ANEXO N° 01

CUADRO DE ADMISIÓN DE OFERTAS

CONCURSO PÚBLICO Nº 004-2024-ANIN

CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE VEINTICUATRO (24) MESES DE PROTECCIÓN AVANZADA ANTIMALWARE PARA 1300 ESTACIONES DE TRABAJO Y SERVIDORES TI DE LA AUTORIDAD NACIONAL DE INFRAESTRUCTURA

LITERAL	DESCRIPCION	POSTORES		
		GRUPO BANTEK S.A.C.	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	INNOVARE E-BUSINESS S.A.C.
a)	**Declaración jurada de datos del postor.** (Anexo N° 1)	CUMPLE (Folio 004)	CUMPLE (Folio 003)	CUMPLE (Folio 005)
b)	**b)Documento que acredite la representación de quien suscribe la oferta**. En caso de persona jurídica, copia del certificado de vigencia de poder del representante legal, apoderado o mandatario designado para tal efecto. En caso de persona natural, copia del documento nacional de identidad o documento análogo, o del certificado de vigencia de poder otorgado por persona natural, del apoderado o mandatario, según corresponda. En el caso de consorcios, este documento debe ser presentado por cada uno de los integrantes del consorcio que suscriba la promesa de consorcio, según corresponda.	CUMPLE (Folio 006)	CUMPLE (Folio 005)	CUMPLE (Folio 006)
c)	**Declaración jurada de acuerdo con el literal b) del artículo 52° del Reglamento** (Anexo N°2)	CUMPLE (Subsanado)	CUMPLE (Folio 012)	CUMPLE (Folio 008)
d)	**Declaración jurada de cumplimiento de los Términos de Referencia contenidos en el numeral 3.1 del Capítulo III de la presente sección.** (Anexo Nº 3) Se deberá acreditar el cumplimiento de las características técnicas indicadas en los numerales 4.2.1, 4.2.2 y 4.3.1 de los términos de referencia, presentando la documentación del fabricante como: brochures y/o catálogos y/o folletos y/U hojas de datos y/o enlaces web y/o whitepapers. Asimismo, esta documentación podrá ser entregada en idioma español y/o inglés. Los documentos que acompañan la oferta se presentan en idioma español. Cuando los documentos no figuren en idioma español, se presenta la respectiva traducción por traductor público juramentado o traductor colegiado certificado, según corresponda, salvo el caso de la información técnica complementaria contenida en folletos, instructivos, catálogos o similares, que puede ser presentada en el idioma original. El postor es responsable de la exactitud y veracidad de dichos documentos.	NO CUMPLE (019)	CUMPLE (Folio 014)	NO CUMPLE (Folio 009)
e)	**Declaración Jurada de plazo de prestación del servicio** (Anexo Nº 4)	CUMPLE (Folio 134)	CUMPLE (Folio 075)	CUMPLE (Folio 131)
f)	**Promesa de consorcio** con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. (Anexo Nº 5)	NO APLICA	NO APLICA	NO APLICA
g)	**El precio de la oferta en SOLES** (Adjuntar obligatoriamente el Anexo Nº 6)	CUMPLE (Folio 138)	CUMPLE (Folio 077)	CUMPLE (Folio 001)
		NO ADMITIDO	**ADMITIDO**	**NO ADMITIDO**

Observaciones:

El portor **GRUPO BANTEK S.A.C., presentó** su Declaración jurada de acuerdo con el literal b) del artículo 52° del Reglamento de forma incompleta, toda vez que omitió el numeral vii) que señala "Comprometerme a mantener la oferta presentada durante el procedimiento de selección y a perfeccionar el contrato, en caso de resultar favorecido con la buena pro"; por ello que, siendo una omisión subsanable en atención al Art. 60° del Reglamento de la Ley de Contrataciones, con fecha 03 de setiembre de 2024 se registró la Carta Nº 001-2024-ANIN/CP-SM-04-2024-ANIN en la plataforma del SEACE, dirigida al postor GRUPO BANTEK S.A.C., a fin de que subsane de su oferta, otorgándole el plazo de un (01) día hábil, siendo debidamente subnsado. Por lo que, de la revisión del documento subsanado por el postor, dentro del plazo estipulado, se verificó que cumplió la subsanación correctamente.

Respecto a la documentación complementaria a la Declaración jurada de cumplimiento de los Términos de Referencia contenidos en el numeral 3.1 del Capítulo III de la presente sección. (Anexo Nº 3), presentada por el portor **GRUPO BANTEK S.A.C.** para la acreditación del cumplimiento de las caracteristicas tecnicas indicadas en los numerales 4.2.1 y 4.2.2, la Oficina de Tenologías de la Información mediante Memorando N° D00000781-2024-ANIN/OTI e Informe Nº D00000219-2024-ANIN/OTI-US-MMC, en calidad de apoyo técnico para la verificación de cumplimiento, señala que el postor **GRUPO BANTEK S.A.C.**, de manera integral **NO CUMPLE** con las caracteristicas principales y funcionalidades de la prestación principal, según detalle en el Anexo Nº 1 que forma parte del Informe del usuario mencionado, determinando su oferta técnica **NO ADMITIDA.**

El postor **INNOVARE E-BUSINESS S.A.C.,** presentó la documentación complementaria a la Declaración Jurada de cumplimiento de los Términos de Referencia contenidos en el numeral 3.1 del Capítulo III de la presente sección. (Anexo Nº 3), para la acreditación del cumplimiento de las caracteristicas tecnicas indicadas en los numerales 4.2.1 y 4.2.2. Al respecto, en base al Memorando N° D000007/81-2024-ANIN/OTI e Informe Nº D00000219-2024-ANIN/OTI-US-MMC remitido por el usuario en calidad de apoyo técnico para la verificación de cumplimiento, el postor **INNOVARE E-BUSINESS S.A.C**, de manera integral **NO CUMPLE** con las caracteristicas principales y funcionalidades de la prestación principal, según detalle en el Anexo Nº 1 que forma parte del Informe del usuario determinando su oferta técnica **NO ADMITIDA.**

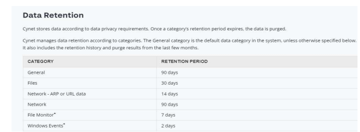
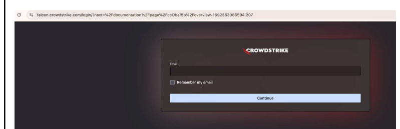
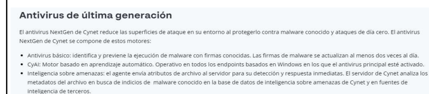
COMITÉ DE SELECCIÓN

EDITH GIOVANNA REYES SURAY
Primer Miembro Titular

JOSÉ ENRIQUE VASQUEZ LIZARRAGA
Presidente Titular

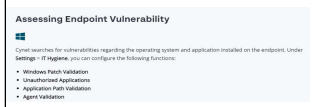
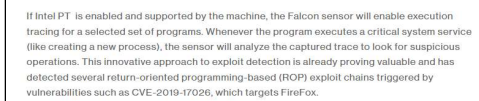
CESAR AUGUSTO BENITES DURAND
Segundo Miembro Titular

ANEXO 1 CORRESPONDIENTE AL INFORME Nº D00000219-2024-ANIN/OTI-US-MMC

Nº	DESCRIPCIÓN	INNOVARE BUSSINES S.A.C. CUMPLIMIENTO	GRUPO BANTEK S.A.C CUMPLIMIENTO	IMPERIA SOLUCIONES TECNOCLÓGICAS S.A.C CUMPLIMIENTO	JUSTIFICACIÓN DEL NO CUMPLIMIENTO
PRESTACIÓN PRINCIPAL					
4.2.1. CARACTERISTICAS PRINCIPALES					
1	*La solución debe consistir en una plataforma de Protección, Detección y Respuesta del endpoint (Endpoint Protection y EDR)*	SI	SI	SI	
2	*La solución debe consistir en una plataforma de Protección, Detección y Respuesta Extendida que ofrezca capacidades de seguridad de endpoint. Opcionalmente, deberá tener capacidades de análisis extendido correlacionando y analizando eventos de diferentes fuentes.*	SI	SI	SI	
4	*El almacenamiento de telemetría del endpoint deberá estar disponible durante al menos 30 días. Opcionalmente, deberá contar con almacenamiento de telemetria de eventos de otras fuentes disponible durante al menos 30 días.*	NO	NO	SI	*INNOVARE BUSSINES S.A.C.* ***NO CUMPLE.*** *Se evidencia que la retención de log para eventos de windows es de 2 días, el requerimiento es de 30 días solicitados para la telemetría.*  **Data Retention** Cynet stores data according to data privacy requirements. Once a category's retention period expires, the data is purged. Cynet manages data retention according to categories. The General category is the default data category in the system, unless otherwise specified below. It also includes the retention history and purge results from the last few months. CATEGORY — RETENTION PERIOD General — 90 days Files — 30 days Network - ARP or URL data — 14 days Network — 90 days File Monitor* — 7 days Windows Events* — 2 days *GRUPO BANTEK S.A.C* ***NO SE PUEDE VALIDAR*** *.En las imagenes presentadas por el postor, se observa distintos dias para la retenccion de eventos.No se pude validar correctamente debido a que no hay acceso al enlace adjunto y de la evaluación integral realizada, se intento indagar en la pagina web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.* 
5	*Deberá contar con soporte del fabricante durante todo el tiempo de servicio.*	SI	SI	SI	
6	*Se deberá otorgar acceso a un portal de e-learning donde la Entidad pueda llevar cursos en línea sobre la plataforma implementada.*	SI	SI	SI	
7	*Deberá haber logrado una efectividad de protección de ataques de 100% según el último reporte de MITRE ATT&CK TURLA 2023*	SI	SI	SI	
8	*Deberá haber logrado una efectividad de Cobertura por Analítica (Analytic Coverage) de al menos 96% según el último reporte MITRE ATT&CK TURLA 2023*	SI	SI	SI	
4.2.2. FUNCIONALIDADES					
Prevención contra exploits					
1	*Debe identificar y bloquear técnicas de explotación sin necesidad de utilizar firmas y/o heurísticas. La solución no deberá tener ningún componente que requiera actualizar una base de datos de firmas.*	NO	SI	SI	*INNOVARE BUSSINES S.A.C.* ***NO CUMPLE.*** *Se evidencia que la solución utiliza AV basado en firmas para realizar analisis. Asimismo, se menciona que las firmas de malware son actualizadas, al menos, 2 veces al día. El requerimiento, es de que ningún componente requiere actualizar la base de datos de firmas.*  **Antivirus de última generación** El antivirus NextGen de Cynet reduce las superficies de ataque en su entorno al protegerlo contra malware conocido y ataques de día cero. El antivirus NextGen de Cynet se compone de estos motores: • Antivirus básico: identifica y previene la ejecución de malware con firmas conocidas. Las firmas de malware se actualizan al menos dos veces al día. • CyAI: Motor basado en aprendizaje automático. Operativo en todos los endpoints basados en Windows en los que el antivirus principal esté activado. • Inteligencia sobre amenazas: el agente envía atributos de archivo al servidor para su detección y respuesta inmediatas. El servidor de Cynet analiza los metadatos del archivo en busca de indicios de malware conocido en la base de datos de inteligencia sobre amenazas de Cynet y en fuentes de inteligencia de terceros.

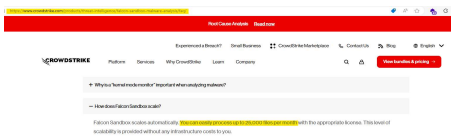
FIRMA DIGITAL

Firmado digitalmente por:
MEZARINA CASTRO Martin Virgilio FAU 20611816953 hard
Motivo: Soy el autor del documento
Fecha: 09/09/2024 14:39:58-0500

2	*El bloqueo de exploits deberá ser posible incluso en procesos desarrollados inhouse, la solución deberá permitir especificar los nombres de los procesos que serán protegidos contra exploits.*	SI	SI	SI	
3	*Deberá proteger la explotación de vulnerabilidades de sistemas operativos y aplicaciones que incluso se encuentren sin el parche de seguridad instalado.*	SI	SI	SI	
4	*La protección contra vulnerabilidades deberá ser independiente al CVE identificado, la solución deberá proteger cualquier intento de explotación incluyendo a vulnerabilidades de día cero que no tengan un CVE.*	SI	SI	SI	
5	*Bloquear técnicas de explotación de vulnerabilidades, como mínimo Retum Oriented Programming (ROP), Heap Spray, Jit Spray, Shell link, Structured Exception Handler, CPL Execution Process.*	NO	NO	SI	*INNOVARE BUSSINES S.A.C.* ***NO CUMPLE.*** *Si bien en el enlace adjunto se observa la proteccion de vulnerabilidades, no se evidencia las técnicas contra ROP, HEAP spray, Jit Spray, Structured Exception Handler, CPL execution Proccess.*  *GRUPO BANTEK S.A.C* ***NO CUMPLE*** *.En el enlace proporcionado por el postor solo se identifica ROP . No se evidencia las técnicas contra HEAP spray, Jit Spray, Structured Exception Handler, CPL execution Proccess.* 
6	*Identificación y prevención de intentos de escalación de privilegios a nivel de Kernel.*	SI	SI	SI	
7	*Deberá ser capaz de proteger contra ataques a vulnerabilidades conocidas y desconocidas (día cero).*	SI	SI	SI	
8	*Capacidad de crear un snapshot (dump) de la memoria RAM al momento de prevenir la ejecución de una técnica de explotación, con la finalidad de proporcionar información forense sobre el evento.*	SI	SI	SI	
9	*Prevención de técnicas de explotación que utilizan Java Deserialization, Kernel Integrity Monitor (KIM), Local Threat Evaluation Engine (LTEE), Reverse Shell Protection, Shellcode Protection, SO Hijacking Protection, Webshell.*	NO	NO	SI	*INNOVARE BUSSINES S.A.C.* ***NO CUMPLE.*** *No se evidencia el cumplimiento de preveción de Java Deserialization y SO Hijacking Protection. Adicionalmente se encontre en uno de los enlaces información sobre el NDR (que seria otra solución y no la compete al EDR)*  *GRUPO BANTEK S.A.C* ***NO CUMPLE.*** *No se evidencia el cumplimiento de preveción de Java Deserialization y SO Hijacking Protection. En uno de los enlaces proporcionado se describe la tecnica de explotacion de Java Deserialization, pero no se evidencia la prevención por parte de la solución ofertada.* 
10	*Todas las capacidades de prevención de exploits deberán estar disponibles de manera offline, sin necesidad de tener una conexión a la consola.*	SI	SI	SI	
Protección contra malware					
1	*Deberá contar con funcionalidades de antimalware de siguiente generación, entiéndase antimalware de siguiente generación como plataformas que utilizan algoritmos de aprendizaje de máquina (machine learning) para detectar y bloquear el malware; no deberá tener ningún componente que requiera actualizar una base de datos de firmas de antivirus/antimalware.*	SI	SI	SI	
2	*El algoritmo de machine learning deberá operar de manera local en el endpoint sin depender de una conexión permanente a la consola.*	SI	SI	SI	
3	*Debe prevenir el robo de contraseña a partir de la lectura de la memoria RAM (mimikatz)*	SI	SI	SI	
4	*Contar con un módulo de prevención contra ransomware que podrá ser configurado en modo normal y riguroso.*	SI	SI	SI	
5	*Capacidad de prevenir ataques de Cryptomining a partir del comportamiento del objeto ejecutado.*	SI	SI	SI	
6	*Adicionalmente a la protección basada en machine learning, deberá contar con la capacidad de identificar el comportamiento de la amenaza, de tal forma que la actividad maliciosa de un archivo se pueda detectar y bloquear en una fase temprana.*	SI	SI	SI	

FIRMA DIGITAL

Firmado digitalmente por:
MEZARINA CASTRO Martin
Virgilio FAU 20611816953 hard
Motivo: Soy el autor del
documento
Fecha: 09/09/2024 14:40:16-0500

7	*Capacidad de prevenir contra shells reversos (reverse shell) para sistemas operativos Linux.*	SI	SI	SI	
8	*Capacidad de poder colocar los malware en una carpeta de cuarentena*	SI	SI	SI	
9	*Capacidad de colocar en lista permitida los archivos o directorios, para exceptuar la inspección.*	SI	NO	SI	GRUPO BANTEK S.A.C *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
10	*Capacidad de realizar escaneos a demanda y programados, con el objetivo de identificar malware dormido en los endpoints.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
11	*El consumo de recursos al momento de realizar el escaneo debe de ser mínimo y no debe impactar en la experiencia del usuario.*	SI	SI	SI	
Plataforma de Sandboxing					
1	*El agente deberá ser capaz de enviar automáticamente el archivo a un entorno de sandbox para ser emulado.*	SI	SI	SI	
2	*El sandbox deberá estar basado en nube y debe tener una disponibilidad del servicio de al menos 99.9% contabilizados mensualmente.*	NO	NO	SI	*INNOVARE BUSSINES S.A.C.* ***NO CUMPLE** . No se evidencia en el contenido del enlace adjunto, no contienen ningún sustento o evidencia del requerimiento solicitado. Si bien su sandbox esta basado en nube tal como se pide no hay información de disponibilidad de servicio 99.9% tal como se pide en bases.*  Configuring Analysis Settings The SSE sandbox enables dynamic file analysis and can be configured for either a local sandbox or a cloud-based sandbox. 1. Navigate to Settings > Analysis. 2. Select Enable SSE Sandbox Analysis. 3. Select the sandbox to enable: a. To enable the cloud-based sandbox, select Enable Cloud Sandbox. b. To enable a local sandbox, select Enable Local Sandbox and enter the Local Sandbox IP address. 4. Click Save. *GRUPO BANTEK S.A.C* ***NO CUMPLE**. No se evidencia en el contenido del enlace adjunto, no contienen ningún sustento o evidencia del requerimiento solicitado. Si bien su sandbox esta basado en nube tal como se pide no hay información de disponibilidad de servicio 99.9% tal como se pide en bases.*  Introducing CrowdStrike Falcon Sandbox CrowdStrike Falcon® Sandbox is a module built on the integrated, cloud-native CrowdStrike Falcon® platform. By coupling its analysis results with threat intelligence, Falcon Sandbox delivers actionable indicators of compromise (IOCs) to your security team. Its cutting-edge analysis technology enables the detection of advanced threats, and it can integrate seamlessly via rich APIs.
3	*El sandbox deberá soportar el análisis de 100 mil archivos por día. El sandbox deberá tener capacidad de analizar archivos de hasta 100 MB de peso.*	NO	NO	SI	*INNOVARE BUSSINES S.A.C.* ***No cumple,** en el enlace presentado no se evidencia la capacidad de soportar 100 mil archivos por día ni analizar archivos de hasta 100 MB de peso. El enlace explica la capacidad de analisis de archivos para la forencia, mas no la capaciadades de analisis realizados en el sandboxing del fabricante.*  Static Analysis — Information collected during the static analysis of the file. Dynamic Analysis — Information collected and generated from a sandboxed execution of the file in the Cynet SSE. Sockets — Network traffic generated to and from this file. Domains — Domains queried by this process to initiate network traffic. *GRUPO BANTEK S.A.C* ***NO CUMPLE,** se evidencia que el sanboxing soporta hasta 25000 archivos mensuales. Se pide 100mil por día .* https://www.crowdstrike.com/products/threat-intelligence/falcon-sandbox-malware-analysis/faq/  Root Cause Analysis Read now CROWDSTRIKE Platform Services Why CrowdStrike Learn Company + Why is a "kernel mode monitor" important when analyzing malware? – How does Falcon Sandbox scale? Falcon Sandbox scales automatically. You can reliably process up to 25,000 files per month with the appropriate license. This level of scalability is provided without any infrastructure costs to you.

4	*Deberá garantizar la privacidad y seguridad del contenido de los archivos analizados, para lo cual se requiere que cuente como mínimo con las certificaciones SOC2 Tipo II Plus de AICPA, ISO 27001.*	SI	SI	SI	
5	*Capacidad de realizar análisis de sandboxing en sistemas Windows, MacOS, Linux.*	*NO*	*SI*	*SI*	*INNOVARE BUSSINES S.A.C.* ***NO CUMPLE.*** *En el enlace que el postor adjunto ,no se evidencia la capacidad de sanboxing en sistemas Windows, MacOS, Linux. El link hace referencia a forma de analisis e investigación de archivos, donde la solución cuenta con sandboxing pero no se detallar información del requermiento.* **Bloquear malware derivado de exploits** Cynet emplea protección contra malware de varias capas, que incluye sandboxing, monitoreo del comportamiento de procesos y análisis estático basado en ML. Cynet también ofrece hash difuso e inteligencia de amenazas. Esto garantiza que incluso si una amenaza avanzada establece una conexión con el atacante y descarga malware adicional, Cynet detendrá su ejecución, evitando así que se produzcan daños.
6	***Control de dispositivos***				
7	*Debe permitir gestionar los puertos USB que permitan conectar dispositivos como: discos duros, unidades lectoras de CD-ROM externas con conexión USB, dispositivos de almacenamiento removibles portátiles, unidades lectoras de discos floppy externas con conexión USB.*	SI	SI	SI	
8	*Debe de permitir generar perfiles de excepciones para poder conectar dispositivos en puertos USB utilizando los siguientes parámetros: tipo de dispositivo, tipo de permiso a asignar (lectura/escritura o sólo lectura), fabricante (debe de contener una lista predeterminada), producto (debe de contener una lista predeterminada) y número de serie.*	SI	SI	SI	
9	*Las políticas generadas deben de poder asignarse a un endpoint en particular, a un grupo de endpoints.*	SI	SI	SI	
10	*Deberá ser capaz de integrarse a Active Directory para establecer políticas de control de USB en base a grupos de LDAP.*	SI	SI	SI	
11	*Debe de permitir la creación de excepciones temporales a partir de una alerta registrada, para permitir el dispositivo solo durante un tiempo configurable.*	SI	SI	SI	
12	*Capacidad de añadir nuevos tipos de dispositivos agregando el GUID de Windows correspondiente*	SI	SI	SI	
Telemetría y Colección de Datos y Eventos					
1	*El agente deberá poder capturar, como mínimo, las siguientes acciones en equipos Windows:*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
2	*Proceso ejecutado, incluyendo el tiempo de inicio, el tamaño del archivo asociado.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
3	*Actividades de creación, escritura, renombre, eliminación, modificación de archivos.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
4	*Archivos DLL: ruta completa, dirección base, id del proceso, tamaño de la imagen, firma, valores hash calculados con los algoritmos MD5 y SHA256 del archivo DLL.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
5	*Creación y terminación de los procesos, incluyendo los siguientes atributos: nombre del proceso padre, ID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma o el certificado utilizado para firmar el archivo.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
6	*Inyecciones en hilos de procesos: ID del hilo padre, ID del hilo nuevo o que se ha terminado, proceso que inició el hilo (en caso de ser un proceso distinto).*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
7	*Interacciones de red de cada enpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP), resolución de dominio (hostname), tráfico entrante y saliente, país destino de la IP pública.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*

FIRMA DIGITAL

Firmado digitalmente por:
MEZARINA CASTRO Martin
Virgilio FAU 20611816953 hard
Motivo: Soy el autor del
documento
Fecha: 09/09/2024 14:40:39-0500

8	*Estadísticas de red: volumen de tráfico en eventos de subida y descarga de tráfico TCP.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
9	*Acciones sobre los registros de Windows: Configuración o eliminación de valores del registro. Creación, modificación, eliminación, adición, restauración y guardar llaves del registro. Con los siguientes parámetros: ruta del registro del valor o llave que fue modificado. Nombre del valor o llave modificado. Datos del valor modificado.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
10	*Sesiones del sistema operativo: inicio de sesión, cierre de sesión, conexión y desconexión. Considerando los siguientes atributos: inicio de sesión interactivo, id de la sesión, estado de la sesión, y si la sesión es local o remota.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
11	*Logs de eventos de Windows.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
12	*El agente deberá poder capturar, como mínimo, las siguientes acciones en equipos MacOS:*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
13	*Actividades de creación, escritura, renombre, eliminación, modificación de archivos.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
14	*Inicio y detención de procesos, con los siguientes parámetros: PID de proceso del proceso padre, PID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma o el certificado utilizado para firmar el archivo.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
15	*Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP).*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
16	*Las siguientes acciones de red: accept, connect, connect failure, disconnect, listen, statistics.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
17	*Logs de eventos de autenticación*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
18	*El agente deberá poder capturar, como mínimo, las siguientes acciones en equipos Linux:*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
19	*Para los archivos: las acciones de creación, apertura, escritura y eliminación, incluyendo la ruta completa del archivo y el hash del archivo (para ciertos archivos y sólo si el archivo fue escrito). Información del copiado o renombrado de los archivos, incluyendo las rutas completas tanto del archivo original como del modificado. Las acciones para cambiar el dueño (chown) y el modo (chmod) de los archivos, incluyendo la ruta completa del archivo, así como el nuevo dueño o nuevos atributos.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*

FIRMA DIGITAL

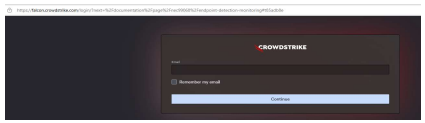
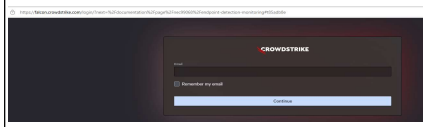
Firmado digitalmente por:
MEZARINA CASTRO Martin
Virgilio FAU 20611816953 hard
Motivo: Soy el autor del
documento
Fecha: 09/09/2024 14:40:49-0500

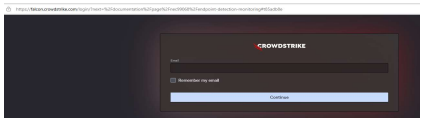
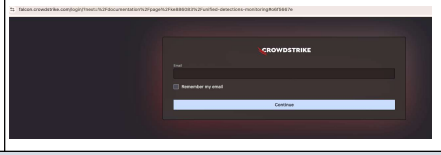
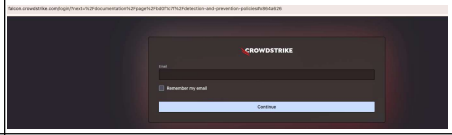
20	*Inicio y detención de procesos, con los siguientes parámetros: PID de proceso del proceso padre, PID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma o el certificado utilizado para firmar el archivo.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
21	*Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP).*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
22	*Las siguientes acciones de red: accept, connect, connect failure, disconnect, listen, statistics.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
23	*Logs de eventos de autenticación.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
Capacidades de Investigación y Threat Hunting					
1	*Deberá mostrar una secuencia gráfica del incidente de seguridad que correlacione las alertas individuales con el objetivo de identificar la causa raíz. Esta secuencia gráfica deberá ser construida de manera automática a partir de la inteligencia artificial de la plataforma.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
2	*Deberá de mostrar información de los procesos correlacionados en la secuencia gráfica, entre los que se encuentran ruta de ejecución, nombre de usuario que ejecutó el proceso, entidad que firmó el proceso, valor SHA256 del ejecutable relacionado con el proceso, veredicto del análisis del sandbox y línea de comandos de la ejecución.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
3	*Por cada proceso correlacionado en la secuencia gráfica del incidente se deberá mostrar lo siguiente:*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
4	*Fecha, hora, hostname, dirección IP, nombre del usuario, sistema operativo del equipo que generó el proceso.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
5	*Alertas relacionadas al proceso analizado con su respectiva descripción, acción tomada sobre la alerta, categoría de la amenaza, ejecutable que lo inicializó, táctica y técnica del ataque según el framework MITRE ATT&CK.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
6	*Actividad de la red del proceso: IP y puerto origen, IP y puerto destino, resolución del DNS, país destino, indicar si la conexión fue exitosa o fallida.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
7	*Creación, escritura, lectura, eliminación, renombre, cambio de atributos, hash en SHA256 y MD5 de los archivos relacionados al proceso analizado. En caso del renombre deberá mostrar el nombre anterior y actual para facilitar la investigación del analista.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
8	*Creación, apertura, escritura, eliminación, renombre, cambio de atributos de los directorios relacionados al proceso analizado.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*

9	*Actividad sobre la clave y valores de registros, tales como creación, eliminación, carga, apertura, renombre, escritura, del proceso analizado.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
10	*Mostrar los system calls, rpc calls y procesos inyectados sobre cada proceso analizado.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
11	*Deberá contar con un mecanismo inteligente que separe de manera automática los binarios y DLLs no significados de la secuencia gráfica del incidente.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
12	*Deberá permitir realizar búsquedas avanzadas sobre la actividad de los endpoints:*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
13	*Actividad de los archivos, identificando las siguientes operaciones: creación, lectura, eliminación, escritura y renombrar.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
14	*Actividad de red, identificando el tráfico saliente, entrante, IP origen e IP destino, Puerto origen y Puerto destino, protocolo de red.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
15	*Actividad en el registro Windows, identificando la creación, eliminación, renombrado, definición de valores, eliminación de valores de las llaves de registro.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
16	*Actividad de procesos, identificando si se trata de una ejecución o inyección, ruta desde donde se ejecuta, comando que inicializa el proceso, usuario, hash en SHA256 y MD5.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
17	*Actividad en el Log de Eventos de Windows, identificando la descripción, ID del evento, nivel, mensaje, nombre del proveedor y usuario.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
18	*Actividad de autenticación al endpoint*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
19	*Permitir realizar búsquedas en base a cualquier dato recopilado por la plataforma.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
20	*Permitir seleccionar las columnas y orden de los datos mostrados como resultados de las búsquedas.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
21	*Los resultados de las búsquedas deberán poder ser mostrados en una tabla o una gráfica de tipo pye, columnas, burbuja y área, con la finalidad de facilitar el análisis del investigador.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*

FIRMA DIGITAL

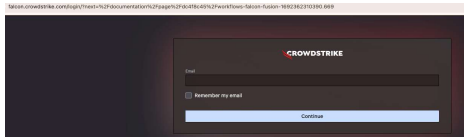
Firmado digitalmente por:
MEZARINA CASTRO Martin
Virgilio FAU 20611816953 hard
Motivo: Soy el autor del
documento
Fecha: 09/09/2024 14:44:31-0500

22	*Deberá contar con una librería predeterminada de búsquedas habituales realizadas en una labor de threat hunting. Esta librería podrá ser editada según la labor del investigador.*	SI	SI	SI	
23	*Las búsquedas deberán estar disponibles tanto para endpoints en línea y fuera de línea.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
24	*Las búsquedas deberán de poder programarse para ser ejecutadas en un día y hora determinados durante una sola ocasión y también de manera recurrente.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
25	*Todas las opciones de búsqueda anteriormente detalladas deberán poder ser utilizadas para configurar reglas personalizadas de seguridad, que permitan generar una alerta cuando un endpoint en particular genere ese comportamiento.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
26	*Deberá de contar con un dashboard que permita visualizar alertas generadas de distintas fuentes.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
27	*El timeline del ataque deberá mostrar el intento de ataque en diferentes fases de explotación acorde al Framework MITRE ATT&CK, tales como Ejecución, Persistencia, Descubrimiento, Desplazamiento Lateral, Command & Control, Exfiltración.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se puede validar. No hay acceso al enlace adjunto y de la evaluación integral realizada, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.* 
28	*Deberá permitir la personalización de reglas de correlación que permitan configurar casos de uso utilizando los eventos recolectados de las diversas fuentes.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se puede validar. No hay acceso al enlace adjunto y de la evaluación integral realizada, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.* 
Capacidades de Gestión de Incidentes					
1	*Deberá agrupar todas las alertas relacionadas a un incidente de seguridad de manera automática.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
2	*Por cada incidente mostrado deberá mostrar los elementos relacionados como ejecutables, hashes, direcciones IP.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
3	*Deberá mostrar los hosts y usuarios asociados al incidente.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
4	*Deberá ser posible asignar la revisión del incidente a un investigador con acceso a la consola, con el objetivo de llevar un orden sobre la atención de incidentes.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*

5	*Capacidad de comentar los incidentes para detallar los avances realizados en la revisión.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
6	*Capacidad de clasificar el estado del incidente como abierto, en revisión, gestionado, cerrado, etc.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se puede validar. No hay acceso al enlace adjuntoy de la evaluación integral realizada, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.* 
7	*Capacidad de agrupar y desagrupar los incidentes de manera manual.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
8	*Capacidad de modificar la severidad del incidente de manera manual.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se pude validar. No hay acceso al enlace adjunto y de la evaluación integral realizada, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.* 
9	***Capacidades de Threat Intelligence***				
10	*Capacidad de alimentar la plataforma de Indicadores de Compromiso (IOC) de manera manual o automática vía API*	SI	SI	SI	
11	*Los IOC soportados deberán ser de tipo Hash, Ruta, Nombre de archivo, Dominio, Dirección IP.*	SI	NO	SI	GRUPO BANTEK S.A.C *No se pude validar. No hay acceso al enlace adjunto y de la evaluación integral realizada, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.* 
12	*Capacidad de agregar IOC de manera individual o masiva (por ejemplo, subiendo un archivo CSV)*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
13	*Capacidad de colocar un nivel de reputación, confiabilidad del IOC y una fecha de expiración.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*

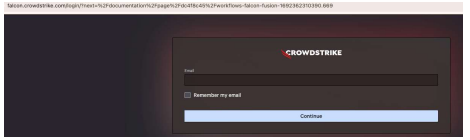
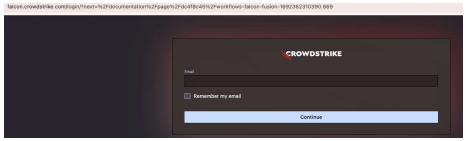
FIRMA DIGITAL

Firmado digitalmente por:
MEZARINA CASTRO Martin
Virgilio FAU 20611816953 hard
Motivo: Soy el autor del
documento
Fecha: 09/09/2024 14:45:00-0500

14	*Debe poder integrarse a una plataforma tercera de Threat Intelligence como Virus Total.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
15	*Mostrar un mapa geográfico que permita analizar la dirección IP detectada como parte de incidente, como mínimo deberá mostrar lo siguiente: fecha de registro, ISP (Internet Service Provider), país. La información deberá poder ser mostrada en base al país, proceso, puerto e IP destino.*	SI	SI	SI	
16	*Deberá contar con un dashboard que permita analizar el comportamiento del hash de un archivo en particular, mostrando su nivel de reputación y si dicho hash ha sido detectado en otras alertas e incidentes.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
Capacidades de respuesta					
1	*Deberá ser posible colocar en lista bloqueada y/o lista permitida uno o más hashes.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
2	*Deberá permitir colocar en cuarentena un archivo malicioso detectado y/o bloqueado. La colocación en cuarentena deberá poder realizarse de manera manual y automática.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
3	*Capacidad de extraer el archivo dump de la memoria RAM del endpoint a partir de una alerta revisada.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
4	*Capacidad de extraer el malware o archivo sospechoso del endpoint hacia la consola, para poder ser analizado por el investigador*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
5	*Debe ser posible aislar el endpoint de la red para que no tenga comunicación con ningún dispositivo de la red interna o externa.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
6	*Capacidad de configurar reglas de automatización que permitan ejecutar una acción determinada en los endpoints en base condiciones de alertas de seguridad, como mínimo estas reglas deberán permitir las siguientes acciones de manera automática: aislar el endpoint, hacer un escaneo de malware, extraer el malware desde el endpoint.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se pude validar. No hay acceso al enlace adjunto y de la evaluación integral realizada, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.* 
7	*Deberá ser posible realizar una conexión remota a cada endpoint que forme parte de una investigación para ejecutar las siguientes acciones:*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
8	*Listar procesos y archivos*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*

FIRMA DIGITAL

Firmado digitalmente por:
MEZARINA CASTRO Martin
Virgilio FAU 20611816953 hard
Motivo: Soy el autor del
documento
Fecha: 09/09/2024 14:45:10-0500

9	*Ejecutar instrucciones por línea de comandos (CMD y Powershell para el caso de Windows; Bash para el caso de Linux).*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
10	*Ejecutar scripts basados en Python*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
11	*Capacidad de ejecutar scripts remotamente a múltiples endpoints de manera concurrentes.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
12	*Deberá contar con una libreria de scripts predefinidos y deberá ser posible configurar scripts personalizados basados en Python.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
13	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
14	*Mostrar sugerencias para las remediaciones de un equipo comprometido.*	SI	SI	SI	
15	*Capacidad de integración con un SIEM vía Syslog y plataformas SOAR.*	SI	SI	SI	
Descubrimiento de activos					
1	*Deberá contar con un mecanismo para descubrir dispositivos de la red sin el agente instalado.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
2	*El descubrimiento deberá tener la capacidad para identificar la dirección IP del equipo y el Sistema Operativo que no tienen el agente instalado.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se pude validar. No hay acceso al enlace adjunto y de la evaluación integral realizada, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.* 
3	*Permitir exceptuar los segmentos de red que no se desean escanear.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se pude validar. No hay acceso al enlace adjunto y de la evaluación integral realizada, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.* 
4	*Deberá contar con el licenciamiento adecuado para el descubrimiento de dispositivos en las diferentes sedes de la entidad.*	SI	SI	SI	
Características del agente					
1	*Deberá ser un agente ligero que incluso pueda convivir con cualquier otro software instalado en el endpoint.*	SI	SI	SI	
2	*Soporte para las siguientes versiones de sistemas operativos:*	SI	SI	SI	
3	*Windows 8.1 y superior, Windows Server 2012 y superior*	SI	SI	SI	
4	*MacOS 10.13 y superior*	SI	SI	SI	

5	*Linux, distribuciones: CentOS 6 y superior, Debian 8 y superior, Red Hat Enterprise Linux 6 y superior, Suse for Enterprise 12.1 y superior, Ubuntu Server 12 y superior, Amazon Linux 2017 y 2018, Oracle Linux 6 y superior.*	SI	SI	SI	
6	*Android y iOS.*	SI	SI	SI	
7	*No debe requerir el reinicio del equipo para que agente se encuentre operativo.*	SI	SI	SI	
8	*Deberá estar protegido ante intentos de desinstalación o manipulación del agente.*	SI	SI	SI	
9	*Deberá ser posible definir diferentes password de seguridad para diferentes grupos de endpoints.*	SI	SI	SI	
Capacidades de Gestión					
1	*La consola deberá estar basada 100% en nube, con el objetivo de no depender ni administrar infraestructura física local. La nube del fabricante deberá contar con las siguientes características:*	SI	SI	SI	
2	*Contar con la certificación SOC2 Tipo II de AICPA, ISO 27001.*	SI	SI	SI	
3	*Contar con doble factor de autenticación para el login.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
4	*Permitir el acceso solo desde un rango de IP pública de la Entidad.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
5	*La consola debe permitir la gestión de usuarios mediante roles preconfigurados y debe ser capaz de crear roles personalizados.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
6	*Permite utilizar cualquier aplicación de un tercero para poder realizar la instalación del agente.*	SI	SI	SI	
7	*Cuenta con la capacidad de crear grupos que pueden alimentarse de forma estática y dinámica.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
8	*Capacidad de personalización del dashboard para mostrar los widgets según las necesidades de la Entidad.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
9	*Capacidad de almacenar una auditoria de eventos sobre las acciones realizadas en la consola*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
10	*Deberá permitir el envío automático de alertas al correo electrónico cuando se identifica una actividad maliciosa. Podrán aplicarse filtros a dichas alertas para solo mostrar las de mayor relevancia.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
11	*Deberá permitir la generación de reportes a través de plantillas preconfiguradas y también permitir definir reportes personalizados.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
12	*Mantener un historial de los reportes que han sido generados para su posterior consulta.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*
13	*Los reportes podrán ser enviados de forma automática y programada a una o más direcciones de correos electrónicos.*	SI	NO	SI	*GRUPO BANTEK S.A.C* *No se evidencia el enlace de referencia, el pantallazo presentado como parte de la documentación técnica que forma parte de la oferta se encuentra ilegible, no obstante, se intentó indagar en la página web de la marca ofertada no pudiendo verificar tampoco el cumplimiento de lo requerido.En ese sentido, de la evaluación integral realizada no acredita lo solicitado.*

FIRMA DIGITAL

Firmado digitalmente por:
MEZARINA CASTRO Martin
Virgilio FAU 20611816953 hard
Motivo: Soy el autor del
documento
Fecha: 09/09/2024 14:45:45-0500

PRESTACION ACCESORIA				
4.3.1 SOPORTE TÉCNICO	SI	SI	SI	*• Siendo que para dicho requisito este debe ser acreditado a través de documentación del fabricante como: brochures y/o catálogos y/o folletos y/u hojas de datos y/o enlaces web y/o whitepapers (…), de la evaluación respecto al servicio de soporte técnico el cual es accesorio a la prestación principal, dos de los postores presentaron declaraciones juradas y solo uno de ellos adjuntó el brochure del fabricante, es por ello que se corroboró a través de las páginas web de los fabricantes de las marcas ofertadas por los postores, que estos cuenten con el respaldo del soporte técnico requerido en el numeral 4.3.1, por lo que se adjuntan al presente dicha verificación y determina que los tres postores cumplen con brindar el servicio de soporte técnico.* *• En ese sentido, de la evaluación integral de la oferta técnica considerando que los tres postores han señalado cumplir con brindar conforme lo solicitado en las bases integradas el soporte técnico, el mismo que ha sido verificado, contando con los conocimientos técnicos, para este punto, dejando las formalidades, se determina que n o es relevante solo para este punto el tipo de documento mediante el cual han acreditado los postores, el requisito de soporte técnico solicitado, no alterando el cumplimiento de las características técnicas de la prestación principal ni de la oferta en general.*
RESULTADOS DE LA VERIFICACIÓN DEL CUMPLIMIENTO	**NO CUMPLE**	**NO CUMPLE**	**CUMPLE**	

FIRMA DIGITAL

Firmado digitalmente por: MEZARINA CASTRO Martin Virgilio FAU 20611816953 hard
Motivo: Soy el autor del documento
Fecha: 09/09/2024 14:45:56-0500

ANEXO N° 02

CUADRO DE EVALUACION DE OFERTAS

CONCURSO PÚBLICO Nº 004-2024-ANIN

CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE VEINTICUATRO (24) MESES DE PROTECCIÓN AVANZADA ANTIMALWARE PARA 1300 ESTACIONES DE TRABAJO Y SERVIDORES TI DE LA AUTORIDAD NACIONAL DE INFRAESTRUCTURA

EVALUACIÓN		PUNTAJE MÁXIMO
A.	PRECIO La evaluación consistirá en otorgar el máximo a la oferta de precio más bajo y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos precios, según la siguiente fórmula: $Pi = \frac{Om \times PMP}{Oi}$ i = Oferta Pi = Puntaje de la oferta a evaluar Oi = Precio i Om = Precio de la oferta más baja PMP = Puntaje máximo del precio	100.00
	Se acreditará mediante el documento que contiene el precio de la oferta (Anexo N° 6)	

N°	POSTOR	MONTO TOTAL OFERTADO (S/.)	PUNTAJE TÉCNICO	ORDEN DE PRELACIÓN
1	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	699,600.00	100.00	1

COMITÉ DE SELECCIÓN

EDITH GIOVANNA REYES SURAY
Primer Miembro Titular

JOSÉ ENRIQUE VÁSQUEZ LIZÁRRAGA
Presidente Titular

CESAR AUGUSTO BENITES DURAND
Segundo Miembro Titular

ANEXO N° 03

CUADRO DE CALIFICACIÓN DE OFERTAS

CONCURSO PÚBLICO Nº 004-2024-ANIN

CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE VEINTICUATRO (24) MESES DE PROTECCIÓN AVANZADA ANTIMALWARE PARA 1300 ESTACIONES DE TRABAJO Y SERVIDORES TI DE LA AUTORIDAD NACIONAL DE INFRAESTRUCTURA

LITERAL	FACTOR	ÚNICA OFERTA VALIDA IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.
B.3	CALIFICACIONES DEL PERSONAL CLAVE	
B.3.1	FORMACIÓN ACADÉMICA	
	Requisitos: UN (01) SUPERVISOR DEL SERVICIO • Profesional titulado en Ingeniería Electrónica o Ingeniería de Sistemas o Ingeniería de Telecomunicaciones. UN (01) ESPECIALISTA EN SEGURIDAD • Ingeniero titulado o Técnico titulado o Bachiller en Ingeniería Electrónica, o en Telecomunicaciones, o en Redes y Comunicaciones de Datos, o Sistemas, o Informática, o de Sistemas de Información. Acreditación: El GRADO O TÍTULO PROFESIONAL REQUERIDO será 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 en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: https://titulosinstitutos.minedu.gob.pe/, según corresponda. En caso el GRADO O TÍTULO PROFESIONAL REQUERIDO no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.	CUMPLE (Folio 082) (folio 085)
B.3.2	CAPACITACIÓN	
	Requisitos: UN (01) SUPERVISOR DEL SERVICIO • Curso Scrum Product Owner Professional Certificate (SPOPC), curso mínimo de 20 horas lectivas. Acreditación: Se acreditará con copia simple de CONSTANCIAS, CERTIFICADOS, U OTROS DOCUMENTOS, SEGÚN CORRESPONDA. Importante Se podrá acreditar la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas lectivas, según la normativa de la materia.	CUMPLE (Folio 088)
B.4	EXPERIENCIA DEL PERSONAL CLAVE	
	[UN (01) SUPERVISOR DEL SERVICIO Requisitos: Experiencia mínima de tres (03) años en supervisión de proyectos de seguridad informática UN (01) ESPECIALISTA EN SEGURIDAD Requisitos: Experiencia mínima de dos (02) años en la implementación y/o soporte de la solución ofertada. De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado. Acreditación: La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.	CUMPLE (Folio 094) (folio 096)

C	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD	
	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a S/ 1'000,000.00 (Un millón con 00/100 Soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. Se consideran servicios similares a los siguientes: •Venta de Licencias de Antivirus •Adquisición de Software Antivirus •Antivirus para PC Y/O Laptop, Antivirus Para Servidores •Licenciamiento Antivirus •Venta de Licencias de Seguridad Perimetral •Licencia de Software Antivirus •Licencias de Antivirus para Servidores •Licencias de Antivirus para Desktop •Licencias Antimalware Endpoint. •Licencias de antivirus para computadoras personales. •Servicio de solución de antivirus. •Adquisición de solución antimalware endpoint. • Servicio de suscripción de solución de protección avanzada Antimalware y Antiransomware. • Suscripción de soluciones para la detección, respuesta, análisis e investigación de puntos finales. • Suscripción de Software de detección y respuesta extendida (XDR). • Licencia de protección avanzada Antimalware y Antiransomware para puntos finales. **Acreditación:** La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago , correspondientes a un máximo de veinte (20) contrataciones. En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el **Anexo N° 8** referido a la Experiencia del Postor en la Especialidad. En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados. En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato. Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales. Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente. Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 9.** Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicios o de cancelación del comprobante de pago, según corresponda. Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo N° 8** referido a la Experiencia del Postor en la Especialidad.	**CUMPLE** **(Folio 098-130)**
	CALIFICADA / DESCALIFICADA	**CALIFICADO**

COMITÉ DE SELECCIÓN

EDITH GIOVANNA REYES SURAY
Primer Miembro Titular

JOSÉ ENRIQUE VÁSQUEZ LIZÁRRAGA
Presidente Titular

CESAR AUGUSTO BENITES DURAND
Segundo Miembro Titular

ANEXO N° 04

CUADRO DE OTORGAMIENTO DE BUENA PRO

CONCURSO PÚBLICO Nº 004-2024-ANIN

CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE VEINTICUATRO (24) MESES DE PROTECCIÓN AVANZADA ANTIMALWARE PARA 1300 ESTACIONES DE TRABAJO Y SERVIDORES TI DE LA AUTORIDAD NACIONAL DE INFRAESTRUCTURA

Nº	POSTOR	MONTO TOTAL OFERTADO (S/.)	PUNTAJE FINAL	ORDEN DE PRELACIÓN
1	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	699,600.00	100.00	1

COMITÉ DE SELECCIÓN

EDITH GIOVANNA REYES SURAY
Primer Miembro Titular

JOSÉ ENRIQUE VÁSQUEZ LIZÁRRAGA
Presidente Titular

CESAR AUGUSTO BENITES DURAND
Segundo Miembro Titular