TÉRMINOS DE REFERENCIA PARA CONTRATOS MENORES
ANEXO N° 2
TÉRMINOS DE REFERENCIA PARA LA CONTRATACIÓN DE SERVICIOS

FECHA: Lima, 30 de abril de 2025	
Unidad de Organización	Oficina de Tecnologías de la Información de la Oficina de General de Apoyo a la Gestión Institucional del Ministerio de Relaciones Exteriores.
Código Tarea / Actividad Operativa	AOI00004501023: Gestión de la Seguridad Digital
Meta Presupuestaria	290
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, 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. NÚMERO DE INCLUSIÓN EN EL CMN

Programado en el Cuadro Multianual de Necesidades Inicial 2025-2027.

III. FINALIDAD PÚBLICA DE LA CONTRATACIPÓN

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 contar con una solución **de detección y respuesta extendida** XDR es para proteger los servidores del Ministerio de Relaciones Exteriores es mejorar la detección, prevención y respuesta ante amenazas cibernéticas avanzadas en tiempo real. Esto permitirá integrar múltiples fuentes de datos, identificar comportamientos sospechosos y actividades maliciosas, y automatizar la respuesta ante incidentes. Además, se fortalecerá la visibilidad de la infraestructura de servidores, garantizando la seguridad de la información sensible y reduciendo el riesgo de brechas de seguridad que puedan afectar las operaciones del ministerio y la protección de datos diplomáticos

Objetivos Específicos:

- Implementar una solución XDR que permita identificar de manera temprana y precisa amenazas avanzadas, como ataques dirigidos, malware sofisticado y técnicas de evasión, en tiempo real, mejorando la visibilidad de posibles incidentes de seguridad.
- Mejorar la capacidad de monitoreo en tiempo real de los servidores del Ministerio, proporcionando información detallada sobre las actividades, transacciones y comportamientos en la red que podrían indicar incidentes de seguridad.
- Fortalecer la prevención de ataques cibernéticos: Integrar la solución XDR con las herramientas y políticas de seguridad existentes para automatizar la detección de vulnerabilidades y prevenir la ejecución de ataques cibernéticos en los servidores del Ministerio, bloqueando accesos no autorizados y actividades maliciosas antes de que puedan comprometer la infraestructura.

V. JUSTIFICACION DE LA NECESIDAD DE LA CONTRATACION

La suscripción de licencias de software de detección y respuesta extendida (XDR) es necesaria para fortalecer la seguridad de los servidores del Ministerio de Relaciones Exteriores frente a amenazas cibernéticas avanzadas. Esta herramienta permitirá mejorar la detección, prevención y respuesta en tiempo real, integrando múltiples fuentes de datos y automatizando la gestión de incidentes.

Dada la naturaleza sensible de la información diplomática que maneja el Ministerio, una brecha de seguridad representaría un alto riesgo institucional, operativo y reputacional. La solución XDR aumentará la visibilidad sobre la infraestructura tecnológica, reducirá los tiempos de respuesta ante ataques y asegurará el cumplimiento de estándares y normativas de seguridad de la información, garantizando la protección de los activos críticos del Estado.

VI. DESCRIPCIÓN GENERAL DEL REQUERIMIENTO

6.1. Descripción general

Los servicios solicitados son los siguientes:

Ítem	Descripción del servicio	Cantidad	Unidad de medida
1	**Servicio de suscripción de Licencias de Software de Detección y Respuesta Extendida para los Servidores Virtuales del Ministerio De Relaciones Exteriores**	200	Suscripciones

6.2. Términos de referencia de los servicios

La presente contratación comprende lo siguiente:

a) Contar con el servicio de suscripción de 200 licencias de software de detección y respuesta extendida (XDR) para servidores, que deberá contar con la versión más reciente y liberada por el fabricante, según las Características Técnicas Mínimas. Esta solución debe proporcionar protección avanzada en servidores, incluyendo detección, análisis, respuesta automatizada ante amenazas y protección extendida a través de todos los vectores de ataque asociados a los servidores.

b) La solución de detección y respuesta extendida (XDR) debe ser desarrollada por un único fabricante, que ofrezca una plataforma unificada que permita la detección, análisis y respuesta ante amenazas, sin requerir soluciones de múltiples fabricantes. Esto garantiza una gestión coordinada y una detección más eficiente de ataques avanzados, eliminando las brechas entre los diferentes puntos de seguridad en los servidores.

6.2.1. Características técnicas mínimas del Servicio

6.2.1.1. Consola de Administración Centralizada

- La solución de detección y respuesta extendida (XDR) debe ser de un solo fabricante, asegurando que todos los componentes de la plataforma estén completamente integrados para ofrecer una detección y respuesta de amenazas optimizada en servidores. No se aceptarán soluciones de múltiples fabricantes, ya que la interoperabilidad podría comprometer la efectividad del sistema.
- La consola de administración de la solución de detección y respuesta extendida (XDR) debe permitir la implementación, configuración y administración remota de la solución de detección y respuesta extendida (XDR) instalada en servidores físicos y virtuales, tanto en sistemas

operativos Windows como Linux, proporcionando protección avanzada en toda la infraestructura de servidores de la organización.

- La consola de administración de la solución de detección y respuesta extendida (XDR) debe permitir gestionar políticas de seguridad avanzadas, monitorizar en tiempo real los servidores en busca de amenazas sofisticadas, y realizar tareas de actualización y remediación de acuerdo con una jerarquía de administración predefinida, asegurando que todos los servidores estén protegidos.

- La consola de administración de la solución de detección y respuesta extendida (XDR) debe permitir la colocación de objetos maliciosos detectados (como archivos infectados o actividades sospechosas) en cuarentena, dejando solo a los administradores como usuarios con acceso para visualizar y gestionar estos objetos, lo cual incrementa la seguridad en los servidores.

- La solución de detección y respuesta extendida (XDR) debe integrarse con **Active Directory** para permitir una gestión centralizada de usuarios y dispositivos en servidores, aplicando políticas de seguridad específicas basadas en roles o perfiles dentro de la infraestructura tecnológica de los servidores.

- La consola de administración de la solución de detección y respuesta extendida (XDR)debe permitir la creación de informes detallados de incidentes de seguridad en servidores, incluyendo análisis forense completo, lecciones aprendidas y ofrecer la opción de exportarlos en formatos como PDF, CSV y/o HTML, para facilitar la toma de decisiones y la auditoría.

    - **Reportes de Malware**: Incluyendo el análisis detallado de cualquier amenaza de malware detectada en los servidores, la fuente, la actividad del malware y las acciones tomadas.

    - **Reportes de Virus**: Que incluyan detalles de las Detecciones de virus en servidores, su propagación y las intervenciones para mitigar los efectos.
    - **Reportes de Servidores Más Afectados**: Detalles sobre los servidores más infectados, el nivel de daño o la actividad sospechosa en cada uno de ellos, permitiendo a los administradores priorizar las acciones de remediación.
    - **Reportes de Incidentes de Seguridad**: Detalle de los incidentes de seguridad en los servidores, incluyendo las amenazas detectadas, la respuesta tomada, el impacto en la infraestructura y el tiempo de resolución. Este reporte debe ser completo y permitir un análisis forense exhaustivo.
    - **Reportes de Actividad en Red**: Información sobre los accesos, intentos de intrusión, escaneos y otras actividades en la red que puedan haber afectado a los servidores.
    - **Reportes de Integridad del Sistema**: Incluye un análisis detallado sobre la integridad del sistema, incluyendo la verificación de parches aplicados, la seguridad del software y la validación de configuraciones de los servidores.
    - **Reportes de Detalle de Alertas**: Desgloses de todas las alertas generadas por el sistema de seguridad en los servidores, indicando la gravedad, la causa y las acciones que se tomaron.
    - **Reportes de Actividad de Respuesta**: Detalles sobre las acciones automáticas de respuesta realizadas por la solución **De Detección Y Respuesta Extendida (XDR)**, como la cuarentena de archivos, la eliminación de malware o la contención de incidentes.

- La consola de administración de la solución de detección y respuesta extendida (XDR)debe permitir la creación de múltiples perfiles de configuración y políticas de escaneo de amenazas avanzadas, que se adapten específicamente a los servidores, para optimizar la seguridad sin comprometer el rendimiento.

- La consola de administración de la solución de detección y respuesta extendida (XDR) debe ser capaz de gestionar y priorizar alertas de seguridad ante incidentes que afecten a los servidores, permitiendo delegar tareas y crear usuarios con perfiles de acceso específicos para garantizar que las funciones de administración se asignen correctamente según el nivel de acceso.

- La consola de administración de la solución de detección y respuesta extendida (XDR)debe generar alertas automáticas y notificaciones cuando se detecten incidentes de seguridad en los servidores, enviando mensajes por correo electrónico de modo que los administradores puedan tomar decisiones rápidas y efectivas.

- La solución de detección y respuesta extendida (XDR) debe permitir configurar reglas de la automatización que permitan ejecutar una acción determinada en los endpoints en base a condiciones de alertas de seguridad, incluyendo la contención de amenazas, aislar el servidor, hacer un escaneo de malware, extraer el malware de los servidores, sin intervención manual.

- La consola de administración de la solución de detección y respuesta extendida (XDR) debe ofrecer visibilidad en tiempo real de la red, mostrando servidores conectados, afectados por amenazas y las acciones tomadas en respuesta a incidentes. Además, debe permitir la creación de políticas de respuesta específicas ante incidentes de seguridad en los servidores, para aplicar medidas correctivas de forma ágil y adecuada.

- La solución de detección y respuesta extendida (XDR) debe ser capaz de realizar escaneos avanzados en tiempo real de los servidores y la red en busca de amenazas, proporcionando visibilidad completa sobre los servidores conectados y las actividades sospechosas que puedan haber pasado desapercibidas por otras soluciones.

- La consola de administración de la solución de detección y respuesta extendida (XDR)debe permitir la creación de un paquete de instalación consolidado (archivo ejecutable) accesible por correo electrónico o web, para facilitar la instalación remota de la solución de detección y respuesta extendida (XDR) en nuevos servidores o en aquellos que hayan sido restaurados tras una vulneración.

- La consola de administración de la solución de detección y respuesta extendida (XDR)debe contar con un **log de eventos detallados** de todas las actividades de la solución de detección y respuesta extendida (XDR) en los servidores, permitiendo un seguimiento exhaustivo de cada acción tomada, lo cual es esencial para auditorías y análisis forenses post-incidente.

- La solución de detección y respuesta extendida (XDR) debe permitir la delegación de tareas de administración de servidores, mediante la creación de usuarios con diferentes perfiles y niveles de acceso (lectura, modificación, ejecución, denegación), para garantizar que las tareas de administración sean realizadas solo por personal autorizado.

- La consola de la solución de detección y respuesta extendida (XDR) debe contar con la capacidad de bloquear el acceso a la consola de gestión a los usuarios no autorizados

- La consola de la solución de detección y respuesta extendida (XDR) debe permitir la **generación de reportes gráficos** personalizados y detallados sobre incidentes de seguridad en servidores, actividad de malware, y otros parámetros relevantes para los servidores. Los reportes deben poder ser exportados en formatos como PDF, CSV y/o HTML.

- La solución de detección y respuesta extendida (XDR) debe generar **alertas específicas** ante eventos de seguridad importantes en servidores, enviando correos electrónicos para mantener informados a los administradores sobre cualquier incidente crítico.

- La comunicación entre los servidores y la consola debe ser **encriptada** usando protocolos seguros como HTTPS, TLS, y certificados digitales provistos por el fabricante, asegurando la integridad y la confidencialidad de la información en los servidores.

- La solución de detección y respuesta extendida (XDR) debe permitir la programación de escaneos periódicos de malware y amenazas en servidores, con la capacidad de seleccionar servidores específicos o grupos de servidores y personalizar la frecuencia y el tipo de escaneo según las necesidades del administrador.

- La solución de detección y respuesta extendida (XDR) debe permitir que los mensajes y alertas generadas por el agente deben estar en español o permitir su edición, asegurando que todos los administradores y operadores de seguridad en la organización puedan entender y reaccionar apropiadamente.

- La solución de la solución de detección y respuesta extendida (XDR)debe ser capaz de detectar automáticamente los IOC (Indicadores de Compromiso) asociados a posibles incidentes de seguridad en los servidores. Esto incluye, pero no se limita a:

    - Direcciones IP maliciosas.
    - Hashes de archivos maliciosos.
    - URLs de phishing o de malware.
    - Dominios comprometidos.

- La consola de la solución de detección y respuesta extendida (XDR) de administración debe permitir la extracción de IOC de los eventos de seguridad y la capacidad de añadir nuevos IOC de manera manual o automática.

- La plataforma de la solución de detección y respuesta extendida (XDR) debe poder integrar IOC de manera sencilla y eficiente en su sistema, garantizando que las alertas de seguridad sean lo más precisas posibles.

- la solución de detección y respuesta extendida (XDR)debe ser capaz de identificar BIOC (Behavioral Indicators of Compromise) en los servidores. Los BIOC son patrones de comportamiento anómalos que pueden indicar un compromiso, incluso si no se han detectado IOC tradicionales. Los BIOC incluyen:

    - Actividades de movimiento lateral dentro de la infraestructura de los servidores.
    - Elevación de privilegios no autorizada.
    - Ejecución de procesos maliciosos o desconocidos en los servidores.
    - Conexiones de red no habituales o inesperadas desde servidores internos a servidores externos.
    - Acceso no autorizado a recursos sensibles, como bases de datos o archivos críticos.

- La solución de detección y respuesta extendida (XDR)debe correlacionar las actividades de BIOC con otras señales de alerta, para proporcionar una visibilidad integral sobre comportamientos anómalos que puedan estar relacionados con un compromiso en curso. Los BIOC ayudan a identificar intrusiones de forma temprana, incluso cuando los IOC aún no son identificados o si los atacantes emplean técnicas para evadir la detección.

- La solución de detección y respuesta extendida (XDR) debe ser capaz de combinar los IOC y BIOC en las políticas de respuesta automatizada. Si se detectan IOC o comportamientos relacionados con BIOC, el sistema debe activar acciones automáticas como:

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.B.
REPÚBLICA DEL PERÚ - Oficina de la Unidad de Redes e Infraestructura - Ministerio de Relaciones Exteriores - Y.G.S.C.
REPÚBLICA DEL PERÚ - Oficina de Tecnologías de la Información - Ministerio de Relaciones Exteriores - E.M.B.V.

- La contención de la amenaza detectada en el servidor afectado, por ejemplo, bloqueando conexiones de red maliciosas o deshabilitando procesos comprometidos.
- La aislación del servidor afectado para evitar la propagación de la amenaza.

Licencia de Software de Detección y Respuesta Extendida

- La licencia del software de Detección Y Respuesta Extendida debe ser instalada en servidores que utilicen los sistemas operativos Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows Server 2008 y Linux. Debe ser compatible tanto con versiones de 32 bits como de 64 bits.

- La licencia del software de Detección Y Respuesta Extendida debe ser capaz de realizar una detección avanzada de amenazas utilizando múltiples técnicas de análisis, incluyendo la detección basada en comportamientos, el análisis de patrones y la correlación de eventos entre diferentes endpoints y servidores, para identificar posibles ataques en tiempo real.

- La licencia del software de Detección Y Respuesta Extendida debe ser capaz de detectar y eliminar de manera continua y en tiempo real amenazas como ransomware, virus, gusanos, troyanos, rootkits, adware, spyware, y bots. Debe aplicar técnicas de análisis dinámico y estático para detectar malware, incluso aquellos que no se encuentran en las bases de datos de firmas tradicionales.

- La licencia del software de Detección Y Respuesta Extendida debe permitir la detección de amenazas a nivel de servidor, realizando un análisis completo de todos los archivos, tanto residentes en memoria como comprimidos (RAR, ZIP, CAB, ARJ, ARZ), ocultos y ejecutables.

- La licencia del software de Detección Y Respuesta Extendida debe incluir un módulo que ofrezca visibilidad total de las actividades del servidor, permitiendo detectar comportamientos inusuales o intentos de explotación, y aplicar medidas automáticas de respuesta ante amenazas, como la cuarentena o la eliminación.

- La licencia del software de Detección Y Respuesta Extendida debe ser capaz de revisar y proteger claves específicas del registro de los servidores (regedit), previniendo modificaciones no autorizadas, y debe permitir la configuración de políticas específicas para cada servidor según sus características y funciones.

- La licencia del software de Detección Y Respuesta Extendida debe supervisar continuamente las actividades del servidor, proporcionando visibilidad sobre todos los procesos que se ejecutan en tiempo real. Debe identificar cualquier intento de manipulación, acceso no autorizado o explotación de vulnerabilidades críticas.

- La licencia del software de Detección Y Respuesta Extendida debe permitir la creación de exclusiones de escaneo a nivel de servidor para optimizar el rendimiento sin comprometer la seguridad, permitiendo excluir archivos, directorios o aplicaciones específicas cuando sea necesario.

- La licencia del software de Detección Y Respuesta Extendida debe contar con capacidades de análisis y remediación avanzada que permitan detectar malware que intente ocultarse en macros o archivos dentro de aplicaciones de productividad como Microsoft Office, ofreciendo protección sin afectar el funcionamiento de estas aplicaciones en los servidores.

- La licencia del software de Detección Y Respuesta Extendida debe incluir una tecnología avanzada para la desinfección de archivos en los servidores, permitiendo la eliminación de virus y malware sin comprometer la integridad de los sistemas y aplicaciones.

- La licencia del software de Detección Y Respuesta Extendida debe incluir un módulo de cuarentena que permita gestionar archivos que han sido identificados como potencialmente maliciosos, permitiendo restaurar o eliminar archivos desde una consola centralizada o desde el servidor mismo, según corresponda.

- La licencia del software de Detección Y Respuesta Extendida debe proteger la configuración del agente de seguridad del servidor, evitando modificaciones no autorizadas de la configuración, ya sea por parte de usuarios o administradores locales, y debe permitir la gestión mediante contraseñas para cambios críticos en las configuraciones del sistema.

- La licencia del software de Detección Y Respuesta Extendida debe incluir mecanismos para bloquear la manipulación de la configuración del agente de seguridad, desactivando módulos de protección y evitando la desinstalación no autorizada del software.

- La licencia del software de Detección Y Respuesta Extendida debe incluir funcionalidades de optimización del escaneo en servidores de producción, garantizando que la seguridad no interfiera con el rendimiento operativo del servidor, manteniendo un equilibrio entre protección y eficiencia.

- La licencia del software de Detección Y Respuesta Extendida debe garantizar que los agentes de seguridad de los servidores no puedan ser reconfigurados, deshabilitados o desinstalados sin la debida autorización del administrador. Esto debe incluir la implementación de contraseñas de protección para cambios críticos.

- La licencia del software de Detección Y Respuesta Extendida debe ofrecer capacidades avanzadas para la detección de indicadores de compromiso (IOC), tanto internos como provenientes de fuentes externas, permitiendo la creación y extracción de IOC, y su adición a las políticas de seguridad del sistema para mejorar la detección de amenazas avanzadas.

- La licencia del software de Detección Y Respuesta Extendida debe ser capaz de realizar la detección de BIOC (Behavioral Indicators of Compromise), permitiendo identificar patrones y comportamientos anómalos en el servidor que puedan ser indicativos de un ataque avanzado, sin depender únicamente de las firmas de virus tradicionales.

- La licencia del software de Detección Y Respuesta Extendida debe contar con un firewall a nivel de host que permita gestionar y controlar el tráfico entrante y saliente directamente en el dispositivo, ofreciendo la capacidad de permitir o denegar el tráfico según políticas específicas, sin depender de equipos de protección de red, mejorando la seguridad a nivel de endpoint.

6.2.1.2. Detección y Respuesta Avanzada

- Análisis en Tiempo Real: Monitoreo continuo de actividades en servidores para identificar comportamientos sospechosos o anomalías.

- Correlación de Eventos: Integración y análisis de datos de múltiples fuentes para detectar patrones de amenazas complejas.

- Inteligencia Artificial y Machine Learning: Uso de algoritmos avanzados para predecir y detectar amenazas desconocidas o ataques sofisticados.

6.2.1.3. Prevención de Amenazas

- Protección contra Exploits: Prevención de vulnerabilidades conocidas y desconocidas en aplicaciones y sistemas operativos.

- Control de Aplicaciones: Restricción de ejecución de software no autorizado o malicioso en servidores.

- Protección de Procesos: Monitoreo y bloqueo de actividades maliciosas a nivel de procesos y servicios.

6.2.1.4. Investigación y Análisis Forense

- Registros Detallados: Recopilación y almacenamiento de telemetria completos para facilitar la investigación de incidentes.
- Visualización de Amenazas: Herramientas gráficas para entender el alcance y origen de un ataque.
- Automatización de Investigaciones: Asistencia automatizada para identificar la causa raíz de un incidente de seguridad.
- **Capacidades de Respuesta**Respuesta Automatizada: Ejecución de acciones predefinidas para contener y remediar amenazas detectadas.
- Integración con Herramientas Externas: Compatibilidad con SIEMs, firewalls, y otras soluciones de seguridad para una respuesta coordinada.
- Playbooks Personalizables: Creación de flujos de trabajo automatizados adaptados a las necesidades del entorno.

6.2.1.5. Gestión Centralizada

- Consola Unificada: Interfaz central para monitorear y gestionar la seguridad de todos los servidores.
- Políticas de Seguridad Configurables: Definición y aplicación de políticas específicas para diferentes entornos o cargas de trabajo.
- Reportes y Dashboards: Generación de informes detallados y visualizaciones para evaluar el estado de seguridad.

6.2.1.6. Protección de Datos y Cumplimiento

- Detección de Fugas de Información: Identificación de actividades sospechosas que puedan comprometer datos sensibles.
- Cumplimiento Normativo: Herramientas para asegurar el cumplimiento de regulaciones como GDPR, HIPAA, PCI-DSS, entre otras.
- Encriptación y Seguridad de Datos: Protección de información crítica almacenada o transmitida desde servidores.

6.2.1.7. Escalabilidad y Rendimiento

- Arquitectura Escalable: Capacidad para adaptarse a entornos de gran tamaño o de alta demanda.
- Bajo Impacto en Rendimiento: Operación eficiente sin afectar significativamente el desempeño de los servidores.
- Soporte para Entornos Híbridos y en la Nube: Compatibilidad con servidores físicos, virtuales y en la nube.

Descripción de la instalación, implementación y configuración

- El contratista deberá activar la licencia, dar acceso a la consola de administración, acceso al portal de soporte del fabricante al personal de OTI designado con plazo de hasta los siete (07) días calendario, contabilizados a partir del día siguiente de notificada la Orden de Servicio. Deberá

hacer entrega de los códigos de licenciamiento al correo electrónico ciberseguridad@rree.gob.pe, asimismo deberá indicar el enlace de descarga oficial del software instalador.

- La instalación, implementación y configuración de la licencia de software De Detección Y Respuesta Extendida se efectuará en la ubicación indicada por el Ministerio de Relaciones Exteriores, en los servidores virtuales.

- La licencia de software De Detección Y Respuesta Extendida ofertada incluirá la configuración de la consola de administración hasta su completa operatividad.

- La instalación, implementación y configuración de la licencia de software De Detección Y Respuesta Extendida ofertada, se realizará sin afectar las labores normales de la institución y sin interrumpir la normal provisión de los servicios que brinda el Ministerio de Relaciones Exteriores, para lo cual se deberá coordinar previamente con el personal de la Oficina de Tecnologías de la Información.

- Culminada la instalación, implementación y configuración de las licencias de software De Detección Y Respuesta Extendida, se deberá suscribir el Acta de Activación de las Licencias de software De Detección Y Respuesta Extendida, entre un representante del Contratista y de la Oficina de Tecnologías de la Información.

6.2.2. Otras condiciones adicionales

- El contratista deberá cumplir con lo indicado en el Termino de Referencia. ***Para tal caso, las características 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.***

6.2.3. Soporte Técnico

- El contratista debe brindar el soporte técnico por trescientos sesenta y cinco (365) días calendario, considerando lo siguiente:

  Brindar soporte técnico durante el periodo de suscripción de las licencias, y de acuerdo con las siguientes características:
  - La atención de incidentes referentes a la operatividad de la solución y actualizaciones de esta deberá realizarse mediante una línea 0800 24x7.
  - El tiempo de atención de incidentes deberá ser resuelto dentro de las 48 horas, contabilizados a partir de que el Ministerio de Relaciones Exteriores reporte la incidencia al contratista.
  - EL contratista priorizará la atención y solución de los requerimientos reportados por Ministerio de Relaciones Exteriores.

- A continuación, los medios de comunicación oficial para el registro de requerimientos deben ser los siguientes:
  - Sistema de tickets vía web y/o teléfono y/o correo electrónico

6.2.4. Capacitación

- El contratista tendrá como plazo máximo, sesenta (60) días calendarios contabilizados a partir del día siguiente de notificada la Orden de Servicio, para realizar la capacitación oficial en el uso de la solución ofertada para la investigación y respuesta (EDU-262), sobre el software de detección y respuesta (XDR),
- La capacitación se realizará de manera virtual en idioma español para 1 persona de la Oficina de Tecnologías de la Información.
- El contratista deberá entregar una constancia de capacitación para la persona capacitada.

REPÚBLICA DEL PERÚ - Ministerio de Relaciones Exteriores - Y.G.G.G.
REPÚBLICA DEL PERÚ - Ministerio de Relaciones Exteriores - R.R.B.
REPÚBLICA DEL PERÚ - Ministerio de Relaciones Exteriores - Y.G.C.
REPÚBLICA DEL PERÚ - Ministerio de Relaciones Exteriores - E.M.B.V.

- El horario y modalidad (virtual) de la capacitación, se deberá realizar en coordinación con la Oficina de Tecnologías de la Información.

VII. CRONOGRAMA DEL SERVICIO

ETAPA	PLAZO
La instalación, implementación y configuración de las licencias de software de Detección y Respuesta Extendida.	Siete (7) días calendario contabilizados a partir del día siguiente de notificada la Orden de Servicio.
Capacitación	Sesenta (60) días calendario, contabilizados a partir del día siguiente de notificada la Orden de Servicio.
Ejecución del servicio: Suscripción de las licencias de software	Trescientos sesenta y cinco (365) días calendario contabilizados a partir de la suscripción del Acta de Activación de las Licencias de software de Detección y Respuesta Extendida

VIII. REQUISITOS DEL PROVEEDOR

8.1. Del proveedor

a. 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.

Acreditación:
Copia simple la Certificación y/o carta expedida por el Fabricante de la Licencia de software de Detección y Respuesta Extendida ofertada.

El *proveedor debe contar con el Registro Único de Contribuyente (RUC) activo y habido (**) Debe contar con Registro Nacional de Proveedores vigente, salvo en aquellas contrataciones cuyo monto sea igual o menor a una (1) UIT) (***).*
(**) (***) El RUC y RNP se deberá acreditarse con copia simple.

b. **Experiencia del proveedor:** El proveedor 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, durante los ocho (8) años anteriores a la fecha de la presentación de cotizaciones que se computan desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

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 del proveedor 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 (sello colocado por el cliente del proveedor), correspondientes a un máximo de veinte (20) contrataciones.

La documentación que acredite el cumplimiento del perfil del proveedor (documento de distribuidor autorizado, RUC, RNP y experiencia) será presentada junto a cotización.

8.2. Personal clave:

8.2.1. Un (01) Consultor en Ciberseguridad

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.

Acreditación:
Copia del Título Profesional o copia del Grado de Bachiller

b) Experiencia académica

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.

Acreditación:
Copia de: constancias y/o certificados y/o cualquier otra documentación que, de manera fehaciente demuestre la experiencia requerida.

c) Certificación

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

Acreditación:
Copia de la certificación.

La documentación que acredite el cumplimiento del perfil 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 no deberá divulgar, revelar, entregar o poner a disposición de terceros, dentro o fuera de la entidad, salvo autorización expresa de la misma, la información proporcionada por esta, para la prestación y en general toda la información a la que tenga acceso o la que pudiera producir con ocasión de la prestación, durante y después de concluida la vigencia del presente documento. Dicha información puede consistir en fotografías, informes, material videográfico, documentos y otros similares.

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 Tecnologías de la Información 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 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. Medidas de control durante la ejecución contractual

a) **Áreas que coordinarán con el proveedor:** Unidad de Redes e Infraestructura, Oficina de Logística, Oficina de Tecnologías de la Información.

b) **Área responsable de las medidas de control:** Oficina de Tecnologías de la Información, a través del Oficial de Seguridad y Confianza Digital.

9.9. Modalidad de pago

Suma alzada

X. GARANTÍA POR PAGO ANTICIPADO

No aplica

XI. LUGAR Y PLAZO DE PRESTACIÓN DEL SERVICIO

11.1. Lugar de prestación del servicio:

El servicio se ejecutará en el Centro de Datos del Ministerio de Relaciones Exteriores, sito en Jr. Ucayali N° 337, distrito, provincia y departamento de Lima.

La capacitación se realizará en modalidad virtual según lo establecido en el numeral 6.2.4. Capacitación

11.2. Plazo de prestación del servicio:

11.2.1. De la instalación, implementación, configuración y capacitación

La instalación, implementación y configuración de las licencias de software de Detección y Respuesta Extendida deberá realizarse en el plazo de siete (7) días calendario contabilizados a partir del día siguiente de notificada la Orden de Servicio.

La capacitación deberá realizarse en el plazo de sesenta (60) días calendario, contabilizados a partir del día siguiente de notificada la Orden de Servicio.

11.2.2. Del plazo de suscripción de las licencias de software

La suscripción de las licencias, tendrán una vigencia de **trescientos sesenta y cinco (365) días calendario, 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 Tecnologías de la Información.

XII. ENTREGABLE

12.1.1. Un 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 Tecnologías de la Información, en el plazo de siete (07) días calendarios, contabilizados a partir del día siguiente de ejecutada la instalación, implementación, configuración de las licencias de software ofertado.

El entregable deberá considerar lo siguiente:

- Informe respecto a la instalación, implementación y configuración de la solución.
- Acta de Activación de las Licencias de software de Detección y Respuesta Extendida.

- Documento 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.

12.1.2. Un informe de la capacitación brindada

El contratista deberá presentar vía Mesa de Partes del Ministerio de Relaciones Exteriores, un (1) Informe Técnico dirigido a la Oficina de Tecnologías de la Información, en el plazo de siete (07) días calendarios, contabilizados a partir del día siguiente de culminada la capacitación indicada en el apartado 6.2.4. de capacitación.

El entregable deberá considerar lo siguiente:

- Constancia de capacitación sobre el curso descrito en el apartado 6.2.4. capacitación

NOTA IMPORTANTE:

El acceso a Mesa de Partes de la Entidad es en la siguiente dirección: https://www.gob.pe/20416-acceder-a-mesa-de-partes?child=27623 la cual está habilitada las veinticuatro (24) horas del día y los siete (7) días de la semana o Mesa de Partes de forma presencial en la dirección: Jr. Lampa 545, Lima, en el horario de 08:30 a 16:30 horas.

Respecto a la mesa de partes digital; Se debe precisar que los documentos presentados entre las 00:00 horas y las 16:30 horas de un día hábil, se considerará presentados en el mismo día hábil. La presentación fuera del horario antes señalado se considerará presentados en el día y hora hábil siguiente. El entregable deberá ser dirigido a la Oficina de Tecnologías de la Información.

La presentación fuera del horario antes señalado se considerará presentados en el día y hora hábil siguiente.

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 Oficina de Tecnologías de la Información, previo informe del personal de seguridad de la información con el visto bueno de la Unidad de Redes e Infraestructura 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

[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.

XV. FORMA Y CONDICIONES DE PAGO

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en SOLES según el siguiente detalle, 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.

Entregables	% pago
1. Informe de instalación, implementación y configuración de la solución, según numeral 12.1.1. del presente TDR.	90% del monto de la Orden de Servicio
2. Informe de la capacitación brindada al personal indicado en el apartado según numeral 12.1.2. del presente TDR.	10% del monto de la Orden de Servicio

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 Tecnologías de la Información emitiendo la conformidad de la prestación efectuada, previo informe del personal de seguridad de la información con el visto bueno de la Unidad de Redes e Infraestructura.
- 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.

Salvo los documentos de conformidad, el contratista debe presentar la documentación restante en la Mesa de Partes de la Entidad a la siguiente dirección: https://www.gob.pe/20416-acceder-a-mesa-de-partes?child=27623 la cual está habilitada las veinticuatro (24) horas del día y los siete (7) días de la semana o Mesa de Partes de forma presencial en la dirección: Jr. Lampa 545, Lima, en el horario de 08:30 a 16:30 horas.

Respecto a la mesa de partes digital; Se debe precisar que los documentos presentados entre las 00:00 horas y las 16:30 horas de un día hábil, se considerará presentados en el mismo día hábil. La presentación fuera del horario antes señalado se considerará presentados en el día y hora hábil siguiente. Los entregables deberán ser dirigidos a la Oficina de Tecnologías de la Información.

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.

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

REPÚBLICA DEL PERÚ - Oficial de Seguridad de la Información - Y.E.G.G. - Ministerio de Relaciones Exteriores

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

REPÚBLICA DEL PERÚ - Jefe de la Unidad de Redes e Infraestructura - Y.G.S.C. - Ministerio de Relaciones Exteriores

REPÚBLICA DEL PERÚ - Oficina de Tecnologías de la Información - E.M.B.V. - Ministerio de Relaciones Exteriores

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

a) Caso fortuito o fuerza mayor que imposibilite la continuación del contrato.
b) 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.
c) Por incumplimiento de la cláusula anticorrupción.
d) Por la presentación de documentación falsa o inexacta durante la ejecución contractual.
e) 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 debe exceder el 10% del monto vigente del contrato o, de ser el caso, del ítem correspondiente.

18.1. Penalidad por mora

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:

  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.

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

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.

REPÚBLICA DEL PERÚ - Ministerio de Relaciones Exteriores - Y.E.G.G.
REPÚBLICA DEL PERÚ - Oficial de Seguridad y Confianza Digital - Ministerio de Relaciones Exteriores - R.R.B.
REPÚBLICA DEL PERÚ - Ministerio de Relaciones Exteriores - Y.G.S.C.
REPÚBLICA DEL PERÚ - Ministerio de Relaciones Exteriores - E.M.B.V.

18.2. Otras penalidades

Adicionalmente a la penalidad por mora, se aplican las siguientes penalidades:

Otras penalidades			
N°	***Supuestos de aplicación de penalidad***	***Forma de cálculo***	***Procedimiento de verificación***
1	El Contratista no presente los entregables dentro de los plazos establecidos en el numeral XII.	2% de una (1) UIT por cada día de retraso.	Informe personal de seguridad de la información

UIT: Unidad Impositiva Tributaria.

(Firma digital o manuscrita)

ÁREA USUARIA

Ing. Erick Manuel Bocanegra Villanueva
Jefe de la Oficina de Tecnologías de la Información
Ministerio de Relaciones Exteriores