

ACTA DECLARACIÓN DE DESIERTO

PROCEDIMIENTO ELECTRÓNICO ADJUDICACIÓN SIMPLIFICADA N° AS-15-2023-SIMA-1 PRIMERA CONVOCATORIA

SERVICIO DE LICENCIAMIENTO DE SOFTWARE ANTIVIRUS DE PROTECCIÓN DE DETECCIÓN Y RESPUESTA DE ENDPOINTS PARA EL SIMA PERÚ S.A.

En la Provincia Constitucional del Callao, siendo las 11:30 horas del día 19 de enero del 2024, se reunieron los integrantes del Comité de Selección nombrado para el presente procedimiento de selección a efectos de llevar a cabo la admisión, evaluación, calificación y el otorgamiento de la buena pro, de la Adjudicación Simplificada N° AS-15-2023-SIMA-1.

El Comité de Selección para el presente acto se encontró integrado por los siguientes miembros designados mediante Formato N° AS-15-2023-SIMA aprobado el 22 de diciembre del 2023.

NOMBRES Y APELLIDOS	DEPENDENCIA	DNI	CARGO
FRANCO LÓPEZ COQUES	AREA USUARIA	45460224	PRESIDENTE
CRHISTIAN ALEJANDRO LA TORRE	AREA USUARIA	44250514	PRIMER INTEGRANTE
ADELAIDA ALBURQUEQUE TORRES	OEC	25604583	SEGUNDO INTEGRANTE

1. DETALLE DE LOS PARTICIPANTES:

De acuerdo con el listado de actividades establecido en el SEACE, se registraron los siguientes participantes:

Entidad convocante	SERVICIO INDUSTRIAL DE LA MARINA S.A.
Nomenclatura	AS-SM-15-2023-SIMA PERU-1
Nro. de convocatoria	1
Objeto de contratación	Servicio
Descripción del objeto	SERVICIO DE LICENCIAMIENTO DE SOFTWARE ANTIVIRUS DE PROTECCIÓN AVANZADA DE ENDPOINTS
Número de Contratación	SIMA PERU SA-2023-505

Búsqueda de participante

Estado de registro

Participante

Nro.	Tipo proveedor	RUC/Código	Nombre e Razón Social	Fecha de registro en el procedimiento	Estado	Advertencia	Fecha de registro	Usuario de Registro	Acciones
1	Proveedor con RUC	10073138561	MARQUEZ RAMIREZ EFRAIN	04/01/2024	Válido		04/01/2024	10073138561	
2	Proveedor con RUC	20475805101	INNOVARE E-BUSINESS S.A.C.	28/12/2023	Válido		28/12/2023	20475805101	
3	Proveedor con RUC	20524531861	THINK NETWORKS PERU S.A.C.	28/12/2023	Válido		28/12/2023	20524531861	
4	Proveedor con RUC	20601223512	CORPORACION DIGI ARCH PERU SOCIEDAD COMERCIAL DE RESPONSABILIDAD LIMITADA	30/12/2023	Válido		30/12/2023	20601223512	
5	Proveedor con RUC	20601234115	GS PERU MG E.I.R.L.	28/12/2023	Válido		28/12/2023	20601234115	
6	Proveedor con RUC	20602497519	CREAINTER SOCIEDAD ANONIMA CERRADA-CREAINTER S.A.C.	07/01/2024	Válido		07/01/2024	20602497519	
7	Proveedor con RUC	20607588067	JAYWAY NET S.A.C.	29/12/2023	Válido		29/12/2023	20607588067	

2. DETALLE DE LOS POSTORES:

Dentro de la fecha prevista en el listado de actividades, para la evaluación y calificación de ofertas presentadas, el comité de selección realiza la apertura de ofertas de manera electrónica a través del SEACE (descarga de las ofertas).

Presentación de ofertas/expresión de interés

Entidad convocante :	SERVICIO INDUSTRIAL DE LA MARINA S.A.
Nomenclatura :	AS-SM-15-2023-SIMA PERU-1
Nro. de convocatoria :	1
Objeto de contratación :	Servicio
Descripción del objeto :	SERVICIO DE LICENCIAMIENTO DE SOFTWARE ANTIVIRUS DE PROTECCIÓN AVANZADA DE ENDPOINTS

Nro. ítem	Descripción del ítem			
RUC / Código	Nombre o Razón Social	Fecha Presentación	Hora Presentación	Forma de presentación
1	SERVICIO DE LICENCIAMIENTO DE SOFTWARE ANTIVIRUS DE PROTECCIÓN AVANZADA DE ENDPOINTS			
20801234115	GS PERU MG E.I.R.L.	10/01/2024	17:23:48	Electronico
20475805101	INNOVARE E-BUSINESS S.A.C.	10/01/2024	21:09:31	Electronico

Acto seguido, se procede a la apertura electrónica de las ofertas a fin de verificar la presentación de lo requerido en la sección específica de las bases, de conformidad con el numeral 73.2 del artículo 73 del Reglamento de la Ley de Contrataciones del Estado (RLCE), y determina si las ofertas responden a las características y/o requisitos funcionales y condiciones de las Especificaciones Técnicas, detallados en las bases integradas.

3. DETALLE DE LA PRESENTACIÓN DE OFERTAS:

De acuerdo al artículo 73 del RLCE, la presentación de ofertas, se realiza de manera electrónica a través del SEACE, durante el periodo establecido en la convocatoria.

Artículo 52 del RLCE.- Contenido mínimo de las ofertas: Los documentos del procedimiento establecen el contenido de las ofertas

CAPITULO II Numeral 2.2.1 Documentación de presentación obligatoria:

CUADRO COMPARATIVO								
ADJUDICACIÓN SIMPLIFICADA Nº 15-2023- SIMA PERÚ-1								
SERVICIO DE LICENCIAMIENTO DE SOFTWARE ANTIVIRUS DE PROTECCIÓN AVANZADA DE ENDPOINTS								
PAC- 17								
EVALUACION DE OFERTAS								
A.- VERIFICACIÓN DE DOCUMENTOS OBLIGATORIOS								
EMPRESAS POSTORAS	a	b	c	d	e	f	g	ADMISIBILIDAD
	Declaración Jurada de datos del postor	Documento de Acreditación de la representación de quien suscribe la oferta	Declaración Jurada Artículo 52º del Reglamento	Declaración Jurada de cumplimiento de las Especificaciones Técnicas contenidas en el numeral 3.1 del Cap. III de la Sección REQUERIMIENTO	Declaración Jurada plazo de prestación del servicio	Promesa de Consorcio (Sólo para el caso en que un consorcio se presente como postor), con firmas legalizadas, de ser el caso	Precio de la Oferta en soles	OBSERVACIONES
	Anexo 1		Anexo 2	Anexo 3	Anexo 4	Anexo 5	Anexo 6	
GS PERÚ MG E.I.R.L.	PRESENTA	PRESENTA	PRESENTA	(*) PRESENTA	PRESENTA	NO APLICA	PRESENTA	(*) Observaciones anexas a la presente Acta, para mejor visualización
INNOVARE E-BUSINESS S.A.C.	PRESENTA	PRESENTA	PRESENTA	(*) PRESENTA	PRESENTA	NO APLICA	PRESENTA	(*) Observaciones anexas a la presente Acta, para mejor visualización

DETALLE EVALUACIÓN FICHA TECNICA (ENTE TECNICO):

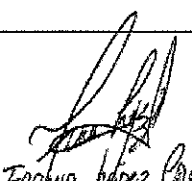
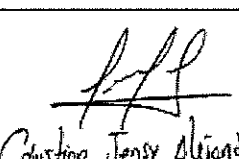
PROCESO: ADJUDICACIÓN SIMPLIFICADA N° 15-2023-SIMA-1- SIMA PERU			
Descripción del Bien:	EVALUACIÓN TÉCNICA PARA EL "SERVICIO DE LICENCIAMIENTO DE SOFTWARE ANTI-VIRUS DE PROTECCIÓN AVANZADA DE ENDPOINTS"		
Plazo:	40 días calendario.		
Presupuesto:			
Forma de pago:	Único pago posterior a la firma del acta de conformidad respectiva.		
Detalle de los oferentes	Proveedor N°1 GS PERU MGEJRL	Proveedor N°2 INNOVARE E-BUSINESS S.A.C.	
5. ALCANCES Y DESCRIPCIÓN DEL SERVICIO A CONTRATAR			
5.1 CANTIDAD DE LICENCIAS Y CARACTERÍSTICAS DEL SERVICIO A CONTRATAR			
5.1.1 CANTIDAD DE LICENCIAS			
915 licencias de software antivirus por el periodo de UN (01) AÑO. De las cuales serán 865 licencias para PCs y 50 para Servidores	CUMPLE	CUMPLE	
5.1.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR			
I. CARACTERÍSTICAS DE LA CONSOLA DE ADMINISTRACIÓN			
a. La solución deberá proveer la consola de administración 100% en la nube.	CUMPLE	CUMPLE	
b. Debe ser una consola multiusuario, multiplataforma multigrupo que permita la creación de usuarios con independencia y accesos con diferentes roles.	CUMPLE	CUMPLE	
c. La consola de administración debe implementar la API RESTful o equivalente para fines de integración con herramientas de cualquier sistema que admita la integración de API.	CUMPLE	CUMPLE	
d. La solución debe contar con la capacidad de heredar políticas en cualquier nivel, así como especificar la política por un sitio específico.	CUMPLE	CUMPLE	
e. La solución para ofrecer debe tener una base de conocimiento y documentación dentro de la consola sin la necesidad de utilizar credenciales de otro sistema.	CUMPLE	CUMPLE	
f. La consola debe ser intuitiva y fácil de navegar con flujos de trabajo que permitan la respuesta ante incidentes.	CUMPLE	CUMPLE	
g. La consola de administración debe permitir el acceso granular basado en roles y por nivel de tenant (cuenta, sitio).	CUMPLE	CUMPLE	
h. La solución debe permitir el acceso vía API completo a todas las capacidades de gestión y acceso a los datos.	CUMPLE	CUMPLE	
i. La solución debe admitir autenticación por 2FA y/o SSO (SAML 2.0) para el acceso a la consola de administración.	CUMPLE	CUMPLE	
j. La auditoría y el registro de actividad deben mantenerse en la consola de administración. La solución debe contar con la capacidad de enviar registros a una fuente externa.	CUMPLE	CUMPLE	
k. Los datos están cifrados tanto en el almacenamiento como en reposo	CUMPLE	CUMPLE	
II. CARACTERÍSTICAS DEL AGENTE DE PROTECCIÓN ENDPOINTS			
a. La solución debe brindar capacidades de EPP (Endpoint Protection Platform) y EDR (Endpoint Detection and Response) disponibles en un solo agente sin necesidad de instalar varios paquetes de software	CUMPLE	CUMPLE	
b. La solución debe contar con Anti-tamper.	CUMPLE	CUMPLE	
c. Capacidad para iniciar análisis bajo demanda para buscar malware o asegurarse de que se haya corregido una amenaza (desde la consola y / o el punto final).	CUMPLE	CUMPLE	
d. Capacidad para programar actualizaciones de agentes desde la consola de administración.	CUMPLE	CUMPLE	
e. La solución debe contar con la opción para limitar la cantidad de agentes que pueden descargar una actualización en un momento dado.	CUMPLE	CUMPLE	
f. La solución debe contar con la opción de "Dar de baja automáticamente" a los agentes antiguos si no se han comunicado con la consola de administración durante un periodo de tiempo configurable.	CUMPLE	CUMPLE	
g. La solución debe permitir la desinstalación del agente de forma remota desde la consola de administración.	CUMPLE	NO CUMPLE	
h. La solución permite deshabilitar temporalmente el agente a través de la consola de administración para solucionar problemas o realizar pruebas temporales.	CUMPLE	CUMPLE	
i. El agente no debe solicitar reinicio cuando se realice una actualización de versión.	CUMPLE	NO CUMPLE	
j. El agente debe permitir la comunicación a través de un proxy web.	CUMPLE	CUMPLE	
k. El agente de Windows se ejecuta en el espacio del Kernel para garantizar el nivel más alto de protección contra manipulaciones (Anti-tamper).	CUMPLE	CUMPLE	
l. El agente de Linux debe ejecutarse únicamente en el espacio del usuario para evitar pánicos del Kernel y kernels contaminados que invalidan el soporte.	NO CUMPLE	NO CUMPLE	
m. La solución debe exportar los inventarios de dispositivos / agentes a CSV.	CUMPLE	CUMPLE	
n. La solución debe proporcionar la capacidad de enviar mensajes de notificación a la computadora del usuario final.	CUMPLE	NO CUMPLE	
III. CARACTERÍSTICAS DE SISTEMA OPERATIVO SOPORTADO			
a. La solución deberá soportar la instalación en Sistemas Operativos para servidores como Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022. El postor podrá considerar dentro de su solución la instalación de algún componente adicional que garantice la continuidad y la seguridad de los equipos asociados a estas versiones.	CUMPLE	NO CUMPLE	
b. La solución deberá soportar la instalación en Sistemas Operativos Windows XP, Windows 7, Windows 8, Windows 10, Windows 11 y Linux. El postor podrá considerar dentro de su solución la instalación de algún componente adicional que garantice la continuidad y la seguridad de los equipos asociados a estas versiones.	CUMPLE	NO CUMPLE	
c. La solución debe permitir la configuración en modo de detección o protección en sistemas operativos Linux.	CUMPLE	CUMPLE	
IV. CARACTERÍSTICA DE PREVENCIÓN DE AMENAZAS			
a. La solución proporciona prevención en todas las principales plataformas operativas: Windows y Linux.	CUMPLE	CUMPLE	
b. La plataforma ofrecida debe unificar y ampliar la capacidad de detección y respuesta a través de múltiples capas de seguridad. Debe incluir protección de endpoints (EPP), detección y respuesta de endpoints (EDR) con agente para Windows y Linux.	CUMPLE	CUMPLE	
c. La solución debe proporcionar protección contra malware conocido y desconocido.	CUMPLE	CUMPLE	
d. La solución debe examinar los archivos al escribir y leer al disco duro.	CUMPLE	CUMPLE	
e. La solución debe brindar protección contra ataques de día cero, mediante el análisis de comportamiento en el punto final, sin depender de firmas.	CUMPLE	CUMPLE	
f. La solución debe proteger el endpoint contra malware, incluso cuando el sistema no está conectado a la red.	CUMPLE	CUMPLE	
g. El agente no debe tener dependencia con la consola de administración, con la nube o cualquier recurso externo para detectar y responder adecuadamente a amenazas sofisticadas (día cero, sin archivos, basado en RAM, cero Exploits diarios, ransomware, mineros, movimiento lateral, APT) en tiempo real a medida que se detectan las amenazas.	NO CUMPLE	NO CUMPLE	
h. El agente examina la información de procesos en el dispositivo antes de enviar información de alerta en la consola de administración y toma acción de remediación automática, reduciendo el tiempo de detección y remediación de un ataque.	NO CUMPLE	NO CUMPLE	
i. La solución aprovecha la inteligencia artificial o el aprendizaje artificial para analizar los archivos antes de la ejecución y comportamientos mientras se ejecuta un archivo.	CUMPLE	CUMPLE	
j. La solución debe permitir monitorear y proteger a los dispositivos finales contra amenazas internas y movimientos laterales.	CUMPLE	CUMPLE	
k. La solución debe permitir la protección de los dispositivos finales ante documentos y scripts maliciosos.	CUMPLE	CUMPLE	
l. La solución debe permitir la búsqueda de programas potencialmente no deseados.	CUMPLE	CUMPLE	
m. La solución debe contar con Motores de Comportamiento On Write (escritura) y On Execute (ejecución).	NO CUMPLE	NO CUMPLE	

n. La solución debe permitir descargar de forma segura un archivo malicioso o archivo enviado a cuarentena desde la consola de administración.	CUMPLE	NO CUMPLE
o. La solución debe permitir visualizar los datos de alerta está disponible durante al menos 365 días.	CUMPLE	NO CUMPLE
p. La solución debe permitir que las alertas se correlacionen entre sí automáticamente si están relacionados con el mismo ataque.	CUMPLE	NO CUMPLE
q. La recolección de logs de EDR por cada endpoint (datos sin procesar / telemetría se mantienen durante un mínimo de 14 días sin cargos adicionales).	CUMPLE	NO CUMPLE
V. CARACTERÍSTICA DE LA CAPACIDAD DE RESPUESTA Y REMEDIACIÓN		
r. La solución admite un Shell remoto completo para los sistemas Windows, Linux principalmente.	CUMPLE	CUMPLE
s. La solución deberá tener la capacidad de alertar sobre comportamientos de amenazas tanto sospechosos como maliciosos.	CUMPLE	CUMPLE
t. La solución deberá tener la capacidad de acceder remotamente al equipo.	CUMPLE	CUMPLE
u. La solución deberá tener la capacidad de tomar acción sobre un proceso malicioso.	CUMPLE	CUMPLE
v. La solución deberá tener la capacidad de tomar acción sobre un archivo que está en cuarentena.	CUMPLE	CUMPLE
w. La solución deberá tener la capacidad para remediar todos los cambios del sistema operativo con un solo clic en caso de ransomware.	CUMPLE	CUMPLE
x. La solución deberá de tener la capacidad para revertir eventos de datos destructivos que incluyen, entre otros, ransomware con un solo clic.	CUMPLE	CUMPLE
y. La solución deberá permitir desconectar a un equipo infectado de la red.	CUMPLE	CUMPLE
z. La solución deberá permitir ejecutar un Script en los equipos que cuenten con el agente instalado.	CUMPLE	CUMPLE
aa. La solución deberá permitir automatizar las capacidades de respuesta ante incidentes.	CUMPLE	CUMPLE
ab. La solución deberá permitir tomar acciones de remediación en múltiples sistemas o eventos a la vez.	CUMPLE	CUMPLE
ac. La solución deberá permitir agregar notas/comentarios a un evento.	CUMPLE	CUMPLE
ad. Opciones para establecer el estado de un problema o evento (ejemplos: resuelto, en progreso, no resuelto).	CUMPLE	CUMPLE
VI. CARACTERÍSTICAS DE LAS POLÍTICAS DE INSTALACIÓN		
ae. La solución deberá tener la capacidad para admitir la herencia de políticas en una cuenta, sitio o grupo de dispositivos.	CUMPLE	CUMPLE
af. La solución deberá soportar la asignación de políticas dinámicas según los atributos del dispositivo final.	CUMPLE	CUMPLE
ag. La solución deberá tener la capacidad de instalar y colocar dispositivos directamente en un grupo de dispositivos específico en el momento de la instalación.	CUMPLE	CUMPLE
ah. Las políticas de la solución deberán brindar la opción de ENCENDER o APAGAR motores únicos a por tipo de motor (Motores de ejecución previa y de tiempo de ejecución).	NO CUMPLE	NO CUMPLE
ai. Las modificaciones de la política se aplican casi en tiempo real.	CUMPLE	CUMPLE
VII. CARACTERÍSTICA DE LISTAS DE EXCLUSIONES		
aj. La solución debe contar una lista predefinida de exclusiones conocidos o recomendados.	CUMPLE	CUMPLE
ak. La solución debe permitir a los administradores de la consola realizar exclusiones mediante: a) Hash b) Ruta c) Certificado o un Signer ID d) Tipo de Archivo	CUMPLE	NO CUMPLE
al. La solución debe permitir a los administradores de la consola realizar exclusiones de políticas en varios niveles (Cuenta, Sitio, Grupo).	CUMPLE	CUMPLE
am. La solución debe permitir configurar las exclusiones para suprimir de forma independiente las alertas relacionadas con el aprendizaje automático basado en archivos y / o las motores de comportamiento.	CUMPLE	CUMPLE
an. La solución debe permitir configurar las exclusiones para manejar los problemas de interoperabilidad hasta rutas específicas o ejecutables únicos reduciendo el monitoreo de los procesos principales y/o todos sus procesos secundarios generados.	CUMPLE	CUMPLE

ao. La solución debe permitir configurar las exclusiones para manejar los problemas de rendimiento hasta rutas específicas o ejecutables individuales deshabilitando la supervisión de los procesos principales y/o todas sus procesos secundarios generados.	CUMPLE	CUMPLE
VIII. CARACTERÍSTICA DEL CONTROL DE DISPOSITIVOS Y VISIBILIDAD DE APLICACIONES		
ap. La solución debe poder controlar dispositivos USB externos.	CUMPLE	CUMPLE
aq. La solución debe contar con acciones como: Bloqueo, Lectura y Escritura y Solo lectura.	CUMPLE	CUMPLE
ar. La solución deberá controlar dispositivos USB de manera granular teniendo como tipo de clasificación, la siguiente información del dispositivo: Clase, Número de serie específico, ID de Producto o ID de Vendor.	CUMPLE	NO CUMPLE
as. La solución debe poder permitir controlar dispositivos USB de manera granular teniendo como tipo de clasificación, la siguiente información del dispositivo: Identificador de Hardware o Versión de Bluetooth.	CUMPLE	NO CUMPLE
at. La solución debe permitir la identificación de aplicaciones de software de terceros que puedan tener vulnerabilidades.	CUMPLE	CUMPLE
au. La solución puede proporcionar un inventario de todas las aplicaciones instaladas para todos los equipos de la entidad.	CUMPLE	CUMPLE
av. La solución debe poder controlar el firewall para dispositivos los sistemas operativos: Windows, Linux.	CUMPLE	CUMPLE
aw. La solución debe permitir la creación de reglas de firewall que se apliquen a varios dispositivos pertenecientes a un Sitio, Grupo.	CUMPLE	CUMPLE
ax. La solución puede crear reglas de firewall para aplicarlas a un grupo específico de dispositivos (aprovechando el etiquetado o los grupos de políticas).	CUMPLE	CUMPLE
IX. CARACTERÍSTICA DE INVENTARIO DE SOFTWARE		
ay. La solución de inventario de software deberá ser capaz de realizar un escaneo automático de todos los endpoints en la red corporativa.	CUMPLE	CUMPLE
az. Debe registrar de manera precisa las versiones de todos los programas y aplicaciones instaladas en cada endpoint.	CUMPLE	CUMPLE
ba. Debe ser capaz de identificar las actualizaciones de software y mantener un historial de las versiones anteriores.	CUMPLE	CUMPLE
bb. Deberá proporcionar información detallada sobre cada programa, incluyendo el nombre del software, el editor o fabricante, la fecha de instalación y la ubicación en el sistema de archivos del endpoint.	CUMPLE	CUMPLE
bc. Debe ser capaz de generar alertas o informes específicos sobre las vulnerabilidades encontradas.	CUMPLE	CUMPLE
bd. Debe generar alertas o notificaciones cuando se detecte software no autorizado.	CUMPLE	CUMPLE
be. Deberá ofrecer la capacidad de generar informes detallados sobre el inventario de software, que incluyan la lista de software instalado, sus versiones y cualquier hallazgo relacionado con vulnerabilidades o software no autorizado.	CUMPLE	CUMPLE
bf. Los informes deben ser personalizables y exportables en diferentes formatos, como PDF o CSV.	CUMPLE	CUMPLE
bg. Deberá ser capaz de generar informes específicos que ayuden a la organización a cumplir con requisitos normativos relacionados con la gestión de software y la seguridad de la información.	CUMPLE	CUMPLE
bh. Debe permitir la forma de medidas automáticas o manuales según las políticas definidas.	CUMPLE	NO CUMPLE
bi. Debe permitir la configuración de acciones automáticas basadas en políticas de seguridad.	CUMPLE	NO CUMPLE
X. CARACTERÍSTICAS DE XDR (Detección y Respuesta Extendida)		
bj. La solución debe permitir realizar acciones de respuesta XDR con un solo clic para que permita detener la exposición del ataque.	CUMPLE	NO CUMPLE
bk. La solución debe permitir suspender el acceso al correo del usuario si se detecta que las credenciales de un usuario intentó ser utilizado para iniciar sesión en el correo electrónico y enviar phishing.	CUMPLE	NO CUMPLE
bl. La solución debe permitir el bloqueo del hash si se detecta un acceso no permitido al correo del usuario.	CUMPLE	NO CUMPLE

5.6 REQUERIMIENTOS DEL PROVEEDOR Y SU PERSONAL CLAVE		
<p>5.6.1 REQUERIMIENTOS COMO PROVEEDOR</p> <p>a) Deberá encontrarse registrado como proveedor en el RNP.</p> <p>b) El postor deberá de tener como mínimo cinco (05) años de experiencia en la venta de soluciones similares como Venta de Software Antivirus, Venta de Software Antimalware y Solución EDR.</p> <p>c) Con el fin de acreditar experiencia, el postor deberá acreditar ser ponente autorizado de la marca ofertada y como mínimo tener la categoría Silver. Esto se acreditará adjuntando documentación oficial del fabricante de la solución ofertada o del Distribuidor Autorizado o representante de la marca en el Perú.</p> <p>d) El postor deberá de contar con un Centro de Operaciones de Seguridad (SOC) propio para brindar el soporte 24x7x365 incluidos domingos y feriados.</p> <p>5.6.1.1 Acreditación:</p> <p>1. El postor deberá demostrar estar registrado como proveedor en el RNP.</p> <p>2. El postor deberá acreditar experiencia en la especialidad con copias simples de contratos u órdenes de servicios con su respectiva conformidad o constancia de prestación, en la venta de soluciones similares como Venta de Software Antivirus, Venta de Software Antimalware y Solución EDR.</p> <p>3. Así mismo con el fin de acreditar experiencia, el postor deberá adjuntar documentación oficial del fabricante de la solución ofertada o del Distribuidor Autorizado o representante de la marca en el Perú.</p> <p>4. El postor deberá presentar una declaración jurada el cual se comprometerá a brindar los servicios de soporte técnico y Centro de Operaciones de Seguridad SOC, por el periodo del servicio de licenciamiento antivirus controlado.</p>	CUMPLE	NO CUMPLE
<p>5.6.2 PERFIL DEL PERSONAL CLAVE</p>		
<p>a) COORDINADOR DE PROYECTO</p> <p>Será el responsable de la coordinación, supervisión y monitoreo de las actividades detalladas en el numeral 5.2, del servicio a implementar, el cual deberá tener el siguiente perfil:</p> <p>1. Formación Académica</p> <p>a. Un (01) Profesional titulado y con colegiatura habilitada en Ingeniería Electrónica y/o Ingeniería de Sistemas y/o Ingeniería de Software y/o Ingeniería de Telecomunicaciones y/o Ingeniería Redes y Comunicaciones y/o Ingeniería Informática y Sistemas.</p> <p>b. Deberá contar con certificación Lead Cybersecurity Manager – ISO 27032</p>		

<p>2. Experiencia</p> <p>a. Deberá contar con experiencia mínima de DOS (02) años como Jefe y/o Supervisor en Gestión de Proyectos de TI y/o Proyectos de Seguridad y Protección Endpoint. El cual deberá de acreditar mediante constancias, certificados, contratos y/u otro documento.</p> <p>3. Acreditación</p> <p>a. Copia simple de título en Ingeniería Electrónica y/o Ingeniería de Sistemas y/o Ingeniería de Software y/o Ingeniería de Telecomunicaciones y/o Ingeniería Redes y Comunicaciones y/o Ingeniería Informática y Sistemas.</p> <p>b. El título profesional podrá ser verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe, o según corresponda.</p> <p>c. Deberá demostrar estar colegiado y estar habilitado en el CIP.</p> <p>d. Copia de la Certificación en Lead Cybersecurity Manager – ISO 27032</p> <p>e. Deberá acreditar experiencia por medio de constancias, certificados, contratos y/u otros documentos.</p>	CUMPLE	NO CUMPLE
<p>b) ESPECIALISTA DE IMPLEMENTACIÓN</p> <p>Será el responsable de la implementación, Configuración, Capacitación y Entrenamiento, así mismo deberá efectuar la ejecución de las actividades detalladas en el numeral 5.2.</p> <p>1. Formación Académica</p> <p>a. Un (01) Profesional titulado en Ingeniería Electrónica y/o Ingeniería de Sistemas y/o Ingeniería de Software y/o telecomunicaciones y/o redes y comunicaciones y/o electrónica y/o redes y comunicaciones de datos y/o informática y sistemas.</p> <p>2. Experiencia</p> <p>a. Deberá contar con una experiencia como mínima de DOS (02) años en implementaciones, soporte técnico de soluciones de seguridad de protección de ENDPOINT.</p> <p>3. Acreditación</p> <p>a. El título profesional podrá ser verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe, o según corresponda.</p> <p>b. Copia simple de título en Ingeniería electrónica, Ingeniería de sistemas, Ingeniería de seguridad y auditoría informática, Ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, informática y sistemas.</p> <p>c. Deberá acreditar experiencia por medio de constancias, certificados, contratos y/u otros documentos</p>	CUMPLE	CUMPLE

5.7.2 PLAZO DE IMPLEMENTACIÓN DEL SERVICIO El plazo de implementación del servicio de licenciamiento de Software Antivirus de Protección Avanzada Endpoints, considerando todos sus componentes, configuraciones, así como la activación de las licencias, deberá realizarse en los siguientes SESENTA (60) días calendario. El inicio de la ejecución del servicio será coordinado con el área usuaria, Experto de Infraestructura y Servicios de la OTC - SIMA PERÚ.	CUMPLE	CUMPLE
4. FECHA DE VALIDACIÓN: 15/01/2024		
5. RESPONSABLE DE VALIDACIÓN (NOMBRE Y FIRMA) <div style="display: flex; justify-content: space-around;"> <div style="text-align: center;">  Ericko López Céspedes </div> <div style="text-align: center;">  Christian Jency Alejandro La Torre </div> </div>		

RESULTADO:

Proveedor N°1
NO CUMPLE
Proveedor N°2
NO CUMPLE

OBSERVACIONES:

1. Se verificó que el postor NO CUMPLE con lo requerido en el siguiente ítem "g. La solución debe permitir la desinstalación del agente de forma remota desde la consola de administración.", mencionado en el "II. CARACTERÍSTICAS DEL AGENTE DE PROTECCIÓN ENDPOINTS" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de los Términos de Referencia.

- INNOVARE E-BUSINESS S.A.C., no detalló la característica solicitada en su oferta.

2. Se verificó que el postor NO CUMPLE con la requerida en el siguiente ítem "i. El agente no debe solicitar reinicio cuando se realice una actualización de versión.", mencionado en el "II. CARACTERÍSTICAS DEL AGENTE DE PROTECCIÓN ENDPOINTS" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de los Términos de Referencia.

- INNOVARE E-BUSINESS S.A.C., no detalló la característica solicitada en su oferta.

3. Se verificó que los siguientes postores NO CUMPLEN con la requerida en el siguiente ítem "l. El agente de Linux debe ejecutarse únicamente en el espacio del usuario para evitar pánicos del Kernel y kernel contaminados que invalidan el soporte.", mencionado en el "II. CARACTERÍSTICAS DEL AGENTE DE PROTECCIÓN ENDPOINTS" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de los Términos de Referencia.

- GS PERU MG EURL, no detalló la característica solicitada en su oferta.
- INNOVARE E-BUSINESS S.A.C., no detalló la característica solicitada en su oferta.

4. Se verificó que el postor NO CUMPLE con la requerida en el siguiente ítem "n. La solución debe proporcionar la capacidad de enviar mensajes de notificación a la computadora del usuario final.", mencionado en el "II. CARACTERÍSTICAS DEL AGENTE DE PROTECCIÓN ENDPOINTS" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de los Términos de Referencia.

- INNOVARE E-BUSINESS S.A.C., no detalló la característica solicitada en su oferta.

5. Se verificó que el postor NO CUMPLE con la requerida en el siguiente ítem "a. La solución deberá soportar la instalación en Sistemas Operativos para servidores como Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022. El postor podrá considerar dentro de su solución la instalación de algún componente adicional que garantice la continuidad y la seguridad de los equipos asociados a estas versiones.", mencionada en el "II. CARACTERÍSTICAS DE SISTEMA OPERATIVO SOPORTADO" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de los Términos de Referencia.

- INNOVARE E-BUSINESS S.A.C., en la oferta presentada (página 56), la solución no es compatible con algunos sistemas operativos requeridos. Asimismo, verificó en la página del fabricante el siguiente anuncio "WiTSecure Business (ahora WiTSecure) comunicó que el soporte de productos para Windows 7 y Windows Server 2008R2 finalizará en enero de 2023 para los productos Elements y Business Suite". También, menciona lo siguiente "WiTSecure brindará soporte para estos productos en sistemas operativos heredados hasta el 30 de junio de 2023."

<https://community.witsecure.com/en/it/articles/29724-end-of-support-for-windows-7-and-windows-server-2008>

6. Se verificó que el postor NO CUMPLE con la requerida en el siguiente ítem "b. La solución deberá soportar la instalación en Sistemas Operativos Windows XP, Windows 7, Windows 8, Windows 10, Windows 11 y Linux. El postor podrá considerar dentro de su solución la instalación de algún componente adicional que garantice la continuidad y la seguridad de los equipos asociados a estas versiones.", mencionada en el "II. CARACTERÍSTICAS DE SISTEMA OPERATIVO SOPORTADO" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de los Términos de Referencia.

- INNOVARE E-BUSINESS S.A.C., en la oferta presentada (página 56), la solución no es compatible con algunos sistemas operativos requeridos. Asimismo, verificó en la página del fabricante el siguiente anuncio "WiTSecure Business (ahora WiTSecure) comunicó que el soporte de productos para Windows 7 y Windows Server 2008R2 finalizará en enero de 2023 para los productos Elements y Business Suite". También, menciona lo siguiente "WiTSecure brindará soporte para estos productos en sistemas operativos heredados hasta el 30 de junio de 2023."

<https://community.witsecure.com/en/it/articles/29724-end-of-support-for-windows-7-and-windows-server-2008>

7. Se verificó que los siguientes postores NO CUMPLEN con lo requerido en el siguiente punto "g. El agente no debe tener dependencia con la consola de administración, con la nube o cualquier recurso externo para detectar y responder adecuadamente a amenazas solicitadas (día cero, sin archivos, basado en RAM, cero Exploits diarios, ransomware, mineros, movimiento lateral, APT) en tiempo real a medida que se detectan las amenazas.", mencionado en el "IV. CARACTERÍSTICA DE PREVENCIÓN DE AMENAZAS" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de los Términos de Referencia.

- GS PERU MG E.I.R.L. no especificó la característica solicitada en su oferta.
- INNOVARE E-BUSINESS S.A.C., no especificó la característica solicitada en su oferta.

8. Se verificó que los siguientes postores NO CUMPLEN con lo requerido en el siguiente punto "h. El agente examinará la información de procesos en el dispositivo antes de enviar información de alerta en la consola de administración y toma acción de remediación automática, reduciendo el tiempo de detección y remediación de un ataque.", mencionado en el "IV. CARACTERÍSTICA DE PREVENCIÓN DE AMENAZAS" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de los Términos de Referencia.

- GS PERU MG E.I.R.L. no detalló en su oferta la característica solicitada.
- INNOVARE E-BUSINESS S.A.C., no detalló en su oferta la característica solicitada.

8. Se verificó que los siguientes postores NO CUMPLEN con lo requerido en el siguiente punto "h. El agente examinará la información de procesos en el dispositivo antes de enviar información de alerta en la consola de administración y toma acción de remediación automática, reduciendo el tiempo de detección y remediación de un ataque.", mencionado en el "IV. CARACTERÍSTICA DE PREVENCIÓN DE AMENAZAS" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de los Términos de Referencia.

- GS PERU MG E.I.R.L. no detalló en su oferta la característica solicitada.
- INNOVARE E-BUSINESS S.A.C., no detalló en su oferta la característica solicitada.

9. Se verificó que los siguientes postores NO CUMPLEN con lo requerido en el siguiente punto "m. La solución debe contar con Motores de Comportamiento On Write (escritura) y On Execute (ejecución).", mencionado en el "IV. CARACTERÍSTICA DE PREVENCIÓN DE AMENAZAS" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de los Términos de Referencia.

- GS PERU MG E.I.R.L. no detalló en su oferta la característica solicitada.
- INNOVARE E-BUSINESS S.A.C., no detalló en su oferta la característica solicitada.

10. Se verificó que el postor NO CUMPLE con lo requerido en las puntas "n, o, p, y q.", mencionado en el "IV. CARACTERÍSTICA DE PREVENCIÓN DE AMENAZAS" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de los Términos de Referencia.

- INNOVARE E-BUSINESS S.A.C., no detalló en su oferta la característica solicitada.

11. Se verificó que los postores NO CUMPLEN con lo requerido en el siguiente punto "d. Las políticas de la solución deberán brindar la opción de ENCENDER o APAGAR motores únicos o por tipo de motor (Motores de ejecución previa y de tiempo de ejecución).", mencionado en el "VI. CARACTERÍSTICAS DE LAS POLÍTICAS DE INSTALACIÓN" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de los Términos de Referencia.

- GS PERU MG E.I.R.L. no detalló en su oferta la característica solicitada.
- INNOVARE E-BUSINESS S.A.C., no detalló en su oferta la característica solicitada.

12. Se verificó que el postor NO CUMPLE con lo requerido en el siguiente punto "b. La solución debe permitir a los administradores de la consola recitar exclusiones mediante: Hash, Ruta, Certificado o un Signer ID, tipo de Archivo.", mencionado en el "VII. CARACTERÍSTICA DE LISTAS DE EXCLUSIONES" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de los Términos de Referencia.

- INNOVARE E-BUSINESS S.A.C., no detalló la característica solicitada en su oferta.

13. Se verificó que el postor NO CUMPLE con lo requerido en los siguientes puntos "c y d", mencionado en el "VIII. CARACTERÍSTICA DEL CONTROL DE DISPOSITIVOS Y VISIBILIDAD DE APLICACIONES" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de los Términos de Referencia.

- INNOVARE E-BUSINESS S.A.C., no detalló la característica solicitada en su oferta.

13. Se verificó que el postor NO CUMPLE con lo requerido en el siguiente punto "d. La solución debe permitir controlar dispositivos USB de manera granular teniendo como tipo de clasificación, la siguiente información del dispositivo: Identificador de Hardware o Versión de firmware.", mencionado en el "VIII. CARACTERÍSTICA DEL CONTROL DE DISPOSITIVOS Y VISIBILIDAD DE APLICACIONES" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de los Términos de Referencia.

- INNOVARE E-BUSINESS S.A.C., no detalló la característica solicitada en su oferta.

14. Se verificó que el postor NO CUMPLE con lo requerido en los puntos "j, y k.", mencionada en el "IX. CARACTERÍSTICA DE INVENTARIO DE SOFTWARE" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de los Términos de Referencia.

- INNOVARE E-BUSINESS S.A.C., no detalló en su oferta la característica solicitada.

15. Se verificó que el postor NO CUMPLE con lo requerido en los puntos "a, b, y c.", mencionado en el "X. CARACTERÍSTICAS DE XDR (Detección y Respuesta Extendida)" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de los Términos de Referencia.

- INNOVARE E-BUSINESS S.A.C., no detalló en su oferta la característica solicitada.

16. Se verificó que el postor NO CUMPLE con lo requerido en los puntos "3 y 4", mencionado en el "5.6.1. REQUERIMIENTOS COMO PROVEEDOR" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de los Términos de Referencia.

- INNOVARE E-BUSINESS S.A.C., no presentó las Declaraciones Juradas solicitadas en los Términos de Referencia.

17. Se verificó que el postor NO CUMPLE con el literal "b. Deberá contar con certificación Lead Cybersecurity Manager – ISO 27032", mencionado en el numeral 5.6.2 PERFIL DEL PERSONAL CLAVE de los Términos de Referencia.

- INNOVARE E-BUSINESS S.A.C., de acuerdo a lo indicado en los Términos de referencia se solicitó un personal con certificación oficial en la Lead Cybersecurity Manager – ISO 27032. Sin embargo, el postor remitió certificado que acredita haber culminado satisfactoriamente el curso ISO/IEC 27032:23 LEAD CYBERSECURITY MANAGER.

Nota: para mejor visualización de los cuadros precedentes, se estarán anexando los originales junto a la presente Acta.


4. ACUERDOS:

Al encontrándose fundamentado la no validez de las ofertas presentadas al procedimiento de selección N° AS-15-2023-SIMA – Primera Convocatoria para la Contratación del Servicio de Licenciamiento de Software Antivirus de Protección de Detección y Respuesta de Endpoints para el SIMA PERÚ S.A., el Comité de Selección, en aplicación del numeral 65.1 del artículo 65 del Reglamento de la Ley de Contrataciones del Estado, acordó por unanimidad:

DECLARAR DESIERTO el citado Procedimiento de Selección, por la causal de "CUANDO NO EXISTA NINGUNA OFERTA VÁLIDA"

Siendo las 14:00 horas del día 19 de enero del 2024, se dio por finalizada la reunión, firmándose la presente Acta en señal de conformidad.


Christian ALEJANDRO La Torre
Primer Integrante del
Comité de Selección
AS-15-2023-1


Esp. Adelaida ALBURQUEQUE Torres
Segundo Integrante del
Comité de Selección
AS-15-2023-1


Franco LÓPEZ Coques
Presidente del Comité de Selección
AS-15-2023

EVALUACIÓN TÉCNICA PARA EL "SERVICIO DE LICENCIAMIENTO DE SOFTWARE ANTIVIRUS DE PROTECCIÓN AVANZADA DE ENDPOINTS"			
Descripción del Bien:			
Plazo:	60 días calendario		
Presupuesto:			
Forma de pago:	Único pago posterior a la firma del acta de conformidad respectiva.		
Detalle de las ofertas		Proveedor N° 1 GS PERU MG E.I.R.L	Proveedor N°2 INNOVARE E-BUSINESS S.A.C.
5. ALCANCES Y DESCRIPCIÓN DEL SERVICIO A CONTRATAR			
5.1 CANTIDAD DE LICENCIAS Y CARACTERÍSTICAS DEL SERVICIO A CONTRATAR			
5.1.1 CANTIDAD DE LICENCIAS			
	915 licencias de software antivirus por el periodo de UN (01) AÑO. De las cuales serán 865 licencias para PCs y 50 para Servidores	CUMPLE	CUMPLE
5.1.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR			
I. CARACTERÍSTICAS DE LA CONSOLA DE ADMINISTRACIÓN			
	a. La solución deberá proveer la consola de administración 100% en la nube.	CUMPLE	CUMPLE
	b. Debe ser una consola multiusuario, multitisito multigrupo que permita la creación de usuarios con independencia y accesos con diferentes roles.	CUMPLE	CUMPLE
	c. La consola de administración debe implementar la API RESTful o equivalente para fines de integración con herramientas de cualquier sistema que admita la integración de API.	CUMPLE	CUMPLE
	d. La solución debe contar con la capacidad de heredar políticas en cualquier nivel, así como especificar la política por un sitio específico.	CUMPLE	CUMPLE
	e. La solución para ofertar debe tener una base de conocimiento y documentación dentro de la consola sin la necesidad de utilizar credenciales de otro sistema.	CUMPLE	CUMPLE
	f. La consola debe ser intuitiva y fácil de navegar con flujos de trabajo que permitan la respuesta ante incidentes.	CUMPLE	CUMPLE
	g. La consola de administración debe permitir el acceso granular basado en roles y por nivel de tenant (cuenta, sitio).	CUMPLE	CUMPLE
	h. La solución debe permitir el acceso vía API completo a todas las capacidades de gestión y acceso a los datos.	CUMPLE	CUMPLE
	i. La solución debe admitir autenticación por 2FA y/o SSO (SAML 2.0) para el acceso a la consola de administración.	CUMPLE	CUMPLE
	j. La auditoría y el registro de actividad deben mantenerse en la consola de administración. La solución debe contar con la capacidad de enviar registros a una fuente externa	CUMPLE	CUMPLE
	k. Los datos están cifrados tanto en el almacenamiento como en reposo	CUMPLE	CUMPLE
II. CARACTERÍSTICAS DEL AGENTE DE PROTECCIÓN ENDPOINTS			
	a. La solución debe brindar capacidades de EPP (EndPoint Protection Platform) y EDR (EndPoint Detection and Response) disponibles en un solo agente sin necesidad de instalar varios paquetes de software	CUMPLE	CUMPLE
	b. La solución debe contar con Anti-tamper.	CUMPLE	CUMPLE
	c. Capacidad para iniciar análisis bajo demanda para buscar malware o asegurarse de que se haya corregido una amenaza (desde la consola y / o el punto final).	CUMPLE	CUMPLE
	d. Capacidad para programar actualizaciones de agentes desde la consola de administración.	CUMPLE	CUMPLE

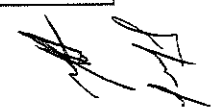


	e. La solución debe contar con la opción para limitar la cantidad de agentes que pueden descargar una actualización en un momento dado.	CUMPLE	CUMPLE
	f. La solución debe contar con la opción de "Dar de baja automáticamente" a los agentes antiguos si no se han comunicado con la consola de administración durante un período de tiempo configurable.	CUMPLE	CUMPLE
	g. La solución debe permitir la desinstalación del agente de forma remota desde la consola de administración.	CUMPLE	NO CUMPLE
	h. La solución permite deshabilitar temporalmente el agente a través de la consola de administración para solucionar problemas o realizar pruebas temporales.	CUMPLE	NO CUMPLE
	i. El agente no debe solicitar reinicio cuando se realice una actualización de versión.	CUMPLE	NO CUMPLE
	j. El agente debe permitir la comunicación a través de un proxy web.	CUMPLE	NO CUMPLE
	k. El agente de Windows se ejecuta en el espacio del kernel para garantizar el nivel más alto de protección contra manipulaciones (Anti-tamper).	CUMPLE	NO CUMPLE
	l. El agente de Linux debe ejecutarse únicamente en el espacio del usuario para evitar pánicos del kernel y kernels contaminados que invalidan el soporte.	NO CUMPLE	NO CUMPLE
	m. La solución debe exportar los inventarios de dispositivos / agentes a CSV.	CUMPLE	CUMPLE
	n. La solución debe proporcionar la capacidad de enviar mensajes de notificación a la computadora del usuario final.	CUMPLE	NO CUMPLE
	III. CARACTERÍSTICAS DE SISTEMA OPERATIVO SOPORTADO		
	a. La solución deberá soportar la instalación en Sistemas Operativos para servidores como Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022. El postor podrá considerar dentro de su solución la instalación de algún componente adicional que garantice la continuidad y la seguridad de los equipos asociados a estas versiones.	CUMPLE	NO CUMPLE
	b. La solución deberá soportar la instalación en Sistemas Operativos Windows XP, Windows 7, Windows 8, Windows 10, Windows 11 y Linux. El postor podrá considerar dentro de su solución la instalación de algún componente adicional que garantice la continuidad y la seguridad de los equipos asociados a estas versiones.	CUMPLE	NO CUMPLE
	c. La solución debe permitir la configuración en modo de detección o protección en sistemas operativos Linux.	CUMPLE	CUMPLE
	IV. CARACTERÍSTICA DE PREVENCIÓN DE AMENAZAS		
	a. La solución proporciona prevención en todos los principales sistemas operativos: Windows y Linux.	CUMPLE	CUMPLE
	b. La plataforma ofrecida debe unificar y ampliar la capacidad de detección y respuesta a través de múltiples capas de seguridad. Debe incluir protección de endpoints (EPP), detección y respuesta de endpoints (EDR) con agente para Windows y Linux	CUMPLE	CUMPLE
	c. La solución debe proporcionar protección contra malware conocido y desconocido.	CUMPLE	CUMPLE
	d. La solución debe examinar los archivos al escribir y leer al disco duro.	CUMPLE	CUMPLE
	e. La solución debe brindar protección contra ataques de día cero, mediante el análisis de comportamiento en el punto final, sin depender de firmas.	CUMPLE	CUMPLE
	f. La solución debe proteger el endpoint contra malware, incluso cuando el sistema no esté conectado a la red.	CUMPLE	CUMPLE
	g. El agente no debe tener dependencia con la consola de administración, con la nube o cualquier recurso externo para detectar y responder adecuadamente a amenazas solicitadas (día cero, sin archivos, basado en RAM, cero Exploits diarios, ransomware, mineros, movimiento lateral, APT) en tiempo real a medida que se detectan las amenazas).	NO CUMPLE	NO CUMPLE
	h. El agente examinará la información de procesos en el dispositivo antes de enviar información de alerta en la consola de administración y toma acción de remediación automática, reduciendo el tiempo de detección y remediación de un ataque.	NO CUMPLE	NO CUMPLE
	i. La solución aprovecha la inteligencia artificial o el aprendizaje artificial para analizar los archivos antes de la ejecución y comportamientos mientras se ejecuta un archivo.	CUMPLE	CUMPLE
	j. La solución debe permitir monitorear y proteger a los dispositivos finales contra amenazas internas y movimientos laterales.	CUMPLE	CUMPLE
	k. La solución debe permitir la protección de los dispositivos finales ante documentos y scripts maliciosos.	CUMPLE	CUMPLE
	l. La solución debe permitir la búsqueda de programas potencialmente no deseados.	CUMPLE	CUMPLE
	m. La solución debe contar con Motores de Comportamiento On Write (escritura) y On Execute (ejecución).	NO CUMPLE	NO CUMPLE

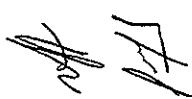
	n. La solución debe permitir descargar de forma segura un archivo malicioso o archivo enviado a cuarentena desde la consola de administración.	CUMPLE	NO CUMPLE
	o. La solución de permitir visualizar los datos de alerta está disponible durante al menos 365 días.	CUMPLE	NO CUMPLE
	p. La solución de permitir que las alertas se correlacionen entre sí automáticamente si están relacionadas con el mismo ataque.	CUMPLE	NO CUMPLE
	q. La recolección de logs de EDR por cada endpoint (datos sin procesar / telemetría se mantienen durante un mínimo de 14 días sin cargos adicionales).	CUMPLE	NO CUMPLE
	V. CARACTERÍSTICA DE LA CAPACIDAD DE RESPUESTA Y REMEDIACIÓN		
	a. La solución admite un Shell remoto completo para los sistemas: Windows, Linux principalmente.	CUMPLE	CUMPLE
	b. La solución deberá tener la capacidad de alertar sobre comportamientos de amenazas tanto sospechosos como maliciosos.	CUMPLE	CUMPLE
	c. La solución deberá tener la capacidad de acceder remotamente al equipo.	CUMPLE	CUMPLE
	d. La solución deberá tener la capacidad de tomar acción sobre un proceso malicioso.	CUMPLE	CUMPLE
	e. La solución deberá tener la capacidad de tomar acción sobre un archivo que está en cuarentena.	CUMPLE	CUMPLE
	f. La solución deberá tener la capacidad para remediar todos los cambios del sistema operativo con un solo clic en caso de ransomware.	CUMPLE	CUMPLE
	g. La solución deberá de tener la capacidad para revertir eventos de datos destructivos que incluyen, entre otros, ransomware con un solo clic.	CUMPLE	CUMPLE
	h. La solución deberá permitir desconectar a un equipo infectado de la red.	CUMPLE	CUMPLE
	i. La solución deberá permitir ejecutar un Script en los equipos que cuenten con el agente instalado.	CUMPLE	CUMPLE
	j. La solución deberá permitir automatizar las capacidades de respuesta ante incidentes.	CUMPLE	CUMPLE
	k. La solución deberá permitir tomar acciones de remediación en múltiples sistemas o eventos a la vez.	CUMPLE	CUMPLE
	l. La solución deberá permitir agregar notas/comentarios a un evento.	CUMPLE	CUMPLE
	m. Opciones para establecer el estado de un problema o evento (ejemplo: resuelto, en progreso, no resuelto).	CUMPLE	CUMPLE
	VI. CARACTERÍSTICAS DE LAS POLÍTICAS DE INSTALACIÓN		
	a. La solución deberá tener la capacidad para admitir la herencia de políticas en una cuenta, sitio o grupo de dispositivos.	CUMPLE	CUMPLE
	b. La solución deberá soportar la asignación de políticas dinámicas según los atributos del dispositivo final.	CUMPLE	CUMPLE
	c. La solución deberá tener la capacidad de instalar y colocar dispositivos directamente en un grupo de dispositivos específico en el momento de la instalación.	CUMPLE	CUMPLE
	d. Las políticas de la solución deberán brindar la opción de ENCENDER o APAGAR motores únicos o por Tipo de motor (Motores de ejecución previa y de tiempo de ejecución).	NO CUMPLE	NO CUMPLE
	e. Las modificaciones de la política se aplican casi en tiempo real.	CUMPLE	CUMPLE
	VII. CARACTERÍSTICA DE LISTAS DE EXCLUSIONES		
	a. La solución debe contar una lista predefinida de exclusiones conocidas o recomendadas.	CUMPLE	CUMPLE
	b. La solución debe permitir a los administradores de la consola realizar exclusiones mediante:		
	<input type="checkbox"/> Hash	CUMPLE	NO CUMPLE
	<input type="checkbox"/> Ruta	CUMPLE	NO CUMPLE
	<input type="checkbox"/> Certificado o un Signer ID	CUMPLE	NO CUMPLE
	<input type="checkbox"/> Tipo de Archivo	CUMPLE	NO CUMPLE
	c. La solución debe permitir a los administradores de la consola realizar exclusiones de políticas en varios niveles (Cuenta, Sitio, Grupo).	CUMPLE	CUMPLE
	d. La solución debe permitir configurar las exclusiones para suprimir de forma independiente las alertas relacionadas con el aprendizaje automático basado en archivos y / o los motores de comportamiento.	CUMPLE	CUMPLE
	e. La solución debe permitir configurar las exclusiones para manejar los problemas de interoperabilidad hasta rutas específicas o ejecutables únicos reduciendo el monitoreo de los procesos principales y/o todos sus procesos secundarios generados.	CUMPLE	CUMPLE



	f.La solución debe permitir configurar las exclusiones para manejar los problemas de rendimiento hasta rutas específicas o ejecutables individuales deshabilitando la supervisión de los procesos principales y/o todos sus procesos secundarios generados.	CUMPLE	CUMPLE
	VIII. CARACTERÍSTICA DEL CONTROL DE DISPOSITIVOS Y VISIBILIDAD DE APLICACIONES		
	a.La solución debe poder controlar dispositivos USB externos.	CUMPLE	CUMPLE
	b.La solución debe contar con acciones como: Bloqueo, Lectura y Escritura y Solo lectura.	CUMPLE	CUMPLE
	c.La solución deberá controlar dispositivos USB de manera granular teniendo como tipo de clasificación, la siguiente información del dispositivo: Clase, Número de serie específico, ID de Producto o ID de Vendor.	CUMPLE	NO CUMPLE
	d.La solución debe poder permitir controlar dispositivos USB de manera granular teniendo como tipo de clasificación, la siguiente información del dispositivo: Identificador de Hardware o Versión de Bluetooth.	CUMPLE	NO CUMPLE
	e.La solución debe permitir la identificación de aplicaciones de software de terceros que puedan tener vulnerabilidades.	CUMPLE	CUMPLE
	f.La solución puede proporcionar un inventario de todas las aplicaciones instaladas para todos los equipos de la entidad.	CUMPLE	CUMPLE
	g.La solución debe poder controlar el firewall para dispositivos los sistemas operativos: Windows, Linux.	CUMPLE	CUMPLE
	h.La solución debe permitir la creación de reglas de firewall que se apliquen a varios dispositivos pertenecientes a un Sitio, Grupo.	CUMPLE	CUMPLE
	i.La solución puede crear reglas de firewall para aplicarlas a un grupo específico de dispositivos (aprovechando el etiquetado o los grupos de políticas).	CUMPLE	CUMPLE
	IX. CARACTERÍSTICA DE INVENTARIO DE SOFTWARE		
	a.La solución de inventario de software deberá ser capaz de realizar un escaneo automático de todos los endpoints en la red corporativa.	CUMPLE	CUMPLE
	b.Debe registrar de manera precisa las versiones de todos los programas y aplicaciones instalados en cada endpoint.	CUMPLE	CUMPLE
	c.Debe ser capaz de identificar las actualizaciones de software y mantener un historial de las versiones anteriores.	CUMPLE	CUMPLE
	d.Deberá proporcionar información detallada sobre cada programa, incluyendo el nombre del software, el editor o fabricante, la fecha de instalación y la ubicación en el sistema de archivos del endpoint.	CUMPLE	CUMPLE
	e.Debe ser capaz de generar alertas o informes específicos sobre las vulnerabilidades encontradas.	CUMPLE	CUMPLE
	f.Debe generar alertas o notificaciones cuando se detecte software no autorizado.	CUMPLE	CUMPLE
	g.Deberá ofrecer la capacidad de generar informes detallados sobre el inventario de software, que incluyan la lista de software instalado, sus versiones y cualquier hallazgo relacionado con vulnerabilidades o software no autorizado.	CUMPLE	CUMPLE
	h.Los informes deben ser personalizables y exportables en diferentes formatos, como PDF o CSV.	CUMPLE	CUMPLE
	i.Deberá ser capaz de generar informes específicos que ayuden a la organización a cumplir con requisitos normativos relacionados con la gestión de software y la seguridad de la información.	CUMPLE	CUMPLE
	j.Debe permitir la toma de medidas automáticas o manuales según las políticas definidas.	CUMPLE	NO CUMPLE
	k.Debe permitir la configuración de acciones automáticas basadas en políticas de seguridad.	CUMPLE	NO CUMPLE
	X. CARACTERÍSTICAS DE XDR (Detección y Respuesta Extendida)		
	a.La solución debe permitir realizar acciones de respuesta XDR con un solo clic para que permita detener la expansión del ataque.	CUMPLE	NO CUMPLE
	b.La solución debe permitir suspender el acceso al correo del usuario si se detecta que las credenciales de un usuario interno se han utilizado para iniciar sesión en el correo electrónico y enviar phishing.	CUMPLE	NO CUMPLE
	c.La solución debe permitir el bloqueo del hash si se detecta un acceso no permitido al correo del usuario.	CUMPLE	NO CUMPLE

5.6 REQUERIMIENTOS DEL PROVEEDOR Y SU PERSONAL CLAVE			
<p>5.6.1 REQUERIMIENTOS COMO PROVEEDOR</p> <p>a) Deberá encontrarse registrado como proveedor en el RNP. b) El postor deberá de tener como mínimo cinco (05) años de experiencia en la venta de soluciones similares como Venta de Software Antivirus, Venta de Software Antimalware y Solución EDR. c) Con el fin de acreditar experiencia, el postor deberá acreditar ser partner autorizado de la marca ofertada y como mínimo tener la categoría Silver. Esto se acreditará adjuntando documentación oficial del fabricante de la solución ofertada o del Distribuidor Autorizado o representante de la marca en el Perú. d) El postor deberá de contar con un Centro de Operaciones de Seguridad (SOC) propia para brindar el soporte 24x7x365 incluidos domingos y feriados.</p> <p>5.6.1.1 Acreditación: 1. El postor deberá demostrar estar registrado como proveedor en el RNP. 2. El postor deberá acreditar experiencia en la especialidad con copias simples de contratos u órdenes de servicios con su respectiva conformidad o constancia de prestación, en la venta de soluciones similares como Venta de Software Antivirus, Venta de Software Antimalware y Solución EDR 3. Así mismo con el fin de acreditar experiencia, el postor deberá adjuntar documentación oficial del fabricante de la solución ofertada o del Distribuidor Autorizado o representante de la marca en el Perú. 4. El postor deberá presentar una declaración jurada el cual se comprometerá a brindar los servicios de soporte técnico y Centro de Operaciones de Seguridad SOC, por el periodo del servicio de licenciamiento antivirus contratado.</p>	CUMPLE	NO CUMPLE	
<p>5.6.2 PERFIL DEL PERSONAL CLAVE</p>			
<p>a) COORDINADOR DE PROYECTO Será el responsable de la coordinación, supervisión y monitoreo de las actividades detalladas en el numeral 5.2. del servicio a implementar, el cual deberá tener el siguiente perfil:</p> <p>1. Formación Académica a. Un (01) Profesional titulado y con colegiatura habilitada en Ingeniería Electrónica y/o Ingeniería de Sistemas y/o Ingeniería de Software y/o Ingeniería de Telecomunicaciones y/o Ingeniería Redes y Comunicaciones y/o Ingeniería Informática y Sistemas. b. Deberá contar con certificación Lead Cybersecurity Manager – ISO 27032</p>			



<p>2.Experiencia</p> <p>a.Deberá contar con experiencia mínima de DOS (02) años como Jefe y/o Supervisor en Gestión de Proyectos de TI y/o Proyectos de Seguridad y Protección Endpoint. El cual deberá de acreditar mediante constancias, certificados, contratos y/u otro documento.</p> <p>3.Acreditación</p> <p>a.Copia simple de título en Ingeniería Electrónica y/o Ingeniería de Sistemas y/o Ingeniería de Software y/o Ingeniería de Telecomunicaciones y/o Ingeniería Redes y Comunicaciones y/o Ingeniería Informática y Sistemas.</p> <p>b.El título profesional podrá ser verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe, o según corresponda.</p> <p>c.Deberá demostrar estar colegiado y estar habilitado en el CIP.</p> <p>d.Copia de la Certificación en Lead Cybersecurity Manager – ISO 27032</p> <p>e.Deberá acreditar experiencia por medio de constancias, certificados, contratos y/u otros documentos.</p>	CUMPLE	NO CUMPLE
<p>b)ESPECIALISTA DE IMPLEMENTACIÓN</p> <p>Será el responsable de la Implementación, Configuración, Capacitación y Entrenamiento, así mismo deberá efectuar la ejecución de las actividades detalladas en el numeral 5.2.</p> <p>1.Formación Académica</p> <p>a.Un (01) Profesional titulado en Ingeniería Electrónica y/o Ingeniería de Sistemas y/o Ingeniería de Software y/o telecomunicaciones y/o redes y comunicaciones y/o electrónica y/o redes y comunicaciones de datos y/o informática y sistemas.</p> <p>2.Experiencia</p> <p>a.Deberá contar con una experiencia como mínimo de DOS (02) años en implementaciones, soporte técnico de soluciones de seguridad de protección de ENDPOINT.</p> <p>3.Acreditación</p> <p>a.El título profesional podrá ser verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe, o según corresponda.</p> <p>b.Copia simple de título en Ingeniería electrónica, Ingeniería de sistemas, Ingeniería de seguridad y auditoría informática, Ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, informática y sistemas.</p> <p>c.Deberá acreditar experiencia por medio de constancias, certificados, contratos y/u otros documentos</p>	CUMPLE	CUMPLE



<p>5.7.2 PLAZO DE IMPLEMENTACION DEL SERVICIO</p> <p>El plazo de implementación del servicio de licenciamiento de Software Antivirus de Protección Avanzada Endpoints, considerando todos sus componentes, configuraciones, así como la activación de las licencias, deberá realizarse en los siguientes SESENTA (60) días calendarios. El inicio de la ejecución del servicio será coordinado con el área usuario, Experto de Infraestructura y Servicios de la OTIC - SIMA PERÚ.</p>	CUMPLE	CUMPLE
<p>4. FECHA DE VALIDACIÓN: 15/01/2024</p>		
<p>5. RESPONSABLE DE VALIDACIÓN (NOMBRE Y FIRMA)</p>	<p> Enrique López Coques</p>	<p> Christian Jency Alejandro Le Tonne</p>

RESULTADO:

Proveedor N°1
NO CUMPLE
Proveedor N°2
NO CUMPLE

OBSERVACIONES:

1. Se verificó que el postor NO CUMPLE con lo requerido en el siguiente literal "g". La solución debe permitir la desinstalación del agente de forma remota desde la consola de administración.", mencionado en el "II. CARACTERÍSTICAS DEL AGENTE DE PROTECCIÓN ENDPOINTS" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de las Términos de Referencia.
 - INNOVARE E-BUSINESS S.A.C., no detalló la característica solicitada en su oferta.
2. Se verificó que el postor NO CUMPLE con lo requerido en el siguiente literal "i". El agente no debe solicitar reinicio cuando se realice una actualización de versión.", mencionado en el "II. CARACTERÍSTICAS DEL AGENTE DE PROTECCIÓN ENDPOINTS" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de las Términos de Referencia.
 - INNOVARE E-BUSINESS S.A.C., no detalló la característica solicitada en su oferta.
3. Se verificó que los siguientes postores NO CUMPLEN con lo requerido en el siguiente punto "I. El agente de Linux debe ejecutarse únicamente en el espacio del usuario para evitar pánicos del Kernel y kernels contaminados que invalidan el soporte.", mencionado en el "II. CARACTERÍSTICAS DEL AGENTE DE PROTECCIÓN ENDPOINTS" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de las Términos de Referencia.
 - GS PERU MG E.I.R.L. no detalló la característica solicitada en su oferta.
 - INNOVARE E-BUSINESS S.A.C., no detalló la característica solicitada en su oferta.
4. Se verificó que el postor NO CUMPLE con lo requerido en el siguiente punto "n. La solución debe proporcionar la capacidad de enviar mensajes de notificación a la computadora del usuario final.", mencionado en el "II. CARACTERÍSTICAS DEL AGENTE DE PROTECCIÓN ENDPOINTS" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de las Términos de Referencia.
 - INNOVARE E-BUSINESS S.A.C., no detalló la característica solicitada en su oferta.
5. Se verificó que el postor NO CUMPLE con lo requerido en el siguiente punto "a. La solución deberá soportar la instalación en Sistemas Operativos para servidores como Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022. El postor podrá considerar dentro de su solución la instalación de algún componente adicional que garantice la continuidad y la seguridad de los equipos asociados a estas versiones.", mencionado en el "III. CARACTERÍSTICAS DE SISTEMA OPERATIVO SOPORTADO" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de las Términos de Referencia.
 - INNOVARE E-BUSINESS S.A.C., en la oferta presentada (página 56), la solución no es compatible con algunos sistemas operativos requeridos. Asimismo, verificó en la página del fabricante el siguiente anuncio "F-Secure Business (ahora WithSecure) comunicó que el soporte de productos para Windows 7 y Windows Server 2008R2 finalizará en enero de 2023 para los productos Elements y Business Suite". También, menciona lo siguiente "WithSecure brindará soporte para estos productos en sistemas operativos heredados hasta el 30 de junio de 2023".
<https://community.withsecure.com/en/kb/articles/29724-end-of-support-for-windows-7-and-windows-server-2008>
6. Se verificó que el postor NO CUMPLE con lo requerido en el siguiente punto "b. La solución deberá soportar la instalación en Sistemas Operativos Windows XP, Windows 7, Windows 8, Windows 10, Windows 11 y Linux. El postor podrá considerar dentro de su solución la instalación de algún componente adicional que garantice la continuidad y la seguridad de los equipos asociados a estas versiones.", mencionado en el "III. CARACTERÍSTICAS DE SISTEMA OPERATIVO SOPORTADO" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de las Términos de Referencia.
 - INNOVARE E-BUSINESS S.A.C., en la oferta presentada (página 56), la solución no es compatible con algunos sistemas operativos requeridos. Asimismo, verificó en la página del fabricante el siguiente anuncio "F-Secure Business (ahora WithSecure) comunicó que el soporte de productos para Windows 7 y Windows Server 2008R2 finalizará en enero de 2023 para los productos Elements y Business Suite". También, menciona lo siguiente "WithSecure brindará soporte para estos productos en sistemas operativos heredados hasta el 30 de junio de 2023".
<https://community.withsecure.com/en/kb/articles/29724-end-of-support-for-windows-7-and-windows-server-2008>



7. Se verificó que los siguientes postores NO CUMPLEN con lo requerido en el siguiente punto "g. El agente no debe tener dependencia con la consola de administración, con la nube o cualquier recurso externo para detectar y responder adecuadamente a amenazas solicitadas (día cero, sin archivos, basado en RAM, cero Exploits diarios, ransomware, mineros, movimiento lateral, APT) en tiempo real a medida que se detectan las amenazas)", mencionado en el "IV. CARACTERISTICA DE PREVENCIÓN DE AMENAZAS" del numeral 5.2 CARACTERISTICAS DEL SERVICIO A CONTRATAR de los Términos de Referencia.

- GS PERU MG E.I.R.L. no especificó la característica solicitada en su oferta.
- INNOVARE E-BUSINESS S.A.C., no especificó la característica solicitada en su oferta.

8. Se verificó que los siguientes postores NO CUMPLEN con lo requerido en el siguiente punto "h. El agente examinará la información de procesos en el dispositivo antes de enviar información de alerta en la consola de administración y toma acción de remediación automática, reduciendo el tiempo de detección y remediación de un ataque.", mencionado en el "IV. CARACTERISTICA DE PREVENCIÓN DE AMENAZAS" del numeral 5.2 CARACTERISTICAS DEL SERVICIO A CONTRATAR de los Términos de Referencia.

- GS PERU MG E.I.R.L. no detalló en su oferta la característica solicitada.
- INNOVARE E-BUSINESS S.A.C., no detalló en su oferta la característica solicitada.

8. Se verificó que los siguientes postores NO CUMPLEN con lo requerido en el siguiente punto "h. El agente examinará la información de procesos en el dispositivo antes de enviar información de alerta en la consola de administración y toma acción de remediación automática, reduciendo el tiempo de detección y remediación de un ataque.", mencionado en el "IV. CARACTERISTICA DE PREVENCIÓN DE AMENAZAS" del numeral 5.2 CARACTERISTICAS DEL SERVICIO A CONTRATAR de los Términos de Referencia.

- GS PERU MG E.I.R.L. no detalló en su oferta la característica solicitada.
- INNOVARE E-BUSINESS S.A.C., no detalló en su oferta la característica solicitada.

9. Se verificó que los siguientes postores NO CUMPLEN con lo requerido en el siguiente punto "m. La solución debe contar con Motores de Comportamiento On Write (escritura) y On Execute (ejecución).", mencionado en el "IV. CARACTERISTICA DE PREVENCIÓN DE AMENAZAS" del numeral 5.2 CARACTERISTICAS DEL SERVICIO A CONTRATAR de los Términos de Referencia.

- GS PERU MG E.I.R.L. no detalló en su oferta la característica solicitada.
- INNOVARE E-BUSINESS S.A.C., no detalló en su oferta la característica solicitada.

10. Se verificó que el postor NO CUMPLE con lo requerido en los puntos "n., o., p., y q.", mencionado en el "IV. CARACTERISTICA DE PREVENCIÓN DE AMENAZAS" del numeral 5.2 CARACTERISTICAS DEL SERVICIO A CONTRATAR de los Términos de Referencia.

- INNOVARE E-BUSINESS S.A.C., no detalló en su oferta la característica solicitada.

11. Se verificó que los postores NO CUMPLEN con lo requerido en el siguiente punto " d. Las políticas de la solución deberán brindar la opción de ENCENDER o APAGAR motores únicos o por Tipo de motor (Motores de ejecución previa y de tiempo de ejecución). ", mencionado en el "VI.CARACTERÍSTICAS DE LAS POLÍTICAS DE INSTALACIÓN" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de las Términos de Referencia.

- GS PERU MG E.I.R.L. no detalló en su oferta la característica solicitada.
- INNOVARE E-BUSINESS S.A.C., no detalló en su oferta la característica solicitada.

12. Se verificó que el postor NO CUMPLE con lo requerido en el siguiente punto " b. La solución debe permitir a los administradores de la consola realizar exclusiones mediante: Hash , Ruta, Certificado o un Signer ID, tipo de Archivo ", mencionado en el "VII.CARACTERÍSTICA DE LISTAS DE EXCLUSIONES" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de las Términos de Referencia.

- INNOVARE E-BUSINESS S.A.C., no detalló la característica solicitada en su oferta.

13. Se verificó que el postor NO CUMPLE con lo requerido en los siguientes puntos " c y d ", mencionado en el "VIII.CARACTERÍSTICA DEL CONTROL DE DISPOSITIVOS Y VISIBILIDAD DE APLICACIONES" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de las Términos de Referencia.

- INNOVARE E-BUSINESS S.A.C., no detalló la característica solicitada en su oferta.

13. Se verificó que el postor NO CUMPLE con lo requerido en el siguiente punto " d. La solución debe permitir controlar dispositivos USB de manera granular teniendo como tipo de clasificación, la siguiente información del dispositivo: Identificador de Hardware o Versión de Bluetooth. ", mencionado en el "VIII.CARACTERÍSTICA DEL CONTROL DE DISPOSITIVOS Y VISIBILIDAD DE APLICACIONES" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de las Términos de Referencia.

- INNOVARE E-BUSINESS S.A.C., no detalló la característica solicitada en su oferta.

14. Se verificó que el postor NO CUMPLE con lo requerido en los puntos " J, y K. ", mencionado en el "IX.CARACTERÍSTICA DE INVENTARIO DE SOFTWARE" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de las Términos de Referencia.

- INNOVARE E-BUSINESS S.A.C., no detalló en su oferta la característica solicitada.

15. Se verificó que el postor NO CUMPLE con lo requerido en los puntos " a, b, y c. ", mencionado en el "X.CARACTERÍSTICAS DE XDR (Detección y Respuesta Extendida)" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de las Términos de Referencia.

- INNOVARE E-BUSINESS S.A.C., no detalló en su oferta la característica solicitada.

16. Se verificó que el postor NO CUMPLE con lo requerido en los puntos " 3 y 4 ", mencionado en el "5.6.1 Acreditación;" del "5.6.1 REQUERIMIENTOS COMO PROVEEDOR" del numeral 5.2 CARACTERÍSTICAS DEL SERVICIO A CONTRATAR de las Términos de Referencia.

- INNOVARE E-BUSINESS S.A.C., no presentó las Declaraciones Juradas solicitadas en las Términos de Referencia.

17. Se verificó que el postor NO CUMPLE con el literal "b. Deberá contar con certificación Lead Cybersecurity Manager – ISO 27032", mencionado en el numeral 5.6.2 PERFIL DEL PERSONAL CLAVE de las Términos de Referencia.

- INNOVARE E-BUSINESS S.A.C., de acuerdo a lo indicado en los Términos de referencia se solicitó un personal con certificación oficial en la Lead Cybersecurity Manager – ISO 27032. Sin embargo, el postor remitió certificado que acredita haber culminado satisfactoriamente el curso ISO/IEC 27032.23 LEAD CIBERSECURITY MANAGER .