

VERIFICACIÓN DEL CUMPLIMIENTO DE LOS DOCUMENTOS DE PRESENTACIÓN OBLIGATORIA

ADJUDICACIÓN SIMPLIFICADA N° 0070-2023-SEDAPAL  
ADQUISICIÓN DE SEGURIDAD ANTIMALWARE CORPORATIVO DE ESTACIONES DE TRABAJO

POSTOR: INNOVARE E-BUSINESS S.A.C.

2.2.1. DOCUMENTACIÓN DE PRESENTACIÓN OBLIGATORIA

2.2.1.1. Documentos para la admisión de la oferta

			FOLIO
a)	Declaración jurada de datos del postor. (Anexo N° 1).	CUMPLE	5
b)	Documento que acredite la representación de quien suscribe la oferta.  En caso de persona jurídica, copia del certificado de vigencia de poder del representante legal, apoderado o mandatario designado para tal efecto.  En caso de persona natural, copia del documento nacional de identidad o documento análogo, o del certificado de vigencia de poder otorgado por persona natural, del apoderado o mandatario, según corresponda.  En el caso de consorcios, este documento debe ser presentado por cada uno de los integrantes del consorcio que suscriba la promesa de consorcio, según corresponda.	CUMPLE (Expedido el 29.09.2023)	6 al 7
c)	Declaración jurada de acuerdo con el literal b) del artículo 52 del Reglamento. (Anexo N° 2).	CUMPLE	8
d)	Declaración jurada de cumplimiento de los Términos de Referencia contenidos en el numeral 3.1 del Capítulo III de la presente sección. (Anexo N° 3).	CUMPLE	9
e)	Adjuntar de manera obligatoria folletos u hojas técnicas o cualquier otro documento emitido por el fabricante, que permita la verificación del cumplimiento de las especificaciones técnicas mínimas detalladas en "Características Técnicas" de las Fichas Técnica establecida en el Capítulo III de las Bases. Tales como: Material, dimensiones, clase y normas.	VERIFICACION DE LOS ASPECTOS DE LAS CARACTERISTICAS Y/O ESPECIFICACIONES TÉCNICAS MÍNIMAS REQUERIDAS.	10 al 124 152 al 217
f)	Declaración jurada de plazo de entrega. (Anexo N° 4).	CUMPLE	125
g)	Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. (Anexo N° 5).	NO APLICA	—
h)	El precio de la oferta en Soles (S/) debe registrarse directamente en el formulario electrónico del SEACE.  Adicionalmente, se debe adjuntar el Anexo N° 6 en el caso de procedimientos convocados a precios unitarios, esquema mixto de suma alzada y precios unitarios, porcentajes u honorario fijo y comisión de éxito, según corresponda.  En el caso de procedimientos convocados a suma alzada únicamente se debe adjuntar el Anexo N° 6 cuando corresponda indicar el monto de la oferta de la prestación accesoria o que el postor goza de alguna exoneración legal.  El precio total de la oferta y los subtotales que lo componen son expresados con dos (2) decimales. Los precios unitarios pueden ser expresados con más de dos (2) decimales.	CUMPLE	126

OFERTA ADMITIDA

CUMPLIMIENTO DE ESPECIFICACIONES TECNICAS

ITEM N°	DESCRIPCIÓN	RESULTADO (*)
ÚNICO	ADQUISICIÓN DE SEGURIDAD ANTIMALWARE CORPORATIVO DE ESTACIONES DE TRABAJO	CUMPLE CON LOS REQUERIMIENTOS TÉCNICOS MÍNIMOS.

Mediante Memorando N° 1825-2023-ETIC de fecha 16.10.2023, el Equipo Tecnologías de la Información y Comunicaciones en su calidad de área usuaria, indicó que la oferta de Innovare E-Business S.A.C. cumple con los requerimientos técnicos mínimos; según verificación de cumplimiento de las especificaciones técnicas requeridas en el procedimiento de selección.

VALOR ESTIMADO:	S/. 478,298.72
VALOR OFERTADO:	S/. 408,520.00
MENOR OFERTA:	S/. 408,520.00

FACTORES DE EVALUACIÓN

FACTOR	Metodología	Precio Ofertado	Puntaje
<b>A. PRECIO</b> <b>Evaluación:</b> Se evaluará considerando el precio ofertado por el postor.  <b>Acreditación:</b> Se acreditará mediante el registro en el SEACE o el documento que contiene el precio de la oferta (Anexo N° 6), según corresponda.	La evaluación consistirá en otorgar el máximo a la oferta de precio más bajo y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos precios, según la siguiente fórmula:  $P_i = \frac{O_m \times PMP}{O_i}$ I = Oferta P <sub>i</sub> = Puntaje de la oferta a evaluar O <sub>i</sub> = Precio i O <sub>m</sub> = Precio de la oferta más baja PMP = Puntaje máximo del precio  <b>100 puntos</b>	S/. 408,520.00	100.00
<b>PUNTAJE TOTAL:</b>			<b>100.00</b>

CESAR MURILLO BENAVIDES

Jefe Equipo Gestión del Abastecimiento (e)

Equipo Gestión del Abastecimiento

VERIFICACIÓN DEL CUMPLIMIENTO DE LOS DOCUMENTOS DE PRESENTACIÓN OBLIGATORIA

ADJUDICACIÓN SIMPLIFICADA N° 0072-2023-SEDAPAL  
ADQUISICIÓN DE SEGURIDAD ANTIMALWARE CORPORATIVO DE ESTACIONES DE TRABAJO

POSTOR: IMPERIA SOLUCIONES TECNOLÓGICAS S.A.C.

2.2.1. DOCUMENTACIÓN DE PRESENTACIÓN OBLIGATORIA

2.2.1.1. Documentos para la admisión de la oferta			FOLIO
a)	Declaración jurada de datos del postor. (Anexo N° 1).	CUMPLE	2
b)	Documento que acredite la representación de quien suscribe la oferta.  En caso de persona jurídica, copia del certificado de vigencia de poder del representante legal, apoderado o mandatario designado para tal efecto.  En caso de persona natural, copia del documento nacional de identidad o documento análogo, o del certificado de vigencia de poder otorgado por persona natural, del apoderado o mandatario, según corresponda.  En el caso de consorcios, este documento debe ser presentado por cada uno de los integrantes del consorcio que suscriba la promesa de consorcio, según corresponda.	CUMPLE (Expedido el 23.09.2023)	3 al 7
c)	Declaración jurada de acuerdo con el literal b) del artículo 52 del Reglamento. (Anexo N° 2).	CUMPLE	8
d)	Declaración jurada de cumplimiento de los Términos de Referencia contenidos en el numeral 3.1 del Capítulo III de la presente sección. (Anexo N° 3).	CUMPLE	9 al 19
e)	Adjuntar de manera obligatoria folletos u hojas técnicas o cualquier otro documento emitido por el fabricante, que permita la verificación del cumplimiento de las especificaciones técnicas mínimas: detalladas en "Característica Técnicas" de las Fichas Técnica establecida en el Capítulo III de las Bases. Tales como: Material, dimensiones, clase y normas.	VERIFICACION DE LOS ASPECTOS DE LAS CARACTERISTICAS Y/O ESPECIFICACIONES TÉCNICAS MÍNIMAS REQUERIDAS.	20 al 37
f)	Declaración jurada de plazo de entrega. (Anexo N° 4).	CUMPLE	38
g)	Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. (Anexo N° 5).	NO APLICA	—
h)	El precio de la oferta en Soles (S/) debe registrarse directamente en el formulario electrónico del SEACE.  Adicionalmente, se debe adjuntar el Anexo N° 6 en el caso de procedimientos convocados a precios unitarios, esquema mixto de suma alzada y precios unitarios, porcentajes u honorario fijo y comisión de éxito, según corresponda.  En el caso de procedimientos convocados a suma alzada únicamente se debe adjuntar el Anexo N° 6 cuando corresponda indicar el monto de la oferta de la prestación accesoria o que el postor goza de alguna exoneración legal.  El precio total de la oferta y los subtotales que lo componen son expresados con dos (2) decimales. Los precios unitarios pueden ser expresados con más de dos (2) decimales.	CUMPLE	39
OFERTA NO ADMITIDA			

CUMPLIMIENTO DE ESPECIFICACIONES TÉCNICAS

ÍTEM N°	DESCRIPCIÓN	RESULTADO (*)
ÚNICO	ADQUISICIÓN DE SEGURIDAD ANTIMALWARE CORPORATIVO DE ESTACIONES DE TRABAJO	NO CUMPLE CON LOS REQUERIMIENTOS TÉCNICOS MÍNIMOS.

Mediante Memorando N° 1825-2023-ETIC de fecha 16.10.2023, el Equipo Tecnologías de la Información y Comunicaciones en su calidad de área usuaria, indicó que la oferta de IMPERIA SOLUCIONES TECNOLÓGICAS S.A.C. No cumple con los requerimientos técnicos mínimos; según verificación de cumplimiento de las especificaciones técnicas requeridas en el procedimiento de selección.

Imperia Soluciones Tecnológicas S.A.C.	NO CUMPLE	Presenta Anexo #3 Declaración Jurada de Cumplimiento de las Especificaciones Técnicas omitiendo el cumplimiento de la actualización http del requerimiento "La solución deberá permitir configurar las actualizaciones en modo HTTP y HTTPS según lo requiera el administrador de la solución."
--	-----------	---

CESAR MURILLO BENAVIDES

Jefe Equipo Gestión del Abastecimiento (e)





Equipo Tecnologías de la  
Información y Comunicaciones



Firmado digitalmente por:  
ASCHIERO PEREA Alejandro  
Rene FAU 20100152356 soft  
Motivo: Soy el autor del  
documento  
Fecha: 16/10/2023 08:40:41-0500

Memorando N° 1825 -2023-ETIC

A : Cesar Murillo Benavides  
Jefe Equipo Gestión del Abastecimiento.

Asunto : Evaluación de Cumplimiento de Especificaciones Técnicas.

Referencia : Memorando N° 1057-2023-EGAb Adjudicación Simplificada Nro. 070-2023-SEDAPAL "Adquisición de Seguridad Antimalware Corporativo de Estaciones de Trabajo" Reg. N° 149039-22

Fecha : Lima, 16 de octubre de 2023

Por medio del presente, nuestra área de soporte a realizado la revisión de las especificaciones técnicas para la Adjudicación Simplificada Nro.070-2023-SEDAPAL "Adquisición de Seguridad Antimalware Corporativo de Estaciones de Trabajo", las mismas que se han registrado según se muestra en el siguiente cuadro de evaluación a los postores participantes:

Empresa	Propuesta	Observaciones
Innovare E-Business S.A.C	CUMPLE	Presenta Anexo #3 Declaración Jurada de Cumplimiento de las Especificaciones Técnicas.
Imperia Soluciones Tecnológicas S.A.C.	NO CUMPLE	Presenta Anexo #3 Declaración Jurada de Cumplimiento de las Especificaciones Técnicas omitiendo el cumplimiento de la actualización http del requerimiento "La solución deberá permitir configurar las actualizaciones en modo HTTP y HTTPS según lo requiera el administrador de la solución."

Para cualquier consulta adicional agradeceré comunicarse con el Sr. Alejandro Aschiero Perea [aaschier@sedapal.com.pe](mailto:aaschier@sedapal.com.pe), celular: 998322429

Se adjunta Archivo con la Evaluación de las Propuestas.

Atentamente,

Hugo Bustamante Mondragon  
Jefe Equipo Tecnologías de la  
Información y Comunicaciones



Firmado digitalmente por  
BUSTAMANTE  
MONDRAGON Hugo  
Ronald FAU 20100152356  
soft  
Fecha: 2023.10.16 09:08:23  
-05'00'



Firmado digitalmente por:  
CRUZ ARMAS Juana Mavila  
FAU 20100152356 soft  
Motivo: En señal de  
conformidad  
Fecha: 16/10/2023 08:49:46-0500

Empresa	Innovare E-Business S.A.C	Impería Soluciones Tecnológicas S.A.C.
Solución Antimalware Presentada	With Secure	Sophos Intercept X with XDR
CARACTERISITICAD TECNICAS DE LA FICHA Nro. 63290		
Deberá soportar los sistemas operativos de estaciones de trabajo en versiones de 64 bits de Microsoft Windows 10 y 11. Opcionalmente sistemas operativos de versiones anteriores. Mac OS 12 en adelante y Linux Desktop en sus últimas versiones.	CUMPLE	CUMPLE
La solución deberá proteger contra virus, troyanos, macrovirus, adware, spyware, gusanos, rootkits y todo tipo de programa malicioso (malware) adicionalmente debe proteger contra amenazas avanzadas tipo ransomware, Dia Cero.	CUMPLE	CUMPLE
La solución contra ransomware deberá ser un módulo específico que realice el bloqueo de amenazas de día cero y ataques de ransomware como Locky, WannCry, Petya, etc. sin requerir actualización de firmas.	CUMPLE	CUMPLE
La solución contra ransomware deberá monitorear y bloquear cambios no autorizados en el endpoint como cifrados masivos, cambios en el sistema, modificación de llaves en el registro o creación de archivos y carpetas en áreas no autorizadas del sistema operativo.	CUMPLE	CUMPLE
La solución deberá estar incorporada en el Cuadrante de Gartner del año 2022 en adelante para soluciones de Endpoint Protección. (RESPUESTA A LA CONSULTA/OBSERVACION N° 22 DEL PLIEGO DE ABSOLUCION DE CONSULTAS Y OBSERVACIONES)	CUMPLE	CUMPLE
La solución deberá incorporar un módulo de protección basado en la nube el cual deberá tener acceso rápido a las amenazas nuevas directamente desde el laboratorio del fabricante.	CUMPLE	CUMPLE
La solución deberá permitir bloquear amenazas en base a indicadores de compromiso (IoCs) como máximo luego de 5 minutos de ser aplicadas en la consola.	CUMPLE	CUMPLE



La solución deberá contar con opciones para incluir o excluir programas que puedan ser detectados como comportamiento sospechoso como los instaladores de aplicaciones internas, actualizadores de programas u otras aplicaciones. La exclusión deberá poder realizarse usando el hash SHA-1 y/o SHA-256 y/o MD5 de la aplicación el cual podrá ser marcado como confiable o No confiable. (RESPUESTA A LA CONSULTA/OBSERVACION N° 09 - 10 DEL PLIEGO DE ABSOLUCION DE CONSULTAS Y OBSERVACIONES

La solución deberá permitir realizar acciones sobre el malware detectado ya sea para informar, desinfectar, eliminar, renombrar, preguntar por la acción al usuario o enviar a la cuarentena tanto para el escaneado en tiempo real como para el escaneado manual.

La solución deberá poder realizar el análisis manual ya sea en prioridad normal o en segundo plano con la finalidad de no interrumpir las labores de los usuarios.

La solución deberá incluir un módulo para el control de aplicaciones que permita controlar la ejecución de ciertas aplicaciones en el equipo del usuario.

La solución deberá preguntar al usuario si desea escanear una unidad extraíble (USB, Disco Externo) cuando la conecta al equipo.

La solución deberá permitir configurar las actualizaciones en modo HTTP y HTTPS según lo requiera el administrador de la solución.

La solución deberá permitir configurar una contraseña de acceso a la cuarentena de los puntos finales.

La solución deberá permitir configurar la cantidad de tiempo en la que los archivos en cuarentena serán automáticamente eliminados.

CUMPLE	CUMPLE
CUMPLE	CUMPLE
CUMPLE	CUMPLE
CUMPLE	CUMPLE
CUMPLE	CUMPLE
CUMPLE	NO CUMPLE
CUMPLE	CUMPLE
CUMPLE	CUMPLE

La solución debe opcionalmente incluir un módulo de protección en la navegación web el cual deberá permitir asegurar la navegación realizando las siguientes acciones: o Navegación basada en la reputación de los sitios web permitiendo bloquear el acceso a un sitio web clasificado como inseguro. o La reputación de sitios deberá realizarse mediante consultas a la nube de seguridad del fabricante. o Reforzamiento de las búsquedas o modo SafeSearch. o Deberá mostrar las reputaciones de los sitios web en los resultados de búsqueda en sitios como Google, Yahoo, Bing, etc. o Permitir al usuario continuar la navegación en páginas bloqueadas la misma que debe poder ser desactivada centralmente. o Deberá permitir crear sitios de confianza a los cuales podrán navegar los usuarios sin necesidad de consultar la reputación de estos. La creación deberá admitir dominios completos (p.e. ejemplo.com) y sub-dominios (p.e. www.ejemplo.com). o Deberá permitir crear sitios no permitidos a los cuales los usuarios no podrán navegar sin necesidad de consultar la reputación de estos. La creación deberá admitir dominios completos (p.e. ejemplo.com) y sub-dominios (p.e. www.ejemplo.com). o Deberá tener una opción para bloquear todos los sitios excepto los indicados por el administrador. (RESPUESTA A LA CONSULTA/OBSERVACION N° 13 - 14 DEL PLIEGO DE ABSOLUCION DE CONSULTAS Y OBSERVACIONES)

CUMPLE	CUMPLE
CUMPLE	CUMPLE

La solución deberá incluir un módulo para el control de contenido web pudiendo realizar las siguientes acciones: o Bloqueo de la navegación en sitios de categorías específicas. o Tener categorías de sitios web predefinidas como aborto, publicidad, adulto, alcohol, anonimizadores, subastas, banca, blogs, chat, citas, drogas, entretenimiento, apuesta juegos, piratería, odio, búsqueda de trabajo, servicios de pago, estafa, compras en línea, redes sociales, descargas de software, spam, medios de transmisión, violencia, warez, armas, correo web, P2P, etc. o Filtrar el tipo de contenido que los usuarios pueden descargar desde el internet pudiendo realizar reglas de bloqueo por tipo de archivo (p.e. application/x-executable) y por extensión (p.e \*.exe).

La solución deberá incluir un módulo para el control de conexiones o protector de navegación el cual deberá permitir proteger la navegación de los usuarios a sitios de banco, sitios de comercio electrónico y sitios confiables que se definan mediante el protocolo HTTPS con la finalidad de evitar el phishing o robo de datos a los usuarios.

La solución de control de conexiones o protector de navegación deberá también permitir activar o desactivar las siguientes acciones: o No interrumpir las conexiones activas. o Borrar el portapapeles al cerrar la conexión. o Bloquear la ejecución de herramientas de línea de comandos y herramientas de scripting. o Bloquear el acceso remoto cuando esté activo esta protección con el fin de evitar el acceso no autorizado y la pérdida de datos.

CUMPLE	CUMPLE
CUMPLE	CUMPLE



La solución opcionalmente debe permitir gestionar el cortafuegos de Windows que permita bloquear el tráfico malicioso en la LAN. Este módulo deberá: (RESPUESTA A LA CONSULTA/OBSERVACION N° 15 - 16 -17 – 28 DEL PLIEGO DE ABSOLUCION DE CONSULTAS Y OBSERVACIONES) o Incluir un IPS a nivel de host o HIPS. o Bloquear fragmentos de IP basados en el tamaño definido en la consola de gestión. o Permitir el filtrado de tráfico IPV6. o Permitir configurar tarjetas de red confiables. o Desactivar el firewall de Windows automáticamente. o Aplicar política de firewall del propio fabricante para evitar y parar ataques laterales. o Incluir al menos 5 tipos de perfiles predefinidos por el fabricante con las mejores prácticas de seguridad informática, así como con una opción para seleccionar el perfil automáticamente en base a reglas como: o IP del Servidor DNS o IP del Servidor DHCP o IP del Gateway del equipo o Segmento LAN y la combinación de todas ellas. o Deberá permitir la creación de nuevos perfiles. o Incluir reglas de cortafuegos predefinidas para bloquear el tráfico de malware usado para ataques laterales en una red LAN. Estás reglas deberán ser actualizadas y mantenidas por el fabricante. Permitir añadir reglas personalizadas en los diferentes perfiles predefinidos. o Permitir activar o desactivar una regla definida. o Deberá permitir crear reglas para la cuarentena o aislamiento de equipos basado en un editor de reglas incorporado en la solución. Además, deberá permitir definir la lista de dominios de internet que serán accesibles durante este proceso

CUMPLE	CUMPLE
--------	--------

La solución opcionalmente deberá incluir un módulo para la protección contra vulnerabilidades y actualizaciones de software (parches) multifabricante centralizada que deberá permitir: (RESPUESTA A LA CONSULTA/OBSERVACION N° 02 - 04 – 05 -20 -29 -30 DEL PLIEGO DE ABSOLUCION DE CONSULTAS Y OBSERVACIONES) o Detectar automáticamente, mediante programación y al inicio del equipo la lista de aplicaciones vulnerables y con actualizaciones pendientes. o Deberá permitir mostrar y ocultar la interface en el punto final donde el usuario final y/o administrador pueda ver la lista de aplicaciones vulnerables y con actualizaciones pendientes. o Configurar la prioridad del análisis (Normal y en segundo plano). o Configurar tareas automáticas para la instalación de las correcciones a las vulnerabilidades o parches según su tipo (Críticas, Importantes y Todos). Así mismo, deberá contener un programador de tareas completo que permita la gestión de la programación por día, día de la semana, horario, fecha específica y otros). o Permitir excluir aplicaciones. o Deberá contar con opciones para obligar y/o permitir el reinicio del equipo en caso de ser necesario para aplicar una corrección de una vulnerabilidad y/o parche. o Deberá permitir la integración con el WSUS para actualizaciones de Microsoft. o Deberá permitir activar o desactivar las opciones de notificación al usuario.

CUMPLE	CUMPLE
--------	--------

<p>La solución deberá incluir un módulo para la protección de dispositivos de almacenamiento extraíble el cual deberá: o Crear políticas para permitir, bloquear la escritura y bloquear el acceso a los dispositivos. o Permitir o bloquear la ejecución de binarios almacenados en el dispositivo (.exe, .bat, .com, etc) con la finalidad de evitar la entrada de malware desde dispositivos desconocidos a la red. o Detectar dispositivos de tipo: <input checked="" type="checkbox"/> USB Mass Storage <input checked="" type="checkbox"/> Wireless DVD/CD-ROM</p> <p><input checked="" type="checkbox"/> Windows CE ActiveSync</p> <p><input checked="" type="checkbox"/> Floppy Drives</p> <p><input checked="" type="checkbox"/> Modems</p> <p><input checked="" type="checkbox"/> COM &amp; LTP</p> <p><input checked="" type="checkbox"/> Impresoras</p> <p><input checked="" type="checkbox"/> Lectores de Smart Cards</p> <p><input checked="" type="checkbox"/> Cámaras y Scanners</p> <p><input checked="" type="checkbox"/> IrDA</p> <p><input checked="" type="checkbox"/> Bluetooth</p> <p><input checked="" type="checkbox"/> Controladores de Bus IEEE</p>	<p>CUMPLE</p>	<p>CUMPLE</p>
<p><b>CARACTERÍSTICAS DEL MÓDULO DE DETECCIÓN Y RESPUESTA DE AMENAZAS (EDR)</b></p>	<p>CUMPLE</p>	<p>CUMPLE</p>
<p>Deberá incluir un sistema de detección y respuesta de amenazas integrada a la solución endpoint propuesta, el mismo que no deberá requerir la instalación de un agente por separado.</p>	<p>CUMPLE</p>	<p>CUMPLE</p>
<p>Deberá activarse desde la consola de administración los módulos de EDR y Respuesta Automatizada.</p>	<p>CUMPLE</p>	<p>CUMPLE</p>
<p>Deberá soportar la instalación de sensores livianos en los sistemas operativos Windows y MacOS, pudiendo desplegarse en las versiones de SO para estaciones</p>	<p>CUMPLE</p>	<p>CUMPLE</p>
<p>La solución deberá incluir el análisis de comportamiento, para detectar todas las amenazas conocidas y desconocidas. El aprendizaje automático debe mejorar las detecciones al reconocer nuevas tácticas, técnicas y procedimientos emergentes con lanzamientos de procesos asociados, conexiones de red y tipos de aplicaciones.</p>	<p>CUMPLE</p>	<p>CUMPLE</p>



Deberá contar con opciones para la respuesta a incidentes avanzada para la: o

- Investigación de ataques e incidentes [\[1\]](#) Recuperar archivos [\[2\]](#) Recuperar el historial de PowerShell [\[3\]](#) Recuperar entradas del registro de eventos [\[4\]](#) Recuperar registro de eventos [\[5\]](#)
- Recuperar registros de antivirus [\[6\]](#) Recuperar MFT [\[7\]](#) Recuperar archivos de registro [\[8\]](#)
- Mapear el registro [\[9\]](#) Recuperar el MBR [\[10\]](#) Mapear el sistema de archivos [\[11\]](#) Netstat [\[12\]](#)
- Enumerar procesos [\[13\]](#) Enumerar tareas programadas [\[14\]](#) Enumerar servicios [\[15\]](#) Volcado de memoria de procesos [\[16\]](#) Volcado de memoria completo o Contención de ataques e incidentes [\[17\]](#) Matar proceso [\[18\]](#) Matar hilo de procesos o Remediación de ataques e incidentes [\[19\]](#) Eliminar archivos [\[20\]](#) Eliminar entradas del registro [\[21\]](#) Eliminar tareas programadas [\[22\]](#) Eliminar servicios [\[23\]](#) Hacer Dump de la mem

Deberá permitir correlacionar los eventos detectados, mostrando la cantidad de equipos con detecciones iguales y similares, pudiendo además realizar el aislamiento de los mismos en forma automática.

Deberá permitir realizar el aislamiento de los equipos afectados.

Deberá permitir filtrar las amenazas de acuerdo al riesgo: Bajo, Medio, Alto y Grave.

Deberá permitir tomar acciones de notificación por correo de la incidencia detectada que deberá incluir en dicho reporte: El # de host afectados o El tipo de detección o El nivel de riesgo o El tipo de seguridad de la incidencia o El nivel de importancia crítica de la incidencia

Deberá contar con un sistema de reportes el cual deberá permitir configurar lo siguiente:

- o El envío de reportes diarios, semanales o mensuales de la detección de amenazas.
- o Programar el envío automático de alertas por correo frente a la detección de una amenaza.

Deberá permitir realizar acciones de supervisión y marcado de las amenazas de acuerdo con los siguientes criterios: o Nuevo o Reconocido o En Curso o En Supervisión o Cerrado o Archivado

Al reconocer un incidente este deberá poder ser enviado al Fabricante desde la misma consola para su análisis e investigación de la amenaza con el fin de contar con mayor detalle de la misma, así como recibir información para su reconocimiento y posterior respuesta frente a incidentes iguales o similares.

La consola deberá contar con versiones en inglés y español como mínimo.

[illegible]

Deberá incluir un sistema de generación de reportes gráficos.	CUMPLE	CUMPLE
La solución deberá ser capaz de notificar los eventos de virus a través de diferentes medios (correo electrónico, alertas de registros, etc.	CUMPLE	CUMPLE
La solución deberá generar reportes gráficos, imprimibles y exportables.	CUMPLE	CUMPLE
La solución deberá contener un mecanismo de reportes que permite ver el estado de la protección de la red en línea.	CUMPLE	CUMPLE
La solución deberá permitir acceder a reportes basados en el usuario que permita conocer rápidamente el cumplimiento de políticas por cada usuario.	CUMPLE	CUMPLE
La solución deberá permitir ver las infecciones detectadas en todos los equipos y mostrar: o Fecha y hora de detección o Equipo o Usuario logueado o Tipo de infección y nombre o Acción realizada o Objeto detectado y/o infectado. o Así mismo deberá permitir crear rangos de fecha a visualizar.	CUMPLE	CUMPLE
CARACTERÍSTICAS DEL MODULO DE SANDBOXING		
Características o La solución debe suministrarse como servicio en la nube. o La solución debe proporcionar una detección en tiempo real de: <input type="checkbox"/> Malware previamente desconocido <input type="checkbox"/> Exploits de día cero <input type="checkbox"/> Nuevos ransomware y virus	CUMPLE	CUMPLE
La solución debe admitir los siguientes tipos de archivos para el análisis dinámico: o Archivos ejecutables o Documentos de Office (Word, Excel, PowerPoint, etc.) o Documentos PDF	CUMPLE	CUMPLE
El sandbox debe estar integrado con la solución de seguridad de endpoints y debe proporcionar una respuesta automatizada a nuevas amenazas complejas y ataques dirigidos capaces de eludir la protección de endpoints.	CUMPLE	CUMPLE
La solución debe detectar el tráfico de red malicioso potencial generado por un objeto malicioso como parte de la emulación.	CUMPLE	CUMPLE
La solución debe tener un caché compartido de veredictos para evitar volver a escanear los archivos.	CUMPLE	CUMPLE
El sandbox debe proporcionar a los administradores la capacidad de configurar varias acciones de respuesta automática para el objeto malicioso detectado: <input type="checkbox"/> Eliminar y poner en cuarentena <input type="checkbox"/> Notificar al usuario <input type="checkbox"/> Iniciar un escaneo de áreas críticas <input type="checkbox"/> Buscar objetos detectados en otras máquinas dentro de la red administrada.	CUMPLE	CUMPLE



Deberá permitir la gestión centralizada de actualizaciones, siendo la Consola Central el único equipo en poder descargar actualizaciones desde el fabricante y como herramienta de backup se deberá poder configurar políticas para la descarga de actualizaciones en los Endpoint, desde el fabricante en caso la Consola Central tenga una falla o se encuentre en mantenimiento.

Deberá permitir la instalación y desinstalación remota del software en el Endpoint centralizadamente.

Deberá contar con una Cuarentena de Malware centralizada.

La consola deberá reportar el estado la red en tiempo real como: o Promedio de protección. o Estado de las actualizaciones. o Estado de la protección de malware o Estado de la instalación del endpoint. o Propiedad de los equipos como (Hostname, IP, Dominio/Grupo)

CUMPLE	CUMPLE
CUMPLE	CUMPLE
CUMPLE	CUMPLE
CUMPLE	CUMPLE



<p>vulnerabilidades y parches de software multi-fabricante para estaciones y servidores que deberá: (RESPUESTA A LA CONSULTA/OBSERVACION N° 02 - 04 – 05 -20 -29 -30 DEL PLIEGO DE ABSOLUCION DE CONSULTAS Y OBSERVACIONES) o Reportar las actualizaciones faltantes del sistema operativo y aplicaciones de terceros en los equipos de la red. o Comparar periódicamente el software instalado en el endpoint e identificar las actualizaciones faltantes y las vulnerabilidades encontradas. o Descargar a la Consola Central los paquetes y/o programas necesarios para corregir las vulnerabilidades y parches encontrados con el fin de optimizar el uso de ancho de banda en la red. o Contar con una opción para visualizar las vulnerabilidades y actualizaciones pendientes encontradas en la red y que endpoints se encuentran afectadas por cada una de ellas. Contar con una opción para visualizar las vulnerabilidades y actualizaciones pendientes encontradas en la red x endpoint.</p> <p>o Permitir enviar mediante una política la actualización centralizada de programas y vulnerabilidades en programas de Microsoft y Sistemas Operativos, Java, Mozilla, Google, Adobe, Services Pack, Winzip, Apple, Sun y otras aplicaciones usadas en entornos corporativos.</p> <p>o Permitir la instalación automática y centralizada de actualizaciones, parches y/o correcciones de vulnerabilidades en el sistema operativo y aplicaciones existentes en el endpoint de acuerdo a las políticas definidas por el administrador de la consola.</p> <p>o Permitir programar la instalación de actualizaciones según su importancia (Crítico, Crítico y Vulnerable y Todas) en forma centralizada.</p> <p>o Permitir programar la instalación automática basado en un día y hora.</p> <p>o Analizar el endpoint en búsqueda de aplicaciones vulnerables al inicio del equipo o según una programación establecida en la consola central.</p> <p>o Permitir excluir la instalación de actualizaciones según el tipo de software el cual deberá poder definirse por diversos criterios como:</p>	CUMPLE	CUMPLE
---	--------	--------

La consola deberá permitir crear repositorios o consolas distribuidas que gestionen las actualizaciones tanto del producto, firmas de malware y gestionar centralizadamente en cada punto las descargas del módulo del control de vulnerabilidades y parches con la finalidad de minimizar el uso del ancho de banda. o Los repositorios de actualizaciones deberán soportar como mínimo los mismos sistemas operativos Windows y Linux que la Consola Central

La solución deberá integrarse con el Directorio Activo ya sea para el despliegue como para la configuración de políticas.

La consola deberá permitir crear tareas automatizadas al menos para: o Análisis rápido de malware o Análisis programado de malware Permitir la actualización del producto antimalware

- o Realizar análisis de vulnerabilidades y parches multi-fabricante faltantes en el equipo
- o Instalar actualizaciones y corregir vulnerabilidades según tipo: Críticos, críticos e Importantes, de Seguridad y Todos.
- o Enviar a reiniciar, apagar y/o hibernar los equipos

Así mismo el sistema de programación de tareas deberá contar con un programador de tareas para ejecutar por día, días de semana, finales de semana, horas, una vez, en cada reinicio, cuando un software se instale, actualice o elimine, a la media noche y mensual.

Así mismo deberá soportar la creación de múltiples tareas que pueden activarse o desactivar en el perfil creado.

Permitir configurar mediante una política para evitar desinstalación de los Endpoints aun cuando el usuario en el endpoint tenga privilegios de administrador.

Deberá contar con un sistema para configurar el producto según la ubicación del equipo ya sea esté en la red, por dirección DNS, por servidor DHCP, por Gateway, por IP Wins, por URL disponible o la combinación de ellas.

Permitir bloquear y/o desactivar mediante políticas el acceso a las opciones de configuración del Endpoint.

[illegible]



La consola deberá agrupar automáticamente los equipos basados en la Ruta del Directorio Activo de los equipos, es decir, no deberá requerir instalar ningún agente en el servidor del AD para que se ejecute este agrupamiento.

La consola deberá tener una opción que permita detectar los equipos en la red que se encuentran sin protección. Esta opción podrá usar el Directorio activo y deberá mostrar la siguiente información: o Como nodos de escaneado cualquier equipo con un agente instalado. o Nombre del host o equipo detectado o Último inicio de sesión o Sistema Operativo o OU y GUID del Directorio Activo Opcionalmente mostrar la Fecha de alta del equipo en el AD. (RESPUESTA A LA CONSULTA/OBSERVACION N° 19 DEL PLIEGO DE ABSOLUCION DE CONSULTAS Y OBSERVACIONES)

La consola deberá permitir visualizar y exportar en formato CSV el inventario de hardware de todos los equipos administrados.

La consola deberá permitir visualizar la lista de vulnerabilidades y parches multifabricante con los siguientes datos: o Proveedor o Aplicación detectada o Versión Actual y Pendiente de Actualizar o Así mismo deberá contar con opciones para visualizar el resumen y el historial de instalaciones y exportar en formato CSV para su análisis posterior. o Deberá contar con opciones para enviar comandos para actualizar todos los equipos y/o seleccionar los equipos donde se quiere ejecutar una tarea de corrección de vulnerabilidades o aplicación de los parches detectados.

CUMPLE	CUMPLE
CUMPLE	CUMPLE
CUMPLE	CUMPLE
CUMPLE	CUMPLE

# CALIFICACIÓN DE OFERTA

## ADJUDICACIÓN SIMPLIFICADA N° 0070-2023-SEDAPAL ADQUISICIÓN DE SEGURIDAD ANTIMALWARE CORPORATIVO DE ESTACIONES DE TRABAJO

POSTOR: INNOVARE E-BUSINESS S.A.C.

### 3.2 Documentos para acreditar los requisitos de calificación (Art. 75° del Reglamento de la Ley de Contrataciones)

B. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD	
<p><b>Requisitos:</b> El postor debe acreditar un monto facturado acumulado equivalente a S/500 000,00 (QUINIENTOS MIL y 00/100 soles) incluido IGV, por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. Se consideran bienes similares a los siguientes: -Servicio y/o venta de sistemas o soluciones de control y seguridad de puntos finales o Endpoint Protection" y/o Servicio y/o venta de sistemas o soluciones de Endpoint Detection and Response" y/o Servicio y/o venta de sistemas o soluciones antimalware para protección de puntos finales o Endpoint Protection. <b>Acreditación:</b> 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 voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago, correspondientes a un máximo de veinte (20) contrataciones.</p> <p>En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo referido a la Experiencia del Postor en la Especialidad.</p> <p>En el caso de suministro, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.</p> <p>En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.</p> <p>Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.</p> <p>Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.</p> <p>Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo N° 9.</p> <p>Cuando en los contratos, órdenes de compra o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de compra o de cancelación del comprobante de pago, según corresponda.</p> <p>Sin perjuicio de lo anterior, los postores deben llenar y presentar el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad.</p> <p><b>Importante</b> En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que se hayan comprometido, según la promesa de consorcio, a ejecutar el objeto materia de la convocatoria, conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".</p> <p><b>Importante</b> • Si como resultado de una consulta u observación corresponde precisarse o ajustarse el requerimiento, se solicita la autorización del área usuaria y se pone de conocimiento de tal hecho a la dependencia que aprobó el expediente de contratación, de conformidad con el numeral 72.3 del artículo 72 del Reglamento. • El cumplimiento de las Especificaciones Técnicas se realiza mediante la presentación de una declaración jurada. De ser el caso, adicionalmente la Entidad puede solicitar documentación que acredite el cumplimiento del algún componente de las características y/o requisitos funcionales. Para dicho efecto, consignará de manera detallada los documentos que deben presentar los postores en el literal e) del numeral 2.2.1.1 de esta sección de las bases. • Los requisitos de calificación determinan si los postores cuentan con las capacidades necesarias para ejecutar el contrato, lo que debe ser acreditado documentalente, y no mediante declaración jurada.</p>	

N°	EMPRESA	PERÍODO DE EXPERIENCIA		RESULTADO
		DOCUMENTO	MONTO	
1	MINISTERIO PUBLICO GERENCIA GENERAL	1. Factura Electrónica F001-000039 (20.07.2018) - Adquisición de solución de protección contra códigos maliciosos. 2. Estado de cuenta de ahorros clásica del BCP. 3. Constancia de depósito - Sistema de pago de obligaciones tributarias D. Leg. 940 Cuenta de detracciones Convencional.	S/. 170,000.00	VALIDO. Acredita con copia simple de Factura Electrónica F001-000039 (20.07.2018). Estado de cuenta de ahorros clásica del BCP por el monto de S/153 000,00 y Constancia de depósito - Sistema de pago de obligaciones tributarias D. Leg. 940 Cuenta de detracciones Convencional S/17 000,00. Se valida de acuerdo al objeto del bien facturado por el postor, considerando que guarda relación con la experiencia requerida en las bases integradas. N° Folio: del 128 al 129.
2	MINISTERIO PUBLICO GERENCIA GENERAL	1. Factura Electrónica F001-000048 (06.08.2018) - Adquisición de solución de protección contra códigos maliciosos. 2. Estado de cuenta de ahorros clásica del BCP. 3. Constancia de depósito - Sistema de pago de obligaciones tributarias D. Leg. 940 Cuenta de detracciones Convencional.	S/. 85,000.00	VALIDO. Acredita con copia simple de Factura Electrónica F001-000048 (06.08.2018). Estado de cuenta de ahorros clásica del BCP por el monto de S/76 500,00 y Constancia de depósito - Sistema de pago de obligaciones tributarias D. Leg. 940 Cuenta de detracciones Convencional S/17 000,00. Se valida de acuerdo al objeto del bien facturado por el postor, considerando que guarda relación con la experiencia requerida en las bases integradas. N° Folio: del 130 al 131.
3	MINISTERIO PUBLICO GERENCIA GENERAL	1. Factura Electrónica F001-000058 (27.08.2018) - Licencia Antivirus para protección contra códigos maliciosos. 2. Estado de cuenta de ahorros clásica del BCP. 3. Constancia de depósito - Sistema de pago de obligaciones tributarias D. Leg. 940 Cuenta de detracciones Convencional.	S/. 595,000.00	VALIDO. Acredita con copia simple de Factura Electrónica F001-000058 (27.08.2018). Estado de cuenta de ahorros clásica del BCP por el monto de S/535 500,00 - Constancia de depósito - Sistema de pago de obligaciones tributarias D. Leg. 940 Cuenta de detracciones Convencional S/59 500,00. Se valida de acuerdo al objeto del bien facturado por el postor, considerando que guarda relación con la experiencia requerida en las bases integradas. N° Folio: del 132 al 133.
4	SEGURO SOCIAL DE SALUD - ESSALUD Equipo Gestión del Abastecimiento	1. Factura Electrónica F001-001867 (06.04.2018) - Adquisición de licencias antivirus. 2. Estado de cuenta de ahorros clásica del BCP. 3. Constancia de depósito - Sistema de pago de obligaciones tributarias D. Leg. 940 Cuenta de detracciones Convencional.	S/. 433,333.33	VALIDO. Acredita con copia simple de Factura Electrónica F001-001867 (06.04.2018). Estado de cuenta de ahorros clásica del BCP por el monto de S/381 333,33 - Constancia de depósito - Sistema de pago de obligaciones tributarias D. Leg. 940 Cuenta de detracciones Convencional S/52 000,00. Se valida de acuerdo al objeto del bien facturado por el postor, considerando que guarda relación con la experiencia requerida en las bases integradas. N° Folio: del 134 al 135.
TOTAL:			S/. 1,283,333.33	CUMPLE CON EL MONTO SOLICITADO EN LAS BASES INTEGRADAS.
B. EXPERIENCIA DEL PERSONAL CLAVE				

SUPERVISOR GENERAL DEL SERVICIO (01)					
DANTE ANTIPOORTA POMACAJA - COLEGIATURA 19.09.2006 (Ingeniero de Sistemas) - Capacitación GESTIÓN DE PROYECTOS (GUÍA DEL PMBOK) 30 Horas lectivas - Certificado de PROJECT MANAGEMENT PROFESSIONAL (PMP) expira el 16.05.2026					
Requisitos: Con experiencia mínima de tres (03) años en la Coordinación y/o Supervisión y/o Conducción en Proyectos de Implementación de Tecnología de Información. La experiencia se computará a partir de la obtención de la colegiatura. Acreditación: La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.					
	EMPRESA	PERÍODO DE EXPERIENCIA			RESULTADO
		DEL	AL	AÑOS	
1	INNOVARE E- BUSINESS	01/01/2018	30/09/2023	5.75	VÁLIDO, copia simple de certificado de trabajo desempeñándose como Jefe de Proyectos ha dirigido, supervisado, gerenciado y participado en proyecto de tecnología de información que implican la implementación integral de nuestra soluciones de seguridad (...); guarda relación con la experiencia establecida en los Requisitos de Calificación relacionado a la Experiencia del personal Clave de las Bases Integradas. (Copia simple del certificado de trabajo presentado en Folio 138).
				5.75	CUMPLE SEGÚN LA EXPERIENCIA SOLICITADA EN BASES
A.3	EXPERIENCIA DEL PERSONAL CLAVE				
	TECNICO ESPECIALISTA EN SOPORTE TECNICO DEL SOFTWARE ANTIVIRUS (02)				
	LINK TELLO FLORES - TITULADO 11.11.2009 (INGENIERO DE SISTEMAS) - Certificaciones técnicas: EPP- WITHSECURE ELEMENTS ENDPOINT PROTECTION ENTRENAMIENTO TECNICO (BASICO) / EDR - WITHSECURE ELEMENTS ENDPOINT DETECTION AND RESPONSE - ENTRENAMIENTO TECNICO (BASICO)				
Requisitos: Con experiencia mínima de dos (02) años en actividades de implementación de Soluciones de Seguridad Antimalware. La experiencia se computará a partir del grado de Bachiller o título profesional. Acreditación: La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.					
	EMPRESA	PERÍODO DE EXPERIENCIA			RESULTADO
		DEL	AL	AÑOS	
1	INNOVARE E- BUSINESS	01/01/2010	30/09/2023	13.75	VÁLIDO, copia simple de constancia de trabajo desempeñado como Jefe de Proyectos y Seguridad, en la implementación integral de soluciones de seguridad; instalación, configuración, actualización, administración, mantenimiento, soporte y renovación de los productos y soluciones de seguridad Sophos y Withsecure (...); guarda relación con la experiencia establecida en los Requisitos de Calificación relacionado a la Experiencia del personal Clave de las Bases Integradas. (Copia simple del certificado de trabajo presentado en Folio 143).
				13.75	CUMPLE SEGÚN LA EXPERIENCIA SOLICITADA EN BASES
	JIMMY ARÉVALO LOZANO - TITULADO 01.06.2009 (INGENIERO DE SISTEMAS Y COMPUTO) - Certificaciones técnicas: EPP- WITHSECURE ELEMENTS ENDPOINT PROTECTION ENTRENAMIENTO TECNICO (BASICO) / ENTRENAMIENTO TECNICO EN F-SECURE PSB AND RDR (AVANZADO)				
Requisitos: Con experiencia mínima de dos (02) años en actividades de implementación de Soluciones de Seguridad Antimalware. La experiencia se computará a partir del grado de Bachiller o título profesional. Acreditación: La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.					
	EMPRESA	PERÍODO DE EXPERIENCIA			RESULTADO
		DEL	AL	AÑOS	
1	INNOVARE E- BUSINESS	02/01/2015	30/09/2023	8.75	VÁLIDO, copia simple de constancia de trabajo desempeñado como Especialista, ha participado en la implementación integral, instalación, configuración actualización, administración, mantenimiento, soporte técnico y renovación de los productos y servicios de seguridad Sophos y Withsecure (...); guarda relación con la experiencia establecida en los Requisitos de Calificación relacionado a la Experiencia del personal Clave de las Bases Integradas. (Copia simple del certificado de trabajo presentado en Folio 147).
				8.75	CUMPLE SEGÚN LA EXPERIENCIA SOLICITADA EN BASES
La Oferta del postor INNOVARE E-BUSINESS S.A.C., CUMPLE con acreditar el Requisito de Calificación; por lo tanto su Oferta es Calificada.					

CESAR MURILLO BENAVIDES

Jefe Equipo Gestión del Abastecimiento (e)

Equipo de Gestión del Abastecimiento

SEDAPAL



EVALUACIÓN DE LAS OFERTAS  
ADJUDICACIÓN SIMPLIFICADA N° 0070-2023-SEDAPAL

ADQUISICIÓN DE SEGURIDAD ANTIMALWARE CORPORATIVO DE ESTACIONES DE TRABAJO

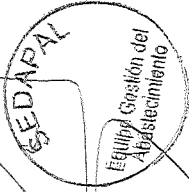
FACTOR DE EVALUACIÓN: PRECIO  
PUNTAJE MAXIMO: 100 PUNTOS  
VALOR ESTIMADO:

S/. 478,298.72

POSTOR	DOCUMENTOS DE PRESENTACIÓN OBLIGATORIA				FACTORES DE EVALUACIÓN					ORDEN DE PRELACIÓN
					PRECIO OFERTADO		PUNTAJE TOTAL	Bonificación del 5% condición de micro y pequeña empresa	PUNTAJE TOTAL	
	DOCUMENTOS PARA LA ADMISIÓN DE LA OFERTA		CUMPLIMIENTO DE ESPECIFICACIONES TÉCNICAS	RESULTADO	PRECIO OFERTADO	PUNTAJE				
	DOCUMENTOS PARA LA ADMISIÓN DE LA OFERTA	CUMPLIMIENTO DE ESPECIFICACIONES TÉCNICAS					RESULTADO	PRECIO OFERTADO	PUNTAJE	
INNOVARE E-BUSINESS S.A.C.	PRESENTA	CUMPLE	OFERTA ADMITIDA	S/. 408,520.00	100.00	100.00	5.00	105.00	1º	
IMPERIA SOLUCIONES TECNOLÓGICAS S.A.C.	PRESENTA	NO CUMPLE	OFERTA ADMITIDA NO							

OBSERVACIONES:

Las ofertas que han cumplido con la presentación de la documentación requerida para la admisión, pasan a la etapa de Calificación de la oferta, según el orden de prelación de conformidad con el Artículo 75 del Reglamento de la Ley de Contrataciones del Estado.



GESAR MURILLO BENAVIDES  
Jefe Equipo Gestión del Abastecimiento (e)

**ACTA DE APERTURA DE OFERTAS Y REVISIÓN DE LOS DOCUMENTOS  
REQUERIDOS**

**ADJUDICACIÓN SIMPLIFICADA N° 0070-2023-SEDAPAL**

**ADQUISICIÓN DE SEGURIDAD ANTIMALWARE CORPORATIVO DE ESTACIONES  
DE TRABAJO**

En Lima, en el Edificio del Centro Operativo Principal La Atarjea, en las instalaciones de Equipo Gestión del Abastecimiento, siendo las 10:50 horas del 06 de Octubre de 2023, se inicia la reunión del Órgano de encargado de las Contrataciones, representado por el Sr. Cesar Murillo Benavides, Jefe del Equipo Gestión del Abastecimiento (e) y la asistencia técnica de la señora Carmen Aguirre Hernández, proceden a realizar la apertura de las ofertas presentadas a través del SEACE por los postores registrados electrónicamente, en el presente procedimiento de selección:

**INFORME:**

1. De a verificado en el SEACE, ocho (08) empresas registradas en el presente procedimiento de selección, las cuales se muestran a continuación en el orden que lo han efectuado:

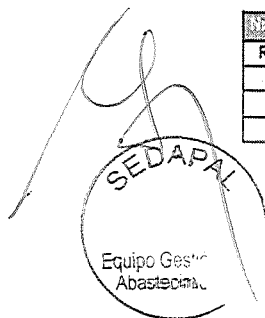
Nro.	Tipo proveedor	RUC/Código	Nombre o Razón Social	Fecha de registro en el procedimiento	Estado
1	Proveedor con RUC	20199144961	BAFING S.A.C.	22/09/2023	Válido
2	Proveedor con RUC	20475805101	INNOVARE E-BUSINESS S.A.C.	22/09/2023	Válido
3	Proveedor con RUC	20535653284	SSG PERU S.A.C.	25/09/2023	Válido
4	Proveedor con RUC	20551407820	NET FUSION CONSULTING SOCIEDAD ANONIMA CERRADA	22/09/2023	Válido
5	Proveedor con RUC	20552075341	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	25/09/2023	Válido
6	Proveedor con RUC	20553404631	DAILY TECHNOLOGY S.A.C.	25/09/2023	Válido
7	Proveedor con RUC	20600432070	KRISATEC S.A.C.	25/09/2023	Válido
8	Proveedor con RUC	20603847203	LOTENGO PERU S.A.C.	25/09/2023	Válido

2. De los participantes en el SEACE se presentaron dos (02) ofertas:

**Presentación de ofertas/expresión de interés**

Entidad convocante :	SERVICIO DE AGUA POTABLE Y ALCANTARILLADO DE LIMA - SEDAPAL
Nomenclatura :	AS-SM-70-2023-SEDAPAL-1
Nro. de convocatoria :	1
Objeto de contratación :	Bien
Descripción del objeto :	ADQUISICIÓN DE SOLUCIÓN DE SEGURIDAD ANTIMALWARE CORPORATIVO DE ESTACIÓN DE TRABAJO

Nro. ítem	Descripción del ítem			
RUC / Código	Nombre o Razón Social	Fecha Presentación	Hora Presentación	Forma de presentación
1	ADQUISICIÓN DE SOLUCIÓN DE SEGURIDAD ANTIMALWARE CORPORATIVO DE ESTACIÓN DE TRABAJO			
20475805101	INNOVARE E-BUSINESS S.A.C.	05/10/2023	21:27:42	Electronico
20552075341	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	05/10/2023	23:01:06	Electronico



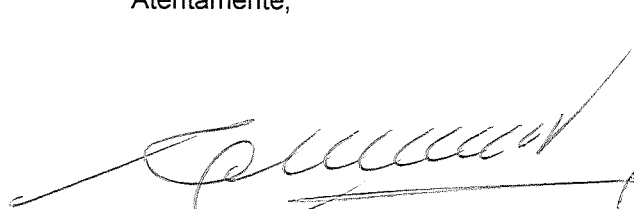


### **VERIFICACIÓN DE LA PRESENTACIÓN DE DOCUMENTOS REQUERIDOS**

La admisibilidad, evaluación y calificación de las ofertas presentadas, serán informados el día del otorgamiento de la buena pro a través del SEACE.

Siendo las 12:00 horas, se levantó la sesión, siendo suscrito el presente por los asistentes en señal de conformidad.

Atentamente,

  
Cesar Murillo Benavides  
Jefe Equipo Gestión del Abastecimiento (e)

