REQUERIMIENTO

3.1 FINALIDAD PÚBLICA DE LA CONTRATACIÓN

Adquirir de LICENCIAS DE SOFTWARE ANTIVIRUS CON CIBERSEGURIDAD EDR MÁS GESTIÓN DE TI CORPORATIVO, que asegure la protección de los equipos de cómputo, servidores y dispositivos móviles para que disminuya el riesgo de vulnerabilidades que pueda tener la infraestructura de la red causada por malware. De esta manera, evitar que los servicios y funciones que se presta a todos los usuarios no se vea afectados.

3.2 DESCRIPCIÓN GENERAL DEL REQUERIMIENTO

Producto de la adquisición DE LICENCIAS DE SOFTWARE ANTIVIRUS CON CIBERSEGURIDAD EDR MÁS GESTIÓN DE TI CORPORATIVO, se debe contemplar la instalación, configuración, despliegue (masivo y manual), puesta en funcionamiento final con todas las funcionalidades requeridas y un análisis completo de todo el parque informático de la entidad (resolviendo cada casuística que se presenta).

3.3 CONDICIONES DE CONTRATACIÓN

a. MODALIDAD DE PAGO

El contrato se rige por la modalidad de pago Suma Alzada de conformidad con el artículo 130 del Reglamento.

b. SISTEMA DE ENTREGA

NO APLICA.

c. PLAZO DE ENTREGA

Los bienes materia de la presente convocatoria se entregan en el plazo de tres (03) días calendario contabilizados desde el día siguiente de emitida la Orden de Compra (Plazo incluye instalación, funcionamiento y despliegue en todos los equipos de cómputo de la entidad).

d. LUGAR DE ENTREGA DE LOS BIENES

Los bienes materia de la presente convocatoria se entregan en el almacén central del Gobierno Regional de Ucayali sito en el Jr. Mariscal Cáceres N° 795.

e. ADELANTO DIRECTO

NO APLICA.

f. PENALIDADES

PENALIDAD POR MORA:

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la entidad contratante le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable, de conformidad con el artículo 120 del Reglamento. 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 bienes y servicios: F = 0.40

OTRAS PENALIDADES:

NO APLICA.

g. SUBCONTRATACIÓN

Se encuentra prohibida la subcontratación de las prestaciones objeto del contrato.

h. FÓRMULAS DE REAJUSTES

No Aplica.

i. SOLUCIÓN DE CONTROVERSIAS CONTRACTUALES

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación, cuando se haya pactado, y arbitraje.

Para dicho efecto, el postor ganador de la buena pro selecciona a uno de las siguientes Instituciones Arbitrales para administrar el arbitraje:

RUC	RAZON SOCIAL	Ubicación de la sede autorizada conforme a la Licencia Municipal
20609725622	Centro de Arbitraje Comercial Inmobiliario S.A.C.	Huánuco/Huánuco /Huánuco
20426255317	MARC PERÚ Asociación para la Prevención y Solución de Conflictos	Lima/Lima/ Miraflores

j. PLAZO PARA RESPUESTAS ENTRE LAS PARTES

El plazo para la respuesta entre las partes será de 15 días calendarios.

k. RESOLUCIÓN DEL CONTRATO

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 68.1 del artículo 68 de la Ley N° 32069, Ley General de Contrataciones Públicas.
De encontrarse en alguno de los supuestos 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.

l. ANTICORRUPCIÓN Y ANTISOBORNO

EL CONTRATISTA 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 los evaluadores del proceso de contratación 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 presente contrato.

Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, 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, el incumplimiento de la presente cláusula conlleva 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.

3.4 ESPECIFICACIONES TÉCNICAS

Especificaciones Técnicas Mínimas: Los atributos técnicos mínimos que debe cumplir el software requerido se detallan en el cuadro siguiente:

ITEM	LICENCIA DE SOFTWARE ANTIVIRUS CON CIBERSEGURIDAD EDR MÁS GESTIÓN DE TI CORPORATIVO.	CANTIDAD
1	Estaciones de Trabajo, Servidores y dispositivos móviles.	420
	TOTAL	**420**

CARACTERÍSTICAS	DESCRIPCION
CARACTERÍSTICAS TÉCNICAS DEL SERVICIO DE DEFENSA, CONTENCIÓN Y PREVENCIÓN CIBERNÉTICA	La licencia de antivirus deberá contar con múltiples barreras cibernéticas para garantizar una protección integral contra amenazas avanzadas. Las soluciones deben estar diseñadas para ofrecer detección, prevención, contención y respuesta ante ciberataques en tiempo real, incorporando tecnologías avanzadas basadas en inteligencia artificial, análisis de comportamiento y seguridad proactiva. A continuación, se detallan las barreras cibernéticas requeridos en la solución: **Protección contra Malware y Código Malicioso** ▪ Motor de detección de amenazas basado en inteligencia artificial y análisis heurístico: El sistema debe identificar, analizar y bloquear malware conocido y desconocido sin depender exclusivamente de firmas tradicionales. ▪ Análisis de archivos en tiempo real: Identificación de software malicioso mediante un escaneo continuo en todos los dispositivos protegidos. ▪ Monitoreo de comportamiento de procesos: Prevención contra amenazas de día cero mediante la detección de patrones sospechosos en aplicaciones y archivos ejecutables. **Cortafuegos de Seguridad (Firewall Avanzado)** ▪ Control de tráfico de red bidireccional: Protección contra accesos no autorizados mediante el filtrado de tráfico entrante y saliente. ▪ Reglas de seguridad personalizables: Configuración de políticas para restringir o permitir conexiones según el nivel de confianza de las aplicaciones o redes. ▪ Prevención contra ataques de red: Bloqueo automático de intentos de explotación de vulnerabilidades y tráfico malicioso.

Sistema de Prevención de Intrusiones

- Detección de cambios no autorizados en el sistema: Supervisión en tiempo real de modificaciones en archivos críticos, registros y procesos del sistema operativo.
- Bloqueo de ejecución de código malicioso: Protección contra amenazas que intentan manipular archivos de sistema o realizar cambios sin permisos.
- Alertas en tiempo real: Notificación inmediata sobre eventos sospechosos para permitir una respuesta rápida.

Detección y Respuesta en Endpoints (EDR – Endpoint Detection & Response)

- Supervisión continua de la actividad del sistema: Captura de eventos detallados para la identificación de incidentes de seguridad.
- Registro de telemetría y trazabilidad de ataques: Capacidad de investigar amenazas con información detallada de eventos pasados.
- Respuesta automatizada ante ataques: Aislamiento de dispositivos afectados para evitar la propagación de amenazas.

Elevación Segura de Archivos y Análisis Avanzado

- Envío automático de archivos sospechosos para evaluación: Todo archivo desconocido debe ser analizado en un entorno seguro antes de permitir su ejecución.
- Verificación en la nube con motores avanzados de seguridad: Análisis dinámico con bases de datos globales para una mejor clasificación de archivos.
- Bloqueo temporal de archivos sospechosos: Restricción de ejecución hasta que se determine su nivel de riesgo.

Contención Automática de Amenazas (Aislamiento de Procesos Maliciosos)

- Ejecución de archivos desconocidos en entornos aislados: Prevención de infecciones mediante el uso de tecnología de virtualización.
- Protección de la integridad del sistema operativo: Evita que amenazas se propaguen a archivos del sistema o realicen cambios permanentes.
- Evaluación segura de archivos y aplicaciones: Determina si un archivo es confiable antes de permitir su ejecución en el entorno real.

Análisis de Comportamiento en Tiempo Real

- Monitorización de actividades de archivos en ejecución: Identificación de comportamientos maliciosos sin necesidad de depender de firmas de virus.
- Detección de cambios sospechosos en memoria y registros: Bloqueo de amenazas que intentan modificar configuraciones clave del sistema.
- Restauración automática de cambios malintencionados: Reversión de modificaciones no autorizadas para mantener la integridad del sistema.

Análisis Avanzado en la Nube

- Evaluación de archivos y procesos en un entorno de análisis global: Comparación de muestras sospechosas con bases de datos de amenazas en la nube.
- Desarrollo de inteligencia de amenazas en tiempo real: Aprendizaje continuo sobre nuevas tácticas utilizadas por atacantes.
- Verificación cruzada con múltiples motores de seguridad: Mayor precisión en la detección y categorización de archivos peligrosos.

Análisis y Control de Scripts Maliciosos

- Bloqueo de scripts ejecutados desde ubicaciones no seguras: Protección contra ataques basados en PowerShell, JavaScript, VBScript y otros lenguajes de automatización.
- Análisis dinámico de ejecución de comandos: Prevención contra ataques fileless y explotación de vulnerabilidades mediante scripts.
- Registro de eventos sospechosos en tiempo real: Generación de alertas para evitar que scripts maliciosos comprometan el sistema.

Control Remoto y Gestión de Incidentes

	▪ Capacidad de acceso remoto para respuesta ante incidentes: Posibilidad de realizar intervenciones en dispositivos comprometidos sin afectar la operación. ▪ Solución de problemas en tiempo real: Administración de endpoints sin necesidad de interacción del usuario. ▪ Soporte centralizado desde una consola unificada: Gestión de incidentes y ejecución de acciones correctivas desde una única plataforma. **Control de Acceso de Usuarios y Permisos** ▪ Restricción de acceso a configuraciones criticas del sistema: Solo usuarios autorizados podrán modificar parámetros clave de seguridad. ▪ Control de privilegios de usuarios: Aplicación de políticas de seguridad basadas en roles dentro de la organización. ▪ Registro de auditoria de accesos y modificaciones: Trazabilidad de todas las acciones realizadas en el sistema. **Control de Dispositivos Externos y USB** ▪ Bloqueo de almacenamiento extraible no autorizado: Prevención de infecciones provenientes de unidades USB o discos externos. ▪ Control de acceso a dispositivos de entrada y salida: Restricción de lectura, escritura o ejecución desde hardware no permitido. ▪ Registro de actividad de dispositivos conectados: Monitoreo del uso de hardware externo en equipos protegidos. **Seguridad de Acceso mediante Control de Contraseñas** ▪ Protección contra ataques de fuerza bruta y robo de credenciales: Detección de intentos de acceso no autorizados. ▪ Políticas de contraseñas seguras: Requisitos de longitud, complejidad y caducidad para fortalecer la seguridad de acceso. ▪ Autenticación de múltiples factores (MFA): Implementación de mecanismos adicionales de validación de identidad.
PROTECCIÓN CONTRA MALWARE Y CÓDIGO MALICIOSO	La solución integral de defensa cibernética debe ▪ Instalarse en estaciones de trabajo en plataformas Windows XP/Vista/7/8, 8.1 y 10, Linux y Mac. ▪ La solución integral de defensa cibernética deberá instalarse en servidores Windows Server 2003, 2008, 2012, 2016, 2019, Linux y Mac. ▪ La solución deberá soportar las versiones de 32 y 64 bits. ▪ Análisis de archivos en tiempo real para detectar y bloquear malware conocido y desconocido. ▪ Monitoreo continuo de procesos en ejecución para identificar actividades sospechosas. ▪ Escaneo heuristico avanzado para detectar amenazas emergentes sin depender de firmas tradicionales. ▪ Detección y bloqueo de ransomware mediante análisis de comportamiento en tiempo real. ▪ Identificación de amenazas de día cero a través de machine learning y análisis predictivo. ▪ Escaneo de archivos comprimidos y encriptados para detectar contenido malicioso oculto. ▪ Protección contra troyanos bancarios mediante análisis de tráfico y comportamiento anómalo. ▪ Bloqueo de exploits y vulnerabilidades utilizadas por malware para comprometer sistemas. ▪ Detección de software espía (spyware) que intenta capturar información del usuario. ▪ Análisis de comportamiento dinámico para evaluar la actividad de archivos en ejecución.

	• Bloqueo automático de archivos sospechosos hasta completar su análisis de seguridad. • Protección contra adware y programas potencialmente no deseados (PUPs). • Escaneo en entornos virtualizados para evitar que el malware detecte análisis automatizados. • Monitoreo de archivos en almacenamiento en la nube para prevenir infecciones en tiempo real. • Protección contra ataques fileless mediante la detección de procesos en memoria sin archivos físicos. • Escaneo programado y bajo demanda para revisar el sistema en momentos específicos. • Actualización automática de bases de datos de amenazas para garantizar la detección de nuevos malware. • Análisis de tráfico HTTP/HTTPS para detectar descargas maliciosas desde la web. • Escaneo de archivos adjuntos en correos electrónicos para evitar la distribución de malware. • Bloqueo de macros maliciosas en documentos que intenten ejecutar código no autorizado. • Protección contra malware persistente que intenta mantenerse activo tras reinicios del sistema. • Identificación de rootkits ocultos mediante técnicas de análisis profundo del sistema. • Escaneo de dispositivos USB y medios extraíbles para detectar amenazas antes de su ejecución. • Monitoreo del registro del sistema para identificar modificaciones sospechosas. • Bloqueo de procesos maliciosos en segundo plano que intenten ejecutarse sin autorización. • Protección contra malware que intenta deshabilitar la seguridad del sistema. • Capacidad de cuarentena automática para aislar archivos maliciosos sin afectar la operación del usuario. • Generación de reportes detallados sobre detecciones, amenazas bloqueadas y acciones correctivas. • Soporte para entornos de múltiples usuarios con configuraciones de seguridad personalizadas. • Protección contra ataques basados en scripts maliciosos como PowerShell y VBScript. • Capacidad de exclusión de archivos y carpetas de análisis según políticas organizacionales. • Prevención de infecciones a través de redes compartidas con monitoreo de actividad sospechosa. • Bloqueo de aplicaciones maliciosas basadas en inteligencia artificial. • Escaneo profundo de sectores de arranque del sistema para detectar malware de bajo nivel. • Protección contra amenazas ocultas en documentos PDF y archivos multimedia. • Monitoreo de claves de registro críticas para prevenir ataques de persistencia. • Detección de intentos de acceso no autorizado a procesos del sistema. • Bloqueo de software que intente modificar archivos críticos del sistema operativo. • Protección contra ataques de criptominería oculta que exploten los recursos del sistema. • Escaneo de archivos grandes sin afectar el rendimiento del sistema. • Respuesta automatizada ante detección de malware con opciones de limpieza y mitigación. • Protección contra ataques de ingeniería social que intenten instalar malware. • Intercepción de intentos de descarga de archivos maliciosos desde navegadores web. • Análisis de múltiples capas para garantizar la detección en diferentes niveles del sistema. • Verificación de procesos y conexiones de red para detectar tráfico malicioso. • Protección contra ataques de inyección de código en procesos legítimos.

	• Monitoreo en la nube para correlacionar amenazas globales en tiempo real. • Bloqueo de ejecución de software no autorizado según políticas de seguridad definidas. • Protección contra malware polimórfico que cambia su código para evadir detección. • Ejecución de archivos sospechosos en un entorno seguro antes de permitir su ejecución real. • Detección de intentos de modificación en archivos del sistema operativo. • Monitoreo de procesos en segundo plano para identificar actividad anormal. • Bloqueo de conexiones a servidores de comando y control (C2) utilizados por malware. • Protección contra técnicas avanzadas de evasión de análisis. • Escaneo en segundo plano sin afectar el rendimiento del usuario. • Actualización de patrones de detección en tiempo real desde una base de datos global. • Desinfección automática de archivos infectados sin necesidad de intervención manual. • Protección contra técnicas de cifrado utilizadas por ransomware. • Bloqueo de procesos que intenten modificar archivos sin autorización. • Escaneo en redes compartidas y dispositivos conectados. • Capacidad de auditoría y trazabilidad de detecciones para reportes de seguridad. • Monitoreo de ejecución de código en la memoria RAM para detectar malware sin archivos. • Protección contra ataques en cadena que combinan múltiples vectores de infección. • Escaneo y bloqueo de amenazas en archivos ejecutables y DLL. • Bloqueo de acceso a servidores maliciosos conocidos. • Capacidad de análisis en múltiples motores de detección para mejorar precisión. • Prevención de ataques que intenten modificar configuraciones de seguridad. • Protección contra malware que explota vulnerabilidades de software desactualizado. • Bloqueo de procesos que intenten ejecutar código arbitrario en el sistema. • Ejecución automática de medidas de mitigación ante la detección de amenazas críticas.
CORTAFUEGOS DE SEGURIDAD (FIREWALL AVANZADO)	La solución integral de defensa cibernética debe realizar: • Monitoreo continuo del tráfico de red entrante y saliente para detectar y bloquear actividades sospechosas. • Aplicación de reglas de filtrado de paquetes para controlar el flujo de datos según políticas de seguridad establecidas. • Inspección profunda de paquetes (DPI) para analizar el contenido de las comunicaciones y detectar amenazas ocultas. • Control de aplicaciones para permitir o bloquear el acceso a la red según la reputación y el comportamiento de las aplicaciones. • Prevención de intrusiones mediante la detección y bloqueo de intentos de explotación de vulnerabilidades conocidas. • Gestión de ancho de banda para priorizar el tráfico crítico y limitar el uso de aplicaciones no esenciales. • Protección contra ataques de denegación de servicio (DoS/DDoS) mediante la identificación y mitigación de patrones de tráfico maliciosos. • Registro detallado de eventos de seguridad para auditoría y análisis forense. • Notificaciones en tiempo real sobre incidentes de seguridad y violaciones de políticas. • Soporte para creación de reglas personalizadas que se ajusten a las necesidades específicas de la organización. • Integración con sistemas de detección y respuesta de endpoints (EDR) para una protección coordinada. • Capacidad de operar en modo de aprendizaje para generar reglas basadas en el comportamiento normal del tráfico.

	▪ Soporte para múltiples zonas de seguridad para segmentar la red y aplicar políticas diferenciadas. ▪ Protección contra suplantación de direcciones IP (spoofing) mediante la verificación de la autenticidad de las fuentes de tráfico. ▪ Control de acceso basado en roles (RBAC) para gestionar permisos de administración del cortafuegos. ▪ Soporte para autenticación de usuarios antes de permitir el acceso a recursos de la red. ▪ Capacidad de inspeccionar y filtrar tráfico cifrado (SSL/TLS) para detectar amenazas ocultas en comunicaciones seguras. ▪ Integración con servicios de inteligencia de amenazas para actualizar dinámicamente las listas de bloqueo. ▪ Soporte para redes privadas virtuales (VPN) para asegurar conexiones remotas. ▪ Detección y prevención de ataques de día cero mediante análisis de comportamiento y firmas emergentes. ▪ Capacidad de bloquear aplicaciones potencialmente no deseadas (PUA) que puedan representar riesgos de seguridad. ▪ Monitoreo de integridad de archivos para detectar cambios no autorizados en archivos críticos del sistema. ▪ Soporte para alta disponibilidad y balanceo de carga para garantizar la continuidad del servicio. ▪ Capacidad de establecer políticas de seguridad basadas en horarios para restringir el acceso en momentos específicos. ▪ Protección contra ataques de intermediario (Man-in-the-Middle) mediante la validación de certificados y autenticación mutua. ▪ Soporte para filtrado de contenido web para bloquear sitios maliciosos o inapropiados. ▪ Capacidad de detectar y bloquear comunicaciones con servidores de comando y control (C2) utilizados por malware. ▪ Integración con soluciones de gestión de eventos e información de seguridad (SIEM) para una correlación avanzada de eventos. ▪ Soporte para actualización automática de firmas y reglas de seguridad para mantener la protección actualizada. ▪ Capacidad de aislar segmentos de la red en caso de detección de amenazas para contener posibles infecciones. ▪ Soporte para autenticación multifactor (MFA) para fortalecer la seguridad de acceso. ▪ Capacidad de generar informes personalizados sobre el estado de la seguridad y el cumplimiento de políticas. ▪ Soporte para análisis de tráfico basado en reputación para bloquear comunicaciones con destinos maliciosos conocidos. ▪ Capacidad de detectar y bloquear intentos de escaneo de puertos que puedan preceder a un ataque. ▪ Soporte para segmentación de red basada en políticas para limitar la propagación de amenazas. ▪ Capacidad de aplicar políticas de seguridad basadas en la ubicación geográfica del tráfico. ▪ Soporte para detección y prevención de ataques de fuerza bruta mediante la limitación de intentos de autenticación fallidos. ▪ Capacidad de bloquear tráfico de redes anónimas o proxies que puedan ocultar actividades maliciosas. ▪ Soporte para análisis de tráfico en tiempo real para una respuesta inmediata a incidentes. ▪ Capacidad de establecer políticas de seguridad basadas en tipos de dispositivos que se conectan a la red. ▪ Soporte para detección de anomalías en el tráfico para identificar comportamientos inusuales. ▪ Capacidad de bloquear aplicaciones que intenten acceder a la red sin autorización.

	• Prevención contra malware de red que intente comunicarse con servidores externos. • Protección contra amenazas internas mediante la detección de tráfico anómalo dentro de la red. • Capacidad de inspeccionar el tráfico de redes Wi-Fi para evitar accesos no autorizados. • Control de tráfico por categorías de aplicaciones para permitir o restringir conexiones según el tipo de software utilizado. • Bloqueo automático de tráfico malicioso detectado por inteligencia de amenazas. • Soporte para restricciones de acceso según políticas corporativas. • Protección contra ataques de explotación de protocolo DNS para evitar secuestros de tráfico. • Soporte para inspección de tráfico FTP, SMTP y POP3 para detectar amenazas ocultas en archivos transferidos. • Protección contra ataques de propagación lateral dentro de la red. • Monitoreo de actividad de dispositivos IoT conectados a la red corporativa. • Bloqueo de tráfico basado en reglas de comportamiento para minimizar falsos positivos. • Prevención de fugas de datos a través de conexiones no autorizadas. • Soporte para detección de actividad de criptominería maliciosa en la red. • Inspección de tráfico en redes IPv6 y compatibilidad con IPv4. • Capacidad de deshabilitar temporalmente reglas de firewall para diagnóstico sin comprometer la seguridad. • Control granular de políticas de firewall para diferentes usuarios o grupos. • Alertas automáticas ante detección de actividad inusual en la red. • Escaneo y bloqueo de tráfico en tiempo real sin afectar el rendimiento del sistema.
SISTEMA DE PREVENCIÓN DE INTRUSIONES EN EL HOST	• La solución integral de defensa cibernética debe realizar monitoreo en tiempo real de procesos del sistema para detectar comportamientos anómalos. • La solución integral de defensa cibernética debe realizar protección de archivos y claves de registro críticos contra modificaciones no autorizadas. • La solución integral de defensa cibernética debe realizar control de integridad de archivos del sistema para identificar alteraciones maliciosas. • La solución integral de defensa cibernética debe realizar detección de intentos de ejecución de código no autorizado en el sistema operativo. • La solución integral de defensa cibernética debe realizar bloqueo de aplicaciones que intenten realizar cambios en áreas sensibles del sistema sin permisos adecuados. • La solución integral de defensa cibernética debe realizar análisis de comportamiento de aplicaciones para identificar actividades sospechosas. • La solución integral de defensa cibernética debe realizar gestión de reglas de seguridad personalizadas para aplicaciones y procesos específicos. • La solución integral de defensa cibernética debe realizar detección de técnicas de evasión utilizadas por malware avanzado. • La solución integral de defensa cibernética debe realizar prevención de inyecciones de código malicioso en procesos legítimos. • La solución integral de defensa cibernética debe realizar control de acceso a recursos del sistema para aplicaciones no confiables. • La solución integral de defensa cibernética debe realizar monitoreo de cambios en el registro del sistema para detectar modificaciones no autorizadas. • La solución integral de defensa cibernética debe realizar bloqueo de scripts maliciosos que intenten ejecutarse sin autorización. • La solución integral de defensa cibernética debe realizar detección de comportamientos anómalos en aplicaciones confiables que puedan indicar una infección. • La solución integral de defensa cibernética debe realizar prevención de escalamiento de privilegios por parte de aplicaciones maliciosas. • La solución integral de defensa cibernética debe realizar control de integridad de módulos de kernel para evitar modificaciones maliciosas.

	• La solución integral de defensa cibernética debe realizar bloqueo de accesos no autorizados a memoria crítica del sistema. • La solución integral de defensa cibernética debe realizar detección de intentos de deshabilitar servicios de seguridad del sistema. • La solución integral de defensa cibernética debe realizar monitoreo de actividades de red para identificar comportamientos sospechosos. • La solución integral de defensa cibernética debe realizar prevención de modificaciones en políticas de seguridad del sistema. • La solución integral de defensa cibernética debe realizar detección de intentos de acceso a archivos protegidos sin autorización. • La solución integral de defensa cibernética debe realizar bloqueo de procesos que intenten ocultarse o evadir la detección. • La solución integral de defensa cibernética debe realizar control de ejecución de aplicaciones basadas en políticas de confianza. • La solución integral de defensa cibernética debe realizar detección de intentos de manipulación de servicios del sistema. • La solución integral de defensa cibernética debe realizar prevención de ataques de desbordamiento de búfer en aplicaciones críticas. • La solución integral de defensa cibernética debe realizar monitoreo de comunicaciones entre procesos para identificar actividades maliciosas. • La solución integral de defensa cibernética debe realizar bloqueo de aplicaciones que intenten modificar configuraciones de seguridad. • La solución integral de defensa cibernética debe realizar detección de intentos de ejecución de código desde áreas restringidas del sistema. • La solución integral de defensa cibernética debe realizar prevención de modificaciones en archivos de sistema protegidos. • La solución integral de defensa cibernética debe realizar monitoreo de actividades de inicio de sesión para detectar comportamientos inusuales. • La solución integral de defensa cibernética debe realizar bloqueo de aplicaciones que intenten acceder a datos sensibles sin autorización. • La solución integral de defensa cibernética debe realizar detección de intentos de deshabilitar componentes críticos del sistema. • La solución integral de defensa cibernética debe realizar prevención de ejecución de aplicaciones desde ubicaciones no confiables. • La solución integral de defensa cibernética debe realizar monitoreo de cambios en permisos de archivos para identificar actividades sospechosas. • La solución integral de defensa cibernética debe realizar bloqueo de procesos que intenten comunicarse con servidores maliciosos. • La solución integral de defensa cibernética debe realizar detección de intentos de modificar configuraciones de red sin autorización. • La solución integral de defensa cibernética debe realizar prevención de ejecución de código malicioso en modo kernel. • La solución integral de defensa cibernética debe realizar monitoreo de actividades de aplicaciones en segundo plano para detectar comportamientos anómalos.
DETECCIÓN Y RESPUESTA EN ENDPOINTS (EDR – ENDPOINT DETECTION & RESPONSE)	• La solución integral de defensa cibernética debe Monitorear continuamente las actividades de los endpoints para detectar comportamientos sospechosos. • La solución integral de defensa cibernética debe Recopilar y analizar datos de eventos en tiempo real para identificar amenazas potenciales. • La solución integral de defensa cibernética debe Proporcionar visibilidad completa de las actividades en todos los endpoints de la red. • La solución integral de defensa cibernética debe Detectar y alertar sobre movimientos laterales dentro de la red. • La solución integral de defensa cibernética debe Identificar y responder a técnicas avanzadas de evasión utilizadas por atacantes. • La solución integral de defensa cibernética debe Generar alertas en tiempo real sobre actividades maliciosas detectadas. • La solución integral de defensa cibernética debe Proporcionar herramientas para la investigación forense de incidentes de seguridad.

	• La solución integral de defensa cibernética debe Permitir la contención y aislamiento de endpoints comprometidos para prevenir la propagación de amenazas. • La solución integral de defensa cibernética debe Ofrecer capacidades de respuesta automatizada para mitigar amenazas de manera eficiente. • La solución integral de defensa cibernética debe Integrarse con inteligencia de amenazas para mejorar la detección y respuesta. • La solución integral de defensa cibernética debe Proporcionar análisis de comportamiento para identificar actividades anómalas. • La solución integral de defensa cibernética debe Facilitar la creación de políticas de seguridad personalizadas para diferentes grupos de endpoints. • La solución integral de defensa cibernética debe Ofrecer capacidades de búsqueda y filtrado de eventos para una investigación eficiente. • La solución integral de defensa cibernética debe Detectar y prevenir ataques de ransomware en los endpoints. • La solución integral de defensa cibernética debe Monitorear y analizar conexiones de red para identificar comunicaciones maliciosas. • La solución integral de defensa cibernética debe Proporcionar informes detallados sobre incidentes de seguridad y tendencias de amenazas. • La solución integral de defensa cibernética debe Ofrecer capacidades de remediación para restaurar sistemas afectados a su estado seguro. • La solución integral de defensa cibernética debe Detectar y bloquear intentos de explotación de vulnerabilidades en los endpoints. • La solución integral de defensa cibernética debe Proporcionar visibilidad de aplicaciones y procesos en ejecución en los endpoints. • La solución integral de defensa cibernética debe Facilitar la gestión de incidentes de seguridad con flujos de trabajo integrados. • La solución integral de defensa cibernética debe Ofrecer capacidades de análisis retrospectivo para identificar amenazas que pasaron desapercibidas. • La solución integral de defensa cibernética debe Integrarse con otras soluciones de seguridad para una defensa coordinada. • La solución integral de defensa cibernética debe Proporcionar alertas priorizadas basadas en el nivel de riesgo de las amenazas detectadas. • La solución integral de defensa cibernética debe Facilitar la creación de listas blancas y negras de aplicaciones y procesos. • La solución integral de defensa cibernética debe Detectar y bloquear intentos de escalamiento de privilegios en los endpoints. • La solución integral de defensa cibernética debe Proporcionar capacidades de análisis de memoria para identificar malware en memoria. • La solución integral de defensa cibernética debe Ofrecer herramientas de análisis de archivos para identificar archivos maliciosos. • La solución integral de defensa cibernética debe Detectar y prevenir ataques basados en scripts en los endpoints. • La solución integral de defensa cibernética debe Proporcionar capacidades de análisis de registros del sistema para identificar actividades sospechosas. • La solución integral de defensa cibernética debe Facilitar la creación de alertas personalizadas basadas en eventos específicos. • La solución integral de defensa cibernética debe Ofrecer capacidades de análisis de tráfico de red para identificar patrones de ataque. • La solución integral de defensa cibernética debe Detectar y bloquear intentos de acceso no autorizado a recursos del sistema. • La solución integral de defensa cibernética debe Proporcionar herramientas para la gestión de vulnerabilidades en los endpoints. • La solución integral de defensa cibernética debe Facilitar la creación de informes de cumplimiento de seguridad para auditorías. • La solución integral de defensa cibernética debe Ofrecer capacidades de análisis de comportamiento de usuarios para detectar actividades sospechosas. • La solución integral de defensa cibernética debe Detectar y prevenir ataques de phishing dirigidos a los endpoints.

	▪ La solución integral de defensa cibernética debe Proporcionar capacidades de análisis de dispositivos USB conectados a los endpoints.
ELEVACIÓN SEGURA DE ARCHIVOS Y ANÁLISIS AVANZADO	▪ La solución integral de defensa cibernética debe Proporcionar un entorno aislado para la ejecución segura de archivos desconocidos. ▪ La solución integral de defensa cibernética debe Analizar el comportamiento de archivos en tiempo real dentro de un contenedor seguro. ▪ La solución integral de defensa cibernética debe Permitir la ejecución de archivos sospechosos sin riesgo para el sistema operativo principal. ▪ La solución integral de defensa cibernética debe Detectar y bloquear actividades maliciosas durante la ejecución de archivos en el entorno aislado. ▪ La solución integral de defensa cibernética debe Ofrecer análisis dinámico de archivos para identificar comportamientos anómalos. ▪ La solución integral de defensa cibernética debe Integrar análisis estático y dinámico para una evaluación completa de archivos. ▪ La solución integral de defensa cibernética debe Proporcionar informes detallados sobre las acciones realizadas por archivos en el entorno aislado. ▪ La solución integral de defensa cibernética debe Permitir la elevación segura de archivos para análisis sin comprometer la seguridad del sistema. ▪ La solución integral de defensa cibernética debe Ofrecer opciones de configuración para definir políticas de elevación de archivos. ▪ La solución integral de defensa cibernética debe Integrar inteligencia de amenazas para mejorar la precisión del análisis de archivos. ▪ La solución integral de defensa cibernética debe Proporcionar capacidades de aprendizaje automático para mejorar la detección de amenazas en archivos. ▪ La solución integral de defensa cibernética debe Permitir la automatización del análisis de archivos basados en políticas predefinidas. ▪ La solución integral de defensa cibernética debe Ofrecer capacidades de análisis forense para archivos ejecutados en el entorno aislado. ▪ La solución integral de defensa cibernética debe Detectar técnicas de evasión utilizadas por malware durante la ejecución de archivos. ▪ La solución integral de defensa cibernética debe Proporcionar alertas en tiempo real sobre comportamientos maliciosos detectados en archivos. ▪ La solución integral de defensa cibernética debe Permitir la integración con otras soluciones de seguridad para compartir información de análisis de archivos. ▪ La solución integral de defensa cibernética debe Ofrecer una base de datos actualizada de firmas de malware para mejorar la detección durante el análisis de archivos. ▪ La solución integral de defensa cibernética debe Proporcionar opciones de cuarentena para archivos que se determinen como maliciosos tras el análisis. ▪ La solución integral de defensa cibernética debe Permitir la restauración de archivos desde la cuarentena si se determina que son seguros. ▪ La solución integral de defensa cibernética debe Ofrecer capacidades de análisis de archivos en múltiples plataformas y sistemas operativos. ▪ La solución integral de defensa cibernética debe Proporcionar herramientas para la gestión centralizada de políticas de elevación y análisis de archivos. ▪ La solución integral de defensa cibernética debe Permitir la personalización de niveles de sensibilidad para la detección de comportamientos maliciosos en archivos. ▪ La solución integral de defensa cibernética debe Ofrecer soporte para análisis de archivos comprimidos y empaquetados. ▪ La solución integral de defensa cibernética debe Proporcionar capacidades de análisis de scripts y macros dentro de archivos. ▪ La solución integral de defensa cibernética debe Detectar y bloquear intentos de exfiltración de datos durante la ejecución de archivos en el entorno aislado. ▪ La solución integral de defensa cibernética debe Ofrecer opciones de integración con sistemas de gestión de incidentes para reportar análisis de archivos maliciosos. ▪ La solución integral de defensa cibernética debe Proporcionar capacidades de análisis de archivos en tiempo real sin afectar el rendimiento del sistema.

	▪ La solución integral de defensa cibernética debe Permitir la creación de listas blancas y negras de archivos basadas en resultados de análisis. ▪ La solución integral de defensa cibernética debe Ofrecer soporte para análisis de archivos en entornos virtualizados y en la nube. ▪ La solución integral de defensa cibernética debe Proporcionar capacidades de análisis de archivos basados en comportamiento y reputación. ▪ La solución integral de defensa cibernética debe Detectar y bloquear intentos de modificación no autorizada de archivos durante su ejecución en el entorno aislado. ▪ La solución integral de defensa cibernética debe Ofrecer opciones de reporte y auditoría de análisis de archivos para cumplimiento normativo. ▪ La solución integral de defensa cibernética debe Proporcionar capacidades de análisis de archivos en múltiples idiomas y codificaciones. ▪ La solución integral de defensa cibernética debe Permitir la integración con soluciones de inteligencia artificial para mejorar la precisión del análisis de archivos. ▪ La solución integral de defensa cibernética debe Ofrecer soporte para análisis de archivos en tiempo real en entornos de alta disponibilidad.
CONTENCIÓN AUTOMÁTICA DE AMENAZAS (AISLAMIENTO DE PROCESOS MALICIOSOS)	▪ La solución integral de defensa cibernética debe Proporcionar un entorno aislado para la ejecución segura de archivos desconocidos. ▪ La solución integral de defensa cibernética debe Analizar el comportamiento de archivos en tiempo real dentro de un contenedor seguro. ▪ La solución integral de defensa cibernética debe Permitir la ejecución de archivos sospechosos sin riesgo para el sistema operativo principal. ▪ La solución integral de defensa cibernética debe Detectar y bloquear actividades maliciosas durante la ejecución de archivos en el entorno aislado. ▪ La solución integral de defensa cibernética debe Ofrecer análisis dinámico de archivos para identificar comportamientos anómalos. ▪ La solución integral de defensa cibernética debe Integrar análisis estático y dinámico para una evaluación completa de archivos. ▪ La solución integral de defensa cibernética debe Proporcionar informes detallados sobre las acciones realizadas por archivos en el entorno aislado. ▪ La solución integral de defensa cibernética debe Permitir la elevación segura de archivos para análisis sin comprometer la seguridad del sistema. ▪ La solución integral de defensa cibernética debe Ofrecer opciones de configuración para definir políticas de elevación de archivos. ▪ La solución integral de defensa cibernética debe Integrar inteligencia de amenazas para mejorar la precisión del análisis de archivos. ▪ La solución integral de defensa cibernética debe Proporcionar capacidades de aprendizaje automático para mejorar la detección de amenazas en archivos. ▪ La solución integral de defensa cibernética debe Permitir la automatización del análisis de archivos basados en políticas predefinidas. ▪ La solución integral de defensa cibernética debe Ofrecer capacidades de análisis forense para archivos ejecutados en el entorno aislado. ▪ La solución integral de defensa cibernética debe Detectar técnicas de evasión utilizadas por malware durante la ejecución de archivos. ▪ La solución integral de defensa cibernética debe Proporcionar alertas en tiempo real sobre comportamientos maliciosos detectados en archivos. ▪ La solución integral de defensa cibernética debe Permitir la integración con otras soluciones de seguridad para compartir información de análisis de archivos. ▪ La solución integral de defensa cibernética debe Ofrecer una base de datos actualizada de firmas de malware para mejorar la detección durante el análisis de archivos. ▪ La solución integral de defensa cibernética debe Proporcionar opciones de cuarentena para archivos que se determinen como maliciosos tras el análisis. ▪ La solución integral de defensa cibernética debe Permitir la restauración de archivos desde la cuarentena si se determina que son seguros. ▪ La solución integral de defensa cibernética debe Ofrecer capacidades de análisis de archivos en múltiples plataformas y sistemas operativos.

	▪ La solución integral de defensa cibernética debe Proporcionar herramientas para la gestión centralizada de políticas de elevación y análisis de archivos. ▪ La solución integral de defensa cibernética debe Permitir la personalización de niveles de sensibilidad para la detección de comportamientos maliciosos en archivos. ▪ La solución integral de defensa cibernética debe Ofrecer soporte para análisis de archivos comprimidos y empaquetados. ▪ La solución integral de defensa cibernética debe Proporcionar capacidades de análisis de scripts y macros dentro de archivos. ▪ La solución integral de defensa cibernética debe Detectar y bloquear intentos de exfiltración de datos durante la ejecución de archivos en el entorno aislado. ▪ La solución integral de defensa cibernética debe Ofrecer opciones de integración con sistemas de gestión de incidentes para reportar análisis de archivos maliciosos. ▪ La solución integral de defensa cibernética debe Proporcionar capacidades de análisis de archivos en tiempo real sin afectar el rendimiento del sistema. ▪ La solución integral de defensa cibernética debe Permitir la creación de listas blancas y negras de archivos basadas en resultados de análisis. ▪ La solución integral de defensa cibernética debe Ofrecer soporte para análisis de archivos en entornos virtualizados y en la nube. ▪ La solución integral de defensa cibernética debe Proporcionar capacidades de análisis de archivos basados en comportamiento y reputación. ▪ La solución integral de defensa cibernética debe Detectar y bloquear intentos de modificación no autorizada de archivos durante su ejecución en el entorno aislado. ▪ La solución integral de defensa cibernética debe Ofrecer opciones de reporte y auditoría de análisis de archivos para cumplimiento normativo. ▪ La solución integral de defensa cibernética debe Proporcionar capacidades de análisis de archivos en múltiples idiomas y codificaciones. ▪ La solución integral de defensa cibernética debe Permitir la integración con soluciones de inteligencia artificial para mejorar la precisión del análisis de archivos. ▪ La solución integral de defensa cibernética debe Ofrecer soporte para análisis de archivos en tiempo real en entornos de alta disponibilidad.
ANÁLISIS DE COMPORTAMIENTO EN TIEMPO REAL	▪ La solución integral de defensa cibernética debe Monitorear continuamente las actividades de los procesos en ejecución para identificar comportamientos anómalos. ▪ La solución integral de defensa cibernética debe Detectar en tiempo real intentos de acceso no autorizados a recursos del sistema. ▪ La solución integral de defensa cibernética debe Analizar patrones de tráfico de red para identificar comunicaciones sospechosas o maliciosas. ▪ La solución integral de defensa cibernética debe Evaluar el comportamiento de aplicaciones para prevenir la ejecución de código malicioso. ▪ La solución integral de defensa cibernética debe Generar alertas inmediatas ante la detección de actividades que coincidan con firmas de amenazas conocidas. ▪ La solución integral de defensa cibernética debe Implementar técnicas de aprendizaje automático para mejorar la precisión en la detección de amenazas emergentes. ▪ La solución integral de defensa cibernética debe Correlacionar eventos de seguridad para identificar posibles ataques coordinados. ▪ La solución integral de defensa cibernética debe Proporcionar visibilidad completa de las actividades del sistema para facilitar la respuesta a incidentes. ▪ La solución integral de defensa cibernética debe Detectar y bloquear intentos de escalamiento de privilegios por parte de aplicaciones maliciosas. ▪ La solución integral de defensa cibernética debe Monitorear el uso de la memoria y el CPU para identificar procesos que consumen recursos de manera inusual. ▪ La solución integral de defensa cibernética debe Analizar el comportamiento de scripts y macros para prevenir ataques basados en ellos. ▪ La solución integral de defensa cibernética debe Detectar y prevenir movimientos laterales dentro de la red por parte de actores maliciosos.

	• La solución integral de defensa cibernética debe Evaluar en tiempo real las modificaciones en el registro del sistema para identificar cambios no autorizados. • La solución integral de defensa cibernética debe Monitorear las actividades de inicio y cierre de sesión para detectar patrones inusuales. • La solución integral de defensa cibernética debe Analizar el comportamiento de dispositivos externos conectados para prevenir la introducción de malware. • La solución integral de defensa cibernética debe Detectar intentos de deshabilitar o modificar servicios de seguridad del sistema. • La solución integral de defensa cibernética debe Monitorear en tiempo real las actividades de los usuarios para identificar comportamientos sospechosos. • La solución integral de defensa cibernética debe Analizar el comportamiento de aplicaciones en entornos virtualizados para detectar amenazas que intentan evadir la detección. • La solución integral de defensa cibernética debe Proporcionar informes detallados sobre comportamientos anómalos detectados para facilitar la investigación de incidentes. • La solución integral de defensa cibernética debe Detectar y bloquear intentos de inyección de código en procesos legítimos. • La solución integral de defensa cibernética debe Monitorear las actividades de aplicaciones recién instaladas para asegurar que no presenten comportamientos maliciosos. • La solución integral de defensa cibernética debe Analizar en tiempo real las comunicaciones entre procesos para identificar interacciones sospechosas. • La solución integral de defensa cibernética debe Detectar y prevenir la ejecución de procesos desde ubicaciones inusuales o no autorizadas. • La solución integral de defensa cibernética debe Monitorear el acceso a archivos sensibles para prevenir filtraciones de información. • La solución integral de defensa cibernética debe Analizar el comportamiento de aplicaciones que solicitan permisos elevados para asegurar su legitimidad. • La solución integral de defensa cibernética debe Detectar y bloquear intentos de explotación de vulnerabilidades conocidas en tiempo real. • La solución integral de defensa cibernética debe Monitorear las actividades de aplicaciones en segundo plano para identificar procesos maliciosos ocultos. • La solución integral de defensa cibernética debe Analizar el comportamiento de aplicaciones que interactúan con servicios de red para prevenir ataques de red. • La solución integral de defensa cibernética debe Detectar y prevenir la ejecución de código malicioso en memoria. • La solución integral de defensa cibernética debe Monitorear en tiempo real las actividades de aplicaciones descargadas recientemente para asegurar su seguridad. • La solución integral de defensa cibernética debe Analizar el comportamiento de aplicaciones que acceden a recursos críticos del sistema para prevenir daños. • La solución integral de defensa cibernética debe Detectar y bloquear intentos de manipulación de archivos de sistema por parte de malware. • La solución integral de defensa cibernética debe Monitorear las actividades de aplicaciones que se ejecutan al inicio del sistema para identificar amenazas persistentes. • La solución integral de defensa cibernética debe Analizar en tiempo real las actividades de aplicaciones que interactúan con hardware específico para prevenir ataques dirigidos.
ANÁLISIS AVANZADO EN LA NUBE	• La solución integral de defensa cibernética debe Realizar análisis dinámicos de archivos y aplicaciones en un entorno de nube seguro para identificar comportamientos maliciosos. • La solución integral de defensa cibernética debe Utilizar técnicas de aprendizaje automático en la nube para mejorar la detección de amenazas emergentes. • La solución integral de defensa cibernética debe Proporcionar análisis en tiempo real de eventos de seguridad mediante recursos en la nube. • La solución integral de defensa cibernética debe Integrar inteligencia de amenazas global para enriquecer el análisis de seguridad basado en la nube.

	▪ La solución integral de defensa cibernética debe Ofrecer capacidades de análisis forense digital en la nube para investigar incidentes de seguridad. ▪ La solución integral de defensa cibernética debe Permitir la escalabilidad del análisis de seguridad aprovechando la infraestructura en la nube. ▪ La solución integral de defensa cibernética debe Facilitar la colaboración entre equipos de seguridad mediante plataformas de análisis en la nube. ▪ La solución integral de defensa cibernética debe Proporcionar actualizaciones automáticas de firmas y reglas de detección a través de la nube. ▪ La solución integral de defensa cibernética debe Realizar análisis de comportamiento de usuarios y entidades (UEBA) utilizando datos agregados en la nube. ▪ La solución integral de defensa cibernética debe Detectar y responder a amenazas avanzadas mediante análisis correlacionados en la nube. ▪ La solución integral de defensa cibernética debe Ofrecer sandboxing en la nube para la ejecución segura de archivos sospechosos. ▪ La solución integral de defensa cibernética debe Proporcionar informes detallados de amenazas y análisis de tendencias a través de dashboards en la nube. ▪ La solución integral de defensa cibernética debe Permitir la integración con otras soluciones de seguridad a través de APIs basadas en la nube. ▪ La solución integral de defensa cibernética debe Ofrecer análisis de vulnerabilidades en sistemas y aplicaciones mediante escaneos en la nube. ▪ La solución integral de defensa cibernética debe Implementar políticas de seguridad adaptativas basadas en análisis de amenazas en la nube. ▪ La solución integral de defensa cibernética debe Proporcionar capacidades de respuesta automatizada a incidentes basadas en análisis en la nube. ▪ La solución integral de defensa cibernética debe Facilitar la gestión centralizada de eventos de seguridad a través de una consola en la nube. ▪ La solución integral de defensa cibernética debe Ofrecer análisis de tráfico de red en la nube para identificar patrones de ataque. ▪ La solución integral de defensa cibernética debe Proporcionar capacidades de detección y prevención de intrusiones basadas en la nube. ▪ La solución integral de defensa cibernética debe Realizar análisis de integridad de archivos y sistemas mediante servicios en la nube. ▪ La solución integral de defensa cibernética debe Ofrecer análisis de seguridad para entornos de nube híbrida y multi-nube. ▪ La solución integral de defensa cibernética debe Proporcionar capacidades de análisis de registros y eventos centralizados en la nube. ▪ La solución integral de defensa cibernética debe Facilitar la detección de amenazas internas mediante análisis en la nube. ▪ La solución integral de defensa cibernética debe Ofrecer análisis de seguridad para aplicaciones y servicios basados en la nube. ▪ La solución integral de defensa cibernética debe Proporcionar capacidades de análisis de malware avanzado utilizando recursos en la nube. ▪ La solución integral de defensa cibernética debe Implementar análisis de riesgos en tiempo real basados en datos de la nube. ▪ La solución integral de defensa cibernética debe Ofrecer capacidades de análisis de amenazas persistentes avanzadas (APT) mediante la nube. ▪ La solución integral de defensa cibernética debe Proporcionar análisis de seguridad para dispositivos IoT conectados a la nube. ▪ La solución integral de defensa cibernética debe Facilitar la detección de amenazas basadas en inteligencia artificial utilizando análisis en la nube. ▪ La solución integral de defensa cibernética debe Ofrecer análisis de seguridad para contenedores y microservicios en la nube. ▪ La solución integral de defensa cibernética debe Proporcionar capacidades de análisis de amenazas móviles mediante servicios en la nube. ▪ La solución integral de defensa cibernética debe Implementar análisis de seguridad para entornos de virtualización basados en la nube. ▪ La solución integral de defensa cibernética debe Ofrecer análisis de amenazas en tiempo real para infraestructuras críticas utilizando la nube.

	▪ La solución integral de defensa cibernética debe Proporcionar capacidades de análisis de amenazas específicas de la industria mediante la nube. ▪ La solución integral de defensa cibernética debe Facilitar la detección y respuesta a amenazas en entornos de trabajo remoto a través de análisis en la nube.
ANÁLISIS Y CONTROL DE SCRIPTS MALICIOSOS	▪ La solución integral de defensa cibernética debe Analizar en tiempo real los scripts ejecutados en el sistema para detectar comportamientos maliciosos. ▪ La solución integral de defensa cibernética debe Implementar técnicas heurísticas para identificar scripts sospechosos basados en patrones de comportamiento. ▪ La solución integral de defensa cibernética debe Monitorear y analizar comandos de línea ejecutados por scripts para detectar posibles amenazas. ▪ La solución integral de defensa cibernética debe Detectar y bloquear scripts que intenten modificar configuraciones críticas del sistema. ▪ La solución integral de defensa cibernética debe Proporcionar alertas en tiempo real cuando se detecten scripts maliciosos o comportamientos anómalos. ▪ La solución integral de defensa cibernética debe Permitir la configuración de políticas de seguridad específicas para la ejecución de scripts. ▪ La solución integral de defensa cibernética debe Ofrecer la capacidad de aislar y contener scripts sospechosos en un entorno seguro para su análisis. ▪ La solución integral de defensa cibernética debe Integrar una base de datos actualizada de firmas de scripts maliciosos conocidos para mejorar la detección. ▪ La solución integral de defensa cibernética debe Analizar scripts embebidos en documentos y otros archivos para identificar posibles amenazas. ▪ La solución integral de defensa cibernética debe Monitorear y controlar la ejecución de scripts en navegadores web para prevenir ataques basados en scripts. ▪ La solución integral de defensa cibernética debe Detectar y bloquear scripts que intenten descargar o ejecutar código malicioso adicional. ▪ La solución integral de defensa cibernética debe Proporcionar informes detallados sobre la actividad de scripts en el sistema para facilitar la auditoría y el análisis forense. ▪ La solución integral de defensa cibernética debe Permitir la creación de listas blancas y negras de scripts basadas en políticas de seguridad definidas por el administrador. ▪ La solución integral de defensa cibernética debe Ofrecer la capacidad de analizar scripts en múltiples lenguajes de programación y scripting. ▪ La solución integral de defensa cibernética debe Monitorear y controlar la ejecución de scripts en entornos de línea de comandos y shells. ▪ La solución integral de defensa cibernética debe Detectar y bloquear scripts que intenten evadir mecanismos de seguridad o análisis. ▪ La solución integral de defensa cibernética debe Integrar capacidades de aprendizaje automático para mejorar la detección de scripts maliciosos basados en comportamientos emergentes. ▪ La solución integral de defensa cibernética debe Proporcionar opciones de cuarentena para scripts sospechosos hasta que se complete un análisis detallado. ▪ La solución integral de defensa cibernética debe Permitir la restauración de scripts desde la cuarentena si se determina que son seguros. ▪ La solución integral de defensa cibernética debe Ofrecer soporte para análisis de scripts en entornos virtualizados y en la nube. ▪ La solución integral de defensa cibernética debe Proporcionar herramientas para la gestión centralizada de políticas de análisis y control de scripts. ▪ La solución integral de defensa cibernética debe Permitir la personalización de niveles de sensibilidad para la detección de scripts maliciosos. ▪ La solución integral de defensa cibernética debe Ofrecer soporte para análisis de scripts en archivos comprimidos y empaquetados. ▪ La solución integral de defensa cibernética debe Proporcionar capacidades de análisis de scripts en múltiples plataformas y sistemas operativos. ▪ La solución integral de defensa cibernética debe Detectar y bloquear intentos de exfiltración de datos realizados a través de scripts maliciosos.

	▪ La solución integral de defensa cibernética debe Ofrecer opciones de integración con sistemas de gestión de incidentes para reportar actividades de scripts maliciosos. ▪ La solución integral de defensa cibernética debe Proporcionar capacidades de análisis de scripts en tiempo real sin afectar el rendimiento del sistema. ▪ La solución integral de defensa cibernética debe Permitir la creación de reglas específicas para la detección y control de scripts basadas en patrones de comportamiento. ▪ La solución integral de defensa cibernética debe Ofrecer soporte para análisis de scripts en entornos de desarrollo y producción. ▪ La solución integral de defensa cibernética debe Proporcionar capacidades de análisis de scripts basados en comportamiento y reputación. ▪ La solución integral de defensa cibernética debe Detectar y bloquear intentos de modificación no autorizada de scripts legítimos por parte de malware. ▪ La solución integral de defensa cibernética debe Ofrecer opciones de reporte y auditoría de análisis de scripts para cumplimiento normativo. ▪ La solución integral de defensa cibernética debe Proporcionar capacidades de análisis de scripts en múltiples idiomas y codificaciones. ▪ La solución integral de defensa cibernética debe Permitir la integración con soluciones de inteligencia artificial para mejorar la precisión del análisis de scripts.
CONTROL REMOTO Y GESTIÓN DE INCIDENTES	▪ La solución integral de defensa cibernética debe Proporcionar conexiones remotas cifradas para garantizar la seguridad y privacidad de las sesiones de control remoto. ▪ La solución integral de defensa cibernética debe Implementar autenticación multifactor para validar la identidad de los usuarios antes de otorgar acceso remoto. ▪ La solución integral de defensa cibernética debe Permitir el monitoreo en tiempo real de las sesiones de control remoto para supervisar actividades y detectar comportamientos sospechosos. ▪ La solución integral de defensa cibernética debe Ofrecer grabación de sesiones remotas para auditorías posteriores y cumplimiento normativo. ▪ La solución integral de defensa cibernética debe Proporcionar compatibilidad multiplataforma para facilitar el acceso remoto desde diversos dispositivos y sistemas operativos. ▪ La solución integral de defensa cibernética debe Establecer controles de acceso granulares que definan los permisos de los usuarios según sus roles y responsabilidades. ▪ La solución integral de defensa cibernética debe Facilitar la transferencia segura de archivos durante las sesiones remotas, garantizando la integridad y confidencialidad de los datos. ▪ La solución integral de defensa cibernética debe Permitir la ejecución remota de scripts y comandos para la resolución eficiente de incidentes. ▪ La solución integral de defensa cibernética debe Ofrecer herramientas de colaboración en tiempo real, como chat y compartición de pantalla, para mejorar la eficiencia en la gestión de incidentes. ▪ La solución integral de defensa cibernética debe Integrarse con sistemas de gestión de tickets para un seguimiento efectivo de los incidentes y su resolución. ▪ La solución integral de defensa cibernética debe Proporcionar alertas instantáneas sobre actividades sospechosas detectadas durante las sesiones remotas. ▪ La solución integral de defensa cibernética debe Ofrecer informes detallados de las sesiones de control remoto, incluyendo actividades realizadas y duración de las mismas. ▪ La solución integral de defensa cibernética debe Permitir la programación de sesiones remotas para tareas de mantenimiento y actualizaciones fuera del horario laboral. ▪ La solución integral de defensa cibernética debe Implementar políticas de tiempo de espera y desconexión automática para sesiones inactivas, mejorando la seguridad.

	▪ La solución integral de defensa cibernética debe Ofrecer soporte para múltiples monitores durante las sesiones remotas, facilitando una visión completa del sistema del usuario. ▪ La solución integral de defensa cibernética debe Proporcionar capacidades de impresión remota segura, permitiendo a los usuarios imprimir documentos en sus ubicaciones locales. ▪ La solución integral de defensa cibernética debe Facilitar la gestión de múltiples sesiones remotas simultáneamente, optimizando la eficiencia del personal de TI. ▪ La solución integral de defensa cibernética debe Ofrecer opciones de personalización de la interfaz de usuario para adaptarse a las necesidades específicas de la organización. ▪ La solución integral de defensa cibernética debe Integrarse con soluciones de directorio activo para una gestión centralizada de usuarios y permisos. ▪ La solución integral de defensa cibernética debe Proporcionar herramientas para la gestión de parches y actualizaciones de software de forma remota. ▪ La solución integral de defensa cibernética debe Permitir el acceso remoto desatendido para la resolución de problemas sin la intervención del usuario final. ▪ La solución integral de defensa cibernética debe Ofrecer soporte para autenticación basada en certificados para fortalecer la seguridad de las conexiones remotas. ▪ La solución integral de defensa cibernética debe Implementar restricciones geográficas para limitar el acceso remoto desde ubicaciones no autorizadas. ▪ La solución integral de defensa cibernética debe Proporcionar capacidades de control remoto para dispositivos móviles, ampliando el soporte a una variedad de endpoints. ▪ La solución integral de defensa cibernética debe Facilitar la escalación de privilegios de manera segura durante las sesiones remotas cuando sea necesario. ▪ La solución integral de defensa cibernética debe Ofrecer opciones de chat en tiempo real entre técnicos y usuarios finales durante las sesiones de soporte remoto. ▪ La solución integral de defensa cibernética debe Proporcionar una consola centralizada para la gestión y monitoreo de todas las sesiones remotas. ▪ La solución integral de defensa cibernética debe Permitir la integración con soluciones de seguridad existentes para una defensa en profundidad. ▪ La solución integral de defensa cibernética debe Ofrecer soporte para la autenticación de dos factores, añadiendo una capa adicional de seguridad.
CONTROL DE DISPOSITIVOS EXTERNOS Y USB	▪ La solución integral de defensa cibernética debe Permitir habilitar o bloquear dispositivos externos conectados a los endpoints. ▪ La solución integral de defensa cibernética debe Ofrecer la capacidad de bloquear clases específicas de dispositivos, como almacenamiento USB, dispositivos Bluetooth o controladores IDE ATA/ATAPI. ▪ La solución integral de defensa cibernética debe Proporcionar la opción de crear excepciones para permitir que dispositivos específicos se conecten, incluso si pertenecen a una clase bloqueada. ▪ La solución integral de defensa cibernética debe Permitir la configuración de perfiles de control de dispositivos externos para diferentes grupos de endpoints. ▪ La solución integral de defensa cibernética debe Ofrecer la capacidad de registrar intentos de conexión de dispositivos bloqueados para fines de auditoría y monitoreo. ▪ La solución integral de defensa cibernética debe Proporcionar notificaciones al usuario final cuando se bloquea o permite un dispositivo externo. ▪ La solución integral de defensa cibernética debe Permitir la identificación y gestión de dispositivos externos mediante identificadores únicos, como el ID del dispositivo. ▪ La solución integral de defensa cibernética debe Ofrecer la capacidad de agregar exclusiones utilizando caracteres comodín en el ID del dispositivo para abarcar una gama de dispositivos similares. ▪ La solución integral de defensa cibernética debe Proporcionar una interfaz para ver y gestionar todas las exclusiones de dispositivos configuradas. ▪ La solución integral de defensa cibernética debe Permitir la eliminación de exclusiones de dispositivos cuando ya no sean necesarias.

	▪ La solución integral de defensa cibernética debe Ofrecer la capacidad de bloquear dispositivos de almacenamiento masivo USB para prevenir la transferencia no autorizada de datos. ▪ La solución integral de defensa cibernética debe Permitir el bloqueo de dispositivos de red externos para prevenir conexiones no autorizadas. ▪ La solución integral de defensa cibernética debe Proporcionar la opción de bloquear dispositivos de imagen, como cámaras digitales, para prevenir la extracción no autorizada de información. ▪ La solución integral de defensa cibernética debe Ofrecer la capacidad de bloquear dispositivos de impresión externos para controlar la impresión no autorizada de documentos sensibles. ▪ La solución integral de defensa cibernética debe Permitir el bloqueo de dispositivos de audio externos para prevenir posibles fugas de información a través de grabaciones no autorizadas. ▪ La solución integral de defensa cibernética debe Proporcionar la opción de bloquear dispositivos de interfaz humana (HID), como teclados y ratones externos, para prevenir posibles ataques de hardware. ▪ La solución integral de defensa cibernética debe Ofrecer la capacidad de bloquear dispositivos de comunicación, como módems y adaptadores de red inalámbrica, para prevenir conexiones no autorizadas. ▪ La solución integral de defensa cibernética debe Permitir el bloqueo de dispositivos de almacenamiento óptico externos, como unidades de CD/DVD, para prevenir la transferencia no autorizada de datos. ▪ La solución integral de defensa cibernética debe Proporcionar la opción de bloquear dispositivos de almacenamiento de cinta externos para prevenir la copia no autorizada de información. ▪ La solución integral de defensa cibernética debe Ofrecer la capacidad de bloquear dispositivos de almacenamiento de disquete para prevenir la transferencia no autorizada de datos. ▪ La solución integral de defensa cibernética debe Permitir el bloqueo de dispositivos de almacenamiento de medios flash, como tarjetas SD, para prevenir la extracción no autorizada de información. ▪ La solución integral de defensa cibernética debe Proporcionar la opción de bloquear dispositivos de almacenamiento de medios extraíbles para prevenir la transferencia no autorizada de datos. ▪ La solución integral de defensa cibernética debe Ofrecer la capacidad de bloquear dispositivos de almacenamiento de medios ópticos para prevenir la copia no autorizada de información. ▪ La solución integral de defensa cibernética debe Permitir el bloqueo de dispositivos de almacenamiento de medios magnéticos para prevenir la transferencia no autorizada de datos.
SEGURIDAD DE ACCESO MEDIANTE CONTROL DE CONTRASEÑAS	▪ La solución integral de defensa cibernética debe Permitir la protección por contraseña de las interfaces de configuración del cliente de seguridad para evitar accesos no autorizados. ▪ La solución integral de defensa cibernética debe Ofrecer la opción de establecer contraseñas personalizadas para acceder a áreas críticas de la aplicación de seguridad. ▪ La solución integral de defensa cibernética debe Implementar autenticación de administrador del sistema para acceder a configuraciones avanzadas del cliente de seguridad. ▪ La solución integral de defensa cibernética debe Proporcionar la capacidad de proteger con contraseña las herramientas de eliminación de agentes para prevenir desinstalaciones no autorizadas. ▪ La solución integral de defensa cibernética debe Permitir la configuración de diferentes niveles de acceso basados en roles de usuario mediante contraseñas. ▪ La solución integral de defensa cibernética debe Ofrecer la opción de requerir contraseñas para modificar configuraciones de antivirus, firewall, HIPS y contención.

	▪ La solución integral de defensa cibernética debe Implementar un sistema de tiempo de espera para contraseñas, requiriendo reautenticación después de un período de inactividad. ▪ La solución integral de defensa cibernética debe Proporcionar la capacidad de habilitar o deshabilitar la protección por contraseña según las políticas de seguridad de la organización. ▪ La solución integral de defensa cibernética debe Ofrecer opciones para restablecer contraseñas en caso de olvido o compromiso, manteniendo la seguridad del sistema. ▪ La solución integral de defensa cibernética debe Permitir la integración con sistemas de gestión de identidades para una administración centralizada de contraseñas. ▪ La solución integral de defensa cibernética debe Implementar políticas de complejidad de contraseñas para garantizar contraseñas fuertes y seguras. ▪ La solución integral de defensa cibernética debe Proporcionar alertas y notificaciones en caso de intentos fallidos de acceso debido a contraseñas incorrectas. ▪ La solución integral de defensa cibernética debe Ofrecer la capacidad de auditar y registrar todos los accesos y cambios realizados mediante autenticación por contraseña. ▪ La solución integral de defensa cibernética debe Permitir la configuración de políticas de expiración de contraseñas para obligar a cambios periódicos. ▪ La solución integral de defensa cibernética debe Implementar medidas contra ataques de fuerza bruta, como el bloqueo temporal de cuentas después de múltiples intentos fallidos. ▪ La solución integral de defensa cibernética debe Ofrecer soporte para autenticación multifactor, añadiendo una capa adicional de seguridad más allá de las contraseñas. ▪ La solución integral de defensa cibernética debe Proporcionar la capacidad de sincronizar contraseñas con otros sistemas de la organización para una gestión unificada. ▪ La solución integral de defensa cibernética debe Permitir la configuración de restricciones de acceso basadas en la ubicación o la dirección IP, además de la protección por contraseña. ▪ La solución integral de defensa cibernética debe Ofrecer la opción de deshabilitar cuentas o accesos después de un número determinado de intentos fallidos de contraseña. ▪ La solución integral de defensa cibernética debe Implementar la capacidad de forzar el cierre de sesión de usuarios después de un período de inactividad definido. ▪ La solución integral de defensa cibernética debe Proporcionar herramientas para la recuperación segura de contraseñas, como preguntas de seguridad o enlaces de restablecimiento. ▪ La solución integral de defensa cibernética debe Ofrecer la capacidad de establecer contraseñas temporales para accesos de corta duración o para usuarios invitados. ▪ La solución integral de defensa cibernética debe Permitir la configuración de políticas que impidan la reutilización de contraseñas anteriores. ▪ La solución integral de defensa cibernética debe Implementar la capacidad de monitorear y alertar sobre actividades sospechosas relacionadas con el uso de contraseñas.
PLATAFORMA CENTRAL EN NUBE	▪ La solución integral de defensa cibernética debe incluir una consola de administración central en la nube que permita la administración simultánea de equipos, servidores y dispositivos móviles bajo sistemas operativos Windows, Linux, Mac IOS y Android. ▪ Debe ser en la nube. Esta consola deberá permitir administrar desde un solo punto administrar todas las oficinas y redes de la organización. ▪ Debe permitir crear usuarios de administración con diferentes roles administrador total, técnicos, o administradores limitados. ▪ Debe ser escalable, lo cual permitirá activar la administración de redes complejas, permitiendo la administración de más de 20000 equipos desde un punto central.

	▪ Debe actualizar cada 15 minutos o menos y mantener al día todas las actualizaciones con los clientes. ▪ Debe permitir la administración basada en políticas y contener al menos políticas: Actualización, Opciones de Antivirus, opciones de contención, control de Aplicaciones y Firewall. ▪ Debe contar con filtros de control que permita detectar de forma rápida los equipos no protegidos o los que no cumplen con las políticas de seguridad para garantizar la seguridad de la red. ▪ Debe permitir al administrador crear políticas desde la consola para evitar el uso de aplicaciones no deseadas, así como eliminar, autorizar y limpiar las mismas en los clientes. ▪ Debe contar con la capacidad para la desinfección y limpieza remota de adware/aplicaciones potencialmente peligrosas, así como también de virus, troyanos, gusanos, rootkits y Spyware. ▪ Debe permitir utilizar al menos 3 tipos diferentes de mecanismos para detectar equipos en la red (TCP/IP, grupo de trabajo, Active Directory y otros). ▪ Debe determinar los equipos que cumplan con las políticas centrales y/o que fueron modificadas localmente. Eventualmente puede "forzar" a los equipos a cumplir con las políticas centrales con tan solo un clic. ▪ Debe contar con un sistema de reportes y mecanismos de notificación de eventos vía correo electrónico. ▪ Debe informar que tipo de malware fue detectado, en qué archivos, en qué computadores y que acción tomo al respecto. ▪ Debe almacenar un histórico de eventos de cada equipo administrado pudiéndose conocer también el Nombre del Equipo, Descripción, SO, Service Pack, IP, Grupo, Usuario que ha iniciado sesión, Última Actualización, Eventos de error, etc. ▪ Debe permitir crear grupos dentro de un grupo principal, con el fin de garantizar la administración ordenada. ▪ Debe realizar junto con la solución de seguridad para estaciones y servidores deberá ser de tipo Integrada; es decir incluir un único agente que brinde protección frente a virus, spyware, adware, rootkits, comportamientos sospechosos, detección Web de ataques de scripts maliciosos, hackers (firewall personal) y aplicaciones potencialmente peligrosas en todos los protocolos de la red. ▪ Debe permitir la capacidad de múltiples políticas de configuración. ▪ Debe permitir las sesiones de intercambio de pantalla directamente en el escritorio del usuario final (Sesión remota sin cerrar la sesión actual del usuario). ▪ Debe permitir la visibilidad global sobre todas las aplicaciones instaladas en todas las computadoras de la red con la capacidad de desinstalar de forma invisible los elementos no deseados. ▪ Debe permitir la visibilidad global de todos los servicios del cliente final con la capacidad de detenerlo, pausarlo e iniciarlo bajo demanda. ▪ Debe permitir la visibilidad global sobre todos los procesos que se ejecutan en todos los clientes finales con la capacidad de terminar procesos sospechosos o que consumen muchos recursos. ▪ Debe brindar la información sobre el cliente final: Usuario conectado y el tipo de sesión, todas las métricas de red, CPU / RAM, sistema operativo con Service Pack y la información de versión, las aplicaciones instaladas, procesos en ejecución. ▪ Debe permitir la visibilidad de aplicación y el criterio de valoración del sistema de seguridad y registros de eventos con capacidad de exportación. ▪ Debe brindar el informe de estado del cliente final sobre las políticas de seguridad aplicadas.

	• Debe brindar el informe de inventario de Hardware detalladamente. • Debe permitir el bloqueo de dispositivos de almacenamiento extraíble USB, óptico y floppy. • Debe tener la opción para reiniciar, apagar y prender los equipos remotos.
CONSIDERACIONES Y VALORES AGREGADOS:	• El proveedor debe contar con una plataforma de mesa de ayuda donde entregará un usuario y contraseña de acceso para la generación de tickets y atender y registrar las solicitudes de soporte técnico los cuales se verán reflejados en la interfaz web. • De ser el caso, el servicio de soporte técnico 24x7 (24 horas del día, de lunes a domingo incluyendo feriados), durante un periodo de un (01) año, sin costo alguno para el GOBIERNO REGIONAL DE UCAYALI. • El postor deberá indicar el procedimiento de atención, los teléfonos, horarios, correo electrónico, contactos y números preferenciales con el fabricante. • El postor capacitará a un mínimo de 05 horas en las herramientas de implementación, administración y solución de problemas relacionados a la solución para el personal que administrará la plataforma antivirus con entrega de certificado de capacitación, para 06 personas como mínimo. (Deberá ser de carácter técnico, no comerciales ni preventa, y deberán ser emitidas por el fabricante). • El postor deberá brindar el servicio de instalación, configuración y pruebas del aplicativo antivirus en el 100% de los equipos de la institución. • Deberá realizar 02 visitas al mes para monitorear la configuración de la política de la seguridad implementada. • Para la validación de las especificaciones técnicas, el potencial proveedor deberá adjuntar una ficha técnica del bien que compone su oferta o cotización.
SOBRE LA INSTALACIÓN Y DESPLIEGUE	• La propuesta debe contemplar asistencia técnica para la implementación de la solución en la red. • La implementación de la solución deberá ser efectuada por técnicos certificados por el fabricante. • Se deberán entregar manuales de usuario y de instalación de todos los productos ofertados en formato electrónico. • Instalación y configuración de la consola de antivirus y componentes en el servidor designado para el servicio de antivirus; según las políticas de seguridad previamente coordinadas con el personal de la Oficina de Tecnologías de la Información. • Instalación de las 420 licencias del software antivirus en los equipos servidores y equipos de cómputo de la red de datos institucional en un periodo de 3 días; debiendo considerar la desinstalación del software de antivirus existente en los equipos de cómputo

CONSIDERACIONES GENERALES	• La suscripción de la solución integral de defensa cibernética debe ser identificados en todas sus características según las especificaciones técnicas y deberán estar a nombre del GOBIERNO REGIONAL DE UCAYALI.
	• Las autorizaciones de uso serán entregadas como máximo en 1 día calendario contabilizados a partir del día siguiente de suscrito el contrato o recepción de la orden de compra.
	• El proveedor al finalizar debe entregar un informe de implementación del servicio.
	  ○ La entrega de la licencia de software deberá incluir:
	  ○ Entrega virtual de las licencias y las credenciales de accesos correo electrónico: **licencias.software@regionucayali.gob.pe**
	  ○ Certificado de licenciamiento
	  ○ Manuales digitales en idioma original para la operación y administración.
	  ○ De existir un problema con los medios de las licencias de software, se comunicará de inmediato al proveedor, el cual deberá brindar la atención y la solución al problema dentro de las 24 horas de recepcionada la notificación.

3.5 FORMA DE PAGO

El pago se realiza de conformidad con lo establecido en el artículo 67 de la Ley.

La entidad contratante paga las contraprestaciones pactadas a favor del contratista dentro de los diez días hábiles siguientes de otorgada la conformidad por parte del área usuaria, y es prorrogable, previa justificación de la demora, por cinco días hábiles

En el caso que se haya suscrito contrato con un consorcio, el pago se realiza, a quien corresponda, de acuerdo con lo que se indique en el contrato de consorcio.

La entidad contratante realiza el pago de la contraprestación pactada a favor del contratista en UN UNICO PAGO.

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

- Documento de recepción y verificación del ÁREA DE ALMACÉN
- Documento en el que conste la conformidad de la prestación efectuada suscrita por el servidor responsable de la Oficina de Tecnologías de la Información de la entidad.
- Comprobante de pago
- Documento donde se especifique que las licencias de antivirus están registrado a nombre del Gobierno Regional de Ucayali, su soporte técnico respectivo, así como una vigencia de un (01) año.
- Informe de instalación, puesta en marcha y despliegue del software antivirus.
- Informe de Capacitación In Situ al personal de la Oficina de Tecnologías de la Información del Gobierno Regional de Ucayali sobre el uso y administración del software antivirus.

3.6 CONFORMIDAD

La Conformidad del Bien será otorgada por el Director de la Oficina de Tecnologías de la Información, previo cumplimiento de entrega de la documentación descrita en el punto 3.5.

3.7 PERFIL DEL POSTOR

Del Proveedor

a. **Perfil**
   - Persona jurídica
   - No tener impedimento para contratar con el Estado.
   - Registro Único de Contribuyente (RUC) vigente.
   - Registro Nacional de Proveedores (RNP) vigente.

b. **Experiencia**

   Experiencia mínima de tres (03) ventas similares relacionadas a la contratación en los últimos tres (03) años, 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 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.

3.8 PARTICIPACIÓN EN CONSORCIO

Requisitos:

D.1 El número máximo de consorciados es de **dos (02) integrantes**.

D.2 El porcentaje mínimo de participación de cada consorciado es de **treinta por ciento (30%)**.

D.3 El porcentaje mínimo de participación en la ejecución del contrato, para el integrante del consorcio que acredite mayor experiencia, es de **setenta por ciento (70%).**

Acreditación:

Se acredita con la promesa de consorcio.

GOBIERNO REGIONAL DE UCAYALI

Ing. Leo Martin Chumbe Rodriguez