



Misión: La Defensa Pública es una institución autónoma y autárquica que brinda asistencia y representación jurídica gratuita a personas en situación de vulnerabilidad, vigilando la efectiva aplicación del debido proceso en el ámbito jurisdiccional.

Nota U.O.C. N°: 421/2024

Asunción, 16 de setiembre del 2024.-

Dr. Agustín Encina

Director Nacional

Dirección Nacional de Contrataciones Públicas

Tengo el agrado de dirigirme a Usted, con el objeto de contestar el punto observado, con relación al proceso **Adquisición De Licencias (Antivirus) con ID N° 446.119.-**

Sobre lo expuesto, en respuesta a los puntos observados, que se transcriben, se expone cuanto sigue:

1- CARGA DE DATOS DE LLAMADOS

Datos de Licitación

Cláusulas incompletas o datos insuficientes

Solicitamos a la convocante completar las cláusulas con los datos correspondientes al proceso

Comentario

Reiteración. Se visualiza que la solución que se pretende adquirir está compuesta por: -Renovación de licencias vigentes Kaspersky Next EDR Optimum, -Adquisición de nuevas licencias Kaspersky Next EDR Optimum, -Plataforma anti Spam correo electrónico, en la modalidad gateway virtual con integración a la plataforma XDR. Se observa que los tres puntos citados anteriormente en un solo ítem. Se solicita desglosar indicando las cantidad a ser requeridas para cada una de ellas, atendiendo a que son producto diferente y por ende costos diferentes.//

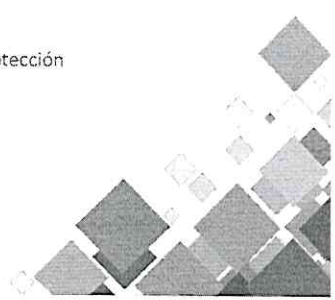
RESPUESTA:

Respuesta: según los antecedentes enviados en las especificaciones técnicas, no se visualiza un ítem con estos tres puntos (Renovación de licencias vigentes Kaspersky Next EDR Optimum, Adquisición de nuevas licencias Kaspersky Next EDR Optimum, Plataforma anti spam correo electrónico en la modalidad Gateway virtual con integración a la plataforma XDR).



Visión: Una Defensa Pública efectiva, confiable y reconocida por su labor institucional en la promoción del acceso a la justicia y la protección de los derechos humanos de las personas en situación de vulnerabilidad.

Ministerio de la Defensa Pública
Avda. Aviadores del Chaco 2432 casi Santa Teresa
Tel: (021) 289 3000
www.mdp.gov.py





Misión: La Defensa Pública es una institución autónoma y autárquica que brinda asistencia y representación jurídica gratuita a personas en situación de vulnerabilidad, vigilando la efectiva aplicación del debido proceso en el ámbito jurisdiccional.

Cabe destacar que el llamado es para renovar las licencias kaspersky, la cantidad de licencias a renovar son de 1.813. Adjunto copia de las especificaciones técnicas remitidas para su consideración

Sin otro particular, en espera a una respuesta favorable, me despido de Usted, con la consideración más distinguida y el aprecio de siempre


Abg. Carolina Ibarra
Directora-Unidad Operativa de Contrataciones
Ministerio de la Defensa Pública



Visión: Una Defensa Pública efectiva, confiable y reconocida por su labor institucional en la promoción del acceso a la justicia y la protección de los derechos humanos de las personas en situación de vulnerabilidad.

Ministerio de la Defensa Pública
Avda. Aviadores del Chaco 2432 casi Santa Teresa
Tel: (021) 289 3000
www.mdp.gov.py



Especificaciones Técnicas

	CÓDIGO DE CATALOGO		ESPECIFICACIONES TÉCNICAS		UNIDAD DE MEDIDA	
1		Antivirus Corporativo con antispymware y antispam	RENOVACIÓN, AMPLIACIÓN Y ACTUALIZACIÓN DE ANTIVIRUS CORPORATIVO, CON LICENCIA POR 3 (AÑOS)	UNIDAD	UNIDAD	1.813

CONSIDERACIONES GENERALES.

SUITE DE SEGURIDAD Y PROTECCIÓN DE SOFTWARE PARA EMPRESAS.
SERVIDOR DE ADMINISTRACIÓN Y CONSOLA ADMINISTRATIVA.

Solución: Kaspersky NEXT EDR Optimum	
1	Información General
1.1	El fabricante de las soluciones ofertadas debe contar con, al menos, 25 años de presencia en el mercado global.
1.2	El fabricante de las soluciones ofertadas debe contar con un equipo de investigación global y con presencia de por lo menos cinco (5) analistas de investigación de amenazas basados en países de Latinoamérica, dedicados a la investigación y el análisis de amenazas para la región.
1.3	El fabricante de las soluciones ofertadas debe contar con experiencia probada en el descubrimiento de vulnerabilidades desconocidas, APTs y malware avanzado y debe haber descubierto al menos dos (2) vulnerabilidades agregadas a la lista de Common Vulnerabilities and Exposures (CVE) durante el 2023.
2	Características Generales
2.1	Se debe proveer una solución tecnológica que incluya una poderosa protección de endpoints basada en IA, controles de seguridad flexibles y características de EDR incorporadas.
2.2	La solución debe contar con una consola fácil de usar, opciones de implementación en la nube y on-premises, así como también una variedad de funciones que simplifiquen la vida del usuario, reduciendo la complejidad y aumentando la eficiencia.

2.3	La solución debe proteger endpoints y servers, sean estos Windows, Linux, macOS, así como también dispositivos móviles iOS y Android.
2.4	La solución debe disponer de una única licencia que debe permitir el uso de la consola nube u on-premise, como así también de todos los endpoints y servers que disponga la organización, independientemente del sistema operativo del dispositivo en cuestión.
2.5	La solución debe permitir la implementación de puntos de distribución en diferentes segmentos de red o ubicaciones geográficas de la organización que permita la distribución de actualizaciones, sondeo de red, instalación remota de aplicaciones, obtención de información sobre equipos de un grupo de administración, y/o difusión de dominio, entre otras.
2.6	La solución debe incluir una infraestructura de servicios en la nube que brinde acceso a la base de conocimientos del fabricante, ofreciendo un recurso en línea que permita conocer la reputación de los archivos, los recursos web y el software, garantizando respuestas más rápidas ante nuevas amenazas, mejorando el rendimiento de algunos componentes de protección y reduciendo el riesgo probable de que se produzcan falsos positivos
2.7	La solución debe contar con la capacidad de eliminar remotamente cualquier solución antivirus (propia o de terceros) que esté presente en los endpoints y servidores, sin la necesidad de la contraseña de remoción del actual antivirus;
2.8	La solución debe disponer de la capacidad de instalar remotamente la solución de antivirus en los endpoints y servidores Windows, a través de la administración compartida, login script y/o GPO de Active Directory;
2.9	La solución debe contar con la capacidad de generar paquetes personalizados (autoejecutables) conteniendo la licencia y configuraciones del producto;
2.10	La solución debe disponer de la capacidad de importar la estructura de Active Directory para encontrar máquinas;
2.11	La solución debe contar con la capacidad de monitorear diferentes subnets de red con el objetivo de encontrar máquinas nuevas para que sean agregadas a la protección;
2.12	La solución debe disponer de la capacidad de, al detectar máquinas nuevas en el Active Directory, subnets o grupos de trabajo, automáticamente importar la máquina a la estructura de protección de la consola y verificar si tiene el antivirus instalado. En caso de no tenerlo, debe instalar el antivirus automáticamente;
3	Protección para Endpoints, Consola de Administración, Anti Spam y Reporting
3.1	La solución debe combinar protección basada en firmas, análisis heurístico y de comportamiento, junto con tecnologías asistidas por la nube para proteger los endpoints contra amenazas de malware conocidas, desconocidas y avanzadas.
3.2	La solución debe permitir habilitar la protección con contraseña con el fin de restringir el acceso de los usuarios a la solución en la estación de trabajo según los permisos que se le otorgaron (por ejemplo, permiso para salir de la aplicación).
3.3	La solución debe proporcionar mecanismos de autoprotección con el fin de evitar que otras aplicaciones realicen acciones que puedan interferir con el funcionamiento de la solución propuesta

3.4	La solución debe permitir realizar un análisis personalizado para cualquiera de los siguientes objetos: Memoria del sistema, Objetos cargados en el inicio del sistema operativo, Copia de seguridad del sistema operativo, Buzón de correo de Microsoft Outlook, Unidades de disco duro, Unidades extraíbles y unidades de red o Cualquier archivo seleccionado
3.5	La solución debe permitir realizar un análisis en segundo plano de manera que la aplicación no le muestre ninguna notificación al usuario y que tenga menos impacto en los recursos del equipo, para cualquiera de los siguientes objetos: objetos de inicio, el sector de arranque, la memoria del sistema y la partición del sistema
3.6	La solución debe permitir establecer una programación para el análisis, de manera que se pueda realizar de forma manual o según programación
3.7	La solución debe permitir analizar archivos compuestos de formatos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos comprimidos
3.8	La solución debe permitir analizar archivos protegidos con contraseña
3.9	La solución debe incorporar un componente de protección frente a amenazas web que permita evitar la descarga de archivos maliciosos de Internet y también bloquee sitios web maliciosos y de phishing
3.10	La solución debe analizar tráfico HTTP, HTTPS y FTP
3.11	La solución debe bloquear el tráfico HTTP que no cumple con los estándares RFC
3.12	La solución debe incluir un componente de protección frente a amenazas en el correo que permita analizar los archivos adjuntos de mensajes de correo electrónico entrantes y salientes en busca de virus y otras amenaza
3.13	La solución de protección frente a amenazas en el correo debe ser compatible con POP3, SMTP, IMAP y NNTP
3.14	La solución de protección frente a amenazas en el correo debe intentar desinfectar un objeto infectado en un mensaje entrante o saliente. Si el objeto no se puede desinfectar, el componente de protección en el correo deberá eliminar el objeto infectado y añadir información sobre la acción realizada al asunto del mensaje, por ejemplo: [Se ha procesado el mensaje] <asunto del mensaje>
3.15	La solución debe incluir un componente de protección frente a amenazas en la red que monitoree el tráfico de red entrante en busca de actividad característica de los ataques de red
3.16	La solución debe bloquear la conexión de red con el equipo atacante
3.17	La solución debe incluir una base de datos que ofrezca descripciones de los tipos de ataques de red actualmente conocidos y los modos para contrarrestarlos
3.18	La solución debe bloquear el equipo que realiza el ataque y restringir el envío de paquetes de red durante un periodo determinado de al menos una hora.
3.19	La solución debe permitir seleccionar el protocolo y el puerto que se van a usar para la comunicación y permitir actividades de red específicas
3.20	La solución debe permitir activar y administrar la protección contra los siguientes tipos de ataques a la red, mínimamente: Inundación de red (flooding) ataques de tipo "Port scan", Ataques de spoofing de MAC
3.21	La solución debe incluir un componente de Firewall de escritorio que bloquee las conexiones no autorizadas al equipo mientras se trabaja en Internet o en la red local.
3.22	El componente de firewall de escritorio debe controlar la actividad de red de las aplicaciones en el equipo
3.23	El componente de firewall de escritorio debe proporcionar protección del equipo con la ayuda de bases de datos antivirus, el servicio de inteligencia global en la nube y reglas de red predefinidas

3.24	El componente de firewall de escritorio debe incluir un componente prevención de intrusiones en el host que proporcione acceso controlado de las aplicaciones a los recursos, procesos y datos personales del sistema operativo mediante el uso de derechos de aplicación
3.25	El componente de firewall de escritorio debe controlar la actividad de la red sobre el protocolo seleccionado: TCP, UDP, ICMP, ICMPv6, IGMP y GRE
3.26	El componente de firewall de escritorio debe permitir seleccionar los adaptadores de red que pueden enviar o recibir paquetes de red
3.27	El componente de firewall de escritorio debe permitir restringir el control de los paquetes de red según su período de vida (TTL)
3.28	El componente de firewall de escritorio debe, de forma predeterminada, crear un conjunto de reglas de red para cada grupo de aplicaciones que la solución detecta en el equipo
3.29	La solución debe incluir un componente de prevención de ataques a nivel de USB impide que dispositivos USB infectados que emulan un teclado se conecten al equipo
3.30	El componente de prevención de ataques a nivel de USB debe permitir que los dispositivos USB que el sistema operativo identifique como teclados y que estén conectados al equipo antes de instalar el componente se consideren autorizados después de la instalación del componente
3.31	El componente de prevención de ataques a nivel de USB debe bloquear automáticamente el dispositivo USB si el código de autorización se introduce incorrectamente un número de veces especificado
3.32	El componente de prevención de ataques a nivel de USB debe permitir utilizar un teclado en pantalla para autorizar dispositivos USB que no permitan introducir caracteres aleatorios (p.ej., escáneres de códigos de barras)
3.33	La solución debe incluir un componente de protección AMSI diseñado para ser compatible con Antimalware Scan Interface de Microsoft
3.34	El componente de protección AMSI debe permitir configurar el análisis de protección AMSI para archivos compuestos, como archivos de almacenamiento, paquetes de distribución o archivos en formatos de Office
3.35	La solución debe incluir un componente de prevención de exploits que permita detectar código de software diseñado para aprovechar vulnerabilidades en el equipo y, a través de estas, realizar acciones maliciosas o abusar de los privilegios de administración
3.36	El componente de prevención de exploits debe incluir un mecanismo de protección de la memoria de procesos del sistema, de manera que la solución bloquee los procesos externos que intentan acceder a los procesos del sistema
3.37	La solución debe incluir un componente de prevención de intrusiones en el host que evite que las aplicaciones realicen acciones que puedan resultar peligrosas para el sistema operativo
3.38	El componente de prevención de intrusiones en el host debe controlar el funcionamiento de las aplicaciones mediante el uso de derechos de las aplicaciones
3.39	Los derechos de las aplicaciones debe incluir los siguientes parámetros de acceso: - Acceso a recursos del sistema operativo (por ejemplo, opciones de inicio automático y claves de registro) - Acceso a datos personales (como archivos y aplicaciones)

3.40	El componente de prevención de intrusiones en el host debe activar la protección del acceso a audio y vídeo, de manera que se evite que los ciberdelincuentes puedan usar programas especiales para intentar obtener acceso a dispositivos que graban audio y vídeo (como micrófonos o cámaras web), controlando cuándo las aplicaciones reciben una transmisión de audio o vídeo y protege los datos contra la interceptación no autorizada
3.41	La solución debe incluir un componente de motor de reparación que le permita revertir las acciones realizadas por aplicaciones maliciosas en el sistema operativo
3.42	El componente de motor de reparación debe permitir anular la actividad de malware en el sistema operativo a los siguientes tipos de actividad de malware: <ul style="list-style-type: none"> - Elimina los archivos ejecutables que el malware ha creado (en cualquier tipo de soporte, excepto unidades de red) - Elimina los archivos ejecutables creados por programas en los que el malware se ha infiltrado - Restaura los archivos que el malware ha modificado o eliminado - Elimina las claves del registro que el malware ha creado - No restaura las claves del registro que el malware ha modificado o eliminado - Finaliza los procesos iniciados por el malware - Finaliza los procesos en los que haya penetrado una aplicación maliciosa - No reanuda procesos que el malware haya suspendido - Bloquea la actividad de red del malware - Bloquea la actividad de red de los procesos en los que el malware se ha infiltrado.
3.43	La solución debe incluir un componente de control web que permita regular el acceso de los usuarios a los recursos web
3.44	El componente de control web debe permitir supervisar tráfico HTTP y HTTPS
3.45	El componente de control web debe permitir configurar el acceso a los sitios web a través de estos criterios: <ul style="list-style-type: none"> - Categorías de sitios web - Tipo de datos - Direcciones individuales
3.46	El componente de control web debe permitir la creación de reglas de acceso a recursos web mediante el uso de filtros y acciones que la solución realiza cuando el usuario visita recursos web
3.47	El componente de control web debe utilizar al menos los siguientes filtros: <ul style="list-style-type: none"> - Filtrar por contenido y tipo de datos - Filtrar por direcciones de recursos web - Filtrar por nombres de usuarios y grupos de usuarios
3.48	El componente de control web debe permitir seleccionar alguna de las siguientes acciones: <ul style="list-style-type: none"> - Permitir - Bloquear - Advertir
3.49	La solución debe incluir un componente de control de dispositivos que administre el acceso de los usuarios a dispositivos instalados o conectados al equipo (por ejemplo, discos duros, cámaras o módulos wifi), con el fin de proteger el equipo de infecciones cuando se conectan los dispositivos; y se evitan pérdidas o fugas de datos

3.50	El componente de control de dispositivos debe controlar el acceso a los siguientes niveles: - Tipo de dispositivo - Bus de conexión - Dispositivos de confianza
3.51	El componente de control de dispositivos debe permitir la creación de reglas de acceso que permitan ajustar la configuración que determina qué usuarios pueden usar dispositivos instalados en un equipo o conectados a él
3.52	El componente de control de dispositivos debe permitir crear reglas del acceso para los siguientes tipos de dispositivo, mínimamente: - Discos duros - Unidades extraíbles (incluidas las unidades flash USB) - Disquetes - Unidades de CD/DVD - Dispositivos portátiles (MTP) - Impresoras locales - Impresoras de red - Módems - Unidades de cinta - Dispositivos multifuncionales - Lectores de tarjetas inteligentes - Dispositivos Windows CE USB ActiveSync - Adaptadores de red externos - Bluetooth - Cámaras y escáneres
3.53	El componente de control de dispositivos debe proporcionar funciones de Anti-Bridging con el fin de impedir establecer conexiones de red simultáneas en un equipo para prevenir la creación de puentes de red.
3.54	La solución debe incluir un componente de control de aplicaciones que permita gestionar el inicio de aplicaciones en los equipos de los usuarios
3.55	El componente de control de aplicaciones debe permitir crear categorías de aplicaciones que se quieren gestionar
3.56	El componente de control de aplicaciones debe permitir crear reglas en la directiva para el grupo de administración
3.57	El componente de control de aplicaciones debe poder funcionar en dos modos: - Lista de rechazados. En este modo, el control de aplicaciones autoriza a todos los usuarios a que inicien todas las aplicaciones, excepto aquellas que se prohíben en las reglas de control de aplicaciones. - Lista de permitidos: en este modo, el control de aplicaciones bloquea a los usuarios para que no inicien ninguna aplicación, excepto las que se permiten y no están prohibidas en las reglas de control de aplicaciones.
3.58	El componente de control de aplicaciones debe crear una imagen propietaria de los programas que garantizan el funcionamiento normal del sistema operativo
3.59	El componente de control de aplicaciones debe realizar un inventario de los archivos con los siguientes formatos: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX y SCR, cuando se añade contenido manualmente
3.60	La solución debe incluir características básicas de Endpoint Detection and Response (EDR)
3.61	La solución debe permitir agregar un Widget de alertas de EDR que muestre información sobre la cantidad de alertas en los dispositivos durante el último mes

3.62	La solución debe contar con la capacidad de mostrar toda la información disponible sobre la amenaza detectada
3.63	La solución debe proveer un gráfico de la cadena de desarrollo de amenazas que proporcione información visual sobre los objetos involucrados, como procesos clave en el dispositivo, conexiones de red, bibliotecas y subárboles de registro.
3.64	La solución debe incluir una API abierta (OpenAPI) que permita personalizar escenarios operativos y tareas a través de la consola de gestión central
3.65	La solución debe incluir, dentro de su licenciamiento, la conexión a una infraestructura de servicios en la nube que brinde acceso a la base de conocimientos en línea del fabricante, que permita conocer la reputación de los archivos, los recursos web y aplicaciones, de manera que la solución de una respuesta más rápida a las amenazas, mejore el rendimiento de los componentes de protección y reduzca la probabilidad de falsas alarmas.
3.66	La solución debe contar, dentro de su licenciamiento, con integración y acceso con un Portal de Inteligencia contra Amenazas, que permita consultar información sobre la reputación de archivos y URLs.
3.67	La solución debe ofrecer un proceso de recomendaciones de respuesta a alertas
3.68	La solución debe proveer información sobre el dispositivo protegido en el que se produce la alerta (por ejemplo, nombre del dispositivo, dirección IP, dirección MAC, lista de usuarios, sistema operativo, entre otros).
3.69	La solución debe proveer información sobre el objeto detectado.
3.70	La solución debe proveer información relacionada con los cambios en el registro asociados con la alerta.
3.71	La solución debe proveer información de historial de la presencia del archivo en el dispositivo.
3.72	La solución debe proveer información de las acciones de respuesta realizadas por la aplicación.
3.73	La solución debe ofrecer la posibilidad de aislar dispositivos de la red a petición (manualmente) o como una acción automática para responder a las amenazas detectadas, desde la consola de administración central sin intervención del usuario final.
3.74	La solución debe incluir una funcionalidad que permita obtener información sobre los dispositivos que se encuentren aislados de la red
3.75	La solución debe permitir establecer exclusiones de aislamiento de red. Es decir que las conexiones de red que cumplan las condiciones de la exclusión especificada no se bloquearán en los dispositivos después de que se active el aislamiento de red.
3.76	La solución debe incluir, dentro de su licenciamiento, un SandBox basado en Nube que permita detectar amenazas complejas en los equipos de los usuarios.
3.77	La solución debe permitir enviar automáticamente al Sandbox basado en Nube los archivos que es necesario analizar.
3.78	La solución debe permitir ver los informes de alertas detectadas por la tecnología de Sandbox basado en Nube.
3.79	La solución debe permitir crear tareas de Análisis de IoC con el fin de encontrar indicadores de compromiso en el dispositivo y realizar acciones de respuesta a la amenaza.
3.80	La solución debe permitir crear tareas de análisis de IoC grupal o local. Es decir que se permita ejecutar en un solo dispositivo o en varios de manera simultánea.
3.81	La solución debe permitir crear tareas de análisis de IoC de forma automática en respuesta a una amenaza detectada por el Sandbox basado en nube.

3.82	La solución debe permitir ejecutar una de las siguientes acciones de respuesta disponibles para los IoC detectados: - Aislar el dispositivo de la red. - Ejecutar análisis de áreas críticas. - Poner la copia en cuarentena y eliminar el objeto
3.83	La solución debe incluir un componente de cifrado de datos que permita cifrar las carpetas y los archivos almacenados en las unidades locales y extraíbles, o las unidades extraíbles y los discos duros por completo, con el fin de minimizar el riesgo de filtraciones de información que se puede producir en caso de pérdida o robo del equipo portátil, unidad extraíble o disco duro, o cuando usuarios y aplicaciones no autorizados acceden a los datos
3.84	El componente de cifrado de datos debe utilizar el algoritmo de cifrado AES (del inglés "Advanced Encryption Standard") con sus variantes de cifrado "fuerte" (AES256) como la de cifrado "ligero" (AES128)
3.85	El componente de cifrado de datos debe ofrecer las siguientes características de protección de datos: - Cifrado de archivos en unidades locales del equipo - Cifrado de unidades extraíbles - Gestión de reglas de acceso de las aplicaciones a los archivos cifrados - Creación de paquetes cifrados - Cifrado de disco completo
3.86	El componente de cifrado de datos debe permitir realizar cifrado de disco completo con la tecnología de cifrado propietaria del fabricante
3.87	El componente de cifrado de datos debe ser compatible con los sistemas de archivos FAT32, NTFS y exFAT.
3.88	El componente de cifrado de datos debe ser capaz de continuar con las operaciones de cifrado de disco completo en caso que el equipo sea apagado o entre en estado de hibernación o suspensión
3.89	El componente de cifrado de datos debe permitir el uso de la tecnología de Single Sign-On (SSO) con el fin de iniciar sesión automáticamente en el sistema operativo utilizando las credenciales del agente de autenticación
3.90	El componente de cifrado de datos debe permitir gestionar el cifrado de Microsoft BitLocker desde la consola central
3.91	El componente de cifrado de datos debe incluir los siguientes estados de cifrado: - No cumple la directiva; cancelado por el usuario. El usuario ha cancelado el cifrado de datos. - No cumple la directiva debido a un error. Error de cifrado de datos; por ejemplo, falta una licencia. - Aplicando la directiva. Reinicio necesario. Cifrado de datos en curso en el equipo. Reinicie el equipo para completar el cifrado de datos. - No se ha especificado ninguna directiva de cifrado. El cifrado de datos está desactivado en la configuración de directiva. - No compatible. Los componentes de cifrado de datos no están instalados en el equipo. - Aplicando la directiva. El cifrado y el descifrado de datos está en curso en el equipo.
3.92	El componente de cifrado de datos debe permitir ver las estadísticas del cifrado en el dashboard de la solución
3.93	El componente de cifrado de datos debe proveer una utilidad de restauración que se pueda emplear para la recuperación de datos

3.94	El componente de cifrado de datos debe permitir la creación de un disco de rescate del sistema operativo que sirva cuando no se pueda acceder a un disco duro cifrado por alguna razón y el sistema operativo no se puede cargar
4	Proteccion para Office 365
4,1	La Solución de Seguridad debe integrarse con Microsoft Office 365 de manera nativa mediante Microsoft Office 365 API sin influir ni requerir cambios en los flujos de tráfico de correo electrónico.
4,2	La solución debe disponer de una consola de gestión que permita la configuración y administración multi-usuario de todas las capacidades ofertadas de manera integral, facilitando la gestión de la seguridad en Microsoft Office 365.
4,3	La solución no debe requerir cambio alguno en los registros MX de correo o en las aplicaciones de Microsoft Office 365 para su funcionamiento.
4,4	La solución debe de validar de Spam, Phishing, Ransomware, BEC, amenazas conocidas y desconocidas en tiempo real para correos electrónicos entrantes, salientes y aquellos que fluyen internamente en la propia instancia de Microsoft Office 365.
4,5	La solución debe utilizar heurística avanzada, aislamiento de procesos, aprendizaje automático y otras tecnologías de última generación para proteger a las empresas que utilizan Microsoft Exchange Online, Microsoft Teams, Microsoft OneDrive y Microsoft SharePoint Online contra el ransomware, archivos adjuntos maliciosos, spam, phishing, correos electrónicos que comprometen la seguridad de la empresa (BEC) y amenazas desconocidas.
4,6	La solución debe cumplir con el Reglamento General de Protección de Datos (RGDP) y protección de los datos.
4,7	La solución debe de contar con tecnologías de detección Anti-Spam, Anti-Phishing, Anti-Malware, Anti-Ransomware, Anti-BEC & capacidades de filtrado de contenido.
4,8	La solución debe de contar con tecnologías proactivas para la detección de amenazas avanzadas o de día 0.
4,9	La solución debe de contar con tecnologías de detección avanzadas para la detección y neutralización de amenazas del tipo Ransomware.
4.10	La solución debe disponer de capacidades de escaneo bajo demanda sobre buzones de correo pudiendo seleccionar. <ul style="list-style-type: none"> - Grupos de usuarios - Usuarios - Todos los usuarios
4,11	La solución debe poder clasificar los correos basura en dos categorías: Spam y correos masivos y poder definir las acciones a tomarse en cada uno de los casos.

4,12	La solución debe contar con capacidades de generar direcciones de lista blanca y negra para cada uno de los módulos de seguridad que propone.
4,13	La solución debe disponer de funciones de validación y autenticación del remitente de manera automática que incluyan: <ul style="list-style-type: none"> - DKIM - DMARK - SPF
4,14	La solución debe de disponer de modulo anti malware para la detección oportuna de amenazas conocidas, desconocidas y avanzadas en Microsoft Exchange Online, Microsoft OneDrive, Microsoft SharePoint Online y Microsoft Teams bajo tecnologías de: <ul style="list-style-type: none"> - Firmas, - Análisis heurísticos - Comportamiento.
4,15	La solución debe de disponer una visibilidad unificada de las amenazas detectadas por los servicios de seguridad base de Microsoft Exchange Online mediante la visualización de una cuarentena única.
4,16	Debe contar con cuadros de mandos, KPIs y reportes de seguimientos de las detecciones realizadas.
4,17	La solución no debe almacenar datos sensibles como usuarios y contraseñas y para esto debe de poder integrarse con Microsoft Office 365 mediante OAuth 2.0
4,18	La protección de anti-malware para Microsoft SharePoint Online debe permitir la exclusión y selección de sitios protegidos.
4,19	La protección de anti-malware para Microsoft OneDrive debe permitir la exclusión y selección de usuarios protegidos.
4,20	Debe contar con protección frente a virus, troyanos y otras clases de malware para MS Teams.
4,21	Debe disponer de un módulo de supervisión de fuga de datos con el objetivo del descubrimiento de información confidencial transmitida y almacenada por los usuarios en los buzones de correo de Exchange Online, en los almacenamientos de OneDrive y en los sitios de SharePoint Online de la organización relacionadas con datos de tarjetas de crédito.
4,22	La solución debe contar con capacidades de escaneo retrospectivo de amenazas que incluya los buzones de correo y de Ms Office 365 y los repositorios de datos de OneDrive.
4,23	Debe contar con protección basada en firmas mediante aprendizaje automático junto con análisis conductuales y heurísticos avanzados.
4,24	Debe usar una combinación de SPF (marco de directivas de remitente), DKIM (DomainKeys Identified Mail), validación de correo electrónico de DMARC (Autenticación de mensajes, informes y conformidad basada en dominios) y el método de detección de similitudes para detectar y prevenir spoofing y phishing de correos electrónicos, ataques BEC y spam.

4,25	Debe proveer heurística mediante redes neurales de aprendizaje profundo.
4,26	Debe incluir protección contra ataques de inyección de código y mailsplit/spoofing que son posibles debido a los errores de los clientes de correo.
4,27	Debe contar con mecanismo de detección de spam al nivel de la dirección IP.
4,28	Debe poder rastrear el intercambio de datos confidenciales de texto o imágenes que se almacenan y transmiten dentro y fuera de su organización, por lo que puede considerar acciones para impedir posibles fugas.

ASPECTOS GENERALES

1. El proveedor local deberá contar con por lo menos 1 técnico con certificación CEH o CEH MASTER o similar.
2. El proveedor local deberá contar como mínimo con 3 técnicos certificados con las certificaciones avanzadas del producto de detección y respuesta extendida XDR.
3. El proveedor local deberá contar como mínimo con 3 técnicos con certificaciones de cifrado.
4. El proveedor local deberá contar con por lo menos 3 técnicos con certificaciones en protección de servidores de correo antispam.
5. Los técnicos certificados deben ser personales dependientes de la Empresa Oferente, se deben acompañar certificados de inscripción en IPS.
6. Contar con 10 contratos o facturas de la provisión de Software de Seguridad entre los años 2020, 2021 y 2022.
7. El proveedor local deberá contar con el mayor nivel de certificación/partnership posible la marca ofertada, para garantizar el buen servicio y respaldo del soporte local.
8. El proveedor local deberá tener la Certificación ISO 9001: "Sistema de Gestión de Calidad" y la Certificación ISO 27001: "Sistema de Gestión de Seguridad de la Información" para garantizar el buen servicio y respaldo del soporte local.
9. El proveedor deberá presentar autorización del fabricante expresamente dirigido a la convocante refiriendo el nro. de ID del llamado.
10. El fabricante de las soluciones ofertadas debe brindar soporte a través de una página web, email y línea telefónica.
11. El fabricante de las soluciones ofertadas debe contar con por lo menos 25 años de presencia en el mercado global.
12. El fabricante de las soluciones ofertadas debe contar con un equipo de investigación global y con presencia de por lo menos cinco (5) analistas de investigación de amenazas en Latinoamérica, dedicados exclusivamente a la investigación y el análisis de amenazas para la región.
13. El fabricante de las soluciones ofertadas debe contar con experiencia probada en el descubrimiento de vulnerabilidades desconocidas, APTs y malware avanzado y debe

haber descubierto al menos dos (2) vulnerabilidades agregadas a la lista de Common Vulnerabilities and Exposures (CVE) en los últimos meses.

PLATAFORMA ANTI SPAM

- 14.
15. Ítem 3: Plataforma Anti-Spam Correo Electrónico
16. La solución debe ser proporcionada mediante Imagen de Software en formato ISO para el despliegue sobre plataforma virtualizada acorde a modalidad gateway virtual.
17. La solución debe disponer capacidades de integración con plataforma XDR con el objetivo de proporcionar capacidades avanzadas de detección de amenazas que incluyan la utilización de reglas Yara y procesamiento de correos acorde a módulo de Sandbox on-premise.
18. La solución debe ser implementada on-premise y debe disponer de una consola Web de gestión centralizada.
19. Los módulos y/o componentes de la solución deben estar basados en software/appliance de uso específico, con sistema operativo, base de datos y servicios configurados para óptimo rendimiento y securitización por el fabricante de la solución.
20. La solución debe proveer un procedimiento por el cual se pueda realizar una actualización de todos y cada uno de los dispositivos que la componen, sin la necesidad de realizar un corte de servicio y sin afectar al resto de los componentes
21. La solución debe inspeccionar en tiempo real el tráfico de correo (Entrada & Salida) para la remoción de todo tipo de amenazas, virus, worms, troyanos y otros tipos de programas maliciosos incluyendo correos indeseados
22. La solución debe de contar con tecnologías de detección Anti-Spam, Anti-Phishing, Anti-Malware, Anti-Ransomware y de filtrado de contenido.
23. La solución tiene la capacidad de integración con servicios de reputación locales sin la necesidad de enviar datos fuera de la organización.
24. La solución dispone de capacidades para el desempaquetado y análisis de archivos compuestos como por ejemplo archivos comprimidos.
25. La solución debe de detectar, bloquear y desinfectar mensajes de correos electrónicos infectados, así como sus anexos con la posibilidad de generar una copia de los mismos al ser almacenada en un Backup.
26. La solución debe detectar y bloquear mensajes que contengan anexos con macros (Por ejemplo, archivos en formato Microsoft Office con macros), eliminar mensajes o sus anexos con la posibilidad de generar una copia de los mismos al ser almacenada en un Backup.
27. La solución debe detectar y bloquear mensajes cifrados, eliminar mensajes o sus anexos con la posibilidad de generar una copia de los mismos al ser almacenada en un Backup.
28. La solución debe disponer de capacidad de filtrado de contenido de los mensajes mínimamente acorde al nombre, tamaño y tipo de anexo, determinando el formato indiferentemente de su extensión, así como eliminar mensajes o sus anexos con la posibilidad de generar una copia de los mismos al ser almacenada en un Backup.

29. Los mensajes que se encuentran en el backup deben poder ser guardados y descargados, así como reenviados a su destinatario original u otros destinatarios a ser seleccionados.
30. La solución debe de procesar los mensajes, acorde a las reglas de seguridad estipuladas para los grupos de remitentes y destinatarios.
31. La solución debe poder validar el remitente acorde a la autenticación del remitente utilizando tecnologías SPF, DKIM y DMARC.
32. La solución debe poder firmar correos salientes mediante tecnologías DKIM.
33. La solución debe permitir la inclusión de un mensaje de alerta en el subject del correo en caso que anexos peligrosos o indeseados sean detectados.
34. La solución debe permitir la definición de listas de correo blancas/negras globales y personales.
35. La solución debe contar con tecnologías de validación de imágenes y anexos gráficos para la detección de mensajes de Spam.
36. La solución debe identificar archivos sospechosos, potencialmente peligrosos, protegidos con contraseña, así como objetos que han tenido algún error en su análisis. Los mismos deben ser adicionalmente enviados al módulo de Sandbox para su procesamiento.
37. La solución debe poder eliminar mensajes o sus anexos para archivos sospechosos, potencialmente peligrosos, protegidos con contraseña, así como objetos que han tenido algún error en su análisis con la posibilidad de generar una copia de los mismos al ser almacenada en un Backup.
38. La solución debe proporcionar capacidades de detección y protección ante ataques del tipo Business Email Compromise (BEC).
39. La solución debe disponer de tecnologías para la detección de Spam basado en el reconocimiento de dominios spoofed (look-alike).
40. La solución debe de contar con tecnologías proactivas para la detección de amenazas avanzadas o de día 0.
41. La solución debe de contar con tecnologías de detección avanzadas para la detección y neutralización de amenazas del tipo ransomware.
42. En caso de objetos infectados la solución debe poder configurar la realización de las siguientes acciones:
 43. Desinfectar
 44. Eliminar Anexo
 45. Borrar mensaje
 46. Rechazar mensaje
 47. Ignorar
48. La solución permite la configuración de notificaciones por lo menos a las siguientes direcciones (Administradores, Remitente, Destinatario, adicionales).
49. La solución debe contar con un sistema de alimentación de contenido por parte del fabricante que proporcione información sobre nuevas amenazas, y bases de reputación. Dicha información debe ser actualizada en forma automática y en tiempo real permitiendo enriquecer el motor de análisis de amenazas de la solución.

1. La totalidad del análisis y operación de la solución debe realizarse en forma local, solo permitiéndose el envío de hashes cuando sea necesario. La solución no debe enviar ninguna otra información sensible fuera de la institución.
2. La solución debe disponer soporte para la integración con Microsoft Active Directory y Open LDAP.
3. La solución incluye el acceso al Backup personal mediante Single Sign-On (SSO) acorde a integración con directorio LDAP.
4. La solución permite la utilización de expresiones regulares para la composición de reglas de filtrado.
5. La consola de administración Web, proporciona capacidades de acceso basado en roles y perfiles de usuario. Role Based Access Control (RBAC).
6. La solución cuenta con capacidades para el envío de eventos a un sistema (SIEM) utilizando protocolo Syslog.
7. La solución permite la generación de reportes y cuadros de mando acorde al periodo seleccionado (día, semana, mes, año) en formato PDF.
8. La solución debe proporcionar un cuadro de mando web que incluye como mínimo información de: Estado de la Salud del Sistema, Mensajes Procesados (Entrada/Salida) & Amenazas Detectadas.
9. La consola Web permite la personalización del cuadro de mando el cual permite configurar múltiples widgets a criterio del administrador de la solución.
10. La solución debe poder gestionar múltiples dominios de correo electrónico.
11. La solución debe permitir generar reportes en forma manual o programados a intervalos de tiempo determinados.