

**ACTA N°5**  
**ABSOLUCIÓN DE CONSULTAS Y/U OBSERVACIONES E INTEGRACIÓN DE LAS BASES**

**Concurso Público N°0060-2023-SUNAT/8B7200**  
**“Servicio de suscripción de un sistema de control y seguridad de puntos finales para equipos de la red de Sunat”**

El 2023-11-17, a través del Microsoft Teams, se reunieron los miembros del Comité de Selección consignados en el Formato de Designación del Comité de Selección N°070-2023-SUNAT/8B7000, encargado de preparar, conducir y realizar el procedimiento de selección de Concurso Público N°0060-2023-SUNAT/8B7200, orientado a la contratación del “Servicio de suscripción de un sistema de control y seguridad de puntos finales para equipos de la red de Sunat”, conformado por las siguientes personas:

<b>Presidente</b>	ERIKA MIA HINOSTROZA MATOS
<b>Primer Miembro</b>	JUAN CARLOS FLORES ALVAREZ
<b>Segundo Miembro</b>	PIERRE ALBERTO DELGADO QUIJANDRIA

En cumplimiento de las actividades programadas en el cronograma del procedimiento de selección, se inició la sesión convocada con el fin de absolver las consultas y/u observaciones, e integrar las Bases.

Los miembros del Comité de Selección señalaron que, dentro del plazo establecido en el cronograma, se presentaron un total de sesenta y un (61) consultas/observaciones de forma electrónica a través del Seace, formuladas por los participantes: (i) SSG PERU S.A.C., (ii) CLADIRECT PERU S.A.C. y (iii) SECURESOFTE CORPORATION S.A.C.

Dado que todas las consultas y/u observaciones presentadas en el procedimiento conciernen al Requerimiento (Términos de Referencia y Requisitos de Calificación), en cumplimiento de las disposiciones de la normativa de contratación pública, fueron derivadas previamente mediante el Memorándum Electrónico N°00441-2023-8B7202-División De Contrataciones de fecha 2023-11-13 a la Oficina de Seguridad Informática, para la absolución correspondiente en su condición de área usuaria/técnica. En respuesta, a través del Seguimiento 1 del citado Memorándum Electrónico, con fecha 2023-11-15 la jefatura de la Oficina de Seguridad Informática remitió la absolución técnica correspondiente.

De otro lado, en mérito a lo dispuesto en el numeral 72.3 del artículo 72 del Reglamento de la Ley de Contrataciones del Estado, con fecha 2023-11-16 el Comité de Selección remitió el mencionado Memorándum Electrónico N°00441-2023-8B7202-División De Contrataciones con el pliego absolutorio consolidado a la División de Programación y Gestión, para conocimiento en su calidad de área que aprobó el expediente de contratación; y en respuesta, con fecha 2023-11-17 la jefatura de la División de Programación y Gestión manifestó lo siguiente: *«En el seguimiento anterior de Pablo Rojas se brinda respuesta a lo solicitado y cuenta con el visto de la supervisión 2 y conformidad de esta división»*, ello refiriéndose a los Seguidos 6 y 7 del Memorándum Electrónico N°00441-2023-8B7202-División De Contrataciones, siendo que en el Seguimientos 6 del Sr. Pablo Rojas se indicó lo siguiente: *«Para informarle que producto de la absolución de las consultas/observaciones formuladas en el Concurso Público N°0060-2023-SUNAT/8B7200 por la contratación del “Servicio de Suscripción de un Sistema de Control y Seguridad de Puntos Finales para equipos de la red de SUNAT”, ya que el área usuaria/técnica ha efectuado las precisiones al requerimiento, por lo que, la División de Programación y Gestión ha tomado conocimiento en concordancia a lo dispuesto en el numeral 72.3 del artículo 72 del Reglamento de la Ley de Contrataciones del Estado. Asimismo, se ha procedido con la revalidación del mercado, el cual las empresas que han participado en la indagación de mercado han ratificado las cotizaciones el cual manifiestan que cumplen con el requerimiento, por lo tanto, se mantiene la pluralidad de postores y se ratifica el valor estimado. Por lo que se sugiere remitir al comité de selección designado para las acciones siguientes»*.

A continuación, después de discutir y debatir las consultas y/u observaciones a las bases, los miembros del Comité de Selección **ACUERDAN**, por unanimidad: (i) Aprobar el pliego absolutorio correspondiente, el mismo que se anexa al presente documento como parte integrante e (ii) Integrar las bases, incorporando al texto original las precisiones producto de las consultas y/u observaciones a las bases conforme a lo señalado en el respectivo pliego absolutorio; y con ello encargar a la presidenta del Comité de Selección efectuar la publicación correspondiente en el Seace.

No habiendo otro asunto que tratar, en la misma fecha, se da por terminada la sesión, firmándose la presente Acta por todos los miembros integrantes del Comité de Selección en señal de conformidad.

ERIKA MIA  
HINOSTROZA MATOS

JUAN CARLOS  
FLORES ALVAREZ

PIERRE ALBERTO  
DELGADO QUIJANDRIA



Firmado digitalmente por:  
HINOSTROZA MATOS Erika  
Ma FAU 20131312955 soft  
Motivo: En señal de  
conformidad  
Fecha: 17/11/2023 15:57:07-0500



Firmado digitalmente por:  
FLORES ALVAREZ Juan  
Carlos FAU 20131312955 soft  
Motivo: En señal de  
conformidad  
Fecha: 17/11/2023 16:05:24-0500



Firmado digitalmente por:  
DELGADO QUIJANDRIA PIERRE  
ALBERTO FIR 45575229 hard  
Motivo: En señal de  
conformidad  
Fecha: 17/11/2023 16:41:04-0500

PLIEGO ABSOLUTORIO

Concurso Público N°0060-2023-SUNAT/8B7200  
"Servicio de suscripción de un sistema de control y seguridad de puntos finales para equipos de la red de Sunat"

Fecha: 2023-11-17

Nro. Orden	RUC/Código	Nombre o Razón Social	Tipo Formulación	Sección	Numeral	Literal	Página	Consulta u Observación	Artículo y norma que se vulnera (en el caso de observaciones)	Análisis respecto de la consulta u observación	Precisión de aquello que se incorporará en las Bases a integrarse, de corresponder
1	20535653284	SSG PERU S.A.C.	Consulta	Específico	3.1	3	20	Se indica: 3.ANTECEDENTES La SUNAT, desde años anteriores ha venido utilizando una solución tecnológica que brinda una eficaz protección sobre la información de la Institución, a fin de que no pueda salir sin autorización y/o ser sustraída de los equipos o componentes informáticos, la misma que no pueda ser leída fuera de la red de SUNAT. Con este servicio los colaboradores de la SUNAT podrán desarrollar sus funciones con un mejor nivel de seguridad en tanto la información contenida en sus equipos de cada trabajador se encontrará protegida en caso de pérdida y/o sustracción, así como los datos institucionales solo podrán ser retirados de la Institución por personal autorizado.  Agradeceremos confirmar que para atender lo requerido por SUNAT "... solución tecnológica que brinda una eficaz protección sobre la información de la Institución, a fin de que no pueda salir sin autorización y/o ser sustraída de los equipos o componentes informáticos, la misma que no pueda ser leída fuera de la red de SUNAT" la entidad usa una combinación de un sistema de cifrado de disco, archivos y carpetas y Data Loss Prevention (DLP).		Se confirma lo mencionado por el Postor. Estas funcionalidades se detallan en el Anexo 01: SOLUCIÓN TECNOLÓGICA DE SEGURIDAD INTERNA DE INFORMACIÓN.	
2	20535653284	SSG PERU S.A.C.	Consulta	Específico	3.1	5.1	21	5.1 Descripción y cantidad del servicio a contratar Servicio de un Sistema de Control y Seguridad de Puntos Finales para equipos de la red de SUNAT, implementado sobre una solución que permita: - Encriptar la información contenida en los dispositivos USB y/o carpetas del personal autorizado a trabajar fuera de los locales institucionales, que utiliza equipos de punto final; evitando el acceso a la información de los equipos extraviados, sustraídos y/o accedidos en forma no autorizada.  Agradeceremos confirmar si SUNAT cuenta actualmente con dispositivos USB cifrados y equipos de punto final con carpetas del personal autorizado a trabajar fuera de los locales institucionales cifrados.		Se confirma que SUNAT cuenta actualmente con dispositivos USB cifrados y equipos de punto final con carpetas cifradas.	
3	20535653284	SSG PERU S.A.C.	Consulta	Específico	3.1	5.2.1	22	Se indica: 5.2.1 Servicio de suscripción de un Sistema de Control y Seguridad de Puntos Finales para equipos de la red de SUNAT El CONTRATISTA debe considerar que SUNAT tiene desplegada a nivel nacional una solución similar del fabricante Trellix (antes McAfee); de ser el caso, el Contratista deberá efectuar previamente las tareas de desinstalación mediante el uso de herramientas propias de la solución ofertada.  Agradeceremos confirmar, que el Contratista deberá efectuar previamente (de ser el caso) las tareas de desinstalación mediante el uso de herramientas propias de la solución ofertada y desplegar a nivel nacional una solución que minimamente cubra lo requerido por SUNAT: - Software de seguridad interna de información. - Software de seguridad contra software malicioso. - Software de detección y remediación frente a amenazas de software malicioso. - Software de seguridad para dispositivos móviles.		Se confirma lo señalado por el participante lo cual se enmarca dentro de lo establecido en el numeral 5.2.1 y en el Anexo 1.	
4	20535653284	SSG PERU S.A.C.	Consulta	Específico	3.1	5.2.1.2	23	Se indica: 5.2.1.2 Instalación, configuración e implementación de la solución tecnológica El Contratista debe proveer todas las funcionalidades y deben ser gestionadas por la consola de administración centralizada que cumpla con las siguientes características técnicas que se detallan en ANEXO 02.  Agradeceremos confirmar que la consola debe centralizar la administración minimamente de los siguientes software requeridos por la SUNAT: - Software de seguridad interna de información. - Software de seguridad contra software malicioso. - Software de detección y remediación frente a amenazas de software malicioso. - Software de seguridad para dispositivos móviles.		Se confirma que minimamente la consola debe centralizar la solución tecnológica de seguridad interna de información y la solución tecnológica de seguridad contra software malicioso.	



Firmado digitalmente por:  
HINOJOSA MATOS Erika  
Mia FAU 20131312955 soft  
Motivo: En señal de conformidad  
Fecha: 17/11/2023 15:58:17-0500



Firmado digitalmente por:  
FLORES ALVAREZ Juan  
Carlos FAU 20131312955 soft  
Motivo: En señal de conformidad  
Fecha: 17/11/2023 16:06:26-0500



Firmado digitalmente por:  
DELGADO QUIJANDRIA PIERRE  
ALBERTO FIR 45575229 hard  
Motivo: En señal de conformidad  
Fecha: 17/11/2023 16:42:37-0500

Nro. Orden	RUC/Código	Nombre o Razón Social	Tipo Formulación	Sección	Numeral	Literal	Página	Consulta u Observación	Artículo y norma que se vulnera (en el caso de observaciones)	Análisis respecto de la consulta u observación	Precisión de aquello que se incorporará en las Bases a integrarse, de corresponder
5	20535653284	SSG PERU S.A.C.	Consulta	Específico	6	6.2.1	29	<p>6. REQUISITOS Y RECURSOS DEL PROVEEDOR</p> <p>6.2.1. Otro Personal</p> <p>(b) Cinco (05) Especialistas de los softwares de protección.</p> <p>- Bachiller o Título Profesional en Ingeniería de Sistemas o Industrial o Informática o Software o Computación o Telecomunicaciones o Electrónica.</p> <p>Agradeceremos considerar también las siguientes carreras profesionales para los Especialistas de los softwares de protección.</p> <ul style="list-style-type: none"> <li>- Ingeniería de Sistemas y Computo.</li> <li>- Ingeniería de Computación y Sistemas.</li> <li>- Ingeniería de Sistemas e Informática.</li> <li>- Ingeniería de Computación.</li> <li>- Ingeniería de Sistemas Empresariales.</li> <li>- Ingeniería de Sistemas de Información.</li> <li>- Ingeniería de Telecomunicaciones y Redes.</li> <li>- Ingeniería de Redes y Comunicaciones de Datos.</li> </ul> <p>Esta solicitud acorde al último "Clasificador Nacional de Programas e Instituciones de Educación Superior Universitaria, Pedagógica, Tecnológica y Técnico Productiva, 2018", desarrollado por el Instituto Nacional de Estadística e Informática (INEI) con colaboración de la Superintendencia Nacional de Educación Superior Universitaria (SUNEDU), Ministerio de Educación (MINEDU) y el Ministerio de Trabajo y Promoción del Empleo (MTPE).</p> <p>Referencia.</p> <p><a href="https://www.gob.pe/institucion/inei/informes-publicaciones/3246178-clasificador-nacional-de-programas-e-instituciones-de-educacion-superior-universitaria-pedagogica-tecnologica-y-tecnico-productiva-2018">https://www.gob.pe/institucion/inei/informes-publicaciones/3246178-clasificador-nacional-de-programas-e-instituciones-de-educacion-superior-universitaria-pedagogica-tecnologica-y-tecnico-productiva-2018</a></p>		Con el fin de propiciar una mayor concurrencia de postores se acepta lo sugerido.	Para el personal "Especialistas de los softwares de protección" bajo el perfil requerido, considerar adicionalmente Bachiller o Título Profesional en Ingeniería de Sistemas y Computo o Computación y Sistemas o Sistemas e Informática o Sistemas Empresariales o Sistemas de Información o Telecomunicaciones y Redes o Redes y Comunicaciones de Datos.
6	20535653284	SSG PERU S.A.C.	Consulta	Específico	6	6.2.1.	29	<p>6. REQUISITOS Y RECURSOS DEL PROVEEDOR.</p> <p>6.2.1. Otro Personal.</p> <p>(c) Un (01) Instructor del software de protección.</p> <p>ii. Perfil:</p> <p>-Bachiller o Título Profesional en Ingeniería de Sistemas o Industrial o Informática o Software o Computación o Telecomunicaciones o Electrónica.</p> <p>Agradeceremos considerar también las siguientes carreras profesionales para el instructor del software de protección.</p> <ul style="list-style-type: none"> <li>- Ingeniería de Sistemas y Computo.</li> <li>- Ingeniería de Computación y Sistemas.</li> <li>- Ingeniería de Sistemas e Informática.</li> <li>- Ingeniería de Computación.</li> <li>- Ingeniería de Sistemas Empresariales.</li> <li>- Ingeniería de Sistemas de Información.</li> <li>- Ingeniería de Telecomunicaciones y Redes.</li> <li>- Ingeniería de Redes y Comunicaciones de Datos.</li> </ul> <p>Esta solicitud acorde al último "Clasificador Nacional de Programas e Instituciones de Educación Superior Universitaria, Pedagógica, Tecnológica y Técnico Productiva, 2018", desarrollado por el Instituto Nacional de Estadística e Informática (INEI) con colaboración de la Superintendencia Nacional de Educación Superior Universitaria (SUNEDU), Ministerio de Educación (MINEDU) y el Ministerio de Trabajo y Promoción del Empleo (MTPE).</p> <p>Referencia.</p> <p><a href="https://www.gob.pe/institucion/inei/informes-publicaciones/3246178-clasificador-nacional-de-programas-e-instituciones-de-educacion-superior-universitaria-pedagogica-tecnologica-y-tecnico-productiva-2018">https://www.gob.pe/institucion/inei/informes-publicaciones/3246178-clasificador-nacional-de-programas-e-instituciones-de-educacion-superior-universitaria-pedagogica-tecnologica-y-tecnico-productiva-2018</a></p>		Con el fin de propiciar una mayor concurrencia de postores se acepta lo sugerido.	Para el personal "Instructor del software de protección" bajo el perfil requerido, considerar adicionalmente Bachiller o Título Profesional en Ingeniería de Sistemas y Computo o Computación y Sistemas o Sistemas e Informática o Sistemas Empresariales o Sistemas de Información o Telecomunicaciones y Redes o Redes y Comunicaciones de Datos.

Nro. Orden	RUC/Código	Nombre o Razón Social	Tipo Formulación	Sección	Numeral	Literal	Página	Consulta u Observación	Artículo y norma que se vulnera (en el caso de observaciones)	Análisis respecto de la consulta u observación	Precisión de aquello que se incorporará en las Bases a integrarse, de corresponder
7	20535653284	SSG PERU S.A.C.	Consulta	Específico	6	6.2.1	29	<p>6. REQUISITOS Y RECURSOS DEL PROVEEDOR.</p> <p>6.2.1. Otro Personal.</p> <p>(d) Un (01) Ingeniero residente</p> <p>ii. Perfil:</p> <p>- Bachiller o Título Profesional en Ingeniería de Sistemas o Industrial o Informática o Software o Computación o Telecomunicaciones o Electrónica.</p> <p>Agradeceremos considerar también las siguientes carreras profesionales para el Ingeniero residente:</p> <ul style="list-style-type: none"> <li>- Ingeniería de Sistemas y Computo.</li> <li>- Ingeniería de Computación y Sistemas.</li> <li>- Ingeniería de Sistemas e Informática.</li> <li>- Ingeniería de Computación.</li> <li>- Ingeniería de Sistemas Empresariales.</li> <li>- Ingeniería de Sistemas de Información.</li> <li>- Ingeniería de Telecomunicaciones y Redes.</li> <li>- Ingeniería de Redes y Comunicaciones de Datos.</li> </ul> <p>Esta solicitud acorde al último "Clasificador Nacional de Programas e Instituciones de Educación Superior Universitaria, Pedagógica y Técnico Productiva, 2018", desarrollado por el Instituto Nacional de Estadística e Informática (INEI) con colaboración de la Superintendencia Nacional de Educación Superior Universitaria (SUNEDU), Ministerio de Educación (MINEDU) y el Ministerio de Trabajo y Promoción del Empleo (MTPE).</p> <p>Referencia.</p> <p><a href="https://www.gob.pe/institucion/inei/informes-publicaciones/3246178-clasificador-nacional-de-programas-e-instituciones-de-educacion-superior-universitaria-pedagogica-tecnologica-y-tecnico-productiva-2018">https://www.gob.pe/institucion/inei/informes-publicaciones/3246178-clasificador-nacional-de-programas-e-instituciones-de-educacion-superior-universitaria-pedagogica-tecnologica-y-tecnico-productiva-2018</a></p>		Con el fin de propiciar una mayor concurrencia de postores se acepta lo sugerido.	Para el personal "Ingeniero residente" bajo el perfil requerido, considerar adicionalmente Bachiller o Título Profesional en Ingeniería de Sistemas y Computo o Computación y Sistemas o Sistemas e Informática o Sistemas Empresariales o Sistemas de Información o Telecomunicaciones y Redes o Redes y Comunicaciones de Datos.
8	20535653284	SSG PERU S.A.C.	Consulta	Específico	6	6.2.1	29	<p>6. REQUISITOS Y RECURSOS DEL PROVEEDOR.</p> <p>6.2.1. Otro Personal.</p> <p>(d) Un (01) Ingeniero residente</p> <p>ii. Perfil:</p> <p>- Bachiller o Título Profesional en Ingeniería de Sistemas o Industrial o Informática o Software o Computación o Telecomunicaciones o Electrónica.</p> <p>Solicitamos a la SUNAT también considerar para la posición de Ingeniero Residente Profesionales Técnicos Titulados en Computación e informática y carreras técnicas afines.</p>		Se mantiene los requisitos indicados en el numeral 6.2.1. dado que la institución requiere profesionales con el perfil mencionado.	
9	20535653284	SSG PERU S.A.C.	Consulta	Específico	3.2	A	47	<p>3.2. REQUISITOS DE CALIFICACIÓN</p> <p>A. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD</p> <p>Requisitos:</p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/ 10,000,000.00 (diez millones y 00/100 soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (08) 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.</p> <p>Se considerarán servicios similares a los siguientes:</p> <ul style="list-style-type: none"> <li>Servicios o suscripciones de un Sistema de control y seguridad de puntos finales.</li> <li>Servicios o suscripciones de software antivirus.</li> <li>Servicios o suscripciones de software de cifrado.</li> <li>Servicios o suscripciones de software de control de dispositivos o DLP.</li> <li>Servicios o suscripciones de software de tipo detección y respuesta.</li> </ul> <p>Agradeceremos confirmar que cuando la SUNAT indica "Suscripciones de un Sistema de control y seguridad de puntos finales, suscripciones de software antivirus, suscripciones de software de cifrado, suscripciones de software de control de dispositivos o DLP y suscripciones de software de tipo detección y respuesta considerará valido la presentación de contratos o facturas de:</p> <ul style="list-style-type: none"> <li>Licencias de software de control y seguridad de puntos finales.</li> <li>Licencias de software antivirus.</li> <li>Licencias de software de cifrado.</li> <li>Licencias de software de control de dispositivos o DLP.</li> <li>Licencias de software de tipo detección y respuesta.</li> </ul>		<p>La necesidad de la Entidad es proteger los equipos de punto final a nivel a nacional ante cualquier ataque cibernético. Esto se materializa con la instalación de los distintos softwares de protección en dichos equipos.</p> <p>Si bien es cierto, el presente procedimiento de selección está referido a la suscripción de licencias, lo que finalmente se requiere es contar con los distintos softwares de protección, independientemente de la forma en que son comercializados, ya sea por suscripción o venta de las licencias.</p> <p>En ese orden de ideas, la evaluación de la experiencia del postor podrá también ser acreditada mediante documentación que demuestre fehacientemente, la venta de las licencias siguientes:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Sistema de control y seguridad de puntos finales,</li> <li><input type="checkbox"/> Software antivirus,</li> <li><input type="checkbox"/> Software de cifrado,</li> <li><input type="checkbox"/> Software de control de dispositivos o DLP,</li> <li><input type="checkbox"/> Software de tipo detección y respuesta.</li> </ul> <p>En ese sentido, se confirma lo consultado.</p>	Adicionalmente a los servicios similares, considerar las licencias siguientes: <ul style="list-style-type: none"> <li><input type="checkbox"/> Sistema de control y seguridad de puntos finales,</li> <li><input type="checkbox"/> Software antivirus,</li> <li><input type="checkbox"/> Software de cifrado,</li> <li><input type="checkbox"/> Software de control de dispositivos o DLP,</li> <li><input type="checkbox"/> Software de tipo detección y respuesta.</li> </ul>

Nro. Orden	RUC/Código	Nombre o Razón Social	Tipo Formulación	Sección	Numeral	Literal	Página	Consulta u Observación	Artículo y norma que se vulnera (en el caso de observaciones)	Análisis respecto de la consulta u observación	Precisión de aquello que se incorporará en las Bases a integrarse, de corresponder
10	20517793630	CLADIRECT PERU S.A.C.	Consulta	Específico	Anexo 01	8	37	<p>Los siguientes dispositivos listados:</p> <ul style="list-style-type: none"> <li>¿ Secure Digital (SD)</li> <li>¿ Mouse, Teclado</li> <li>¿ Cámaras web</li> <li>¿ Reproductores de audio</li> <li>¿ Antenas de TV</li> <li>¿ Lector de tarjetas electrónicas</li> </ul> <p>Estos dispositivos, estadísticamente no representan un riesgo significativo para la seguridad y productividad. Se solicita a la entidad, a fin de fomentar una mayor participación de postores, excluirlos como parte del control de dispositivos y de esta forma mejorar la experiencia del Usuario.</p>		La SUNAT requiere controlar los dispositivos mencionados para salvaguardar la seguridad, por lo cual se mantiene lo señalado en el ítem 08 del Anexo 01.	
11	20517793630	CLADIRECT PERU S.A.C.	Consulta	Específico	Anexo 01	16	38	<p>Dice: Deberá permitir cifrar los archivos que adjuntan a correos externos institucionales o correos privados que se realicen desde equipos administrados, según el perfil definido para el usuario.</p> <p>Consulta: Usualmente, la necesidad de colaboración externa puede requerir el envío de archivos no cifrados. Por lo tanto, se solicita a la entidad Confirmar que este punto será opcional ya que facilita la comunicación y colaboración con socios externos, proveedores y otros contactos.</p>		La SUNAT requiere cifrar los archivos adjuntos en correos externos para salvaguardar la seguridad, por lo cual se mantiene lo señalado en el ítem 16 del Anexo 01.	
12	20517793630	CLADIRECT PERU S.A.C.	Consulta	Específico	Anexo 01	22	38	<p>Dice: Deberá proporcionar un procedimiento que permita descifrar archivos desde la consola centralizada de una carpeta o de los equipos institucionales que tengan archivos encriptados.</p> <p>Consulta: La implementación de cifrado a nivel de archivos o carpetas puede ofrecer mayor granularidad en términos de qué archivos se cifran, pero a la vez puede introducir una mayor complejidad en la gestión de claves y un mayor impacto en el rendimiento del sistema. Por lo tanto, se solicita a la entidad Confirmar la aceptación de implementación de cifrado a nivel de disco duro ya que proporciona una capa de seguridad robusta y completa para toda la información almacenada en el disco, sin requerir acciones manuales por parte de los usuarios y ofreciendo una mayor eficiencia en el proceso de cifrado.</p>		Se mantiene lo requerido en el ítem 22 del Anexo 01 respecto al procedimiento para descifrar archivos por tratarse de un requerimiento funcional de SUNAT.	
13	20517793630	CLADIRECT PERU S.A.C.	Consulta	Específico	ANEXO 01	24	39	<p>Dice: ¿ Debe disponer, como mínimo, de dos modos de protección (Estándar / Máximo)¿</p> <p>La obligación de contar con dos modos de protección (Estándar / Máximo) puede generar complejidad innecesaria y aumentar la carga administrativa. La efectividad de la prevención de explotación no debería depender exclusivamente de la configuración de modo, sino garantizar una protección óptima en cualquier configuración.</p> <p>Por lo tanto, se solicita a la entidad que considere opcional modos de operación para la prevención de explotación.</p>		Se mantiene lo requerido en el ítem 24 del Anexo 01 respecto a los modos de protección porque la SUNAT requiere de ambos modos de protección con el fin de garantizar la seguridad de los dispositivos.	
14	20517793630	CLADIRECT PERU S.A.C.	Consulta	Específico	ANEXO 01	24	39	<p>Dice:</p> <ul style="list-style-type: none"> <li>¿Debe ser posible activar / desactivar la protección contra el escalamiento de privilegios genéricos.</li> <li>¿Debe ser posible habilitar / deshabilitar la prevención de ejecución de datos de Windows</li> </ul> <p>OBSERVACIÓN: Las terminologías usadas y características listadas en este apartado hacen referencias a la documentación de un fabricante en particular (Trellix). Se puede evidenciar en el siguiente enlace:  <a href="https://docs.trellix.com/bundle/endpoint-security-10.7.x-common-client-interface-reference-guide-windows/page/GUID-3D9AB771-0415-45C5-B62A-1EC74738BAB8.html">https://docs.trellix.com/bundle/endpoint-security-10.7.x-common-client-interface-reference-guide-windows/page/GUID-3D9AB771-0415-45C5-B62A-1EC74738BAB8.html</a></p> <p>Por lo tanto, basándonos en los Principios del Régimen de la Contratación Pública:</p> <ul style="list-style-type: none"> <li>¿ Principio de Libre Concurrencia y Competencia.</li> <li>¿ Principio de Imparcialidad.</li> <li>¿ Principio de Razonabilidad.</li> <li>¿ Principio de Transparencia.</li> <li>¿ Principio de Vigencia Tecnológica.</li> <li>¿ Principio de Trato Justo e Igualitario.</li> <li>¿ Principio de Equidad.</li> </ul> <p>Se solicita a la entidad el uso de terminologías y características generales con el objetivo de permitir la participación de otras marcas y que cumplan de diferentes formas lo solicitado.</p>		No se acoge la observación. El requerimiento funcional no alude a marca o fabricante específico por tanto se mantiene el texto señalado en el ítem 24 del Anexo 01.	

Nro. Orden	RUC/Código	Nombre o Razón Social	Tipo Formulación	Sección	Numeral	Literal	Página	Consulta u Observación	Artículo y norma que se vulnera (en el caso de observaciones)	Análisis respecto de la consulta u observación	Precisión de aquello que se incorporará en las Bases a integrarse, de corresponder
15	20517793630	CLADIRECT PERU S.A.C.	Consulta	Específico	ANEXO 01	26	40	<p>Las siguientes características:</p> <ul style="list-style-type: none"> <li>- El administrador de la solución debe especificar el tiempo máximo de análisis para un único archivo</li> <li>- Debe permitir al administrador analizar instaladores de confianza.</li> <li>- Debe permitir la configuración del nivel de agresividad del análisis en diferentes niveles.</li> <li>- Debe permitir aplicar la configuración a todos los procesos del sistema operativo o a una lista específica creada por el administrador.</li> <li>- Debe permitir en análisis cuando se produce lecturas y/o escrituras en disco y/o permitiendo que la solución misma tome la decisión de la técnica más adecuada.</li> </ul> <p>Han sido tomadas de un vendor en específico desde el siguiente enlace:  <a href="https://docs.trellix.com/bundle/endpoint-security-10.7.x-common-client-interface-reference-guide-windows/page/GUID-E9B7F5D0-D67D-4F23-BC48-E75FAC86FC31.html">https://docs.trellix.com/bundle/endpoint-security-10.7.x-common-client-interface-reference-guide-windows/page/GUID-E9B7F5D0-D67D-4F23-BC48-E75FAC86FC31.html</a></p> <p>Por lo tanto, basándonos en los Principios del Régimen de la Contratación Pública:</p> <ul style="list-style-type: none"> <li>¿ Principio de Libre Concurrencia y Competencia.</li> <li>¿ Principio de Imparcialidad.</li> <li>¿ Principio de Razonabilidad.</li> <li>¿ Principio de Transparencia.</li> <li>¿ Principio de Vigencia Tecnológica.</li> <li>¿ Principio de Trato Justo e Igualitario.</li> <li>¿ Principio de Equidad.</li> </ul> <p>Se solicita a la entidad el uso de terminologías y características generales con el objetivo de permitir la participación de otras marcas y que cumplan de diferentes formas lo solicitado</p>		No se acoge la observación. El requerimiento funcional no alude a marca o fabricante específico por tanto se mantiene el texto señalado en el ítem 26 del Anexo 01.	
16	20517793630	CLADIRECT PERU S.A.C.	Consulta	Específico	ANEXO 01	27	40	<p>Para minimizar el impacto en el usuario, la solución debe permitir:</p> <p>Dice: El uso de la memoria caché, es decir, los archivos que ya han sido analizados y no han cambiado su contenido no serán reanalizados</p> <p>Confirmar que se aceptarán otras formas similares que cumplan con el objetivo de minimizar el impacto en el usuario, como escanear únicamente archivos nuevos o modificados. Esto permitirá optimizar la utilización de recursos del endpoint.</p> <p>Dice: Comience a escanear solo cuando el sistema esté inactivo.</p> <p>Consulta: Dado que la solución a ofertar se basa en una tecnología de escaneo en tiempo real, programado, manual y en la nube y que no requiere inactividad del sistema para funcionar eficazmente. Esta tecnología permite la detección proactiva de amenazas sin afectar el rendimiento del sistema o las actividades del usuario. Por lo tanto, exigir que el escaneo solo se realice en momentos de inactividad podría limitar la eficacia de esta tecnología avanzada. Solicitamos a la entidad Confirmar que este punto será Opcional.</p> <p>Dice: Limitar el porcentaje de CPU, memoria a ser utilizado por la tarea de análisis.</p> <p>Consulta : En el ámbito de la seguridad informática, el CPU suele ser el recurso más crítico para el rendimiento general del sistema. Limitar el uso de CPU asegura que las operaciones del sistema y las aplicaciones críticas no se vean afectadas negativamente por la tarea de análisis de la solución de seguridad. Por lo tanto, esta característica debería tener una prioridad más alta en la evaluación de las soluciones de seguridad. Por lo tanto, se solicita a la entidad Confirmar que aceptará la limitación al menos a nivel de CPU.</p>		Se mantiene lo requerido en el numeral 27 del Anexo 01, porque los puntos detallados se refieren a requerimientos que aplican al análisis bajo demanda.	

Nro. Orden	RUC/Código	Nombre o Razón Social	Tipo Formulación	Sección	Numeral	Literal	Página	Consulta u Observación	Artículo y norma que se vulnera (en el caso de observaciones)	Análisis respecto de la consulta u observación	Precisión de aquello que se incorporará en las Bases a integrarse, de corresponder
17	20517793630	CLADIRECT PERU S.A.C.	Consulta	Específico	ANEXO 01	28	40	<p>Dice: Debe permitir el tráfico saliente solo después de iniciar los servicios de Firewall. (Pag.40)</p> <p>Consulta: La capacidad de bloquear tráfico saliente es esencial para prevenir la comunicación no autorizada con servidores maliciosos o para evitar la propagación de amenazas. Sin embargo, esto no debería requerir la espera de que el servicio de Firewall se inicie, ya que podría afectar en la productividad e impactar negativamente la eficiencia del negocio. Por lo tanto, se solicita que este punto sea considerado opcional.</p> <p>Dice: Deber ser posible bloquear el tráfico bridge. (Pag.40)</p> <p>Consulta: La capacidad de bloquear el tráfico bridge puede ser esencial en entornos específicos de red, pero no es una necesidad universal. Consideramos que la solución a proponer se debe adaptar a diversos entornos y debe proporcionar seguridad efectiva sin la necesidad de esta capacidad específica. Por lo tanto, a fin de fomentar mayor competencia y participación de postores se solicita a la entidad Confirmar que este punto será opcional.</p> <p>Dice: El módulo debe permitir la creación de reglas de manera adaptativa, es decir, en una estación modelo definida por el administrador, debe poder crear las reglas automáticamente. (Pag.41)</p> <p>OBSERVACIÓN: Si bien la capacidad de crear reglas adaptativas puede ser valiosa en ciertos contextos, puede no ser una prioridad en un entorno donde la prevención proactiva de amenazas es la principal estrategia de seguridad. Por otro lado, de información pública, se concluye que esta es característica es del fabricante Trellix en específico: Apartado "Enable Adaptive mode" <a href="https://docs.trellix.com/bundle/endpoint-security-10.7.x-common-client-interface-reference-guide-windows/page/GUID-4C618EF0-B4F7-45E7-8ACF-DA8C6B155BD7.html">https://docs.trellix.com/bundle/endpoint-security-10.7.x-common-client-interface-reference-guide-windows/page/GUID-4C618EF0-B4F7-45E7-8ACF-DA8C6B155BD7.html</a></p> <p>Por lo tanto, se solicita a la entidad que este punto sea considerado como opcional.</p> <p>Dice: Debe ser posible bloquear el tráfico de protocolos no compatibles. (Pag.41)</p> <p>OBSERVACIÓN: Bloquear el tráfico de protocolos no compatibles es una medida esencial para prevenir amenazas desconocidas o malware que podrían explotar vulnerabilidades en protocolos no autorizados. Sin embargo, esta funcionalidad y concepto es propiamente del fabricante Trellix: <a href="https://docs.trellix.com/bundle/endpoint-security-10.7.x-common-client-interface-reference-guide-windows/page/GUID-4C618EF0-B4F7-45E7-8ACF-DA8C6B155BD7.html">https://docs.trellix.com/bundle/endpoint-security-10.7.x-common-client-interface-reference-guide-windows/page/GUID-4C618EF0-B4F7-45E7-8ACF-DA8C6B155BD7.html</a> en el apartado "Allow traffic for unsupported protocols".</p> <p>En consecuencia apelando al principio de pluralidad de participación y garantizar la transparencia en el presente proceso, es fundamental que se evalúen y consideren las soluciones de diferentes proveedores, por lo cual se solicita que es punto sea considerado como opcional.</p>		Se considerará como opcional solamente: "Debe ser posible bloquear el tráfico de protocolos no compatibles" y "El módulo debe permitir la creación de reglas de manera adaptativa, es decir, en una estación modelo definida por el administrador, debe poder crear las reglas automáticamente". Se mantienen los otros requerimientos respecto a "Protección de red" porque la SUNAT requiere garantizar la seguridad de los dispositivos.	Las siguientes funcionalidades indicadas en el ítem 28 del Anexo 01 podrán considerarse opcionales: • Debe ser posible bloquear el tráfico de protocolos no compatibles. • El módulo debe permitir la creación de reglas de manera adaptativa, es decir, en una estación modelo definida por el administrador, debe poder crear las reglas automáticamente
18	20517793630	CLADIRECT PERU S.A.C.	Consulta	Específico	ANEXO 01	29	41	<p>Dice: Debe poder usar la lista de categorías para bloquear sitios relacionados con contenido no autorizado</p> <p>CONSULTA: Soportar listas de categorizaciones de páginas web está mas orientado a soluciones de Web Proxy, Firewalls, entre otros. Por lo tanto, favor de confirmar que la solución a ofertar deba soportar como mínimo el bloqueo a páginas maliciosas y/o altamente sospechosas para proteger a los usuarios de la organización.</p> <p>Dice: Debe permitir la personalización de los mensajes presentados al usuario.</p> <p>CONSULTA: La personalización de mensajes es una característica útil, pero puede no ser una prioridad en un entorno donde la prevención proactiva de amenazas a nivel web es lo principal. Por tal motivo, se solicita que la entidad confirme que este punto será considerado como opcional.</p>		Se mantiene lo requerido en el ítem 29 del Anexo 01 respecto a la "Protección web" porque la SUNAT requiere de estas funcionalidades con el fin de garantizar la seguridad de los dispositivos.	

Nro. Orden	RUC/Código	Nombre o Razón Social	Tipo Formulación	Sección	Numeral	Literal	Página	Consulta u Observación	Artículo y norma que se vulnera (en el caso de observaciones)	Análisis respecto de la consulta u observación	Precisión de aquello que se incorporará en las Bases a integrarse, de corresponder
19	20517793630	CLADIRECT PERU S.A.C.	Observación	Específico	ANEXO 01	30	41	<p>Dice: Protección adaptativa de amenazas (TODO EL PUNTO 30)</p> <p>OBSERVACIÓN: Las terminologías usadas en este apartado, son usadas específicamente por un solo fabricante (Trellix), y las características mencionadas han sido obtenidas desde la documentación pública de Trellix: ""Adaptive Threat Protection"" - <a href="https://docs.trellix.com/bundle/endpoint-security-10.7.x-common-client-interface-reference-guide-windows/page/GUID-BE50D5B7-B73F-4D75-971F-22E2E8E9A2B9.html">https://docs.trellix.com/bundle/endpoint-security-10.7.x-common-client-interface-reference-guide-windows/page/GUID-BE50D5B7-B73F-4D75-971F-22E2E8E9A2B9.html</a></p> <p>Por lo tanto, basándonos en los Principios del Régimen de la Contratación Pública:</p> <ul style="list-style-type: none"> <li>¿ Principio de Libre Concurrencia y Competencia.</li> <li>¿ Principio de Imparcialidad.</li> <li>¿ Principio de Razonabilidad.</li> <li>¿ Principio de Transparencia.</li> <li>¿ Principio de Vigencia Tecnológica.</li> <li>¿ Principio de Trato Justo e Igualitario.</li> <li>¿ Principio de Equidad.</li> </ul> <p>Se solicita a la entidad el uso de terminologías y características generales con el objetivo de permitir la participación de otras marcas y que cumplan de diferentes formas lo solicitado.</p> <p>SOLUCIÓN TECNOLÓGICA Y REMEDIACIÓN FRENTE A AMENAZAS DE SOFTWARE MALICIOSO</p> <p>REQUISITOS MÍNIMOS DE LA SOLUCIÓN DE DETECCIÓN Y REMEDIACIÓN FRENTE A AMENAZAS DE SOFTWARE MALICIOSO (PAG. 42)</p>	<p>¿ Principio de Libre Concurrencia y Competencia.</p> <p>¿ Principio de Imparcialidad.</p> <p>Principio de Transpa</p>	<p>No se acoge la observación.</p> <p>El requerimiento funcional no alude a marca o fabricante específico por tanto se mantiene el texto señalado en el ítem 30 del Anexo 01.</p>	
20	20517793630	CLADIRECT PERU S.A.C.	Observación	Específico	ANEXO 01	16	43	<p>Dice: Para amenazas donde se hayan generado reglas de detección, debe ser posible exportarlas como reglas expertas, reglas sigma, reglas Yara y reglas de Snort</p> <p>OBSERVACIÓN: Este conjunto de reglas son soportadas unicamente por un fabricante (Trellix) como se puede apreciar en la parte ""Hunting rules associated with a campaign"" del siguiente enlace: <a href="https://docs.trellix.com/es-ES/bundle/trellix-insights-product-guide/page/GUID-3ECA3929-DAE2-4422-A43D-449D7A97BAAD.html">https://docs.trellix.com/es-ES/bundle/trellix-insights-product-guide/page/GUID-3ECA3929-DAE2-4422-A43D-449D7A97BAAD.html</a></p> <p>Por lo tanto, basándonos en los Principios del Régimen de la Contratación Pública:</p> <ul style="list-style-type: none"> <li>¿ Principio de Libre Concurrencia y Competencia.</li> <li>¿ Principio de Imparcialidad.</li> <li>¿ Principio de Razonabilidad.</li> <li>¿ Principio de Transparencia.</li> <li>¿ Principio de Vigencia Tecnológica.</li> <li>¿ Principio de Trato Justo e Igualitario.</li> <li>¿ Principio de Equidad.</li> </ul> <p>Se solicita a la entidad el uso de terminologías y características generales con el objetivo de permitir la participación de otras marcas y que cumplan de diferentes formas lo solicitado.</p>	<p>Por lo tanto, basándonos en los Principios del Régimen de la Contratación Pública:</p> <p>¿ Principio de Li</p>	<p>No se acoge la observación.</p> <p>Se mantiene lo requerido en el ítem 16 del Anexo 01 respecto a la "Inteligencia de amenazas" porque la SUNAT requiere de estas funcionalidades con el fin de garantizar la seguridad de los dispositivos.</p>	
21	20517793630	CLADIRECT PERU S.A.C.	Consulta	Específico	ANEXO 02	2	44	<p>Dice: La solución debe permitir ser implementada tanto on-premise como SaaS (Software as a Service), permitiendo elegir cual modalidad se desea utilizar (incluso ambas al mismo tiempo) y sin incurrir en costos adicionales para la SUNAT.</p> <p>CONSULTA: Optar por una plataforma de gestión centralizada basada en la nube ofrece una serie de ventajas en términos de acceso remoto, escalabilidad, costos, automatización y resiliencia. Estos factores pueden ser críticos para las organizaciones que buscan una gestión de seguridad de endpoints eficiente y flexible.</p> <p>Por lo contrario, una plataforma de gestión centralizada local ofrece ciertos niveles de control y personalización, pero también conlleva desafíos y responsabilidades adicionales en términos de costos, complejidad, mantenimiento y escalabilidad.</p> <p>Por lo tanto, por el principio de pluralidad de postores se solicita a la entidad confirmar que la gestión de la solución también podrá ser brindada 100% en nube el cual permita obtener los beneficios de un servicio SaaS.</p>		<p>Se mantiene lo requerido respecto a la "Consola de Administración Centralizada" porque la SUNAT requiere de estos modos de implementación con el fin de garantizar la gestión de los dispositivos.</p>	



Nro. Orden	RUC/Código	Nombre o Razón Social	Tipo Formulación	Sección	Numeral	Literal	Página	Consulta u Observación	Artículo y norma que se vulnera (en el caso de observaciones)	Análisis respecto de la consulta u observación	Precisión de aquello que se incorporará en las Bases a integrarse, de corresponder
22	20517793630	CLADIRECT PERU S.A.C.	Consulta	Específico	-	-	-	Es importante entender si la expectativa del cliente es contar con una única consola de administración para las 4 soluciones, o contempla la coexistencia las soluciones de diversos fabricantes cada una con su administración si bien centralizada, separada de la administración de las demás		La gestión de los dispositivos debe ser preferentemente desde una única consola centralizada; sin embargo podría aceptarse mas de una consola pero del mismo fabricante. Tal como se menciona en el ítem 5.1. y en el Anexo 01.	
23	20517793630	CLADIRECT PERU S.A.C.	Consulta	Específico	5	5.1	21	Dice: Proteger proactivamente los equipos móviles institucionales, Smartphones y Tablets que soporten los sistemas operativos iOS o Android. Esta solución debe ser del mismo fabricante.  El pliego solo muestra el número de dispositivos, sin mayor detalle sobre el tipo y sistema operativo, lo cual es clave para entender si todos son soportados o no por las soluciones que ustedes planean ofertar. En el caso de nuestro MDM, hay una matriz de compatibilidad para smartphones y tablets, por lo que es necesario conocer esta información		En el ítem 5.1 se precisa la información de los Sistemas Operativos de los equipos móviles a soportar: Android 11 o superior y iOS 14 o superior	
24	20517793630	CLADIRECT PERU S.A.C.	Consulta	Específico	ANEXO 01	8	37	Dice: Antenas de TV CONSULTA: Dentro del tipo de elementos que se pretende controlar, habla de antenas de TV. Sería bueno saber a qué tipo de dispositivo se refieren que eventualmente contaría con este tipo de componente.		Se precisa que los dispositivos que podrían utilizar este componente son los equipos de punto final.	
25	20517793630	CLADIRECT PERU S.A.C.	Consulta	General	2	2.5	18	En cuanto a la variación de la cantidad de suscripciones para el 2do y 3er año, es importante conocer si hay un % de incremento establecido. Dice: Suscripciones ¿ Segunda anualidad: -33.33% aproximado del monto del Servicio de Suscripción de un Sistema de Control y Seguridad de Puntos Finales para equipos de la red de SUNAT por cada anualidad (el porcentaje del monto dependerá de la cantidad de suscripciones que se solicite su activación). Pago sobre el número de suscripciones indicada por la OSI (Numeral 5.1).  Suscripciones Tercera anualidad: -33.34% aproximado del monto del Servicio de Suscripción de un Sistema de Control y Seguridad de Puntos Finales para equipos de la red de SUNAT por cada anualidad (el porcentaje del monto dependerá de la cantidad de suscripciones que se solicite su activación). Pago sobre el número de suscripciones indicada por la OSI (Numeral 5.1). CONSULTA: ¿cuál sería el mecanismo para determinar esas cantidades, de manera que ustedes puedan definir una estrategia de compra con el fabricante?		El mecanismo para determinar las cantidades de las suscripciones está señalado en el numeral 5.3.2.1: "Para la SEGUNDA y TERCERA ANUALIDAD, la OSI emitirá un informe de conformidad por la cantidad de suscripciones que se utilizan en cada una de las anualidades que correspondan"	
26	20535653284	SSG PERU S.A.C.	Consulta	Específico	3.2	A	47	3.2. REQUISITOS DE CALIFICACIÓN A. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a S/ 10,000,000.00 (diez millones y 00/100 soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (08) 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.  Agradeceremos confirmar a la SUNAT que se pondrán considerar como similares a los siguientes:  Licencias de mantenimiento de software antivirus. Licencias de software Cloud Access Security Broker (CASB).		Tomar en consideracion lo respondido en la consulta 09. No se aceptará la licencias de software Cloud Access Security Broker (CASB) porque corresponde a un servicio diferente.	
27	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	5.1	.	21	DICE: Sistemas Operativos por soportar: Para estaciones de trabajo: Windows 8.1, Windows 10, Windows 11.  CONSULTA: Se solicita a la entidad poder indicar la cantidad exacta de los dispositivos finales Windows (workstation) a proteger.		Esta informacion detallada sera entregada al contratista.	
28	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	5.1	.	21	DICE: Sistemas Operativos por soportar: MacOS Big Sur 11.x. Catalina 10.15.x.  CONSULTA: Se solicita a la entidad poder indicar la cantidad exacta de los dispositivos finales MacOS a proteger.		Esta informacion detallada sera entregada al contratista.	

Nro. Orden	RUC/Código	Nombre o Razón Social	Tipo Formulación	Sección	Numeral	Literal	Página	Consulta u Observación	Artículo y norma que se vulnera (en el caso de observaciones)	Análisis respecto de la consulta u observación	Precisión de aquello que se incorporará en las Bases a integrarse, de corresponder
29	20601317461	SECURESOF T CORPORATION S.A.C	Consulta	Específico	5.1	.	21	DICE: Sistemas Operativos por soportar: Para servidores: Windows Server 2008, Windows Server 2012, Windows Server 2016 o superior  CONSULTA: Se solicita a la entidad poder indicar la cantidad exacta de los servidores Windows a proteger.		Esta información detallada será entregada al contratista.	
30	20601317461	SECURESOF T CORPORATION S.A.C	Consulta	Específico	8	.	37	DICE: Se requiere poder efectuar las funciones de control, monitoreo y administración como mínimo de los siguientes dispositivos: ¿Almacenamiento de memoria USB ¿Secure Digital (SD) ¿Mouse, Teclado, Impresoras ¿Unidades de CD/DVD/Blu-ray ¿Cámaras web ¿Discos externos ¿Conexión vía Bluetooth ¿Conexión vía Wireless ¿Conexión de celulares ¿Reproductores de audio ¿Dispositivos plug and play ¿Wireless USB ¿Antenas de TV ¿Lector de tarjetas electrónicas  CONSULTA: Los dispositivos listados: ¿ Secure Digital (SD) ¿ Mouse, Teclado ¿ Cámaras web ¿ Reproductores de audio ¿ Antenas de TV ¿ Lector de tarjetas electrónicas  no representan un riesgo significativo para la seguridad y productividad. Por lo que se le solicita a la entidad, excluirlos o colocarlos como opcional como parte del control de dispositivos para mejorar la experiencia del usuario.		La SUNAT requiere controlar los dispositivos mencionados para salvaguardar la seguridad, por lo cual se mantiene lo señalado en el ítem 08 del Anexo 01.	
31	20601317461	SECURESOF T CORPORATION S.A.C	Consulta	Específico	16	.	38	DICE: Deberá permitir cifrar los archivos que adjuntan a correos externos institucionales o correos privados que se realicen desde equipos administrados, según el perfil definido para el usuario.  CONSULTA: Usualmente, la necesidad de colaboración externa puede requerir el envío de archivos no cifrados. Por lo tanto, se solicita a la entidad considerar este punto como opcional ya que facilita la comunicación y colaboración con socios externos, proveedores y otros contactos.		La SUNAT requiere cifrar los archivos adjuntos en correos externos para salvaguardar la seguridad, por lo cual se mantiene lo señalado en el ítem 16 del Anexo 01.	
32	20601317461	SECURESOF T CORPORATION S.A.C	Consulta	Específico	22	.	38	DICE: Deberá proporcionar un procedimiento que permita descifrar archivos desde la consola centralizada de una carpeta o de los equipos institucionales que tengan archivos encriptados.  CONSULTA: La implementación de cifrado a nivel de archivos o carpetas puede ofrecer mayor granularidad en términos de qué archivos se cifran, pero también puede introducir una mayor complejidad en la gestión de claves y un mayor impacto en el rendimiento del sistema. Por lo tanto, se solicita a la entidad confirmar la aceptación de implementación de cifrado a nivel de disco duro ya que proporciona una capa de seguridad robusta y completa para toda la información almacenada en el disco, sin requerir acciones manuales por parte de los usuarios y ofreciendo una mayor eficiencia en el proceso de cifrado.		Se mantiene lo requerido respecto al procedimiento para descifrar archivos por tratarse de un requerimiento funcional de SUNAT.	
33	20601317461	SECURESOF T CORPORATION S.A.C	Consulta	Específico	24	.	39	DICE: Prevención de explotación: Debe disponer, como mínimo, de dos modos de protección (Estándar / Máximo).  CONSULTA: La obligación de contar con dos modos de protección (Estándar / Máximo) puede generar complejidad innecesaria y aumentar la carga administrativa. La efectividad de la prevención de explotación no debería depender exclusivamente de la configuración de modo, sino garantizar una protección óptima en cualquier configuración.  Por lo tanto, se solicita a la entidad que considere opcional los modos de operación para la prevención de explotación.		Se mantiene lo requerido respecto a los modos de protección porque la SUNAT requiere de ambos modos de protección con el fin de garantizar la seguridad de los dispositivos.	

Nro. Orden	RUC/Código	Nombre o Razón Social	Tipo Formulación	Sección	Numeral	Literal	Página	Consulta u Observación	Artículo y norma que se vulnera (en el caso de observaciones)	Análisis respecto de la consulta u observación	Precisión de aquello que se incorporará en las Bases a integrarse, de corresponder
34	20601317461	SECURESOF T CORPORATION S.A.C	Observación	Específico	24	.	39	<p>DICE: Prevención de explotación:</p> <p>Debe ser posible activar / desactivar la protección contra el escalamiento de privilegios genéricos.</p> <p>Debe ser posible habilitar / deshabilitar la prevención de ejecución de datos de Windows.</p> <p>CONSULTA: Las terminologías usadas y características listadas en este apartado hacen referencias a la documentación de un vendor en particular (Trellix). Se puede evidenciar en el siguiente enlace:  <a href="https://docs.trellix.com/bundle/endpoint-security-10.7.x-common-client-interface-reference-guide-windows/page/GUID-3D9AB771-0415-45C5-B62A-1EC74738BAB8.html">https://docs.trellix.com/bundle/endpoint-security-10.7.x-common-client-interface-reference-guide-windows/page/GUID-3D9AB771-0415-45C5-B62A-1EC74738BAB8.html</a></p> <p>Por lo tanto, basándonos en los Principios del régimen de la contratación pública:</p> <ul style="list-style-type: none"> <li>¿ Principio de Libre Concurrencia y Competencia.</li> <li>¿ Principio de Imparcialidad.</li> <li>¿ Principio de Razonabilidad.</li> <li>¿ Principio de Transparencia.</li> <li>¿ Principio de Vigencia Tecnológica.</li> <li>¿ Principio de Trato Justo e Igualitario.</li> <li>¿ Principio de Equidad.</li> </ul> <p>Se solicita a la entidad el uso de terminologías y características generales con el objetivo de permitir la participación de otras marcas y que cumplan de diferentes formas lo solicitado. o en tal caso considerar este punto como opcional.</p>	Artículo 2 de la Ley de Contrataciones del Estado	No se acoge la observación. El requerimiento funcional no alude a marca o fabricante específico por tanto se mantiene el texto señalado en el Anexo 01.	
35	20601317461	SECURESOF T CORPORATION S.A.C	Observación	Específico	26	.	40	<p>DICE: Escaneo de acceso:</p> <ul style="list-style-type: none"> <li>¿ El administrador de la solución debe especificar el tiempo máximo de análisis para un único archivo.</li> <li>¿ Debe permitir al administrador analizar instaladores de confianza.</li> <li>¿ Debe permitir la configuración del nivel de agresividad del análisis en diferentes niveles.</li> <li>¿ Debe permitir aplicar la configuración a todos los procesos del sistema operativo o a una lista específica creada por el administrador.</li> <li>¿ Debe permitir en análisis cuando se produce lecturas y/o escrituras en disco y/o permitiendo que la solución misma tome la decisión de la técnica más adecuada.</li> </ul> <p>CONSULTA: Las características listadas:</p> <p>Han sido tomadas de un vendor en específico desde el siguiente enlace: <a href="https://docs.trellix.com/bundle/endpoint-security-10.7.x-common-client-interface-reference-guide-windows/page/GUID-E9B7F5D0-D67D-4F23-BC48-E75FAC86FC31.html">https://docs.trellix.com/bundle/endpoint-security-10.7.x-common-client-interface-reference-guide-windows/page/GUID-E9B7F5D0-D67D-4F23-BC48-E75FAC86FC31.html</a></p> <p>Por lo tanto, basándonos en los Principios del régimen de la contratación pública:</p> <ul style="list-style-type: none"> <li>¿ Principio de Libre Concurrencia y Competencia.</li> <li>¿ Principio de Imparcialidad.</li> <li>¿ Principio de Razonabilidad.</li> <li>¿ Principio de Transparencia.</li> <li>¿ Principio de Vigencia Tecnológica.</li> <li>¿ Principio de Trato Justo e Igualitario.</li> <li>¿ Principio de Equidad.</li> </ul> <p>Se solicita a la entidad el uso de terminologías y características generales con el objetivo de permitir la participación de otras marcas y que cumplan de diferentes formas lo solicitado y no orientarlo a una sola marca en particular. o en tal caso considerar estos puntos como opcionales.</p>	Artículo 2 de la Ley de Contrataciones del Estado	No se acoge la observación. El requerimiento funcional no alude a marca o fabricante específico por tanto se mantiene el texto señalado en el Anexo 01.	
36	20601317461	SECURESOF T CORPORATION S.A.C	Consulta	Específico	27	.	40	<p>DICE: Para minimizar el impacto en el usuario, la solución debe permitir:</p> <p>El uso de la memoria caché, es decir, los archivos que ya han sido analizados y no han cambiado su</p> <p>CONSULTA: Se pide a la entidad confirmar que se aceptarán otras formas similares que cumplan con el objetivo de minimizar el impacto en el usuario, como escanear únicamente archivos nuevos o modificados. Esto permitirá optimizar la utilización de recursos del endpoint.</p>		Se mantiene lo requerido porque este punto se refiere a requerimientos que aplican al análisis bajo demanda.	

Nro. Orden	RUC/Código	Nombre o Razón Social	Tipo Formulación	Sección	Numeral	Literal	Página	Consulta u Observación	Artículo y norma que se vulnera (en el caso de observaciones)	Análisis respecto de la consulta u observación	Precisión de aquello que se incorporará en las Bases a integrarse, de corresponder
37	20601317461	SECURESOF T CORPORATION S.A.C	Consulta	Específico	27	.	40	DICE: Para minimizar el impacto en el usuario, la solución debe permitir:  Comience a escanear solo cuando el sistema esté inactivo.  CONSULTA: Dado que la solución a ofertar se basa en una tecnología de escaneo en tiempo real, programado, manual y en la nube y que no requiere inactividad del sistema para funcionar eficazmente. Esta tecnología permite la detección proactiva de amenazas sin afectar el rendimiento del sistema o las actividades del usuario. Por lo tanto, exigir que el escaneo solo se realice en momentos de inactividad podría limitar la eficacia de esta tecnología avanzada. Por lo que se solicita retirar este punto o colocarlo como opcional.		Se mantiene lo requerido porque este punto se refiere a requerimientos que aplican al análisis bajo demanda.	
38	20601317461	SECURESOF T CORPORATION S.A.C	Consulta	Específico	27	.	40	DICE: Para minimizar el impacto en el usuario, la solución debe permitir: Limitar el porcentaje de CPU, memoria a ser utilizado por la tarea de análisis  CONSULTA: En un entorno de seguridad informática, la CPU suele ser el recurso más crítico para el rendimiento general del sistema. Limitar el uso de CPU asegura que las operaciones del sistema y las aplicaciones críticas no se vean afectadas negativamente por la tarea de análisis de la solución de seguridad. Por lo tanto, esta característica debería tener una prioridad más alta en la evaluación de las soluciones de seguridad. Por lo tanto, se solicita a la entidad aceptar la limitación al menos a nivel de CPU.		Se mantiene lo requerido porque este punto se refiere a requerimientos que aplican al análisis bajo demanda.	
39	20601317461	SECURESOF T CORPORATION S.A.C	Consulta	Específico	28	.	40	DICE: Protección de red: Debe permitir el tráfico saliente solo después de iniciar los servicios de Firewall.  CONSULTA: La capacidad de bloquear tráfico saliente es esencial para prevenir la comunicación no autorizada con servidores maliciosos o para evitar la propagación de amenazas. Sin embargo, esto no debería requerir la espera de que el servicio de Firewall se inicie, ya que podría afectar en la productividad e impactar negativamente la eficiencia del negocio. Por lo tanto, se solicita a la entidad confirmar que este punto sea considerado como opcional.		Se mantienen lo requerido respecto a "Protección de red" porque la SUNAT requiere garantizar la seguridad de los dispositivos.	
40	20601317461	SECURESOF T CORPORATION S.A.C	Consulta	Específico	28	.	40	DICE: Protección de red: Deber ser posible bloquear el tráfico bridge.  CONSULTA: La capacidad de bloquear el tráfico bridge puede ser esencial en entornos específicos de red, pero no es una necesidad universal. Nuestra solución a proponer se adapta a diversos entornos y puede proporcionar seguridad efectiva sin la necesidad de esta capacidad específica. Por lo tanto, se solicita a la entidad considerar este punto como opcional.		Se mantienen lo requerido respecto a "Protección de red" porque la SUNAT requiere garantizar la seguridad de los dispositivos.	
41	20601317461	SECURESOF T CORPORATION S.A.C	Observación	Específico	28	.	41	DICE: Protección de red El módulo debe permitir la creación de reglas de manera adaptativa, es decir, en una estación modelo definida por el administrador, debe poder crear las reglas automáticamente.  CONSULTA: Si bien la capacidad de crear reglas adaptativas puede ser valiosa en ciertos contextos, puede no ser una prioridad en un entorno donde la prevención proactiva de amenazas es la principal estrategia de seguridad. Por otro lado, esta es característica es propiamente de Trellix: Apartado "Enable Adaptive mode" <a href="https://docs.trellix.com/bundle/endpoint-security-10.7.x-common-client-interface-reference-guide-windows/page/GUID-4C618EF0-B4F7-45E7-8ACF-DA8C6B155BD7.html">https://docs.trellix.com/bundle/endpoint-security-10.7.x-common-client-interface-reference-guide-windows/page/GUID-4C618EF0-B4F7-45E7-8ACF-DA8C6B155BD7.html</a>  Por lo tanto, para respetar la pluralidad de participación y garantizar la transparencia en el concurso de licitación se solicita a la entidad confirmar que este punto será considerado como opcional.	Artículo 2 de la Ley de Contrataciones del Estado	Se acoge la observación. Se considerará como opcional: "El módulo debe permitir la creación de reglas de manera adaptativa, es decir, en una estación modelo definida por el administrador, debe poder crear las reglas automáticamente".	La siguiente funcionalidad indicada en el ítem 28 del Anexo 01 podrá considerarse opcional: • El módulo debe permitir la creación de reglas de manera adaptativa, es decir, en una estación modelo definida por el administrador, debe poder crear las reglas automáticamente
42	20601317461	SECURESOF T CORPORATION S.A.C	Observación	Específico	28	.	41	DICE: Protección de red Debe ser posible bloquear el tráfico de protocolos no compatibles.  CONSULTA: Bloquear el tráfico de protocolos no compatibles es una medida esencial para prevenir amenazas desconocidas o malware que podrían explotar vulnerabilidades en protocolos no autorizados. Sin embargo, esta funcionalidad y concepto es propiamente de Trellix ( <a href="https://docs.trellix.com/bundle/endpoint-security-10.7.x-common-client-interface-reference-guide-windows/page/GUID-4C618EF0-B4F7-45E7-8ACF-DA8C6B155BD7.html">https://docs.trellix.com/bundle/endpoint-security-10.7.x-common-client-interface-reference-guide-windows/page/GUID-4C618EF0-B4F7-45E7-8ACF-DA8C6B155BD7.html</a> ), en el apartado "Allow traffic for unsupported protocols".  Para respetar la pluralidad de participación y garantizar la transparencia en el concurso de licitación, es fundamental que se evalúen y consideren las soluciones de diferentes proveedores, por lo cual se solicita que es punto sea considerado como opcional.	Artículo 2 de la Ley de Contrataciones del Estado	Se acoge la observación. Se considerará como opcional: "Debe ser posible bloquear el tráfico de protocolos no compatibles".	La siguiente funcionalidad indicada en el ítem 28 del Anexo 01 podrá considerarse opcional: • Debe ser posible bloquear el tráfico de protocolos no compatibles.

Nro. Orden	RUC/Código	Nombre o Razón Social	Tipo Formulación	Sección	Numeral	Literal	Página	Consulta u Observación	Artículo y norma que se vulnera (en el caso de observaciones)	Análisis respecto de la consulta u observación	Precisión de aquello que se incorporará en las Bases a integrarse, de corresponder
43	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	29	.	41	DICE: Protección web:  Debe poder usar la lista de categorías para bloquear sitios relacionados con contenido no autorizado.  CONSULTA: Soportar listas de categorizaciones de paginas web está más orientado a soluciones de Web Proxy, Firewalls, entre otros. Por lo tanto, se le pide a la entidad confirmar que la solución a ofertar deba soportar como mínimo el bloqueo a paginas maliciosas, altamente sospechosas para proteger a los usuarios de la organización.		Se mantiene lo requerido respecto a la "Protección web" porque la SUNAT requiere de esta funcionalidad con el fin de garantizar la seguridad de los dispositivos.	
44	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	29	.	41	DICE: Protección web: Debe permitir la personalización de los mensajes presentados al usuario.  CONSULTA: La personalización de mensajes es una característica útil, pero puede no ser una prioridad en un entorno donde la prevención proactiva de amenazas a nivel web es principal. Por tal motivo, se solicita a la entidad que este punto sea considerado como opcional.		Se mantiene lo requerido respecto a la "Protección web" porque la SUNAT requiere de esta funcionalidad con el fin de garantizar la seguridad de los dispositivos.	
45	20601317461	SECURESOFT CORPORATION S.A.C	Observación	Específico	30	.	41	DICE: Protección adaptativa de amenazas: ¿El módulo de inteligencia de amenazas debe contener los siguientes mecanismos: oContención dinámica de aplicaciones: La solución debe permitir la contención dinámica de aplicaciones y archivos ejecutables con características maliciosas (Ejemplo: ransomware) Debe permitirle indicar aplicaciones confiables para que no caigan en el filtro de contención dinámica La solución debe mantener una caché de reputación local con información de la aplicación ¿conocida, desconocida y maliciosa. Debe ser posible ordenar cada aplicación manualmente e incluso su reclasificación a través de la consola de administración central. Entre los comportamientos maliciosos, debe ser capaz de: Bloquear el acceso local desde las cookies Creación de archivos en cualquier lugar de la red Bloquear la desactivación de ejecutables críticos del sistema operativo Leer/eliminar/escribir archivos dirigidos por ransomware Bloqueo de modificación de carpetas de tareas de Windows Bloqueo de modificación de archivos críticos de Windows y ubicaciones del registro Modificación de bloqueo de archivos ejecutables portátiles Bloqueo de modificación de bits de atributo oculto Bloqueo de modificación de bits de atributo de solo lectura Bloqueo de cambio de ubicación del registro de lanzamiento Bloqueo de modificación de carpetas de datos de usuario Bloqueo de la suspensión de un proceso Bloqueo de terminación de otro proceso A partir de los comportamientos observados, debe ser posible bloquear o sólo informar si ocurre. Debe ser capaz de informar al usuario de las amenazas encontradas a través de mensajes personalizados Modo de activación de bloqueo dinámico para cualquier archivo desconocido al que acceda el sistema operativo y nunca visto por la solución Debe ser posible asignar la regla de acuerdo con una política equilibrada, con el objetivo de una mayor seguridad o productividad del usuario La protección debe estar contenida en el mismo agente de protección, sin requerir otro software o aplicación adicional en la estación de trabajo para la ejecución y activación de la protección oAnálisis Avanzado Debe permitir que el motor funcione sólo en modo de observación Debe permitir el análisis de los procesos iniciados en unidades asignadas a la red Debe ser capaz de trabajar con técnicas de análisis matemático para identificar amenazas sin necesidad de firmas. Al seleccionar el análisis sólo en el cliente, debe ser posible indicar la sensibilidad del motor de análisis. Debe permitir la selección del mejor modo de operación de la solución en base a recomendaciones del fabricante de ambientes de trabajo Debe activar el módulo de contención dinámica automáticamente si una amenaza alcanza un cierto nivel de criticidad que debe indicar el administrador de la solución oReputación local de amenazas El módulo de reputación local debe mantener una base de datos con todos los ejecutables detectados en el entorno. Para cada ejecutable, las reputaciones deben mostrarse utilizando diferentes técnicas, tanto como parte de técnicas del mismo fabricante como en interacción con terceros Debe permitirle rastrear la ejecución del archivo malicioso a través del entorno indicando cuál fue su primera ejecución y su última. Debe permitir la identificación de la estación de trabajo y el usuario asociado con el mismo.  CONSULTA: Las terminologías usadas en este apartado, son usadas específicamente por un solo vendor (Trellix), y las características mencionadas han sido obtenidas desde la documentación pública de Trellix: "Adaptive Threat Protection" - <a href="https://docs.trellix.com/bundle/endpoint-security-10.7.x-common-client-interface-reference-guide-windows/page/GUID-BE50D5B7-B73F-4D75-971F-22E2E8E9A2B9.html">https://docs.trellix.com/bundle/endpoint-security-10.7.x-common-client-interface-reference-guide-windows/page/GUID-BE50D5B7-B73F-4D75-971F-22E2E8E9A2B9.html</a>	Artículo 2 de la Ley de Contrataciones del Estado	No se acoge, toda vez que el requerimiento funcional no alude a marca o fabricante específico por tanto se mantiene el texto señalado en el Anexo 01.	
46	20601317461	SECURESOFT CORPORATION S.A.C	Observación	Específico	16	.	43	DICE: Para amenazas donde se hayan generado reglas de detección, debe ser posible exportarlas como reglas expertas, reglas sigma, reglas Yara y reglas de Snort  CONSULTA: Este conjunto de reglas son soportadas unicamente por Trellix como parte de "Hunting rules associated with a campaign" en el siguiente enlace: <a href="https://docs.trellix.com/es-ES/bundle/trellix-insights-product-guide/page/GUID-3ECA3929-DAE2-4422-A43D-449D7A97BAAD.html">https://docs.trellix.com/es-ES/bundle/trellix-insights-product-guide/page/GUID-3ECA3929-DAE2-4422-A43D-449D7A97BAAD.html</a>  Por lo tanto, basándonos en los Principios del régimen de la contratación pública: ¿ Principio de Libre Concurrencia y Competencia. ¿ Principio de Imparcialidad. ¿ Principio de Razonabilidad. ¿ Principio de Transparencia. ¿ Principio de Vigencia Tecnológica. ¿ Principio de Trato Justo e Igualitario. ¿ Principio de Equidad.  Se solicita a la entidad aceptar otras formas y/o procedimientos en la cual se pueda cumplir con el objetivo, tales como el uso de IoC, integraciones con soluciones de seguridad de terceros, o considerar este punto como opcional.	Artículo 2 de la Ley de Contrataciones del Estado	Se acoge la observacion, otras formas tales como el uso de IoC, integraciones con soluciones de seguridad de terceros.	La funcionalidad "Para amenazas donde se hayan generado reglas de detección, debe ser posible exportarlas como reglas expertas, reglas sigma, reglas Yara y reglas de Snort." soportará también otras formas y/o procedimientos tales como el uso de IoC o integraciones con soluciones de seguridad de terceros .

Nro. Orden	RUC/Código	Nombre o Razón Social	Tipo Formulación	Sección	Numeral	Literal	Página	Consulta u Observación	Artículo y norma que se vulnera (en el caso de observaciones)	Análisis respecto de la consulta u observación	Precisión de aquello que se incorporará en las Bases a integrarse, de corresponder
47	20601317461	SECURESOF T CORPORATION S.A.C	Consulta	Específico	2	.	44	DICE: La solución debe permitir ser implementada tanto on-premise como SaaS (Software as a Service), permitiendo elegir cual modalidad se desea utilizar (incluso ambas al mismo tiempo) y sin incurrir en costos adicionales para la SUNAT.  CONSULTA: Optar por una plataforma de gestión centralizada basada en la nube ofrece una serie de ventajas en términos de acceso remoto, escalabilidad, costos, automatización y resiliencia. Estos factores pueden ser críticos para las organizaciones que buscan una gestión de seguridad de endpoints eficiente y flexible.  Por lo contrario, una plataforma de gestión centralizada local ofrece ciertos niveles de control y personalización, pero también conlleva desafíos y responsabilidades adicionales en términos de costos, complejidad, mantenimiento y escalabilidad.  Por lo tanto, se solicita a la entidad confirmar que la gestión de la solución sea brindada 100% en nube el cual permita obtener los beneficios de un servicio SaaS.		Se mantiene lo requerido respecto a la "Consola de Administración Centralizada" porque la SUNAT requiere de estos modos de implementación con el fin de garantizar la gestión de los dispositivos.	
48	20601317461	SECURESOF T CORPORATION S.A.C	Consulta	Específico	5.2.1.3	.	23	DICE: Entrenamiento en la instalación, operación y administración de la solución tecnológica  CONSULTA: Se pide a la entidad especificar la cantidad mínima de participantes y el tiempo de duración del entrenamiento solicitado.		Se precisa dicha información en el ítem 5.2.1.3: El entrenamiento se dará como mínimo para 15 personas. El tiempo mínimo es de 32 horas lectivas.	
49	20601317461	SECURESOF T CORPORATION S.A.C	Consulta	Específico	5.2.2.2	.	26	DICE: Los incidentes de virus o software malicioso detectado en la red interna serán tratados de acuerdo con la siguiente clasificación:  Crítico: aplica para los incidentes que comprometen la operatividad de los servicios de red proporcionados a los usuarios, y tendrán un tiempo máximo de reparación de cuatro (04) horas contadas a partir de que SUNAT reporte el incidente. Grave: aplica para los incidentes que estén comprometiendo parcialmente la operatividad de los usuarios, y tendrán un tiempo máximo de reparación de veinticuatro (24) horas contadas a partir de que SUNAT reporte el incidente.  CONSULTA: Sirvase confirmar que en caso la solución de un incidente demande la atención del fabricante (a través de la apertura de un ticket de soporte) o se espere la respuesta de un tercero o de la misma entidad el tiempo de solución podrá variar siempre y cuando el postor lo sustente de forma correcta, mientras esto no afecte la continuidad del servicio en caso de avería total.		De presentarse la situación indicada ésta será evaluada oportunamente por la entidad.	
50	20601317461	SECURESOF T CORPORATION S.A.C	Consulta	Específico	5.2.1.2	.	23	DICE: El Contratista realizará la instalación, configuración y puesta en funcionamiento de la solución en todos los equipos a nivel nacional.  CONSULTA: Se pide a la entidad confirmar que todos los equipos que se encuentran a nivel nacional estarán conectados de manera local o vía vpn a la red de la entidad para que los agentes puedan ser desplegados de forma remota.		Se confirma que los equipos estarán disponible en las redes internas o vía VPN para el despliegue de los agentes.	
51	20601317461	SECURESOF T CORPORATION S.A.C	Consulta	Específico	5.2.1.2	.	23	DICE: El Contratista realizará la instalación, configuración y puesta en funcionamiento de la solución en todos los equipos a nivel nacional.  CONSULTA: En caso no se pueda desplegar de manera remota algún agente, se pide a la entidad confirmar que se encargará de la instalación manual en estos equipos		El contratista es responsable de la instalación de todos los componentes, pudiendo coordinar en todo momento con personal técnico de la institución.	
52	20601317461	SECURESOF T CORPORATION S.A.C	Consulta	Específico	5.3.2.1	.	27	DICE: Instalación y configuración de las suscripciones A partir del día siguiente de emitida la conformidad de las suscripciones Hasta el plazo máximo de ochenta y cinco (85) días calendario  CONSULTA: Se pide a la entidad confirmar que el despliegue de los agentes no se encuentra contemplado dentro del plazo de instalación de la solución y esto se podrá realizar durante todo el servicio.		El despliegue de los agentes, y de cualquier otro software necesario, a nivel nacional, está considerado dentro del plazo de instalación y configuración de las suscripciones.	
53	20601317461	SECURESOF T CORPORATION S.A.C	Consulta	Específico	5.2.1.2	.	27	DICE: El Contratista realizará la instalación, configuración y puesta en funcionamiento de la solución en todos los equipos a nivel nacional.  CONSULTA: Para acelerar los tiempos de despliegue de los agentes, se pide a la entidad confirmar que podrá trabajar en conjunto en el correcto despliegue de los agentes mediante el manual de instalación que se brindará.		El contratista es responsable de la instalación de todos los componentes, pudiendo coordinar en todo momento con personal técnico de la institución.	
54	20601317461	SECURESOF T CORPORATION S.A.C	Consulta	Específico	5.2.1.2	.	23	DICE: El Contratista realizará la instalación, configuración y puesta en funcionamiento de la solución en todos los equipos a nivel nacional.  CONSULTA : Se pide a la entidad especificar las ubicaciones geográficas de los equipos donde se desplegarán los agentes y la cantidad estimada de agentes a desplegar por ubicación.		Esta información detallada será entregada al contratista.	

Nro. Orden	RUC/Código	Nombre o Razón Social	Tipo Formulación	Sección	Numeral	Literal	Página	Consulta u Observación	Artículo y norma que se vulnera (en el caso de observaciones)	Análisis respecto de la consulta u observación	Precisión de aquello que se incorporará en las Bases a integrarse, de corresponder
55	20601317461	SECURESOFT CORPORATION S.A.C	Observación	Específico	6.2.1	.	29	DICE: Otro Personal (a) Un (01) Jefe del Proyecto ii. Perfil: Bachiller o Título Profesional en Ingeniería de Sistemas o Industrial o Informática o Software o Computación o Telecomunicaciones o Electrónica.  CONSULTA: A fin de permitir mayor apertura de postores por libre competencia, se solicita a la entidad se sirva confirmar que también se aceptará como similar la carrera de: Ingeniero Informático y de Sistemas.	Artículo 2 de la Ley de Contrataciones del Estado	Se acoge la observación.	Para el personal "Jefe del Proyecto", bajo el perfil requerido, considerar adicionalmente Bachiller o Título Profesional en Ingeniería Informática y de Sistemas.
56	20601317461	SECURESOFT CORPORATION S.A.C	Observación	Específico	6.2.1	.	29	DICE: Otro Personal (b) Cinco (05) Especialistas de los softwares de protección ii. Perfil: Bachiller o Título Profesional en Ingeniería de Sistemas o Industrial o Informática o Software o Computación o Telecomunicaciones o Electrónica.  CONSULTA: A fin de permitir mayor apertura de postores por libre competencia, se solicita a la entidad se sirva confirmar que también se aceptará como similares las carreras de: Ingeniero Informático y de Sistemas o Ingeniería Electrónica y Telecomunicaciones o Ingeniero de Seguridad y Auditoría Informática.	Artículo 2 de la Ley de Contrataciones del Estado	Se acoge la observación.	Para el personal "Especialistas de los softwares de protección", bajo el perfil requerido, considerar adicionalmente Bachiller o Título Profesional en Ingeniería Informática y de Sistemas o Electrónica y Telecomunicaciones o Seguridad y Auditoría Informática.
57	20601317461	SECURESOFT CORPORATION S.A.C	Observación	Específico	6.2.1	.	29	DICE: Otro Personal (b) Cinco (05) Especialistas de los softwares de protección iii. Experiencia: Tres (03) años de experiencia mínima en la instalación y/o configuración y/o soporte técnico de soluciones corporativas de software de protección de puntos finales y/o servidores.  CONSULTA: A fin de permitir mayor pluralidad de postores por libre competencia, se solicita a la entidad se sirva confirmar que se aceptará como mínimo dos (02) años de experiencia para los Especialistas de los softwares de protección.	Artículo 2 de la Ley de Contrataciones del Estado	No se acoge. Se mantiene los requisitos indicados en el numeral 6.2.1. dado que la institución requiere profesionales con la experiencia mencionada.	
58	20601317461	SECURESOFT CORPORATION S.A.C	Observación	Específico	6.2.1	.	30	DICE: (d) Un (01) Ingeniero residente ii. Perfil: Bachiller o Título Profesional en Ingeniería de Sistemas o Industrial o Informática o Software o Computación o Telecomunicaciones o Electrónica.  CONSULTA: A fin de permitir mayor apertura de postores por libre competencia, se solicita a la entidad se sirva confirmar que también se aceptará como similares las carreras de: Redes y Comunicaciones o Bachiller en Ciencias con mención en Ingeniería de Telecomunicaciones.	Artículo 2 de la Ley de Contrataciones del Estado	Se acoge la observación.	Para el personal "Ingeniero residente", bajo el perfil requerido, considerar adicionalmente Bachiller o Título Profesional en Ingeniería de Redes y Comunicaciones.
59	20601317461	SECURESOFT CORPORATION S.A.C	Observación	Específico	6.2.2	.	31	DICE: (d) Un (01) Ingeniero residente iii. Experiencia: Dos (02) años de experiencia, como mínimo, en labores de análisis o diseño de soluciones de seguridad informática.  CONSULTA: A fin de permitir mayor pluralidad de postores por libre competencia, se solicita a la entidad se sirva confirmar que se aceptará como mínimo Un (01) año de experiencia para el Ingeniero Residente.	Artículo 2 de la Ley de Contrataciones del Estado	No se acoge. Se mantiene los requisitos indicados en el numeral 6.2.1. dado que la institución requiere profesionales con la experiencia mencionada.	

Nro. Orden	RUC/Código	Nombre o Razón Social	Tipo Formulación	Sección	Numeral	Literal	Página	Consulta u Observación	Artículo y norma que se vulnera (en el caso de observaciones)	Análisis respecto de la consulta u observación	Precisión de aquello que se incorporará en las Bases a integrarse, de corresponder
60	20601317461	SECURESOFT CORPORATION S.A.C	Observación	Específico	3.2	A	47	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD Se considerarán servicios similares a los siguientes Servicios o Suscripciones de un Sistema de control y seguridad de puntos finales Servicios o suscripciones de software antivirus Servicios o suscripciones de software de cifrado Servicios o suscripciones de software de control de dispositivos o DLP Servicios o suscripciones de software de tipo detección y respuesta OBSERVACION: A fin de permitir mayor pluralidad de postores por libre competencia, se solicita a la entidad se sirva confirmar que también se aceptará como similares los siguientes servicios: - SERVICIO DE LICENCIAMIENTO PARA EL SISTEMA DE SEGURIDAD INFORMÁTICA ANTIMALWARE - ADQUISICIÓN DE SISTEMAS DE SEGURIDAD ANTI- MALWARE - IMPLEMENTACIÓN ANTIMALWARE CORTEX XDR - TRAPS ADVANCED ENDPOINT PROTECTION FOR AGENTS, INCLUDES PREMIUM SUPPORT - SERVICIO DE SEGURIDAD PARA PROTECCION ANTIMALWARE PARA ENDPOINTS - SOLUCION ANTIMALWARE PARA ENDPOINT,INSTALACION Y CONFIGURACION DE SOLUCION Y CAPACITACIÓN - ADQUISICION DE SISTEMAS DE SEGURIDAD ANTI- MALWARE - LICENCIAS ENDPOINT - COMPRA DE PLATAFORMA O SUSCRIPCION DE LICENCIAS PARA GOD - APLICACIONES TI-SERVICIOS OPERATIVOS ANTIMALWARE DE HOST TRAPS - SUSCRIPCIÓN WEB DLP - SERVICIO DE IMPLEMENTACIÓN Y CONFIGURACIÓN, RENOVACIÓN TECNOLÓGICA ANTIVIRUS - RENOVACIÓN DE LICENCIAS TRENDMICRO - LICENCIAS ANTIVIRUS - LICENCIAS ANTIVIRUS Y ANTIMALWARE ENDPOINTS RENOVACIÓN - RENOV.LIC.EDR TRENDMICRO - SERVICIO DE SOPORTE,ADMINISTRACIÓN Y MONITOREO TRENDMICRO - PROTECCIÓN DEL ENDPOINT - SERVICIO, REVISIÓN CASO DE USO RELACIONADOS A TRAPS EN SIEM GRADAR - DBF ASSESSMENT TECNOLÓGICO, PAN XDR PRVT CORTEX XDR PREVENT - SERVICIOS SOPORTE, FORCEPOINT WEB DLP MODULE - RENOVACIÓN DE LAS LICENCIAS DLP FORCEPOINT TRITON AP WEB, RENOVACIÓN DE LAS LICENCIAS PREMIUM SUPPORT - CORTEX XDR PRO FOR 1 ENDPOINT - CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE LICENCIAS Y SERVICIOS DE SOPORTE TÉCNICO Y ACTUALIZACIÓN DEL SOFTWARE DE SEGURIDAD CHECK POINT SANDBLAST - SERVICIO DE IMPLEMENTACIÓN, SOLUCIÓN DE MONITOREO DE ACTIVIDAD DE BASES DE DATOS (DAM) - SERVICIO DE SOPORTE DE MANTENIMIENTO RENTING DE EQUIPOS Y SERVICIO DE MONITOREO DE EVENTOS DE SEGURIDAD (SOC) - SERVICIO DE SOPORTE DE MANTENIMIENTO<-MANTENIMIENTO Y SOPORTE DE FIREWALLS CHECKPOINT - SERVICIO DE SOPORTE DE MANTENIMIENTO<-ACCESO SEGURO REMOTO (SSL VPN) - SERVICIO DE SOPORTE DE MANTENIMIENTO<-RSA SERVICIO DE AUTENTICACIÓN - SERVICIO DE SOPORTE DE MANTENIMIENTO<-MANTENIMIENTO Y SOPORTE DE PROXY BLUECOAT - Servicios de Licencias o Servicio de CyberSOC o Administración y Monitoreo de Plataformas de Seguridad y Correlación Inteligente de Eventos de Seguridad - Servicio de soporte de mantenimiento o servicio de monitoreo y administración de plataformas de seguridad TI - Servicio de monitoreo de eventos de seguridad (SOC) - Servicio de CyberSOC	Artículo 2 de la Ley de Contrataciones del Estado	Se acoge parcialmente. Tomar en consideracion lo respondido en la consulta 09. No nos pronunciaremos para cada caso particular de los servicios citados como similares por el postor, toda vez que se hace alusión a marcas específicas. Aquellos servicios similares que no hacen alusión a marcas específicas ya están referenciados en la respuesta a la consulta 09.	
61	20601317461	SECURESOFT CORPORATION S.A.C	Observación	Específico	6.2.1	c	29	DICE: (c)Un (01) Instructor del software de protección i. Actividades: -Realizar el entrenamiento correspondiente a las suscripciones ofertadas, de acuerdo con las especificaciones técnicas. -Debe contar con certificación vigente como instructor en la versión de la suscripción ofertada. Para ello deberá adjuntar certificado o diploma correspondiente.  CONSULTA: A fin de permitir mayor pluralidad de postores por libre competencia, se solicita a la entidad se sirva confirmar que se aceptará que el certificado del instructor no necesariamente indique la palabra instructor o entrenador, dado que no todos los fabricantes emiten ese tipo de certificado, y solo es necesario para poder dar un entrenamiento o capacitación con un certificado técnico de la solución ofertada. Adicionalmente, el entrenamiento solicitado es al Contratista y no se solicita que sea una capacitación o entrenamiento oficial, lo cual desvirtua la necesidad de que el instructor posea un certificado que indique que sea instructor, ya que al dar el entrenamiento no garantizaría que el mismo sea uno oficial ni que las constancias sean emitidas por el fabricante. La práctica indica que un entrenador o instructor certificado como tal, dicte cursos oficiales de los fabricantes en centros autorizados y certificados para ello, lo cual no es el caso.	Artículo 2 de la Ley de Contrataciones del Estado	No se acoge. La entidad requiere que el Instructor este preparado y cuente con la documentación que lo sustente.	

ERIKA MIA  
HINOSTROZA MATOS

JUAN CARLOS  
FLORES ALVAREZ

PIERRE ALBERTO  
DELGADO QUIJANDRIA



Firmado digitalmente por:  
HINOSTROZA MATOS Erika  
Mia FAU 20131312955 soft  
Motivo: En señal de conformidad  
Fecha: 17/11/2023 15:58:28-0500



Firmado digitalmente por:  
FLORES ALVAREZ Juan  
Carlos FAU 20131312955 soft  
Motivo: En señal de conformidad  
Fecha: 17/11/2023 16:06:44-0500



Firmado digitalmente por:  
DELGADO QUIJANDRIA PIERRE  
ALBERTO FIR 46575229 hard  
Motivo: En señal de conformidad  
Fecha: 17/11/2023 16:42:57-0500