IPnet Consulting
REDES Y COMUNICACIONES
NIT: 900584931-2

Bogotá, octubre 04 de 2025

Señores
MUNICIPIO DE FUSAGASUGA
Fusagasuga.-

De acuerdo a su amable solicitud A continuación les cotizamos a Uds., los elementos de la referencia, repuestos, y otros elementos, para atender las necesidades planteadas.

La información técnica que permite verificar que los bienes se acogen a las exigencias de la necesidad planteada y determinadas por el área técnica, se puede comprobar mediante la consulta de las marcas y modelos en cada uno de los website del correspondiente fabricante y si es del caso el proponente aportara tal información si es requerido por la entidad.

Descripción del producto: LICENCIA DE SOFTWARE PARA CORTAFUEGOS FORTINET 401F FG4H1FT923904283

Nombre resumido: Licencia de suscripción para MAXIMO 500 endpoints **(DOS (2) años)**

Detalles principales:

- **Tipo de servicio**: Suscripción anual — Incluye FortiClient con capacidades de **EPP (Endpoint Protection Platform)**, **APT (Advanced Persistent Threat defense)**, y agente **VPN/ZTNA (Zero Trust Network Access)**.
- Además, incluye soporte continuo con **FortiCare 24x7**. La gestión se realiza a través de **EMS (Endpoint Management Server)** alojado en **FortiCloud. Cobertura**: Hasta **500 endpoints** (usuarios o dispositivos).
- **Duración**: 1 año de suscripción.
- **Soporte incluido**: Servicio completo de **FortiCare Premium** o **FortiCare 24x7** para asistencia continua, actualizaciones y mantenimiento.

Los compontenentes de este producto son:

- **FCZ-15-0401F-100-02-00**
  Descripción: Licencia de **Advanced Malware Protection / Antivirus / FortiSandbox (AMP)** para FortiGate-401F — protección contra malware, análisis en sandbox y firmas
- **FCZ-15-0401F-108-02-00**
  Descripción: Licencia del servicio **IPS (Intrusion Prevention Service)** para FortiGate-401F — detección y bloqueo de intentos de intrusión y exploits.

- **FCZ-15-0401F-112-02-00**
  Descripción: Licencia de **Web / URL Filtering (y/o filtrado DNS / contenido multimedia)** — control de acceso web por categorías/URL y filtrado de contenido para FortiGate-401F.
- **FCZ-15-0401F-114-02-00 AS Services FortiGate-401F**
- **FCZ-15-0401F-149-02-00**
  Descripción (confirmado / mapeo): Asociado a servicios de **Threat Detection / Indicator of Compromise (IOC) / Threat Intelligence** (servicios de detección/telemetría). **Confirmado** que 149 se usa para IOC/Threat Detection en otras familias Fortinet; por tanto para 0401F es muy probable que represente **servicio de detección de compromisos / Threat Detection. (Recomiendo confirmar duración / alcance con el distribuidor).**
- **FCZ-15-0401F-208-02-00**
  Descripción : SKU de **servicio complementario / bundle** (podría ser licencia de algún complemento de FortiAnalyzer, FortiGuard o extensión de reporting).
- **FCZ-15-0401F-241-02-00**
  Descripción : Variante de **servicio de soporte / renovación FortiCare (24x7 web support / acceso a portal)** o SKU de co-terminación/renovación. Hay listados de partners que usan sufijos similares para soporte/renovación por modelo. Confirmar alcance exacto (SLA, R&R, depot locales).
- **FCZ-15-0401F-242-02-00**
  Descripción: Otra **variante de FortiCare / renovación** (nivel/paquete distinto al 241/243). Verificar con distribuidor si corresponde a "FortiCare Premium", "Advanced R&R" u otro add-on.
- **FCZ-15-0401F-243-02-00**
  Descripción: Licencia de tipo "Premium / Advanced Return & Replace" o un SKU de FortiCare con reemplazo avanzado.

Valor de 485 Licencias = numero de equipos gestionados (sin incluir el IVA 19%)	**$ 81.500.000**
Valor IVA de 485 Licencias (IVA 19%)	**$ 15.485.000**
Valor de 485 Licencias = numero de equipos gestionados (incluye el IVA 19%)	**$ 96.985.000**

Descripción del producto: SERVICIOS GESTIONADO DE SOPORTE FIREWALL MARCA: FORTINET MODELO 401F (UN (1) año)

IPNet Consulting
REDES Y COMUNICACIONES
NIT: 900584931-2

OBJETO: Proveer un servicio gestionado de seguridad perimetral sobre el equipo Fortinet FortiGate 401F ya adquirido por la entidad, incluyendo monitoreo continuo, administración de políticas, actualizaciones, soporte técnico especializado y generación de informes, en cumplimiento con la normativa del Estado colombiano.	
Incluye los siguientes servicios:	
Administración remota	Gestión completa de configuración, políticas y reglas de seguridad del FG-401F
Monitoreo 24/7	Supervisión continua de logs, alertas, consumo y eventos críticos
Gestión de cambios	Aplicación de cambios bajo procedimientos definido por la entidad
Actualizaciones de firmware	Planificación y ejecución de actualizaciones del FortiOS conforme al soporte oficial del fabricante
Soporte técnico	Mesa de ayuda para incidentes en modalidad 8*5
Análisis de tráfico	Informes detallados sobre amenazas, ancho de banda, uso de aplicaciones
Respaldo de configuración	Respaldos periódicos automáticos, con recuperación ante fallos
Auditoría y cumplimiento	Informes para revisión por entes de control (Contraloría, MINTIC, etc.)
Transferencia de conocimiento	Sesiones de capacitación básica para el personal de TI local
Garantía de cumplimiento de SLA	**99.9**
Personal certificado	En Productos como firewall de la marca Fortinet
Suscripcion:	Un (1) Año
Valor Annual sin incluir IVA	$ 25,000,000
Valor IVA 19%	$ 4,750.000
Valor anual incluido IVA (19%)	$ 29,750,000
*** Incluye despliegue inicial para el monitoreo del equipo**	

PROTECCION ANTIVIRUS PARA ENDPOINT (UN (1) año)

Marca y Modelo "ESET PROTECT Cloud + ESET ENDPOINT ANTIVIRUS/SECURITY + ESET SERVER SECURITY + ESET ENDPOINT FOR ANDROID + EL + EFDE + ECOS

"

CARACTERISTICAS GENERALES La solucion debe realizar exploraciones en estado inactivo para poder brindar de esa forma, una protección proactiva mientras el equipo no está en uso

Debe tener un caché local para aumentar el rendimiento de los entornos virtuales, garantizando que el archivo sólo se explora una vez.

El producto debe tener un control web para limitar el acceso a los sitios web por categoría, además de poderle mostrar al usuario una notificación de bloqueo.

El bloqueo web deberá poder asignarse por un rango de tiempo, por grupo y por equipo.

Deberá tener la capacidad de enviar una tarea para la actualización de los parches del sistema operativo.

Dentro del módulo de firewall deberá contar con la funcionalidad de bloqueo de exploits.

"La solución de antivirus debe ejecutar un escaneo únicamente en los siguientes estados en la computadora:

o Protector de pantalla activo

o Sesión de usuario bloqueada

o Sesión de usuario finalizada"

"La solución debe ser capaz de permitir o negar el uso de los dispositivos en base a los siguientes criterios:

o Fabricante

o Modelo

o Número de serie"

"La solución debe ser capaz de definir un listado específico de usuarios quienes pueden hacer uso de los dispositivos. Para dispositivos de almacenamiento, la solución debe permitir configurar únicamente de los siguientes permisos:

o Lectura/Escritura

o Bloqueo

o Solo de lectura

o Advertir"

"Cuando se conecta o usa un dispositivo de almacenamiento, la solución de antivirus debe proporcionar las siguientes opciones:

o Escanear

o No realizar ninguna acción

o Recordar esta acción"

"Sistema de prevención de intrusiones basado en el host (HIPS)

La solución debe tener sistema de prevención de intrusiones basado en el host. El sistema HIPS debe tener los siguientes modos de configuración:

o Modo automático

o Modo inteligente

IPnet Consulting
REDES Y COMUNICACIONES
NIT: 900584931-2

o Modo interactivo

o Modo basado en políticas

o Modo aprendizaje"

El aprendizaje automático avanzado o "machine learning" deberá tener cuatro umbrales: Intenso, Balanceado, Cauteloso y Desactivado.

Debe tener una tarea para aislar a un equipo de la red.

El HIPS debe incluir una inspección a fondo del comportamiento de todos los programas en ejecución, archivos y llaves de registro

Debe contar con filtrado para mantener libre de SPAM a los clientes de correo.

La solución debe capaz de verificar las comunicaciones usando protocolos SSL para hallar amenazas.

"Firewall personal, la solución de antivirus debe contar con un firewall personal. El firewall debe tener los siguientes modos de configuración:

o Modo automático

o Modo interactivo

o Modo basado en políticas

o Modo aprendizaje"

"Las reglas de firewall creadas deberán ser capaces de permitir todas las siguientes acciones:

o Denegar

o Permitir

o Preguntar"

CONSOLA Deberá permitir la ejecución remota de scripts, batch files y paquetes personalizados a través de la consola, de terceros.

Deberá ser una solución que pueda ser usada y sea administrable desde la consola de antivirus en sistemas operativos Windows, Linux y Mac.

"Debe permitir generar grupos de clientes dinámicos y grupos estáticos.

El fabricante debe proporcionar al menos tres diferentes formas de realizar la instalación de la consola de administración.

o Instalador todo en uno

o Instalación por componentes

o Aparato virtual"

"El Appliance virtual debe soportar al menos las siguientes plataformas de virtualización

o VMWare vSphere

o Oracle Virtual Box

o Microsoft Hyper-V

o Azure - ambiente basado en la nube"

La consola de Administración deberá estar basada en Cloud.

Activar el acceso a la consola de antivirus con doble factor de autenticación, deber estar

integrada a la misma consola de antivirus, sin ningún add-on o software adicional.

Debe contar con des instalador de antivirus de terceros.

Debe contar con un módulo específico para la protección contra ransomware.

Deberá tener la capacidad para aplicar durante cierto periodo de tiempo las reglas de control de dispositivo y de control de acceso web a través de la consola de administración.

Deberá contar con etiquetas independiente al LDAP, para identificar y buscar objetos similares.

Obtener a través de la consola de administración de seguridad del punto final inventario de aplicaciones y de hardware de cada uno de los equipos protegidos.

A través de la misma consola de administración de seguridad de punto final debe manejar la tecnología de Sandboxing en nube para el análisis de posibles amenazas, cifrado de los discos de almacenamiento de los puntos finales e integrarse con la solución de detección y respuesta del punto final.

A través de la consola de administración de seguridad del punto final debe ser posible administrar dispositivos móviles iOS y Android.

"Por disponibilidad de la solución de protección de punto final, la consola de administración debe tener la capacidad para construir ambientes distribuidos donde pueda asignarse roles independientes a cada componente, así tener un componente diferente para:

o Administrador de equipos móviles.

o Distribuidor de actualizaciones, paquetes de instalación y reenvío de comunicación entre el punto final y el servidor.

o Detector de puntos finales no administrados.

Y a su vez debe mostrar toda la información en la consola central de administración del punto final de forma nativa."

"La solución debe tener el mecanismo para desinstalar otras soluciones antivirus presentes en el equipo final. Este mecanismo debe ser y estar:

o Integrado al paquete de instalación de la solución de protección de punto final.

o Disponible solamente a través de la misma consola de administración de protección al punto final."

Seguridad del Servidor En servidores que usan "OneDrive for Business" debe explorar los archivos almacenados en esta nube, en búsqueda de algún archivo comprometido o posible malware.

La solución de protección en servidores debe incluir la detección y bloqueo de intrusiones, agregar a lista negra aquellas direcciones que han sido identificadas con este comportamiento malicioso.

La solución deberá agregar de forma automática las exclusiones que correspondan a aplicaciones críticas del servidor.

Optimizar el rendimiento de infraestructuras mixtas (hardware y virtuales) siendo capaz de eliminar la duplicidad de exploraciones en archivos, excluyendo los archivos ya explorados y limpios.

LiveGuard Uso de Sandboxing en la nube para analizar el comportamiento de archivos.

Es posible crear una exclusión por ruta, detección y su hash (SHA-1).

Capacidad de sincronizar su licenciamiento con la nube y la consola de administración en sitio o en la nube.

Detectar un archivo sospechoso ejecutado por primera vez se debe mostrar una advertencia, si el análisis se completa antes de ejecutar el archivo por primera vez, no se muestra el aviso archivo en análisis.

Debe borrar automáticamente las muestras de los archivos/ejecutables en los servidores donde fue analizado el comportamiento.

Capacidad para enviar correos SPAM para su análisis

Debe tener únicamente estos umbrales de detección: desconocido, limpio, sospechoso, altamente sospechoso y malicioso.

Debe tener la siguiente información de un archivo enviado al Sanboxing en la nube: nombre del equipo desde donde se ingresó el archivo, el usuario que lo ingresó, la razón, hash en SHA-1, nombre del archivo ingresado, tamaño del archivo, categoría.

Debe tener protección proactiva, es decir, que el archivo/ejecutable sea bloqueado hasta recibir el resultado del Sandbox en la nube.

Se debe tener capacidad para integrarse con la solución de antivirus o protección del punto final, para tener mayores posibilidades de protección y aplicación de políticas.

Enviar un archivo/ejecutable a través de una consola de administración del punto final.

permite la configuración detallada de políticas por equipo, de modo que el administrador puede controlar lo que se envía y lo que debe ocurrir en función del resultado recibido.

Disk Encryption La solución deberá ser capaz de cifrar los Endpoints con sistemas operativos Windows y MacOS.

La solución deberá disponer de diversas posibilidades de recuperación de Passwords para usuarios remotos que se vean bloqueados.

La solución deberá poder programar las tareas de cifrado sobre los Endpoints deseados con la posibilidad de pausar la ejecución para retomar luego desde el último punto.

La solución deberá poder ser administrada desde la misma consola central junto con las otras soluciones descriptas en el TDR.

La solución de cifrado debe permitir anular la contraseña de inicio de sesión de la estación de trabajo.

Cloud Office SecurityLa solución deberá ser capaz de analizar el contenido de Microsoft Exchange Online vía API.

La solución deberá ser capaz de analizar el contenido de Microsoft OneDrive for Business vía API.

La solución deberá ser capaz de analizar el contenido de Microsoft Sharepoint Online via API.

La solución deberá ser capaz de analizar el contenido de Microsoft Teams via API.

La solución deberá contar con un servicio integrado de Sandboxing ofrecido por el mismo fabricante.

La solución deberá ser capaz de poder discriminar que usuarios se desean proteger.

"La solución deberá ser capaz de discriminar los niveles de protección que se brindará proporciona configuraciones de protección basadas en:

❖ Antispam.

- Anti-Phishing.
- Antimalware."

La solución deberá prestar protección inmediata a los usuarios con una política por defecto.

"La política personalizada puede asignarse a:

- Usuarios: se aplica a usuarios concretos seleccionados manualmente.
- Grupos: política que se aplica a todos los miembros del grupo de usuarios.
- Inquilinos: política que se aplica a todas las entidades del inquilino.
- Grupos de equipos: política que se aplica a un grupo de Team.
- Sitios de SharePoint: política que se aplica a un sitio de SharePoint."

La solución deberá poder proteger de forma inmediata a los futuros usuarios que se creen dentro del Tenant de Microsoft 365.

La solución deberá ser Multi Tenant.

OTRAS CARACTERISTICAS El fabricante deberá tener soporte técnico en castellano.

Que el fabricante directamente brinde servicios de seguridad informática como por ejemplo penetration testing, vulnerability assessment o análisis de GAP

El fabricante deberá tener la capacidad de ofrecer directamente un servicio de caza de amenazas.

El fabricante deberá tener un laboratorio de análisis y detección de malware en Latinoamérica.

Que tenga oficinas de la marca en Latinoamérica y presencia local en el país.

El fabricante deberá tener programas de "colaborador seguro"

Instalación y configuración "El proveedor debe garantizar:

- Configuracion del producto indicaciones del la entidad
- Configuracion los reportes basicos
- El Personal debe ser certficado en la marca del producto que propone para instalacion y configuracion"

Capacitacion Capacitacion a funcionarios que determinen la entidad y proveedor debe garantizar que el personal sea certificado de la marca

Licencias 500 usuarios

Suscripcion 1 año

VALOR UNITARIO $ 34.700.000 (VALOR TOTAL, product excluido de IVA, por norma tributaria)

ELEMENTO	VALOR UNITARIO	IVA ITEM	VALOR ITEM
LICENCIA DE SOFTWARE PARA CORTAFUEGOS FORTINET 401F FG4H1FT923904283, DOS AÑOS	$ 81.500.000	$ 15.485.000	$ 96.585.000
SERVICIOS GESTIONADO DE SOPORTE FIREWALL MARCA: FORTINET MODELO 401F UN AÑO	$ 25.900.000	$ 4.750.000	$ 29.750.000
PROTECCION ANTIVIRUS PARA ENDPOINT (excluido de IVA) UN AÑO	$ 34.700.000	Excluido	$ 34.700.000

IPnet Consulting
REDES Y COMUNICACIONES
NIT: 900584931-2

	SUBTOTAL	IVA	TOTAL OFERTA
	$ 141.200.000	$ 20.235.000	$ 161.435.000

Condiciones comerciales

Forma de Pago:	Contado
Tiempo de entrega:	45 días
Moneda:	Pesos colombianos
Garantía:	1 año
Validez de la oferta:	30 días

Atentamente

Jenny Ariza Caycedo
Ejecutiva de cuenta
IPnet Consulting SAS
Mail: jenny.ariza@ipnetconsulting.com.co
Pbx 4673490 Ext. 304

CONSULTORIA TECNICA Y
SERVICIOS DE INGENIERIA
NIT 800127892.1

35 AÑOS
Hardware & Software Gold Reseller
Centro Autorizado de Servicio
Antivirus Authorized Reseller

Bogota, septiembre 24 de 2025 2409202504

Señores
MUNICIPIO DE FUSAGASUGA
Fusagasuga.-

De acuerdo a su amable solicitud A continuación les cotizamos a Uds., los elementos de la referencia, repuestos, y otros elementos, para atender las necesidades planteadas.

La información técnica que permite verificar que los bienes se acogen a las exigencias de la necesidad planteada y determinadas por el área técnica, se puede comprobar mediante la consulta de las marcas y modelos en cada uno de los website del correspondiente fabricante y si es del caso el proponente aportara tal información si es requerido por la entidad.

Descripción del producto: LICENCIA DE SOFTWARE PARA CORTAFUEGOS FORTINET 401F FG4H1FT923904283

Nombre resumido: Licencia de suscripción para MAXIMO 500 endpoints **(DOS (2) años)**

Detalles principales:

- **Tipo de servicio**: Suscripción anual — Incluye FortiClient con capacidades de **EPP (Endpoint Protection Platform)**, **APT (Advanced Persistent Threat defense)**, y agente **VPN/ZTNA (Zero Trust Network Access)**.
- Además, incluye soporte continuo con **FortiCare 24×7**. La gestión se realiza a través de **EMS (Endpoint Management Server)** alojado en **FortiCloud**. **Cobertura**: Hasta **500 endpoints** (usuarios o dispositivos).
- **Duración**: 1 año de suscripción.
- **Soporte incluido**: Servicio completo de **FortiCare Premium** o **FortiCare 24×7** para asistencia continua, actualizaciones y mantenimiento.

Los compontenentes de este producto son:

- **FCZ-15-0401F-100-02-00**
  Descripción: Licencia de **Advanced Malware Protection / Antivirus / FortiSandbox (AMP)** para FortiGate-401F — protección contra malware, análisis en sandbox y firmas
- **FCZ-15-0401F-108-02-00**
  Descripción: Licencia del servicio **IPS (Intrusion Prevention Service)** para FortiGate-401F — detección y bloqueo de intentos de intrusión y exploits.
- **FCZ-15-0401F-112-02-00**
  Descripción: Licencia de **Web / URL Filtering (y/o filtrado DNS / contenido**

multimedia) — control de acceso web por categorías/URL y filtrado de contenido para FortiGate-401F.

- **FCZ-15-0401F-114-02-00 AS Services FortiGate-401F**
- **FCZ-15-0401F-149-02-00**
  Descripción (confirmado / mapeo): Asociado a servicios de **Threat Detection / Indicator of Compromise (IOC) / Threat Intelligence** (servicios de detección/telemetría). **Confirmado** que 149 se usa para IOC/Threat Detection en otras familias Fortinet; por tanto para 0401F es muy probable que represente **servicio de detección de compromisos / Threat Detection. (Recomiendo confirmar duración / alcance con el distribuidor).**
- **FCZ-15-0401F-208-02-00**
  Descripción : SKU de **servicio complementario / bundle** (podría ser licencia de algún complemento de FortiAnalyzer, FortiGuard o extensión de reporting).
- **FCZ-15-0401F-241-02-00**
  Descripción : Variante de **servicio de soporte / renovación FortiCare (24x7 web support / acceso a portal)** o SKU de co-terminación/renovación. Hay listados de partners que usan sufijos similares para soporte/renovación por modelo. Confirmar alcance exacto (SLA, R&R, depot locales).
- **FCZ-15-0401F-242-02-00**
  Descripción: Otra **variante de FortiCare / renovación** (nivel/paquete distinto al 241/243). Verificar con distribuidor si corresponde a "FortiCare Premium", "Advanced R&R" u otro add-on.
- **FCZ-15-0401F-243-02-00**
  Descripción: Licencia de tipo "Premium / Advanced Return & Replace" o un SKU de FortiCare con reemplazo avanzado.

Valor de 485 Licencias = numero de equipos gestionados (sin incluir el IVA 19%) $ 80.016.500,00
Valor IVA de 485 Licencias (IVA 19%) $ 15.203.135,00
Valor de 485 Licencias = numero de equipos gestionados (incluye el IVA 19%) $ 95.219.635,00

Descripción del producto: SERVICIOS GESTIONADO DE SOPORTE FIREWALL MARCA: FORTINET MODELO 401F (UN (1) año)

OBJETO: Proveer un servicio gestionado de seguridad perimetral sobre el equipo Fortinet FortiGate 401F ya adquirido por la entidad, incluyendo monitoreo continuo, administración de políticas, actualizaciones, soporte técnico especializado y generación de informes, en cumplimiento con la normativa del Estado colombiano.	
Incluye los siguientes servicios:	
Administración remota	Gestión completa de configuración, políticas y reglas de seguridad del FG-401F

CONSULTORIA TECNICA Y
SERVICIOS DE INGENIERIA
NIT 800127892.1

35 AÑOS
Hardware & Software Gold Reseller
Centro Autorizado de Servicio
Antivirus Authorized Reseller

Monitoreo 24/7	Supervisión continua de logs, alertas, consumo y eventos críticos
Gestión de cambios	Aplicación de cambios bajo procedimientos definido por la entidad
Actualizaciones de firmware	Planificación y ejecución de actualizaciones del FortiOS conforme al soporte oficial del fabricante
Soporte técnico	Mesa de ayuda para incidentes en modalidad 8*5
Análisis de tráfico	Informes detallados sobre amenazas, ancho de banda, uso de aplicaciones
Respaldo de configuración	Respaldos periódicos automáticos, con recuperación ante fallos
Auditoría y cumplimiento	Informes para revisión por entes de control (Contraloría, MINTIC, etc.)
Transferencia de conocimiento	Sesiones de capacitación básica para el personal de TI local
Garantía de cumplimiento de SLA	**99.9**
Personal certificado	En Productos como firewall de la marca Fortinet
Suscripcion:	Un (1) Año
Valor Annual sin incluir IVA	$ 24,840,000.00
Valor IVA 19%	$ 4,719,600.00
Valor anual incluido IVA (19%)	$ 29,559,600.00
*** Incluye despliegue inicial para el monitoreo del equipo**	

PROTECCION ANTIVIRUS PARA ENDPOINT (UN (1) año)

Marca y Modelo "ESET PROTECT Cloud + ESET ENDPOINT ANTIVIRUS/SECURITY + ESET SERVER SECURITY + ESET ENDPOINT FOR ANDROID + EL + EFDE + ECOS
"

CARACTERISTICAS GENERALES La solucion debe realizar exploraciones en estado inactivo para poder brindar de esa forma, una protección proactiva mientras el equipo no está en uso

Debe tener un caché local para aumentar el rendimiento de los entornos virtuales, garantizando que el archivo sólo se explora una vez.

El producto debe tener un control web para limitar el acceso a los sitios web por categoría, además de poderle mostrar al usuario una notificación de bloqueo.

El bloqueo web deberá poder asignarse por un rango de tiempo, por grupo y por equipo.

Deberá tener la capacidad de enviar una tarea para la actualización de los parches del sistema operativo.

Dentro del módulo de firewall deberá contar con la funcionalidad de bloqueo de exploits.

"La solución de antivirus debe ejecutar un escaneo únicamente en los siguientes estados en la computadora:

o Protector de pantalla activo

o Sesión de usuario bloqueada

o Sesión de usuario finalizada"

"La solución debe ser capaz de permitir o negar el uso de los dispositivos en base a los siguientes criterios:

o Fabricante

o Modelo

o Número de serie"

"La solución debe ser capaz de definir un listado específico de usuarios quienes pueden hacer uso de los dispositivos. Para dispositivos de almacenamiento, la solución debe permitir configurar únicamente de los siguientes permisos:

o Lectura/Escritura

o Bloqueo

o Solo de lectura

o Advertir"

"Cuando se conecta o usa un dispositivo de almacenamiento, la solución de antivirus debe proporcionar las siguientes opciones:

o Escanear

o No realizar ninguna acción

o Recordar esta acción"

"Sistema de prevención de intrusiones basado en el host (HIPS)

La solución debe tener sistema de prevención de intrusiones basado en el host. El sistema HIPS debe tener los siguientes modos de configuración:

o Modo automático

o Modo inteligente

o Modo interactivo

o Modo basado en políticas

o Modo aprendizaje"

El aprendizaje automático avanzado o "machine learning" deberá tener cuatro umbrales: Intenso, Balanceado, Cauteloso y Desactivado.

Debe tener una tarea para aislar a un equipo de la red.

El HIPS debe incluir una inspección a fondo del comportamiento de todos los programas en ejecución, archivos y llaves de registro

Debe contar con filtrado para mantener libre de SPAM a los clientes de correo.

La solución debe capaz de verificar las comunicaciones usando protocolos SSL para hallar amenazas.

"Firewall personal, la solución de antivirus debe contar con un firewall personal. El firewall debe tener los siguientes modos de configuración:

o Modo automático

o Modo interactivo

o Modo basado en políticas

o Modo aprendizaje"

"Las reglas de firewall creadas deberán ser capaces de permitir todas las siguientes acciones:

o Denegar

o Permitir

o Preguntar"

CONSOLA Deberá permitir la ejecución remota de scripts, batch files y paquetes personalizados a través de la consola, de terceros.

Deberá ser una solución que pueda ser usada y sea administrable desde la consola de antivirus en sistemas operativos Windows, Linux y Mac.

"Debe permitir generar grupos de clientes dinámicos y grupos estáticos.

El fabricante debe proporcionar al menos tres diferentes formas de realizar la instalación de la consola de administración.

o Instalador todo en uno

o Instalación por componentes

o Aparato virtual"

"El Appliance virtual debe soportar al menos las siguientes plataformas de virtualización

o VMWare vSphere

o Oracle Virtual Box

o Microsoft Hyper-V

o Azure - ambiente basado en la nube"

La consola de Administración deberá estar basada en Cloud.

Activar el acceso a la consola de antivirus con doble factor de autenticación, deber estar integrada a la misma consola de antivirus, sin ningún add-on o software adicional.

Debe contar con des instalador de antivirus de terceros.

Debe contar con un módulo específico para la protección contra ransomware.

Deberá tener la capacidad para aplicar durante cierto periodo de tiempo las reglas de control de dispositivo y de control de acceso web a través de la consola de administración.

Deberá contar con etiquetas independiente al LDAP, para identificar y buscar objetos similares.

Obtener a través de la consola de administración de seguridad del punto final inventario de aplicaciones y de hardware de cada uno de los equipos protegidos.

A través de la misma consola de administración de seguridad de punto final debe manejar la tecnología de Sandboxing en nube para el análisis de posibles amenazas, cifrado de los discos de almacenamiento de los puntos finales e integrarse con la solución de detección y respuesta del punto final.

A través de la consola de administración de seguridad del punto final debe ser posible administrar dispositivos móviles iOS y Android.

"Por disponibilidad de la solución de protección de punto final, la consola de administración debe tener la capacidad para construir ambientes distribuidos donde pueda asignarse roles independientes a cada componente, así tener un componente diferente para:

o Administrador de equipos móviles.

o Distribuidor de actualizaciones, paquetes de instalación y reenvío de comunicación entre el punto final y el servidor.

o Detector de puntos finales no administrados.

Y a su vez debe mostrar toda la información en la consola central de administración del punto final de forma nativa."

"La solución debe tener el mecanismo para desinstalar otras soluciones antivirus presentes en el equipo final. Este mecanismo debe ser y estar:

o Integrado al paquete de instalación de la solución de protección de punto final.

o Disponible solamente a través de la misma consola de administración de protección al punto final."

Seguridad del Servidor En servidores que usan "OneDrive for Business" debe explorar los archivos almacenados en esta nube, en búsqueda de algún archivo comprometido o posible malware.

La solución de protección en servidores debe incluir la detección y bloqueo de intrusiones, agregar a lista negra aquellas direcciones que han sido identificadas con este comportamiento malicioso.

La solución deberá agregar de forma automática las exclusiones que correspondan a aplicaciones críticas del servidor.

Optimizar el rendimiento de infraestructuras mixtas (hardware y virtuales) siendo capaz de eliminar la duplicidad de exploraciones en archivos, excluyendo los archivos ya explorados y limpios.

LiveGuard Uso de Sandboxing en la nube para analizar el comportamiento de archivos.

Es posible crear una exclusión por ruta, detección y su hash (SHA-1).

Capacidad de sincronizar su licenciamiento con la nube y la consola de administración en sitio o en la nube.

Detectar un archivo sospechoso ejecutado por primera vez se debe mostrar una advertencia, si el análisis se completa antes de ejecutar el archivo por primera vez, no se muestra el aviso archivo en análisis.

Debe borrar automáticamente las muestras de los archivos/ejecutables en los servidores donde fue analizado el comportamiento.

Capacidad para enviar correos SPAM para su análisis

Debe tener únicamente estos umbrales de detección: desconocido, limpio, sospechoso, altamente sospechoso y malicioso.

Debe tener la siguiente información de un archivo enviado al Sanboxing en la nube: nombre del equipo desde donde se ingresó el archivo, el usuario que lo ingresó, la razón, hash en SHA-1, nombre del archivo ingresado, tamaño del archivo, categoría.

Debe tener protección proactiva, es decir, que el archivo/ejecutable sea bloqueado hasta recibir el resultado del Sandbox en la nube.

Se debe tener capacidad para integrarse con la solución de antivirus o protección del punto final, para tener mayores posibilidades de protección y aplicación de políticas.

Enviar un archivo/ejecutable a través de una consola de administración del punto final.

permite la configuración detallada de políticas por equipo, de modo que el administrador puede controlar lo que se envía y lo que debe ocurrir en función del resultado recibido.

Disk Encryption La solución deberá ser capaz de cifrar los Endpoints con sistemas operativos Windows y MacOS.

La solución deberá disponer de diversas posibilidades de recuperación de Passwords para usuarios

CONSULTORIA TECNICA Y
SERVICIOS DE INGENIERIA
NIT 800127892.1

35 AÑOS
Hardware & Software Gold Reseller
Centro Autorizado de Servicio
Antivirus Authorized Reseller

remotos que se vean bloqueados.

La solución deberá poder programar las tareas de cifrado sobre los Endpoints deseados con la posibilidad de pausar la ejecución para retomar luego desde el último punto.

La solución deberá poder ser administrada desde la misma consola central junto con las otras soluciones descriptas en el TDR.

La solución de cifrado debe permitir anular la contraseña de inicio de sesión de la estación de trabajo.

Cloud Office SecurityLa solución deberá ser capaz de analizar el contenido de Microsoft Exchange Online vía API.

La solución deberá ser capaz de analizar el contenido de Microsoft OneDrive for Business vía API.

La solución deberá ser capaz de analizar el contenido de Microsoft Sharepoint Online via API.

La solución deberá ser capaz de analizar el contenido de Microsoft Teams via API.

La solución deberá contar con un servicio integrado de Sandboxing ofrecido por el mismo fabricante.

La solución deberá ser capaz de poder discriminar que usuarios se desean proteger.

"La solución deberá ser capaz de discriminar los niveles de protección que se brindará proporciona configuraciones de protección basadas en:

- Antispam.
- Anti-Phishing.
- Antimalware."

La solución deberá prestar protección inmediata a los usuarios con una política por defecto.

"La política personalizada puede asignarse a:

- Usuarios: se aplica a usuarios concretos seleccionados manualmente.
- Grupos: política que se aplica a todos los miembros del grupo de usuarios.
- Inquilinos: política que se aplica a todas las entidades del inquilino.
- Grupos de equipos: política que se aplica a un grupo de Team.
- Sitios de SharePoint: política que se aplica a un sitio de SharePoint."

La solución deberá poder proteger de forma inmediata a los futuros usuarios que se creen dentro del Tenant de Microsoft 365.

La solución deberá ser Multi Tenant.

OTRAS CARACTERISTICAS El fabricante deberá tener soporte técnico en castellano.

Que el fabricante directamente brinde servicios de seguridad informática como por ejemplo penetration testing, vulnerability assessment o análisis de GAP

El fabricante deberá tener la capacidad de ofrecer directamente un servicio de caza de amenazas.

El fabricante deberá tener un laboratorio de análisis y detección de malware en Latinoamérica.

Que tenga oficinas de la marca en Latinoamérica y presencia local en el país.

El fabricante deberá tener programas de "colaborador seguro"

Instalación y configuración "El proveedor debe garantizar:

- Configuracion del producto indicaciones del la entidad
- Configuracion los reportes basicos

- El Personal debe ser certficado en la marca del producto que propone para instalacion y configuracion"

Capacitacion Capacitacion a funcionarios que determinen la entidad y proveedor debe garantizar que el personal sea certificado de la marca

Licencias 500 usuarios

Suscripcion 1 año

VALOR UNITARIO $ 34.263.700 (VALOR TOTAL, product excluido de IVA, por norma tributaria)

ELEMENTO	VALOR UNITARIO	IVA ITEM	VALOR ITEM
LICENCIA DE SOFTWARE PARA CORTAFUEGOS FORTINET 401F FG4H1FT923904283, DOS AÑOS	$ 80.016.500,00	$ 15.203.135,00	$95.219.635,00
SERVICIOS GESTIONADO DE SOPORTE FIREWALL MARCA: FORTINET MODELO 401F. UN AÑO	$ 24.840.000,00	$ 4.719.600,00	$ 29.559.600,00
PROTECCION ANTIVIRUS PARA ENDPOINT (excluido de IVA), UN AÑO	$ 34.263.700,00	Excluido	$ 34.263.700,00
	SUBTOTAL	IVA	TOTAL OFERTA
	$ 139.120.200,00	$19.922.735,00	$159.042.935,00

SERVICIOS DE SOPORTE

TERRITORIALIDAD

Consultoría Técnica y Servicios de Ingeniería Cotec SAS, NIT 800127892-1, tributa en el municipio de Tunja, para ventas realizadas en Tunja, el impuesto de Industria y comercio.

CUENTA PARA PAGOS

Para efectos de pagos, Consultoría Técnica y Servicios de Ingeniería Cotec SAS, NIT 800127892-1 tiene la cuenta bancaria de ahorros en el banco de Bogotá, # 618718416.

CODIGOS CIIU: 4651, 4652, 4741, 7730

GASTOS E IMPUESTOS

Todos los gastos, tasas, fletes, aranceles y demás Impuestos, excepción hecha del IVA (+19%), están incluidos dentro del precio unitario indicado.

ACUERDO DE NIVEL DE SERVICIO

PROTOCOLO DE SERVICIO Y ATENCIÓN AL USUARIO FINAL, en el caso de requerirse soporte posterior a la implementación.

CONDICIONES TÉCNICAS

- Garantía de Fabricación: En la modalidad de repuestos, mano de obra y ON SITE. La garantía cubre todos los defectos de fabricación. Los tiempos de garantía se contabilizan a partir del acta de entrada y el acta de verificación hechas por la Entidad

CONSULTORIA TECNICA Y
SERVICIOS DE INGENIERIA
NIT 800127892.1

35 AÑOS
Hardware & Software Gold Reseller
Centro Autorizado de Servicio
Antivirus Authorized Reseller

- Garantía de Repuestos: La garantía de Repuestos incluye todos los componentes. No incluye elementos de consumo.
- Garantía de Mano de Obra: En la modalidad ON SITE.
- Mantenimiento Correctivo: COTEC S.A.S y/o Fabricante, garantizará el suministro de los repuestos o equipos que sean necesarios para la reparación de los equipos, reemplazará los elementos defectuosos con repuestos que serán de la misma calidad de los existentes y pertenecientes a la línea de producción del fabricante, dejará en perfecto funcionamiento cualquiera de los elementos ofertados, este servicio no tendrá costo alguno para Entidad;

ACUERDO DE NIVEL DE SERVICIO (APLICA/ COMPLEMENTA PARA TODOS LOS FABRICANTES)

Lo anterior, sin perjuicio de la responsabilidad de Consultoría Técnica y Servicios de Ingeniería Cotec SAS, NIT 800127892-1, dada su relación vinculante, contractual, así:

- En caso de requerir soporte la Entidad deberá enviar la solicitud al siguiente contacto.
- Correo electrónico:: gerencia@cotec-ltda.com
- TELEFAX: (8)7603654 - 3107637363
  Horario de atención: lunes a viernes de 8:00 AM – 6:00PM

COTEC S.A.S. cuenta con personal encargado de coordinar y ejecutar las labores objeto del contrato. La garantía, será responsabilidad de COTEC S.A.S, y ejecutada directamente por el fabricante con personal especializado, El fabricante de los equipos ofrecidos cuenta con Centros Autorizados de Servicio en las principales ciudades del país, servicios que estarán a disposición de la Entidad para llevar a cabo tramites de Soporte y Garantía.

Recepción del Servicio: Cualquier solicitud de un usuario es registrada en el sistema esta solicitud debe ser llenada de tal manera que permita asignar un código al servicio, así mismo debe ser complementada con información básica del usuario con datos como nombre, dirección, teléfono, etc.

COTEC S.A.S., realizara el Escalamiento con el fin de realizar un seguimiento adecuado a todos los problemas reportados por los usuarios de tal manera que estos sean atendidos en los tiempos estipulados

Ante una solicitud de garantía o prestación de servició por parte de la Entidad, servicios que serán prestados en el sitio en donde se encuentren instalados los equipos, previo el desarrollo del siguiente procedimiento:

- Atención de la llamada de servicio. (Teléfono, Fax o Correo Electrónico)
- Asesoría inmediata de nuestro departamento técnico, vía telefónica, para intentar la solución ó por el contrario para identificar el tipo de inconveniente que se pueda estar presentando de tal forma que se pueda preparar un kit de repuestos y de soluciones.
- En caso de determinar la necesidad de enviar un técnico se programará, el mismo se hará presente en las instalaciones del Cliente acompañado del Kit de repuestos y de soluciones pre-identificado en el punto anterior de tal manera que inmediatamente pueda iniciar a

efectuar la reparación.

- Si la falla presentada no es posible de corregir de manera local se procederá a retirar el equipo por nuestra cuenta para su correspondiente tramite de garantía ante el fabricante.
- Personal de mantenimiento: Será de total responsabilidad del Contratista
- Valor de los repuestos para cubrir la garantía: Será de total responsabilidad del Contratista
- Número de visitas correctivo: Las que haya lugar.
- Cubre el Suministro de Partes o Repuestos originales y Mano de obra de reparación, en sitio (on site) sin costo para la Entidad, durante el periodo de Garantía.
- Las visitas de mantenimiento correctivo serán coordinadas y programadas con la Entidad esta visita involucra mano de obra, repuestos, materiales necesarios para corregir los problemas y las fallas que se presenten, y el desplazamiento de los ingenieros y/o técnicos
- Se Asumirá cualquier costo por concepto de cambio de los equipos a suministrar que resulten defectuosos, de mala calidad durante el tiempo que dure la garantía.

Se realizará el Seguimiento: Durante el intervalo de tiempo que el problema persista se hará el seguimiento de la solicitud, en especial a aquellas que tienen prioridad Critica o Urgente, esto implica estar en constante comunicación con el apoyo respectivo para garantizar que la solución del problema sea implementada en los tiempos de respuesta definidos y poder mantener continuamente informado al usuario acerca de la evolución del proceso.

El Área de Soporte Técnico trabaja en forma continuada hasta dar solución al problema, todo dentro del horario de cobertura estipulado. Se involucran todos aquellos recursos necesarios y escalando tantos niveles como sea preciso hasta dar completa satisfacción al usuario en cuanto a la resolución del problema.

Cuando la solución se haya hecho efectiva, el responsable debe anotar dentro del cuerpo de la orden de servicio la descripción de los procedimientos realizados para implementar la solución y la fecha en la cual la concluyó. Lo anterior con el fin de mantener la base de datos de nuestro sistema actualizada con las soluciones aplicadas.

SERVICIOS ADICIONALES DE COTEC SAS, COMPLEMENTARIOS:

VIGENCIA DE LA OFERTA: 30 días, se recomienda tomar una decisión muy rápida dado que los precios de estos elementos por ser de importación están sujetos a variaciones de la TRM.

TIEMPO DE ENTREGA: 30 días.

FORMA DE PAGO: dentro de los 30 días de la fecha de facturación o la señalada ´por las normas de la Entidad.

Cordialmente

Ing. JOSE ANTONIO MATHEUS ROCHA
Gerente Comercial – Representante Legal

Bogota, septiembre 29 de 2025

Señores
MUNICIPIO DE FUSAGASUGA
Fusagasuga. -

De acuerdo a su amable solicitud A continuación les cotizamos a Uds., los elementos de la referencia, repuestos, y otros elementos, para atender las necesidades planteadas.

La información técnica que permite verificar que los bienes se acogen a las exigencias de la necesidad planteada y determinadas por el área técnica, se puede comprobar mediante la consulta de las marcas y modelos en cada uno de los website del correspondiente fabricante y si es del caso el proponente aportara tal información si es requerido por la entidad.

Descripción del producto: LICENCIA DE SOFTWARE PARA CORTAFUEGOS FORTINET 401F FG4H1FT923904283

Nombre resumido: Licencia de suscripción para MAXIMO 500 endpoints **(DOS (2) años)**

Detalles principales:

- **Tipo de servicio**: Suscripción anual — Incluye FortiClient con capacidades de **EPP (Endpoint Protection Platform)**, **APT (Advanced Persistent Threat defense)**, y agente **VPN/ZTNA (Zero Trust Network Access)**.
- Además, incluye soporte continuo con **FortiCare 24x7**. La gestión se realiza a través de **EMS (Endpoint Management Server)** alojado en **FortiCloud**. **Cobertura**: Hasta **500 endpoints** (usuarios o dispositivos).
- **Duración**: 1 año de suscripción.
- **Soporte incluido**: Servicio completo de **FortiCare Premium** o **FortiCare 24x7** para asistencia continua, actualizaciones y mantenimiento.

Los compontenentes de este producto son:

- **FCZ-15-0401F-100-02-00**
  Descripción: Licencia de **Advanced Malware Protection / Antivirus / FortiSandbox (AMP)** para FortiGate-401F — protección contra malware, análisis en sandbox y firmas
- **FCZ-15-0401F-108-02-00**
  Descripción: Licencia del servicio **IPS (Intrusion Prevention Service)** para FortiGate-401F — detección y bloqueo de intentos de intrusión y exploits.
- **FCZ-15-0401F-112-02-00**
  Descripción: Licencia de **Web / URL Filtering (y/o filtrado DNS / contenido multimedia)** — control de acceso web por categorías/URL y filtrado de contenido para FortiGate-401F.
- **FCZ-15-0401F-114-02-00 AS Services FortiGate-401F**
- **FCZ-15-0401F-149-02-00**
  Descripción (confirmado / mapeo): Asociado a servicios de **Threat Detection /**

Indicator of Compromise (IOC) / Threat Intelligence (servicios de detección/telemetría). **Confirmado** que 149 se usa para IOC/Threat Detection en otras familias Fortinet; por tanto, para 0401F es muy probable que represente **servicio de detección de compromisos / Threat Detection. (Recomiendo confirmar duración / alcance con el distribuidor).**

- **FCZ-15-0401F-208-02-00**
  Descripción: SKU de **servicio complementario / bundle** (podría ser licencia de algún complemento de FortiAnalyzer, FortiGuard o extensión de reporting).
- **FCZ-15-0401F-241-02-00**
  Descripción: Variante de **servicio de soporte / renovación FortiCare (24x7 web support / acceso a portal)** o SKU de co-terminación/renovación. Hay listados de partners que usan sufijos similares para soporte/renovación por modelo. Confirmar alcance exacto (SLA, R&R, depot locales).
- **FCZ-15-0401F-242-02-00**
  Descripción: Otra **variante de FortiCare / renovación** (nivel/paquete distinto al 241/243). Verificar con distribuidor si corresponde a "FortiCare Premium", "Advanced R&R" u otro add-on.
- **FCZ-15-0401F-243-02-00**
  Descripción: Licencia de tipo "Premium / Advanced Return & Replace" o un SKU de FortiCare con reemplazo avanzado.

Valor de 485 Licencias = numero de equipos gestionados (sin incluir el IVA 19%) $ 80.200.000
Valor IVA de 485 Licencias (IVA 19%) $ 15.238.000
Valor de 485 Licencias = numero de equipos gestionados (incluye el IVA 19%) $ 95.438.000

Descripción del producto: SERVICIOS GESTIONADO DE SOPORTE FIREWALL MARCA: FORTINET MODELO 401F (UN (1) año)

OBJETO: Proveer un servicio gestionado de seguridad perimetral sobre el equipo Fortinet FortiGate 401F ya adquirido por la entidad, incluyendo monitoreo continuo, administración de políticas, actualizaciones, soporte técnico especializado y generación de informes, en cumplimiento con la normativa del Estado colombiano.	
Incluye los siguientes servicios:	
Administración remota	Gestión completa de configuración, políticas y reglas de seguridad del FG-401F
Monitoreo 24/7	Supervisión continua de logs, alertas, consumo y eventos críticos
Gestión de cambios	Aplicación de cambios bajo procedimientos definido por la entidad
Actualizaciones de firmware	Planificación y ejecución de actualizaciones del FortiOS conforme al soporte oficial del fabricante
Soporte técnico	Mesa de ayuda para incidentes en modalidad 8*5
Análisis de tráfico	Informes detallados sobre amenazas, ancho de banda, uso de

	aplicaciones
Respaldo de configuración	Respaldos periódicos automáticos, con recuperación ante fallos
Auditoría y cumplimiento	Informes para revisión por entes de control (Contraloría, MINTIC, etc.)
Transferencia de conocimiento	Sesiones de capacitación básica para el personal de TI local
Garantía de cumplimiento de SLA	**99.9**
Personal certificado	En Productos como firewall de la marca Fortinet
Suscripcion:	Un (1) Año
Valor Annual sin incluir IVA	$ 24,900,000
Valor IVA 19%	$ 4,731.000
Valor anual incluido IVA (19%)	$ 29,631,000
*** Incluye despliegue inicial para el monitoreo del equipo**	

PROTECCION ANTIVIRUS PARA ENDPOINT (UN (1) año)

Marca y Modelo "ESET PROTECT Cloud + ESET ENDPOINT ANTIVIRUS/SECURITY + ESET SERVER SECURITY + ESET ENDPOINT FOR ANDROID + EL + EFDE + ECOS
"

CARACTERISTICAS GENERALES La solucion debe realizar exploraciones en estado inactivo para poder brindar de esa forma, una protección proactiva mientras el equipo no está en uso

Debe tener un caché local para aumentar el rendimiento de los entornos virtuales, garantizando que el archivo sólo se explora una vez.

El producto debe tener un control web para limitar el acceso a los sitios web por categoría, además de poderle mostrar al usuario una notificación de bloqueo.

El bloqueo web deberá poder asignarse por un rango de tiempo, por grupo y por equipo.

Deberá tener la capacidad de enviar una tarea para la actualización de los parches del sistema operativo.

Dentro del módulo de firewall deberá contar con la funcionalidad de bloqueo de exploits.

"La solución de antivirus debe ejecutar un escaneo únicamente en los siguientes estados en la computadora:

o Protector de pantalla activo

o Sesión de usuario bloqueada

o Sesión de usuario finalizada"

"La solución debe ser capaz de permitir o negar el uso de los dispositivos en base a los siguientes criterios:

o Fabricante

o Modelo

o Número de serie"

"La solución debe ser capaz de definir un listado específico de usuarios quienes pueden hacer uso

de los dispositivos. Para dispositivos de almacenamiento, la solución debe permitir configurar únicamente de los siguientes permisos:

o Lectura/Escritura

o Bloqueo

o Solo de lectura

o Advertir"

"Cuando se conecta o usa un dispositivo de almacenamiento, la solución de antivirus debe proporcionar las siguientes opciones:

o Escanear

o No realizar ninguna acción

o Recordar esta acción"

"Sistema de prevención de intrusiones basado en el host (HIPS)

La solución debe tener sistema de prevención de intrusiones basado en el host. El sistema HIPS debe tener los siguientes modos de configuración:

o Modo automático

o Modo inteligente

o Modo interactivo

o Modo basado en políticas

o Modo aprendizaje"

El aprendizaje automático avanzado o "machine learning" deberá tener cuatro umbrales: Intenso, Balanceado, Cauteloso y Desactivado.

Debe tener una tarea para aislar a un equipo de la red.

El HIPS debe incluir una inspección a fondo del comportamiento de todos los programas en ejecución, archivos y llaves de registro

Debe contar con filtrado para mantener libre de SPAM a los clientes de correo.

La solución debe capaz de verificar las comunicaciones usando protocolos SSL para hallar amenazas.

"Firewall personal, la solución de antivirus debe contar con un firewall personal. El firewall debe tener los siguientes modos de configuración:

o Modo automático

o Modo interactivo

o Modo basado en políticas

o Modo aprendizaje"

"Las reglas de firewall creadas deberán ser capaces de permitir todas las siguientes acciones:

o Denegar

o Permitir

o Preguntar"

CONSOLA Deberá permitir la ejecución remota de scripts, batch files y paquetes personalizados a través de la consola, de terceros.

Deberá ser una solución que pueda ser usada y sea administrable desde la consola de antivirus en sistemas operativos Windows, Linux y Mac.

"Debe permitir generar grupos de clientes dinámicos y grupos estáticos.

El fabricante debe proporcionar al menos tres diferentes formas de realizar la instalación de la consola de administración.

o Instalador todo en uno

o Instalación por componentes

o Aparato virtual"

"El Appliance virtual debe soportar al menos las siguientes plataformas de virtualización

o VMWare vSphere

o Oracle Virtual Box

o Microsoft Hyper-V

o Azure - ambiente basado en la nube"

La consola de Administración deberá estar basada en Cloud.

Activar el acceso a la consola de antivirus con doble factor de autenticación, deber estar integrada a la misma consola de antivirus, sin ningún add-on o software adicional.

Debe contar con des instalador de antivirus de terceros.

Debe contar con un módulo específico para la protección contra ransomware.

Deberá tener la capacidad para aplicar durante cierto periodo de tiempo las reglas de control de dispositivo y de control de acceso web a través de la consola de administración.

Deberá contar con etiquetas independiente al LDAP, para identificar y buscar objetos similares.

Obtener a través de la consola de administración de seguridad del punto final inventario de aplicaciones y de hardware de cada uno de los equipos protegidos.

A través de la misma consola de administración de seguridad de punto final debe manejar la tecnología de Sandboxing en nube para el análisis de posibles amenazas, cifrado de los discos de almacenamiento de los puntos finales e integrarse con la solución de detección y respuesta del punto final.

A través de la consola de administración de seguridad del punto final debe ser posible administrar dispositivos móviles iOS y Android.

"Por disponibilidad de la solución de protección de punto final, la consola de administración debe tener la capacidad para construir ambientes distribuidos donde pueda asignarse roles independientes a cada componente, así tener un componente diferente para:

o Administrador de equipos móviles.

o Distribuidor de actualizaciones, paquetes de instalación y reenvío de comunicación entre el punto final y el servidor.

o Detector de puntos finales no administrados.

Y a su vez debe mostrar toda la información en la consola central de administración del punto final de forma nativa."

"La solución debe tener el mecanismo para desinstalar otras soluciones antivirus presentes en el equipo final. Este mecanismo debe ser y estar:

o Integrado al paquete de instalación de la solución de protección de punto final.

o Disponible solamente a través de la misma consola de administración de protección al punto final."

Seguridad del Servidor En servidores que usan "OneDrive for Business" debe explorar los archivos almacenados en esta nube, en búsqueda de algún archivo comprometido o posible malware.

La solución de protección en servidores debe incluir la detección y bloqueo de intrusiones, agregar a lista negra aquellas direcciones que han sido identificadas con este comportamiento malicioso.

La solución deberá agregar de forma automática las exclusiones que correspondan a aplicaciones críticas del servidor.

Optimizar el rendimiento de infraestructuras mixtas (hardware y virtuales) siendo capaz de eliminar la duplicidad de exploraciones en archivos, excluyendo los archivos ya explorados y limpios.

LiveGuard Uso de Sandboxing en la nube para analizar el comportamiento de archivos.

Es posible crear una exclusión por ruta, detección y su hash (SHA-1).

Capacidad de sincronizar su licenciamiento con la nube y la consola de administración en sitio o en la nube.

Detectar un archivo sospechoso ejecutado por primera vez se debe mostrar una advertencia, si el análisis se completa antes de ejecutar el archivo por primera vez, no se muestra el aviso archivo en análisis.

Debe borrar automáticamente las muestras de los archivos/ejecutables en los servidores donde fue analizado el comportamiento.

Capacidad para enviar correos SPAM para su análisis

Debe tener únicamente estos umbrales de detección: desconocido, limpio, sospechoso, altamente sospechoso y malicioso.

Debe tener la siguiente información de un archivo enviado al Sanboxing en la nube: nombre del equipo desde donde se ingresó el archivo, el usuario que lo ingresó, la razón, hash en SHA-1, nombre del archivo ingresado, tamaño del archivo, categoría.

Debe tener protección proactiva, es decir, que el archivo/ejecutable sea bloqueado hasta recibir el resultado del Sandbox en la nube.

Se debe tener capacidad para integrarse con la solución de antivirus o protección del punto final, para tener mayores posibilidades de protección y aplicación de políticas.

Enviar un archivo/ejecutable a través de una consola de administración del punto final.

permite la configuración detallada de políticas por equipo, de modo que el administrador puede controlar lo que se envía y lo que debe ocurrir en función del resultado recibido.

Disk Encryption La solución deberá ser capaz de cifrar los Endpoints con sistemas operativos Windows y MacOS.

La solución deberá disponer de diversas posibilidades de recuperación de Passwords para usuarios remotos que se vean bloqueados.

La solución deberá poder programar las tareas de cifrado sobre los Endpoints deseados con la posibilidad de pausar la ejecución para retomar luego desde el último punto.

La solución deberá poder ser administrada desde la misma consola central junto con las otras soluciones descriptas en el TDR.

La solución de cifrado debe permitir anular la contraseña de inicio de sesión de la estación de trabajo.

Cloud Office SecurityLa solución deberá ser capaz de analizar el contenido de Microsoft Exchange Online vía API.

La solución deberá ser capaz de analizar el contenido de Microsoft OneDrive for Business vía API.

La solución deberá ser capaz de analizar el contenido de Microsoft Sharepoint Online via API.

La solución deberá ser capaz de analizar el contenido de Microsoft Teams via API.

La solución deberá contar con un servicio integrado de Sandboxing ofrecido por el mismo fabricante.

La solución deberá ser capaz de poder discriminar que usuarios se desean proteger.

"La solución deberá ser capaz de discriminar los niveles de protección que se brindará proporciona configuraciones de protección basadas en:

- Antispam.
- Anti-Phishing.
- Antimalware."

La solución deberá prestar protección inmediata a los usuarios con una política por defecto.

"La política personalizada puede asignarse a:

- ❖ Usuarios: se aplica a usuarios concretos seleccionados manualmente.
- ❖ Grupos: política que se aplica a todos los miembros del grupo de usuarios.
- ❖ Inquilinos: política que se aplica a todas las entidades del inquilino.
- ❖ Grupos de equipos: política que se aplica a un grupo de Team.
- ❖ Sitios de SharePoint: política que se aplica a un sitio de SharePoint."

La solución deberá poder proteger de forma inmediata a los futuros usuarios que se creen dentro del Tenant de Microsoft 365.

La solución deberá ser Multi Tenant.

OTRAS CARACTERISTICAS El fabricante deberá tener soporte técnico en castellano.

Que el fabricante directamente brinde servicios de seguridad informática como por ejemplo penetration testing, vulnerability assessment o análisis de GAP

El fabricante deberá tener la capacidad de ofrecer directamente un servicio de caza de amenazas.

El fabricante deberá tener un laboratorio de análisis y detección de malware en Latinoamérica.

Que tenga oficinas de la marca en Latinoamérica y presencia local en el país.

El fabricante deberá tener programas de "colaborador seguro"

Instalación y configuración "El proveedor debe garantizar:

- Configuracion del producto indicaciones del la entidad
- Configuracion los reportes basicos
- El Personal debe ser certficado en la marca del producto que propone para instalacion y configuracion"

Capacitacion Capacitacion a funcionarios que determinen la entidad y proveedor debe garantizar que el personal sea certificado de la marca

Licencias 500 usuarios

Suscripcion 1 año

VALOR UNITARIO $ 34.300.000 (VALOR TOTAL, product excluido de IVA, por norma tributaria)

ELEMENTO	VALOR UNITARIO	IVA ITEM	VALOR ITEM
LICENCIA DE SOFTWARE PARA CORTAFUEGOS FORTINET 401F FG4H1FT923904283, DOS AÑOS	$ 80.200.000	$ 15.238.000	$ 95.438.000
SERVICIOS GESTIONADO DE SOPORTE FIREWALL MARCA: FORTINET MODELO 401F UN AÑO	$ 24.900.000	$ 4.731.000	$ 29.631.000
PROTECCION ANTIVIRUS PARA ENDPOINT (excluido de IVA) UN AÑO	$ 34.300.000	Excluido	$ 34.300.000
	SUBTOTAL	**IVA**	**TOTAL OFERTA**
	$ 139.400.000	$ 19.969.000	$ 159.369.000

JOSE FRANCISCO SARMIENTO
Sales Marketing Colombia
Teléfono: (601) 4325127 ext. 144
Móvil: 3154190769
jose.sarmiento@onescreensolutions.com
www.onescreensolutions.com
Monday, 6 de October de 2025