SUITE DE SEGURIDAD ENDPOINT INSTITUCIONAL

Órgano : GERENCIA DE OPERACIONES
Fecha : Tacna, 21 de julio de 2025
Actividad del POI : SI
Forma parte del SGC : SI
N° de Producto Priorizado del SCI :

I. FINALIDAD PUBLICA (Obligatorio)

Contar con una suite de seguridad endpoint para el equipamiento informático institucional (servidores, las estaciones de trabajo y dispositivos portátiles de usuario final) de la infraestructura Tics de ZOFRATACNA.

II. OBJETIVOS DE LA CONTRATACION (Obligatorio)

La presente contratación tiene como objetivos los siguientes:

Objetivo General:
Suministrar e instalar a todo costo de la suite de seguridad endpoint institucional, para reforzar la protección de los activos informáticos, contra: virus, troyanos, adware, spyware, ransomware y otros programas maliciosos.

Objetivo Específico:

- Suministrar e instalar a todo costo de la suite de seguridad endpoint para los servidores institucionales
- Suministrar e instalar a todo costo de la suite de seguridad endpoint para las estaciones de trabajo desktop institucionales
- Garantizar y dar Soporte 24x7 de la suite de seguridad endpoint institucional

III. DESCRIPCIÓN DE LAS CARACTERÍSTICAS TECNICAS DEL BIEN (Obligatorio)

3.1 CONDICIONES GENERALES:

- ✓ La solución propuesta deberá cubrir el parque de DOSCIENTOS (200) equipos informáticos (estaciones de trabajo, móviles y servidores institucionales) por un periodo de TRES (03) años.
- ✓ La totalidad de bienes a suministrar deberán ser nuevos, de primer uso y deberán estar libres de defectos y adulteraciones, que puedan manifestarse durante su utilización, ya sea producto del resultado de alguna acción u omisión o provengan del diseño, los materiales o la mano de obra; tampoco serán aceptados equipos y elementos refabricados, reparados o reacondicionados.
- ✓ Los suministros, deberán considerar todas las actividades, elementos y/o accesorios necesarios para su adecuada instalación y operación, así como el soporte técnico 24x7 y garantía requerida para la totalidad de los elementos que formarán parte de la solución propuesta.
- ✓ Las licencias deberán ser registradas a nombre de ZOFRATACNA, en una cuenta corporativa registrada en la base de datos de clientes del fabricante que será entregada por el postor ganador.
- ✓ El proveedor será una empresa asociada y/o distribuidor y/o Partner autorizado para la comercializar y/o revender de productos del fabricante

- ✓ El servicio comprenderá los siguientes rubros genéricos:
  a. Suministro e instalación de sistema suite de seguridad endpoint para los equipos informáticos institucionales.
  b. Habilitación de los servicios y demás funcionalidades ofertadas.
  c. Puesta en servicio y puesta en producción.
  d. Protocolos de Pruebas y aceptación de implementación.
  e. Capacitación técnica del personal.

3.2 SUITE DE SEGURIDAD INFORMATICA PARA ENDPOINT:

- ✓ La solución deberá de ser compatibles con los sistemas operativos de escritorio MS Windows 7 y superiores
- ✓ La solución deberá de ser compatibles con todos los sistemas operativos de servidor MS Windows SERVER 2008 R2 y superiores
- ✓ La solución deberá de ser compatibles con todos los sistemas operativos Móviles ANDROID 4.2 y superiores
- ✓ La solución deberá de ser compatibles con todos los sistemas operativos Móviles iOS 10 y superiores
- ✓ La solución debe tener una tecnología de escaneo y detección de todo tipo de amenazas como entre los más comunes: virus, gusanos, troyanos, spyware, adware, rootkits, bots malware etc, y un motor dedicado para la detección y el bloqueo de ransomware.
- ✓ Debe contar con Escáner proactivo con inteligencia artificial y capacidades de aprendizaje automático
- ✓ La solución debe tener un sistema de autoprotección inteligente
- ✓ La solución deberá de tener un escáner de correo electrónico en tiempo real en el punto final
- ✓ Debe ser capaz de proteger contra Keylogger, File-less Malware, Rootkits, Sypware, Ransomwares y ataques de día cero y debe cumplir con EDR.
- ✓ La solución debe tener un monitor de archivos en tiempo real con capacidades EDR.
- ✓ La solución debe bloquear ataques sin archivos, comportamiento de explotación, ransomware usando IOC.
- ✓ La solución debe identificar el comportamiento malicioso de los archivos ejecutados\procesos en ejecución\modificaciones de registro\acceso a la memoria y terminarlos en tiempo de ejecución, o generar una alerta (exploits, sin archivos, macros, PowerShell, WMI, etc.).
- ✓ La solución debe admitir la creación de reglas para excluir archivos según el hash, el nombre de archivo y las carpetas.
- ✓ La solución debe identificar y bloquear/alertar sobre el movimiento lateral
- ✓ La solución debería detectar cuando se usan herramientas sin archivos y sin malware, como PowerShell.
- ✓ La solución debe recopilar y visualizar continuamente datos sobre todas las entidades y sus actividades dentro del entorno.
- ✓ La solución debe admitir y establecer una conexión de respuesta en tiempo real a los puntos finales.
- ✓ La solución debe soportar el aislamiento y la mitigación de presencia y actividad maliciosa.
- ✓ La solución debe incluir la caza de amenazas
- ✓ La solución debe tener la capacidad de habilitar/deshabilitar ciertos tipos de notificaciones

- ✓ La solución debe tener la capacidad de calificar la gravedad de las alertas de seguridad.
- ✓ La solución debe admitir informes estandarizados y personalizables.
- ✓ La solución debe tener una prevención de brotes automática y configurable.
- ✓ La solución debe proporcionar una visualización completa del ataque.
- ✓ La solución debe proporcionar análisis de causa raíz automáticos y manuales
- ✓ la solución debe tener un escáner bajo demanda
- ✓ la solución debe tener capacidades de mitigación de malware de URL con inteligencia en la nube.
- ✓ la solución debe tener capacidades para realizar escaneos rápidos con tecnologías basadas en lógicas de ahorro de tiempo durante los escaneos
- ✓ La solución debería poder controlar el acceso del ejecutable a través de la red.
- ✓ la solución debe poder controlar el acceso de ejecutables específicos y definidos en el punto final.
- ✓ La solución debería poder controlar la funcionalidad de ejecución automática desde dispositivos externos.
- ✓ la solución debería haber sido capaz de detectar/bloquear ataques de fuerza bruta sobre la sesión de terminal hasta el punto final.
- ✓ La solución debe poder proporcionar acceso controlado (modificación y eliminación) de carpetas definidas.
- ✓ La solución debe poder proporcionar acceso controlado (modificación y eliminación) de archivos definidos y también en función de usuarios remotos/locales.
- ✓ Protección de puerta de enlace en la capa winsock de cada puerta de enlace de punto final.
- ✓ la solución debe escanear los correos electrónicos entrantes/salientes en el cliente
- ✓ la solución debería poder bloquear archivos adjuntos según el tipo
- ✓ La solución debe incluir archivos adjuntos en la lista blanca
- ✓ la solución debería poder archivar correos electrónicos y archivos adjuntos
- ✓ la solución debe ser capaz de tomar medidas en correos electrónicos maliciosos en función de las acciones definidas por el usuario
- ✓ la solución debe tener notificaciones de alerta personalizables para varios eventos
- ✓ Solución Debe incluir la funcionalidad EDR con respecto al manejo de contenido de correo electrónico malicioso.
- ✓ la solución debe tener un motor antispam en tiempo real basado en inteligencia artificial y aprendizaje automático
- ✓ La solución también debe incluir un filtro antiphishing inteligente
- ✓ La solución debería permitir que el cliente defina frases para categorizar como spam
- ✓ La solución debe identificar y poner en cuarentena el correo electrónico publicitario
- ✓ La solución debe integrarse con la tecnología NILP
- ✓ La solución debe incluir un nivel de sensibilidad de protección de correo electrónico para categorizar un correo electrónico como spam.
- ✓ La solución debería poder publicar una lista de propietarios de dominios autorizados para reducir el spam y los fraudes.
- ✓ La solución debería poder integrarse con múltiples servicios externos que proporcionan bases de datos de contenido malicioso de URL
- ✓ La solución también debería poder proporcionar un configurador automático para la lista blanca de dominios.
- ✓ La solución debe tener parámetros sólidos de etiquetado de correo
    - Pasar el correo electrónico tal como está incluso si se detecta como spam

- Etiqueta de spam añadida en el asunto
- Etiquetado inteligente X-mailscan-Spam para líneas de asunto y como encabezado.

- ✓ La solución debe tener descargos de responsabilidad personalizables.
- ✓ La solución debería poder enviar notificaciones personalizadas o alertas base de eventos.
- ✓ La solución debería ser capaz de proporcionar informes de correo resumidos.
- ✓ La solución debe tener una configuración de filtro inteligente para identificar el juego de caracteres chino y coreano
- ✓ La solución debe tener un filtro de base de categoría integrado para URLS y debe ser personalizable según las políticas y la cultura de acceso de una organización.
- ✓ la solución debe tener capacidades de inteligencia en la nube para comprender y bloquear las URL maliciosas.
- ✓ La solución debería poder completar automáticamente la categoría de bloque por sitio rechazado.
- ✓ La solución debe poder registrar infracciones de políticas y debe incluir la función EDR.
- ✓ La solución debe tener la capacidad de controlar el puerto de acceso a Internet
- ✓ La solución debe permitir el acceso a la web en un mecanismo de control de políticas de base de cuadrícula de tiempo.
- ✓ la solución debe tener un filtro antiphishing inteligente
- ✓ La solución debería permitir personalizaciones de acceso a puertos para accesos a Url.
- ✓ la solución debe ser compatible con EDR en función de las infracciones de registro
- ✓ la solución debe incluir un cortafuegos inteligente completo de estado bidireccional y funcionalidad EDR
- ✓ La solución debe tener varios modos de control intrusivos y no intrusivos basados en políticas.
- ✓ La solución debe tener reglas de zona que se puedan personalizar según los segmentos de dirección IP/nombre de host/dirección MAC.
- ✓ La solución debería poder establecer reglas complejas basadas en el Protocolo
- ✓ la solución debería ser capaz de mitigar los ataques DDOS y el escaneo de puertos
- ✓ La solución debe ser capaz de proporcionar un monitoreo de red.
- ✓ la solución debe poder proporcionar todos los eventos en tiempo real e informes de violaciones
- ✓ la solución debe tener protección con contraseña para dispositivos USB
- ✓ la solución debería poder bloquear la reproducción automática de USB
- ✓ la solución debería poder bloquear unidades USB, unidades de CD/DVD, cámaras web, dispositivos Bluetooth
- ✓ la solución debe proporcionar una instalación de modo de solo lectura de dispositivos de almacenamiento USB
- ✓ la solución debe bloquear otros modos que se pueden usar para la transferencia de datos (por ejemplo, transferencia de archivos desde IM)
- ✓ la solución debe tener un módulo de control de aplicaciones completo con listas blancas/listas negras según las restricciones de tiempo
- ✓ La solución debe tener herramientas de vacunación USB. Para que el pendrive no se infecte si se inserta en una máquina infectada.
- ✓ la solución debería poder bloquear la carga a la URL.
- ✓ La solución debe tener un módulo de control de aplicaciones dedicado.
- ✓ La solución debe incluir una lista blanca para las aplicaciones auténticas de la empresa.
- ✓ la solución debería poder borrar archivos temporales de Internet y Windows

- ✓ la solución debería poder borrar el caché, las cookies, los complementos ActiveX, el historial en un horario.
- ✓ la solución debe tener una función de eliminación segura
- ✓ La solución debe tener capacidades para proporcionar un inventario completo de hardware y software.
- ✓ Solución Debe tener capacidades para proporcionar detalles de licencia de SO.
- ✓ La solución debe tener capacidades para configurar la notificación de cualquier cambio de hardware y software.
- ✓ La solución debe tener capacidades para monitorear la creación, copia, modificación y eliminación de archivos del sistema a unidades externas, unidades de red y unidades locales
- ✓ Monitor de actividad de impresión
- ✓ La solución debe tener capacidades para monitorear todas las impresoras compartidas de la red y proporcionar una lista resumida de todas las actividades de impresión según el nombre de la impresora/nombre del host/dirección IP/nombre del documento.
- ✓ La solución debe poder administrar toda la funcionalidad desde un servidor administrado centralmente a través de la consola y en una plataforma heterogénea (Windows, Linux, Mac)
- ✓ La solución debería poder proporcionar un panel de control en tiempo real sobre el estado de los puntos finales
- ✓ La solución debe ser capaz de proporcionar informes detallados con facilidad de exportación para todas las características y funcionalidades en varios formatos (Pdf, Excel, HTML, etc.).
- ✓ La solución debe poder proporcionar una categorización basada en grupos para visualización, implementación de políticas, programación de tareas y para MIS completo
- ✓ La solución debe proporcionar una instalación de OTP para el acceso temporal que debe basarse en el tiempo
- ✓ la solución debe tener una tarea de prevención de brotes en caso de un ataque de virus
- ✓ La solución debe tener una creación de usuarios basada en roles administrativos jerárquicos
- ✓ La solución debe ser configurable a través de actualizaciones de http y FTP para el cliente
- ✓ La solución debe poder integrarse con CRM de terceros a través de SNMP y tener capacidades de EDR con aplicaciones de terceros como el servidor syslog y los reenviadores splunk
- ✓ La solución debe poder administrar el ancho de banda con QOS y definir los tamaños de las actualizaciones
- ✓ La solución debe poder proporcionar agrupaciones automáticas para la funcionalidad de puntos finales que se pueden integrar en configuraciones personalizadas
- ✓ La solución debe tener la opción de administración del servidor secundario para administrar el consumo de ancho de banda en las actualizaciones de firmas en entornos de bajo ancho de banda.
- ✓ La solución debe tener la opción Informe de actividad para monitorear la actividad de la sesión de las computadoras Cliente (por ejemplo, conexión/desconexión de sesión remota, inicio/apagado)
- ✓ La solución debe tener un módulo para monitorear y registrar las tareas de impresión

realizadas por los puntos finales administrados.

- ✓ La solución debe tener la funcionalidad de copia de seguridad a través de la red.
- ✓ La solución debe tener la opción de copia de seguridad y restauración para la configuración del servidor AV.
- ✓ La solución debe tener una opción de Implementación de tareas para deshabilitar los módulos requeridos por un período breve.
- ✓ La solución debe tener sincronización de directorio activo
- ✓ La solución debe tener la opción "Transmisión de mensajes"
- ✓ La solución debe tener una opción basada en políticas para mover las computadoras sin licencia si no están conectadas por un número específico de días.
- ✓ La solución debe tener la opción de alertas de eventos críticos. (por ejemplo, ransomware detectado, computadora movida a sin licencia, nueva computadora detectada, etc.)
- ✓ La solución debe tener una funcionalidad automática para eliminar la computadora de la Consola de Gestión si se desinstala AV.
- ✓ Con la ayuda de un actualizador en vivo de cliente propio del agente de antivirus, los eventos relacionados con el antivirus y el estado de seguridad de todos los puntos finales se capturan y registran y se pueden monitorear en tiempo real.
- ✓ La solución debería poder crear un USB de arranque con un kit de herramientas AV integrado
- ✓ La solución debería poder restaurar la configuración predeterminada
- ✓ La solución debe tener una interfaz integrada para cargar muestras de virus
- ✓ La solución debería poder descargar actualizaciones de Windows Essential
- ✓ La solución debe tener un limpiador de registro incorporado
- ✓ Debe tener una opción de arranque en modo de rescate para que sea posible escanear sin cargar el sistema operativo instalado
- ✓ La solución debe tener un soporte de red de seguridad en la nube
- ✓ La solución debe estar protegida con contraseña en los clientes.
- ✓ La solución debe tener una contraseña de desinstalación separada.
- ✓ la solución debe integrarse con el cliente de soporte remoto para que el OEM pueda brindar soporte rápido
- ✓ La solución debe integrarse con una herramienta de entrada de generación de datos que no debe ser susceptible a los registradores de teclas
- ✓ La solución debe tener una función DLP cuyos datos se puedan marcar para protegerlos contra el acceso y la modificación a través de la red
- ✓ La solución debe tener una funcionalidad integrada que brinde control total sobre el punto final para realizar análisis, instalaciones, visualización de pantalla

OTRAS FUNCIONALIDAES NECESARIAS

- ✓ Integración directa con MITRE ATT&CK Framework que permite Correlación basada en TTPs reales de atacantes conocidos
- ✓ Búsqueda automatizada de IoC vía integración con MISP que permita integración directa con servidor MISP
- ✓ Bloqueo en tiempo real de IoCs, esto a partir de hashes maliciosos, bloqueo inmediato
- ✓ Visualización de alertas con contexto forense enriquecido con Información detallada de procesos, árbol de ejecución, DLLs, etc.
- ✓ Consulta rápida a endpoints en tiempo real Ideal para respuesta inmediata desde consola

- ✓ Visibilidad de procesos activos y su árbol de relaciones, que permita análisis de ataques avanzados y fileless
- ✓ Monitoreo de actividad de archivos confidenciales con notificación ante copia, renombrado o eliminación
- ✓ Soporte para protección y monitoreo de endpoints roaming que funciona incluso fuera de red corporativa
- ✓ Gestión multisede que usa consola centralizada para múltiples ubicaciones
- ✓ Alta disponibilidad (HA) para continuidad operativa ante fallos de hardware
- ✓ Sandboxing en la nube como complemento para análisis profundo sin requerir hardware adicional
- ✓ Integración con BitLocker para gestión de cifrado que permita aplicar y controlar políticas de cifrado
- ✓ EFS – Enterprise File Search para búsqueda avanzada de archivos maliciosos en todos los endpoints
- ✓ Modo solo monitoreo en control de aplicaciones que permite registrar sin bloquear para evaluar impactos
- ✓ Auditoría de políticas con comparativo antes/después para el Ideal para cumplimiento regulatorio y análisis forense
- ✓ Visualización de dashboards en tiempo real con indicadores clave de seguridad, cumplimiento, licencias, etc.
- ✓ Integración con SIEM, SNMP y plataformas externas (Syslog, Splunk) para envío de logs estructurados en tiempo real
- ✓ Política de seguridad dedicada para servidores Windows que es más restrictiva y especializada
- ✓ Eliminación automatizada de endpoints sin protección activa con ayuda a mantener la higiene del entorno
- ✓ Herramienta USB de arranque con motor AV integrado que es ideal para recuperación ante incidentes graves
- ✓ Monitoreo de sesión de usuarios (conexión, desconexión, etc.) para detección de actividad sospechosa fuera de horario, por ejemplo
- ✓ Restricción de módulos de AV por tiempo definido (modo mantenimiento), útil para tareas administrativas o pruebas internas
- ✓ Transmisión de mensajes desde la consola al usuario final, para alertas, mantenimiento, notificaciones

IV. REGLAMENTOS TECNICOS, NORMAS METROLOGICAS Y/O SANITARIAS (De corresponder)

No aplica

V. ACONDICIONAMIENTO, MONTAJE O INSTALACION (De corresponder)

INSTALACION Y PUESTA EN PRODUCCION.

- ✓ El postor podrá realizar la implementación o instalación de la solución de forma remota o presencial.
- ✓ Al ser una solución de tipo **LLAVE EN MANO**, el postor deberá de realizar los trabajos de instalación, configuración y puesta en producción de la solución propuesta a cuenta del postor.
- ✓ El postor deberá realizar la instalación de mínimo: el 100% de estaciones de trabajo y el 100% de servidores de red, esto forma parte de los bienes a adquirir, así como

en el caso se requiera desinstalar el antivirus existente, el postor efectuará esta labor en los equipos sin costo para la ZOFRATACNA debiendo garantizar que la operatividad de los servicios brindados por la ZOFRATACNA, no se afecten y que la red se encuentre protegida.

- ✓ Por razones de seguridad de la información y continuidad de operaciones debe asegurarse la integridad de la información y la protección de los equipos (estaciones de trabajo y servidores de red) de la red de datos contra los ataques originados por virus informáticos y sus variantes.
- ✓ Si fuera el caso, que el producto ofertado, fuera el mismo que viene utilizando ZOFRATACNA, el portor deberá de verificar la actual consola de administración, eliminando todo evento anterior al actual servicio.
- ✓ En el caso de las instalaciones (estaciones de trabajo y servidores de red), se deberá de considerar dentro de la configuración, retirar toda ventana emergente que afecte toda productividad del usuario.

ENTREGABLES

- ✓ **Licencias de Software:**
  - Licencias activadas a nombre de ZOFRATACNA en cuenta corporativa del fabricante.
  - Documento oficial del fabricante que acredite la activación y vigencia de licencias.
- ✓ **Informe Técnico de Instalación y Configuración:**
  - Documento detallado con topologías y diagramas de conexión y funcionamiento y capturas de pantalla que respalden el proceso de instalación efectiva del software en servidores y estaciones de trabajo (100%).
- ✓ **Protocolos de Pruebas y Acta de Aceptación:**
  - Documento con protocolos detallados de las pruebas funcionales realizadas (detección de amenazas, pruebas de firewall, control USB, etc.).
  - Acta de conformidad técnica firmada por el responsable de ATIC.
- ✓ **Informe de Capacitación:**
  - Registro de asistencia, contenido programático, certificados emitidos por el fabricante, archivos de video de las sesiones de capacitación técnica (mínimo 12 horas efectivas).
- ✓ **Plan de Gestión y Soporte Técnico:**
  - Documento protocolos y procedimientos de soporte técnico proactivo, procedimientos de soporte reactivo, números de contacto directo, celulares y correos electrónicos y esquema de mesa de ayuda (Help Desk).
  - Cronograma anual de soporte preventivo y emisión de informes anuales del estado de la solución antivirus instalada.
- ✓ **Documentación Técnica del Fabricante:**
  - Manuales oficiales completos, guías técnicas, guías de administración y operación de la solución adquirida, en formato digital.

VI. GARANTÍA COMERCIAL (Obligatorio)

- ✓ **Condiciones de la garantía**:
  Se cubrirán las actualizaciones para la versión de software que publique el fabricante durante el periodo de garantía vigente. Aplicable para nuevas ediciones de las estaciones de trabajo, servidores de red y consola de administración.

- ✓ **Periodo de la garantía**:
  Las licencias ofertadas deben contar con tres (03) años de garantía, para ello, el postor deberá acreditar a través de una declaración jurada simple acompañada obligatoriamente de una constancia oficial emitida por el fabricante, certificando la vigencia y cobertura específica para la solución ofertada.

- ✓ **Inicio del cómputo del periodo de la garantía**:
  El periodo de la garantía se inicia a partir de la fecha en la que se emite la conformidad por la implementación de la solución de antivirus

VII. MUESTRAS (De corresponder)

No aplica

VIII. SERVICIOS CONEXOS (Opcional) -

TRANSFERENCIA DE CONOCIMIENTO Y CAPACITACION TÉCNICA.

- ✓ Capacitación técnica por parte de personal acreditado por el fabricante con una duración mínima de 12 horas, para el personal que administrará la plataforma antivirus (sesiones de 04 sesiones diarias que pueden ser virtuales) para CUATRO (04) participantes. Temas resaltantes que deberán estar incluidas relacionados a la solución ofertada como mínimo deberá de contener:
  1. Procedimiento de Instalación de la plataforma en la ZOFRATACNA.
  2. Administración y gestión de incidente de la plataforma
  3. Solución de problemas.
- ✓ La capacitación se realizará dentro del plazo que tiene el postor para realizar la implementación de la solución propuesta y podrá ser IN SITU o VIRTUAL.
- ✓ Los certificados/constancias deberán formar parte del informe final a presentarse y estarán emitidos por el fabricante.

IX. PRESTACIONES ACCESORIAS (De corresponder)

9.1 SOPORTE PROACTIVO Y DE GESTION.

- ✓ Servicio Proactivo, el postor deberá emitir un informe anual del estado de la solución de antivirus implementada en ZOFRATACNA, en ella deberá de considerar el estado de la solución, incidentes presentados y correcciones realizadas (como parte de la gestión del postor) con la finalidad que la consola de administración solo presente avisos relevantes/urgentes sobre el servicio. Dicho informe deberá ser enviado vía mesa de partes virtual con atención al jefe del Área de TIC en un plazo no mayor a los CINCO (5) días calendario, contabilizado a partir del día siguiente de finalizado el año.

9.2 SOPORTE TECNICO ON LINE 24X7

- ✓ Soporte Técnico por el periodo contratado, a cargo de personal propio certificado y especializado sobre el producto ofertado. Este soporte técnico se brindará a través de comunicación electrónica como e-mail y medios de telefonía fija o celular, teniendo como objetivo absolver consultas técnicas y dar soporte a incidentes reportados.
- ✓ El servicio y soporte telefónico recibirá las llamadas telefónicas y asegurará el seguimiento de solicitudes de soporte técnico hasta su completa resolución mediante sistemas de Help Desk o Mesa de Ayuda.

X. REQUISITOS DEL PROVEEDOR Y/O PERSONAL (De corresponder)

Del Proveedor:

- ✓ El postor debe acreditar un monto facturado acumulado equivalente a S/ 126,000.00 soles (Ciento Veinte y Seis mil con 00/100 soles), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los diez (10) años anteriores a la fecha de la presentación de ofertas que se computaran desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

  Se consideran bienes similares a los siguientes:
  - Adquisición y/o Venta de antivirus endpoint para estaciones de trabajo y servidores; y/o
  - Venta y/o Renovación de licencias de software antivirus; y/o
  - Venta de soluciones de seguridad antivirus; y/o
  - Suscripción de Licencias Antivirus; y/o
  - Licenciamiento de software de soluciones y/o bienes, relacionados a: seguridad informática y/o seguridad de la información y/o análisis y gestión de riesgos cibernéticos.
  - Venta de Licencias EDR
  - Venta de plataformas de protección y seguridad de Endponint.

- ✓ Por otro lado, deberá de estar registrado como canal autorizado del fabricante de la solución propuesta; estar autorizado en el Perú por el fabricante y/o mayorista asociado al fabricante de la solución ofertada; se podrá acreditar mediante una declaración jurada simple.

  Acreditación

  - ✓ La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de compra, 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 la cancelación del mismo con comprobante de pago [1], o comprobante de retención electrónico emitido por SUNAT por la retención del IGV, correspondientes a un máximo de veinte contrataciones. En caso el postor sustente su experiencia en la especialidad mediante contrataciones realizadas con privados [2], para acreditarla debe presentar de forma obligatoria lo indicado en el numeral (ii) del presente párrafo; no es posible que acredite su experiencia únicamente con la presentación de contratos u órdenes de compra con conformidad o constancia de prestación.

    [1] El solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Es válido el sello colocado por el cliente del postor (sea utilizando el término “cancelado” o “pagado”).
    [2] Entendiéndose por estas a aquellos que no son entidades contratantes.

Del Personal.

Contar como mínimo con el siguiente personal para la ejecución del proyecto:

- ✓ **Un (01) Gerente de Proyectos**
  - Profesional titulado de formación como Ingeniero Eléctrico y/o electrónico y/o telecomunicaciones y/o Sistemas y/o Informático y/o afines.
  - Contar con una experiencia mínima de cinco (05) años en el puesto solicitado o similar.
  - La experiencia que se pretenda acreditar deberá ser posterior a la titulación.
  - Contar con Certificado de Ethical Hacker.
  - Deberá de estar certificado por el fabricante de la solución propuesta.

- ✓ **Un (01) Especialista**
  - Grado de bachiller en Ingeniería de Sistemas y/o Informática, Electrónica y/o Telecomunicaciones y/o Redes y/o Computación e Informática.
  - Debe contar con al menos un (01) certificación técnica vigente del fabricante de la solución ofertada, vigencia máxima dos (02) años de fecha anterior a la convocatoria.
  - Experiencia no menor de dos (02) años como Administrador y/o Implementador de soluciones de seguridad.

- ✓ **Nota:** Como parte de la propuesta, se deberá de acreditar el título profesional y el grado de bachiller del gerente y especialista; así como copias de los certificados respectivos (toda la documentación en copias simples).

XI. LUGAR Y PLAZO DE ENTREGA (Obligatorio)

Lugar: "Los bienes deben ser entregados en el almacén de la ZOFRATACNA, sito en Carretera Panamericana Sur Km. 1308, Complejo ZOFRATACNA MZ-G, de lunes a viernes en el horario de 09.00 am a 16:30 horas.

Plazo: QUINCE (15) días calendario, 07 días para la entrega de los bienes y 08 días para la instalación, licenciamiento, puesta en producción y capacitación, contados a partir del día siguiente de notificada la orden de compra y/o suscrito el contrato.

XII. CONFORMIDAD DEL BIEN (Obligatorio)

La conformidad estará a cargo de la jefatura del área de tecnologías de la información y comunicaciones de la Gerencia de Operaciones de ZOFRATACNA.

De existir observaciones la entidad las comunica al contratista indicando claramente el sentido de estas, otorgándole un plazo para subsanar. El plazo de subsanación no debe ser mayor del 30% del plazo del entregable correspondiente. Si pese al plazo otorgado, el contratista no cumpliese a cabalidad con la subsanación, la entidad puede otorgar plazos adicionales o resolver el contrato. En caso de otorgarse plazo adicional 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 contratante para efectuar las revisiones y notificar las observaciones correspondientes.

XIII. FORMA Y CONDICIONES DE PAGO (Obligatorio)

PRESTACION PRINCIPAL:

El pago será único, una vez se cuente con la conformidad del responsable del Área de Tecnologías de la Información y Comunicaciones y a la presentación de la factura.

"El pago se efectuará mediante abono en cuenta bancaria o cheque de gerencia, para cuyo efecto el postor comunicará el medio elegido, mediante una Carta de Autorización según el modelo que remitirá el Área de Logística."

PRESTACIÓN ACCESORIA:
El pago será parcial, para los servicios de Soporte Proactivo y de Gestión por tres (03) años, el postor deberá de presentar un informe anual por el periodo de contratación.

Para efectos del pago de las contraprestaciones ejecutadas por el postor, la entidad debe contar con la siguiente documentación:
- Informe del responsable del Área de Tecnologías de la Información, emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.
- Informe anual del estado de la plataforma antivirus elaborada por el portor.

"El pago se efectuará mediante abono en cuenta bancaria o cheque de gerencia, para cuyo efecto el postor comunicará el medio elegido, mediante una Carta de Autorización según el modelo que remitirá el Área de Logística."

XIV. RESPONSABILIDAD DEL CONTRATISTA

El contratista es el responsable por la calidad ofrecida y por los vicios ocultos del servicio ofertado por un plazo no menor de 03 años, contado a partir de la conformidad otorgada por la Entidad

XV. PENALIDADES (Obligatorio)

Penalidad por Mora en la ejecución de la prestación:
Si EL CONTRATISTA incurre en retraso injustificado en la ejecución de las prestaciones objeto del contrato, LA ENTIDAD le aplica automáticamente una penalidad por mora por cada día de atraso, de acuerdo con la siguiente fórmula:

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

Donde:
F = 0.40

- Tanto el monto como el plazo se refieren, según corresponda, a la ejecución total o a la obligación parcial, de ser el caso, que fuera materia de retraso.
- Se considera justificado, el retraso cuando el contratista acredite de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable.
- Esta calificación del retraso como justificado no da lugar al pago de gastos generales de ningún tipo.
- Las penalidades se deducen de los pagos a cuenta, pagos parciales o del pago final, según corresponda.

- Cuando se llegue a cubrir el monto máximo de la aplicación de la penalidad por mora y otras penalidades, de ser el caso, LA ENTIDAD puede resolver el contrato por incumplimiento.
- El monto máximo a aplicar es del diez por ciento (10%) del contrato vigente.

XVI. OTRAS PENALIDADES

Se establecen penalidades técnicas adicionales, según la siguiente tabla:

Supuestos de aplicación	Forma de cálculo	Procedimiento
Incumplimiento de instalación total del parque informático (servidores y estaciones)	0.2% del monto total contratado por cada equipo no instalado	Verificación física por parte de ATIC
Incumplimiento del plazo para entrega de documentación técnica completa	0.1% del monto total contratado por cada día calendario de retraso	Revisión documental por parte de ATIC
No presentación o presentación incompleta de informe anual del estado de la solución antivirus	0.5% del monto correspondiente al servicio anual por cada día de retraso	Verificación documental ÁTIC

XVII RESOLUCION CONTRACTUAL

Se puede resolver el contrato, en los siguientes casos:

a) Por el incumplimiento injustificado de las obligaciones contractuales, legales o reglamentarias a su cargo, pese a haber sido requerido para ello.
b) Por la acumulación del monto máximo de la penalidad por mora o por el monto máximo para otras penalidades, en la ejecución de la prestación a su cargo.
c) Por la paralización o reducción injustificada de la ejecución de la prestación, pese a haber sido requerido para corregir tal situación.
d) Por caso fortuito o fuerza mayor que imposibilite de manera definitiva la continuidad de la ejecución, amparado en un hecho o evento extraordinario, imprevisible e irresistible; o por un hecho sobreviniente al perfeccionamiento del contrato, orden de compra o servicio, que no sea imputable a las partes.

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.

XVIII CLAÚSULA ANTICORRUPCION 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.

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 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 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.

XIX. SOLUCION DE CONTROVERSIAS

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

FIRMA Y SELLO DEL JEFE DEL ÁREA USUARIA

FIRMA DIGITAL

Firmado digitalmente por:
ROJAS MORALES Ivan Cesar
FAU 20147797011 hard
Motivo: Soy el autor del documento
Fecha: 22/07/2025 14:16:41-0500