INVERSIONES Y SERVICIOS TECNOLOGICOS S.A.S.

INVSERTEC S.A.S.
NIT: 901.038.266 - 5
CL 66 A No 18 - 51 SOLEDAD ATLANTICO
TELEFONO: 3175654

Soledad, 13 de agosto de 2025

Tenemos el gusto de presentar propuesta comercial en los siguientes productos, con las siguientes características:

Cotización:	**CM-23-00012012023-1**				
Cliente: Contacto: Cargo: Consultor:	ALCALDIA DE SANTA MARTA JHON VELASQUEZ INGENIERO DE TI	NIT: Correo: Teléfono: Direccion: Web:			
Ítem	**Descripción**	**MARCA**	**Und**	**Ctd**	**Valor Total**
1	Kaspersky Embedded Systems Security Latin America Edition. 100-149 Node 1 year Base Plus License	KASPERSKY	100	$ 170.000	USD 17.000.000
2	Kaspersky Next EDR Optimum Latin America Edition. 250-499 User 1 year Base Plus License	cisco	300	$ 99.000	$ 29.700.000
SUBTOTAL DEL PROYECTO					$ 46.700.000
IVA					EXENTO
TOTAL					**$ 46.700.000**

CONDICIONES COMERCIALES

FORMA DE PAGO	DE CONTADO
VALIDEZ DE LA OFERTA	3 DÍAS
TIEMPO DE ENTREGA	10 DIAS
GARANTÍA	1 AÑO
IMPUESTO A LAS VENTAS	

INVSERTEC S.A.S.

Características Generales de la Solución

Característica	Descripción
Protección para endpoints consola de administración	Análisis de archivos compuestos de formatos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos comprimidos
	Tráfico HTTP, HTTPS y FTP.
	Compactibilidad con POP3, SMTP, IMAP y NNTP.
	Protección frente a amenazas en la red que monitoree el tráfico de red entrante en busca de actividad característica de los ataques de red.
	Bloqueo de host y restricción de envío de paquetes de red durante un periodo determinado de al menos una hora.
	Activación y administración de la protección contra ataques a la red, Inundación de red (flooding) ataques de tipo "Port scan", Ataques de spoofing de MAC.
	Control de actividad de la red sobre los protocolos: TCP, UDP, ICMP, ICMPv6, IGMP y GRE. A través del Firewall de escritorio
	Prevención de ataques a nivel de USB
	El componente de prevención de ataques a nivel de USB permite a los dispositivos USB detectados por el sistema operativo identifique teclados y que conectados al equipo antes de la instalación del componente se consideren autorizados después de su instalación.
	El componente de prevención de ataques a nivel de USB bloquea automáticamente el dispositivo USB si el código de autorización se introduce incorrectamente un número de veces especificado.
	El componente de prevención de ataques a nivel de USB permite utilizar un teclado en pantalla para autorizar dispositivos USB que no admitan introducir caracteres aleatorios.
	Motor de reparación para revertir las acciones realizadas por aplicaciones maliciosas en el sistema operativo.
	El motor de reparación permite anular la actividad de malware en el sistema operativo a los siguientes tipos de actividad:
	- 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.

	Control web que permite regular el acceso de los usuarios a los recursos web.
	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.
	Control de aplicaciones que permita gestionar el inicio de aplicaciones en los equipos de los usuarios.
	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.
	Características básicas de Endpoint Detection and Response (EDR).
	Licenciamiento, con integración y acceso a portal de inteligencia contra amenazas, y consulta de información sobre la reputación de archivos y URL.
	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.
	Creación de tareas de análisis de IoC de forma automática en respuesta a amenazas detectadas por el Sandbox basado en nube.
	Cifrado de datos para el cifrado de carpetas archivos almacenados en las unidades locales y extraíbles, unidades extraíbles y discos duros, con el fin de minimizar el riesgo de filtraciones de información en caso de pérdida o robo del equipo, unidad extraíble, disco duro, o cuando usuarios y aplicaciones no autorizados accedan a los datos.
	Cifrado de datos con las siguientes características:
	- 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.
	El cifrado de datos permite realizar cifrado de disco completo con la tecnología de cifrado propietario del fabricante.
Protección para office 365	Cumplimiento del Reglamento General de Protección de Datos (RGDP) y protección de los datos.
	Tecnologías de detección Anti-Spam, Anti-Phishing, Anti-Malware, Anti-Ransomware, Anti-BEC y capacidades de filtrado de contenido.
	Tecnologías proactivas para la detección de amenazas avanzadas o de día 0.
	Tecnologías de detección avanzadas para la detección y neutralización de amenazas del tipo Ransomware.
	Capacidades de escaneo bajo demanda sobre buzones de correo
	- Grupos de usuarios
	- Usuarios
	- Todos los usuarios.
	Clasificación de correos basura en dos categorías: Spam y correos masivos

	Generación de direcciones de lista blanca y negra para cada uno de los módulos de seguridad.
	Funciones de validación y autentificación del remitente de manera automática que incluyan:
	- DKIM.
	- DMARK.
	- SPF.
	Módulo antimalware 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:
	- Firmas,
	- Análisis heurísticos
	- Comportamiento.
	Almacenamiento de datos sensibles de usuarios y contraseñas en integración con Microsoft Office 365 mediante OAuth 2.0
	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.
	Supervisión de fuga de datos con el objetivo del descubrimiento de información confidencial transmitida y almacenada por usuarios en los buzones de correo de Exchange Online, en los almacenamientos de OneDrive y en los sitios de SharePoint Online.
	Escaneo retrospectivo de amenazas en buzones de correo de Ms Office 365 y repositorios de datos de OneDrive.
	Formación en ciberseguridad dentro de la aplicación.
Plataforma de entrenamiento	Entrenamiento en varios módulos, con módulo serie de secciones.
	Teoría relevante y capacidad de realizar tareas interactivas en un entorno simulado.
	Descarga de certificado de acreditación de logros, una vez completadas todas las secciones de un módulo.
	Solución 100% en nube.
	Módulos de entrenamientos en ciberseguridad agnósticos entre los que se encuentren respuestas a incidentes, Software Malicioso, aseguramiento de Directorio Activo y Seguridad para servidores, entre otros.
Detención proactiva de protección contra ransomware	Protección contra ransomware basada en comportamiento.
	Remediación de la acción de encriptación de los ransomware.
	Detención del cifrado malicioso de forma local o remota.
	Protección antiransomware para el sector de booteo (master boot record).
	Restauración automática de archivos cifrados por progreso malicioso de ransomware.
	Informe de consola de administración web con detalle incidentes – análisis de causa raíz sin instalación de agente o dispositivo en la red.
Protección	Bloqueo de ataques basados en la explotación de vulnerabilidades conocidas

contra vulnerabilidades y técnicas de explotación	o de día cero.
	Protección de las siguientes técnicas de explotación:
	1. Enforce Data Execution Prevention
	2. Mandatory Address Space Layout Randomization
	3. Bottom-up ASLR.
	4. Null Page (Null Deference Protection)
	5. Heap Spray Allocation
	6. Dynamic Heap Spray
	7. Dynamic Heap Spray.
	8. Stack Pivot
	9. Stack Exec (MemProt)
	10. Stackbased -ROP Mitigations (Caller)
	11. Branch-based ROP Mitigations (Hardware Assisted)
	12. Structured Exception Handler Overwrite (SEHOP)
	13. Import Address Table Filtering (IAF)
	14. Load Library
	15. Reflective DLL Injection
	16. Shellcode
	17. VBScript God Mode
	18. Wow64
	19. Syscall
	20. Hollow Process
	21. DLL Hijacking
	22. Squiblydoo Applocker Bypass
	23. APC Protection (Double Pulsar / AtomBombing)
	24. Process Privilege Escalation.
	25. Mitigación de inyección de códigos en procesos.
	26. Protección contra robo de credenciales
	27. Protección contra malware escondido en aplicaciones legitimas (code cave).
	28. Denegación de migración de procesos maliciosos, evitando que un proceso malicioso migre a otro.
	29. Denegación de escalamiento de privilegios.
	30. Impedimento de modificación de las claves de registro para la ejecución de código arbitrario.
Requisitos de instalación.	1. Compatibilidad con máquinas con arquitectura de 32 bits y 64 bits.
	2. compatibilidad con sistemas operativos: Windows 7 en adelante, Mac 0s×10.10 en adelante y Linux Amazon Linux, Amazon Linux 2, CentOS 6, 7 y 8, Debian 9 y 10, Oracle Linux 6, 7 y 8, SuSe 12 y 15. Ubuntu 16 y 18 LTS.

Cordialmente,

INVSERTEC S.A.S.