
Prevent	12 meses	200	$0.00	$0.00
Falcon Firewall Management	12 meses	200	$0.00	$0.00
MSSP Device Control	12 meses	200	$0.00	$0.00
Express Support	12 meses	1	$1,618.09	$1,618.09
			TOTAL	$15,718.09

SUBTOTAL US$	$15,718.09
TOTAL US$ (IGV)	$18,547.35

Imagen N° 04