ANEXO No. 001 - CONTRATO N° 008-2022
- COMUNICACIÓN DE ACEPTACIÓN DE OFERTA
CONTRATACIÓN DE MÍNIMA CUANTÍA.

- **CARACTERÍSTICAS GENERALES DE LA PLATAFORMA DE PROTECCIÓN**

El producto es una plataforma de protección de punto final que admite una solución de seguridad de información modular capaz de proteger cualquier entorno empresarial en un método escalable y de alta disponibilidad. El producto debe incluir los siguientes módulos:

- Consola de administración que proporciona las funcionalidades básicas y avanzadas de gestión de productos.
- Servicios de seguridad para equipos de escritorio físicos, portátiles y servidores.
- Servicios de seguridad para entornos virtualizados que proporcionan un servicio antimalware creado especialmente para un entorno virtualizado.
- Servicios de seguridad para dispositivos móviles que brindan seguridad y control de cumplimiento para teléfonos inteligentes y tabletas basados en sistemas operativos iOS y Android.
- Servicios de seguridad para la introspección del hipervisor que proporciona la introspección en tiempo real de la memoria de la máquina virtual para prevenir e identificar ataques avanzados.
- Servicios de seguridad para servidores que ofrecen opciones de antimalware, antispam, control de contenido y filtrado de archivos adjuntos

1.1. CONSOLA DE ADMINISTRACIÓN

1.1.1. Instalación y configuración:

1. El paquete de instalación debe entregarse como un solo dispositivo virtual (imagen virtual). Las plataformas de virtualización soportadas deben ser:

    a. VMware vSphere, VMware View, VMware Horizon suites
    b. Citrix XenServer, Citrix XenApp, Citrix XenDesktop
    c. Microsoft Hyper-V
    d. Red Hat Enterprise Virtualization
    e. Kernel-based Virtual Machine or KVM
    f. Oracle VM
    g. Nutanix

    Se deben admitir otras plataformas de virtualización si se realiza una solicitud al desarrollador de productos antimalware.

2. El producto debe permitir la implementación centralizada de máquinas de escaneo dedicadas.
3. Para fines de escalabilidad, el producto debe permitir que cualquier componente o servicio se instale de forma independiente o en un método agrupado
4. Para propósitos de escalabilidad, el producto debe tener componentes dedicados para servicios de base de datos, servicios de comunicación, actualización y servicios we1.2.
5. Para alta disponibilidad y balanceo de carga, el producto debe incluir un módulo dedicado de balanceador de carga disponible.

1.1.2. Características generales. El producto debe ofrecer las siguientes capacidades:

1. Licencia flexible (clave separada para cada servicio de seguridad que permite un número diferente de objetos con licencia y fechas de vencimiento diferentes, historial de todas las claves ingresadas) o licencia única que puede administrar todos los servicios de seguridad.
2. Actualización con un clic: un clic para actualizar todos los componentes de la consola de administración, sin depender de su orden de instalación ni de ningún otro requisito.
3. Actualizaciones a pedido que permitirán a los administradores elegir qué paquetes de servicios de seguridad se actualizarán para ahorrar ancho de banda.
4. Debería usar una base de datos no relacional / no SQL, sin requerir ninguna clave de licencia de terceros para implementaciones mayores que un cierto número de puntos finales.
5. Las notificaciones deben mostrarse en el menú principal, con aspectos destacados de los elementos no leídos, con la capacidad de enviarlo por correo electrónico, alertando al administrador sobre problemas importantes: problemas de licencias, alertas de brotes de malware y / o máquinas desactualizadas.
6. Debe contar con doble factor de autenticación gestionado con un código generado por la app Google Authenticator en su dispositivo móvil.
7. Capacidad para configurar reglas para eliminar automáticamente las máquinas virtuales, Servidores, Equipos sin utilizar del inventario de red y liberar sus puestos de licencia.

1.1.3. Panel de consola de administración. Para monitoreo y manejo de incidentes, el producto debe ofrecer:

1. Capacidad para agregar, eliminar, organizar, configurar y personalizar múltiples portlets de seguridad
2. Capacidad de soportar múltiples páginas con múltiples portlets de seguridad.
3. Capacidad para ofrecer información de seguridad en tiempo real con gráficos fáciles de leer.
4. Capacidad para configurar el destino de los informes, el fondo del tipo de informe de seguridad, el intervalo de tiempo para la información presentada y mostrada y el nombre del portlet.

1.1.4. Consola de Administración del inventario de red. Para la gestión de la seguridad de la infraestructura, el producto debe ofrecer:

1. Integración con Microsoft Active Directory, VMware vCenter, Citrix Xen para importar el inventario e información de estas plataformas.
2. Tiempo de sincronización configurable (en horas) con Microsoft Active Directory.
3. Integración con Microsoft Hyper-V, RedHat Linux Virtual Machine, Oracle VM, KVM y cualquier otra máquina virtual que se descubra a través del descubrimiento de la red.
4. Descubrimiento de redes para máquinas no integradas en Microsoft Active Directory, VMware vCenter, Citrix XenServer, tanto para estaciones de trabajo físicas como virtuales y servidores.
5. Búsqueda en tiempo real, clasificación y filtrado por nombre, sistema operativo, dirección IP, FQDN o etiqueta.
6. Capacidades de implementación remota y desinstalación del producto antimalware existente.
7. Paquetes de instalación manual y configurable para el producto antimalware.
8. Capacidad para configurar y ejecutar tareas de escaneo remoto.
9. Capacidad para reiniciar remotamente un punto final.
10. Capacidad para ver la sección de resultados de tareas centralizada con información detallada de cada subtarea.
11. Capacidad para asignar pólizas en todos los niveles de gestión.
12. Capacidad para configurar la herencia de políticas y forzar la configuración de políticas.
13. Capacidad para ver las propiedades detalladas de los puntos finales administrados, como el nombre, IP, sistema operativo, grupo, política asignada, el estado más reciente del malware, los últimos registros de análisis.

1.1.5. Políticas de la consola de Administración. Para la gestión de la seguridad de la infraestructura, el producto debe ofrecer:

1. Capacidad para aplicar políticas basadas en la ubicación y basadas en el usuario registrado.
2. Capacidad para aplicar varias políticas a un único punto final, pero solo una activa a la vez.
3. Capacidad para aplicar una política a un grupo de puntos finales.
4. Una plantilla única para cada servicio de seguridad.
5. Cada servicio de seguridad tiene su plantilla de política configurable con opciones específicas para activar / desactivar y configurar funcionalidades como el análisis antimalware, las capacidades de la zona de pruebas en la nube, las opciones de aprendizaje automático, la introspección del hipervisor, el cortafuegos, el control de acceso a la red, la inclusión en la lista blanca de aplicaciones, la lista negra de aplicaciones y el acceso a la we1.2. control, control de dispositivos, ubicación de dispositivos, aplicación de autenticación y acciones a tomar en caso de malware y dispositivos no compatibles detectados, como bloqueo remoto, desbloqueo, borrado, cifrado SD.

1.1.6. Informes de la consola de administración:

1. Gran cantidad de informes.
2. Fácil de usar desde una vista: resumen y detalles en la misma página, sección de resumen activo (filtra los detalles haciendo clic en la sección de resumen).
3. Programado, se puede enviar por correo a cualquier número de destinatarios (no es necesario tener también una cuenta en la consola).
4. Filtros para informes programados para recibir por correo únicamente información relevante para cada usuario.
5. Archivar con todas las instancias generadas de un informe programado.
6. Exportar resumen a archivo .pdf, detalles a archivo .csv.

1.1.7. Cuarentena:

1. Restauraciones remotas, con ubicación configurable y borrar.
2. Capacidad de centralizar la cuarentena para archivos infectados.
3. Descargue archivos, disponibles solo para máquinas virtuales integradas con vShield o NSX.
4. Personalice la hora en que los archivos se almacenan en cuarentena hasta 180 días.

1.1.8. Usuarios:

1. Administración basada en roles.
2. Múltiples tipos predefinidos: root, administrador, reporte o usuario personalizado.
   a. Root: gestiona los componentes de la solución.
   b. Administrador: gestiona los servicios de seguridad.
   c. Reporte: monitorea y crea informes.
1. Lista de usuarios que se puede importar desde Microsoft Active Directory (la autenticación AD se usará para iniciar sesión).
2. Configuración detallada de los derechos de destino administrativos, para seleccionar qué servicios y objetos puede administrar un usuario. Cierre de sesión automático para cualquier tipo de usuario para mayor seguridad con respecto a la información que se muestra en la consola de administración.

1.1.9. Logs:

1. Registrar las acciones del usuario para su cumplimiento.
2. Registros detallados para cada acción del usuario.
3. Búsqueda compleja.

1.1.10. Certificados de seguridad:

1. El acceso a la consola de administración debe estar protegido (https).
2. El servidor web, desde la consola de administración central, debe permitir la importación de certificados digitales emitidos por una autoridad de certificación con licencia o por su propia organización. Importar certificados para que sea intuitivo y hecho desde la consola de administración central.
3. Le permite importar la cadena de certificados de PKI (infraestructura de clave pública).
4. Debe admitir claves de cifrado de certificado digital con una longitud mínima de 1024 bits.
5. Los certificados digitales, una vez importados, deben ser reemplazables en caso de que caduquen o sean revocados.
6. Los certificados aceptados en el proceso de importación deben estar en formato pfx o p12 y protegidos por una contraseña.
7. La solución debe ser capaz de generar certificados digitales por sí misma.
8. La solución debe poder mostrar en la consola central información sobre los certificados: nombre, autoridad de emisión, fecha de emisión y fecha de vencimiento de los certificados emitidos.

1.1.11. Actualizaciones:

1. La solución debe permitir la prueba de nuevos kits o actualizaciones de productos en un entorno cerrado.
2. La solución debe poder definir y aplicar diferentes políticas para los puntos finales críticos de producción y actualizarlos después de que se haya probado el nuevo paquete.
3. El servidor de actualización puede actuar como una puerta de enlace para los datos.
4. La consola y la plataforma de pruebas deben poder descargar automáticamente nuevos kits.
5. La consola debe poder configurar el número máximo de kits que puede almacenar.
6. La opción de organización puede definir varios anillos de actualización para aplicar actualizaciones de productos.

1.2. PROTECCIÓN PARA ESTACIONES DE TRABAJO Y SERVIDORES

1.2.1. Características mínimas y mandatarias:

1. La existencia de un único motor antimalware.
2. Para minimizar el consumo de recursos, los productos antimalware deben permitir la instalación de módulos personalizados (por ejemplo, la instalación del producto antimalware sin el módulo de control de acceso web o sin el módulo Firewall).
3. **Agente y consola únicos:** Desarrollado desde cero como una solución de agente y consola únicos, que incorpora todas las tecnologías necesarias para proteger eficazmente los endpoints empresariales y detener todas las amenazas digitales. Elimina la necesidad de ejecutar varios agentes y simplifica significativamente la implementación y la operativa.

1.2.2. Requisitos del sistema:

- Sistemas operativos para estaciones de trabajo: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista (SP1), Windows XP (SP3).

- Tabletas y sistemas operativos integrados: Windows Embedded Standard 7, Windows Embedded POSReady 7, Windows Embedded Enterprise 7, Windows Embedded POSReady 2009, Windows Embedded Standard 2009, Windows XP Embedded con Service Pack 2, Windows XP Tablet PC Edition.
- Sistemas operativos de servidor: Windows Server 2016, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Small Business Server (SBS) 2008, Windows Server 2008 R2, Windows Server 2008, Windows Small Business Server (SBS) 2003,

Windows Server 2003 R2, Windows Server 2003 with Service Pack 1, Windows Home Server.

- Sistemas Operativos Linux: Ubuntu 14.04 LTS o superior, Red Hat Enterprise Linux / CentOS 6.0 o superior, SUSE Linux Enterprise Server 11 SP4 o superior, OpenSUSE Leap 42.x, Fedora 25 o superior(1), Debian 8.0 o superior, Oracle Linux 6.3 o superior, Amazon Linux AMI 2016.09 o superior.

- Sistemas Operativos macOS: macOS Catalina (10.15), macOS Mojave (10.14), macOS High Sierra (10.13), macOS Sierra (10.12), OS X El Capitan (10.11).

- Navegadores Web soportados: Internet Explorer 8+, Mozilla Firefox 30+, Google Chrome 34+, Safari 4+, Microsoft Edge 20+, Opera 21+

Administración e instalación remota:

1. Antes de la instalación, el administrador puede personalizar los paquetes de instalación incluyendo solo los módulos deseados: análisis basado en el comportamiento, cifrado completo del disco, firewall, control de contenido, control de dispositivos, control de aplicaciones, administración de parches.
2. La instalación se puede realizar de varias formas:
   a. Al descargar el paquete antimalware directamente a la estación de trabajo donde se instalara.
   b. Mediante la instalación remota, directamente desde la consola we1.2.
3. La instalación en máquinas desde una ubicación remota se realizará utilizando un cliente instalado existente en estas ubicaciones para minimizar el tráfico WAN.
4. La consola de administración informará el número de estaciones de trabajo que tienen el antimalware instalado y el número de estaciones de trabajo que están desprotegidas.
5. La consola de administración incluirá en los paneles / widgets configurables del panel de control.
6. La consola de administración incluirá información detallada sobre las estaciones de trabajo / servidores: nombre, IP, sistema operativo, módulos instalados, política aplicada, información de actualización, etc.
7. La consola de administración permitirá al administrador enviar una política para configurar todo el producto antimalware, tanto para estaciones de trabajo como para servidores.
8. La consola de administración permitirá dos tipos de cuentas, Administrador y Reportero, que pueden asignarse a qué grupos de usuarios pueden cambiar la configuración o generar informes.
9. La consola de administración incluirá una sección de registro donde se mencionarán todas las acciones, con información detallada: iniciar sesión, editar, crear, cerrar sesión, mover, etc.
10. La consola de administración permitirá la posibilidad de crear un paquete único, utilizado para sistemas operativos de 32 bits y de 64 bits, MAC y Linux.
11. La consola de administración permitirá al administrador crear grupos o subgrupos para la administración de estaciones de trabajo.
12. Tenga la posibilidad de seleccionar qué cliente descubrirá las otras computadoras en la red.

1.2.3. Las principales características y funcionalidades del antimalware y el módulo antispyware:

1. El administrador de la solución puede configurar el escaneo automático en tiempo real para que no analice archivos o archivos con un tamaño mayor que "x" M1.2.
2. El escaneo automático en tiempo real puede admitir escanear archivos con hasta 16 niveles de profundidad.
3. Escaneo heurístico del comportamiento y monitoreo de procesos.
4. Escaneo en la nube y tecnología de aprendizaje automático.
5. Capacidad para detectar ataques sin archivos, incluidos aquellos que utilizan herramientas legítimas del sistema operativo, como Powershell o intérpretes de scripts. La solución no debe bloquear globalmente los scripts para lograr esto.
6. Escaneo bajo demanda y en acceso de cualquier medio de almacenamiento de información (CD, discos duros externos, disco compartido). Además, el proceso de exploración se puede detener si los dispositivos de medios de almacenamiento contienen información de más de "x" M1.2.
7. Escaneo automático de correos electrónicos a nivel de estación de trabajo, independientemente del cliente de correo electrónico, para los protocolos SMTP y POP3.
8. Configuración de las rutas a escanear, hasta el nivel de archivo.

9. La solución debe proporcionar Exclusiones incorporadas para roles de servidor de Microsoft (DNS, DHCP, AD, Exchange, Sharepoint).
10. El producto antimalware permitirá definir la lista de exclusión del análisis, tanto para el análisis "en acceso" como para el análisis "a pedido", para ciertas carpetas, discos, archivos, extensiones o procesos.
11. Con una base de datos completa de firmas de spyware y detección heurística de estos programas, el producto tendrá que ofrecer protección antispyware.
12. Para no sobrecargar los recursos del sistema, el producto antimalware debe contener un solo motor de análisis. Podrá ejecutar exploraciones programadas con baja prioridad y puede apagarse automáticamente después de explorar la estación de trabajo.
13. Para una mayor protección, antimalware debe tener 4 tipos de detección: basada en firmas, basada en heurísticas, procesos de monitoreo continuo y escaneo en la nube.
14. Para una mayor protección, antimalware debería poder escanear HTTP y SSL también.
15. Para una mejor administración del antimalware instalado en las estaciones de trabajo, el producto incluirá la opción de establecer una contraseña para la protección de la desinstalación.
16. Para la seguridad del usuario, el cliente incluirá un módulo antiphishing que tendrá la opción de verificar los enlaces buscados con los motores de búsqueda (Asesor de búsqueda).
17. La aplicación antimalware debería ofrecer acceso para el sistema operativo Linux.

1.2.4. Firewall:

1. El módulo se puede instalar / desinstalar de acuerdo con las preferencias del administrador.
2. Se debe permitir bloquear el análisis de puertos.
3. Se debe permitir o denegar la conexión compartida a internet.
4. Capacidad de mostrar o no notificaciones cuando se une un nuevo equipo a la red Wifi
5. Capacidad de tener un sistema de detección de intrusos IDS tuneable.
6. Debe permitir aplicar perfiles basados en nivel de confianza (De confianza, Hogar/Oficina, Publico, Insegura, Dejar que decida Windows)
7. Capacidad de realizar reglas para aplicaciones y conexiones
8. Debe permitir los siguientes protocolos (TCP,UDP, 3PC,A/N,AH,ARGUS, ARIS,AX.25,BNA,BBC-RCC-MON,BNA,BR-SAT-MON, CBT,CFTP,CHAOS,CPHB,CPNX,CRTP,CRUDP,DCCP,DDP,DDX,DGP,EGP,EIGRP,EMCON,ENCAP,ESP, ETHERIP,FC,FIRE,GGP, GMTP,GRE,HIP,HMP,I-NLSP,IATP,ICMP,IDRP,IDRP-CMTP,IFMP,IGMP,IGP,IL,IPCV,IPcomp,IPIP,IPLT,IPPC,IPTM,IPX-in-IP,IPV6-FRAG,IPV6-ICMP,IPV6-NONXT,IPV6-OPTS,IPV6-ROUTE,IRTP,ISO-IP,ISO-TP4,KRYPTOLAN,L2TP,LARP,LEAF-1,LEAF-2,MANET,MERIT-INP,MFE-NSP,MHRP,MICP,MOBILE,MTP,MUX,NARP,NETBLT,NSFNET-IGP,NVP-II,OSPF,PGM,PIM,PIPE,PNNI,PRM,PTP,PUP,PVP,QNX,RDP,RSVP,RVD,SAT-EXPAK,SAT-MON,SCC-SP,SCPS,SCTP,SDRP,SECURE-VMT,SKIP,SM,SMP,SNP,SPS,SRP,SSCOPMCE,ST,STP,SUN-ND,SWIPE,SHIM6,SPRITE-RPC,TCF,TLSP,TP++,TRUNK-1,TRUNK-2,UTI,VINES,VISA,VMTP,VRRP,WB-EXPAK,WB-MON,WSN,XNET,XNS-IDP,XTP.

1.2.5. Cuarentena:

1. El producto antimalware debe permitir el envío automático de los archivos en cuarentena al laboratorio de virus.
2. El envío de los archivos en cuarentena se realizará automáticamente en un intervalo de tiempo predefinido (número de horas) establecido por el administrador.
3. El producto antimalware debe permitir la eliminación automática de archivos en cuarentena más antiguos que un período determinado, sin ocupar espacio de almacenamiento innecesario.
4. La capacidad de mover un archivo de la cuarentena a su ubicación original.
5. Cuarentena centralizaa.La capacidad de recopilar de forma segura todos los archivos en cuarentena desde puntos finales protegidos a una ubicación única para una investigación más profunda.
6. La cuarentena permitirá que los objetos se escaneen después de cada actualización de la firma.
7. El producto antimalware debe poder guardar una copia de un archivo de malware y enviarlo a cuarentena antes de realizar acciones de Eliminar o Desinfectar.

1.2.6. Protección de datos:

1. Permite el bloqueo de datos confidenciales (tarjeta de identificación personal, cuenta bancaria, etc.) tanto para HTTP como para SMTP, mediante la creación de reglas específicas.

1.2.7. Control de Usuario:

1. El producto habrá integrado un módulo de control de usuario con las siguientes características:
    a. Bloqueo del acceso a Internet para clientes específicos o grupos de clientes.
    b. Bloqueando el acceso a ciertas aplicaciones.
    c. Bloqueando el acceso a internet por ciertos periodos de tiempo.
    d. Bloqueo de páginas web que contengan determinadas palabras clave.
    e. Permitiendo el acceso a páginas web específicas especificadas por el administrador.
    f. Restringir el acceso a ciertos sitios web por algunas categorías predeterminadas (por ejemplo, citas en línea, violencia, etc.).

1.2.8. Control de dispositivos:

1. Previene las fugas de datos confidenciales y las infecciones de malware a través de dispositivos conectados.
2. Aplique reglas de bloqueo y exclusiones a través de políticas a una amplia gama de dispositivos y tipos.
3. Enviará información como el nombre del dispositivo, ID de clase, fecha y hora de conexión.
4. Tenga tipos predefinidos de dispositivos como: CDROM, dispositivos de imagen, unidades de cinta, puertos COM / LPT, incursión SCSI, impresoras, NIC, almacenamiento interno y externo, etc.
5. Admite diferentes configuraciones y privilegios como Permitido, Bloqueado o Personalizado
6. Admite el modo de solo lectura para dispositivos de almacenamiento.
7. Capacidad para bloquear solo el USB y permitir que se utilicen todos los demás puertos.
8. Permitir la configuración de exclusiones para diferentes tipos de dispositivos.
9. Soporte para definir exclusiones de dispositivos:
    a. Por ID de producto
    b. Por ID de dispositivo, ID de hardware
10. Habilidad para descubrir dispositivos.

1.2.9. Defensa a ataques de RED:

1. Capacidad para detectar ataques avanzados y actividades sospechosas en la fase previa de ejecución.
2. Personalización para adaptarse a los requisitos de seguridad de la empresa
3. Capacidad detectar las siguientes técnicas de ataques:
    a) Acceso Inicial
    b) Acceso a Credenciales
    c) Detección
    d) Movimientos Laterales
    e) Crimeware
4. Capacidad para poder tomar acciones de acuerdo a la incidencia identificada, las acciones que deben estar disponibles son las siguientes,
    a) Bloquear o Solo informar

1.2.10. Actualizar:

1. Posibilidad de esperar a que se reinicie la computadora después de la actualización, sin notificar al usuario.
2. Sistema de actualización en cascada utilizando un servidor de actualización local (Relay).
3. Actualice los clientes en una ubicación remota a través de un cliente existente con la función de servidor de actualización integrada.
4. La función del servidor de actualización del cliente debe estar disponible para los sistemas operativos Windows y Linux.

1.2.11. Capacidad para realizar diversas acciones en los correos electrónicos que coincidan con las reglas de filtrado de contenido, incluido el prefijo del asunto del correo electrónico con una etiqueta específica, eliminar, poner en cuarentena o redirigir el correo electrónico a un buzón específico.

1. La solución debe proporcionar capacidades de filtrado de archivos adjuntos para el tráfico de correo electrónico entrante, interno y saliente, según el tipo de archivo adjunto o nombre de archivo.
2. Capacidad para realizar diversas acciones en los correos electrónicos que coinciden con las reglas de filtrado de archivos adjuntos, incluida la eliminación o el reemplazo del archivo adjunto, el prefijo del asunto del correo electrónico con una etiqueta específica, la eliminación, la puesta en cuarentena o la redirección del correo electrónico a un buzón específico.
3. Capacidad para bloquear conexiones SMTP según la dirección de correo electrónico o el dominio del remitente.
4. Capacidad para definir direcciones IP autorizadas para enviar correos electrónicos para dominios propios para chequeos antispoofing.
5. Capacidad para definir reglas de filtrado personalizadas basadas en grupos de usuarios.
6. Capacidad para ver estadísticas e informes sobre la actividad de filtrado de correo electrónico.
7. Capacidad para ver y administrar de manera centralizada los elementos en cuarentena, incluida la capacidad para descargar o restaurar elementos en cuarentena.

1.2.12. Anti Exploit Avanzado.

1. Debe proporcionar protección en ejecución contra intentos de explotación dirigidos a vulnerabilidades conocidas y desconocidas en aplicaciones de uso común.
2. Capacidad para agregar aplicaciones personalizadas y presentar una lista de aplicaciones predefinidas.
3. Se debe tener las siguientes técnicas de detección para exploits:

- ROP Emulation
- ROP Stack Pivot
- ROP Illegal Call
- ROP Stack Misaligned
- ROP Return To Stack
- ROP Make Stack Executable
- Flash Generic
- Shellcode Execution
- Shellcode LoadLibrary UNC
- Anti-Detour
- Flash Payload
- ROP Create Thread
- Anti-Meterpreter
- Obsolete Process Creation
- Child Process Creation
- Enforce Windows DEP
- Enforce Module Relocation (ASLR)

Las acciones que se deben permitir de acuerdo a cada técnica de detección serán, solo informar o detener proceso.

1.2.13. Administración del Riesgo.

1. Se debe proporcionar un módulo para la administración del riesgo que proporcione indicadores de riesgo de todos los endpoints junto con la descripción de cada punto de riesgo y su correspondiente recomendación para mitigar la afectación por configuración.
2. Se debe tener la capacidad de resolver características de riesgo de forma automática con un botón de acción.
3. La administración de riesgo debe gestionar los diferentes puntos de riesgo a nivel de sistema operativo, navegadores y a nivel de red.
4. A nivel de seguridad de navegadores se debe tener la capacidad de detectar hasta 114 indicadores de riesgo

5. A nivel de Red y credenciales se deben tener la capacidad de detectar hasta 49 indicadores de riesgo.
6. A nivel de sistema operativo se deben tener la capacidad de detectar hasta 94 indicadores de riesgo
7. Desde la política se debe tener la opción de habilitar o deshabilitar el módulo de Administración del riesgo
8. Se tiene que contar con un programador en el cual se gestione el escaneo de riesgos de seguridad por días, semanas y horarios en específico.
9. Capacidad de resolver automáticamente ciertos indicadores de riesgo.
10. Capacidad de resolver problemas y recopilar registros remotamente de los Endpoints desde un solo lugar.
11. Capacidad de tener un registro avanzado en el endpoint para recopilar registros específicos mientras reproduce el problema.
12. Capacidad de recopilar registros de endpoints e información general necesaria para la resolución de problemas.

2. SERVICIOS DE CAPACITACIÓN PRESENCIAL ASISTIDA POR TECNOLOGÍA

Se requiere que el contratista realice capacitación del antivirus a suministrar. La capacitación se debe realizar en las oficinas de la entidad , y será dirigida al personal técnico de sistemas.

La capacitación debe abarcar las siguientes temáticas:

- Introducción al antivirus a suministrar
- Mecanismo de instalación, configuración y parametrización segura de antivirus
- Identificación de ataques y vulnerabilidades
- Administración de ambientes
- Protección contra amenazas basada en
- Aprendizaje automático (Machine Learning – ML)
- Protección de datos
- Capacidad de instalar la solución de seguridad en smartphones y tablets Android, IOS
- Creación de perfiles
- Configuración de seguridad y protección para correos electrónicos
- Capacidad Control de funciones y Control web
- Activación de Cloud
- Políticas y configuraciones

3. MANTENIMIENTO REMOTO DE SOFTWARE DE ANTIVIRUS POR 24 MESES

Se requiere que el contratista ofrezca el servicio de soporte y asistencia técnica del software antivirus a suministrar. El servicio de soporte y asistencia técnica debe contar con las siguientes características:

- Jornadas de asistencia técnica de revisión preventiva cada tres (3) meses.
- Soporte técnico por problemas técnicos.
- Habilitación de Help Desk sobre las demandas más comunes de los usuarios, el cual debe contener un centro de ayuda (documento) donde los usuarios encuentran asistencia sobre las funcionalidades y módulos del antivirus a suministrar.
- Posibilidad de ofrecer el servicio de soporte y asistencia técnica habilitado con múltiples canales.