QUINTANA ROO
GOBIERNO DEL ESTADO
2016 • 2022

MÁS Y MEJORES OPORTUNIDADES

SEDE
SECRETARÍA DE DESARROLLO ECONÓMICO

IQIT
INSTITUTO QUINTANARROENSE DE INNOVACIÓN Y TECNOLOGÍA

INSTITUTO QUINTANARROENSE DE INNOVACIÓN Y TECNOLOGÍA

CARACTERÍSTICAS MÍNIMAS PARA LA ADQUISICIÓN O RENOVACIÓN DE LA SUITE DE SEGURIDAD

CONTENIDO

1. Módulo de Antivirus.

Un antivirus es un programa informático que tiene el propósito de detectar y eliminar virus y otros programas perjudiciales antes de que ingresen al sistema. Estas aplicaciones han sido diseñadas como medida de protección, y seguridad para resguardar los datos, y el correcto funcionamiento de los sistemas informáticos ya sea casero, empresarial, gubernamental y educativo, de aquellas aplicaciones conocidas comúnmente como virus o malware que tienen el fin de alterar, perturbar o destruir el correcto desempeño de las computadoras.

Características mínimas necesarias en esta funcionalidad:

1.1. Protección de la capa de **WinSock** o **Comunicaciones** (ejemplo: WWW, HTML, FTP etc.)
1.2. Dos motores de detección como mínimo, con protección heurística proactiva.
1.3. Inicio del equipos usando un ***CD de Rescate***, esto en caso de falla del Sistema Operativo.
1.4. Protección del sector de arranque en el modo seguro basado en una contraseña.
1.5. Vacunación de USB
1.6. Protección de direcciones IP, Registro de Windows y Host.
1.7. Uso de derecho de acceso a archivos, y prevención de la posible modificación de los mismos.
1.8. Copia de seguridad automática, y restauración de archivos de sistema operativo.
1.9. Escaneo de registro, archivos críticos de Windows y en memoria al momento de su instalación.
1.10. Descarga automática de las actualizaciones de seguridad del Sistema operativo Windows
1.11. Teclado Virtual para evitar los Keyloggers (registrador de teclas).
1.12. Protección de archivo y carpeta definido por el usuario para evitar su modificación o eliminación.
1.13. Cuente con Certificado ICSALAB y esté presente en el Cuadrante de RAP de Virus Bulleting. En los primeros lugares.

2. Módulo de Antivirus para correo electrónico.

Uno de los principales objetivos en la actualidad de las empresas que se dedican al Malware es el correo electrónico, debido al auge y amplitud de su uso a nivel mundial. El correo electrónico o email es un medio de comunicación bastante seguro, ya que los principales proveedores emplean para su transmisión un protocolo seguro (HTTPS), lo que hace casi imposible en la práctica que puedan ser alterados a propósito el contenido de los mensajes.

El punto débil o talón de Aquiles del correo son los archivos adjuntos. En ellos se tratan de introducir principalmente ejecutables de virus, Troyanos (Caballos de Troya) o Spyware. Para eso aprovechan los programadores de los virus residentes en el equipo, introducidos previamente, que los adjuntan de forma inadvertida a mensajes enviados por el usuario, además se aprovechan del descuido y candidez de los que reciben estos mensajes contaminados.

Características mínimas necesarias en esta funcionalidad:

2.1. Escaneo de Correos Electrónicos con tecnologías Modelo de aprendizaje no intrusivo (NILP) & Consulta sobre la reputación del dominio y dirección de IP (DIRC).
2.2. Verificación de archivos adjuntos en correo y bloqueo de archivos adjuntos por tipo de archivo.
2.3. Verificación de correos entrantes y salientes vía puerto SMTP (protocolo para transferencia simple de correo) y POP3 (Protocolo de oficina de correos o Protocolo de Oficina Postal).
2.4. Autoarchivado de correos y adjuntos en un disco loca o en la red.

3. Anti-Spam.

El AntiSpam es lo que se conoce como método para prevenir el correo basura. Tanto los usuarios finales como los administradores de sistemas de correo electrónico utilizan diversas técnicas contra ello. Algunas de estas técnicas han sido incorporadas en productos, servicios y software para aliviar la carga que cae sobre usuarios y administradores.

Las técnicas AntiSpam se pueden diferenciar en cuatro categorías: las que requieren acciones por parte humana; las que de manera automática son los mismos correos electrónicos los administradores; las que se automatizan por parte de los remitentes de correos electrónicos; las empleadas por los investigadores y funcionarios encargados de hacer cumplir las leyes.

Características mínimas necesarias en esta funcionalidad:

3.1. Escaneo de Correos Electrónicos con tecnologías Modelo de aprendizaje no intrusivo (NILP) & Consulta sobre la reputación del dominio y dirección de IP (DIRC).
3.2. Verificación del correo electrónico por frases (ejemplo: Sexo, Viagra.).
3.3. Verificación de dominios a través de servidores de RBL (Real Time Blackhole List) para evitar que nos llenen el servidor con spam o correo no deseado.
3.4. Clasificación de servidores de confianza a través de una lista blanca de forma automática.
3.5. Filtro Phishing para correo.
3.6. Escaneo de correos a 8 y 16 bits.

4. Protección Web o Navegación Web Segura.

El Navegación Web Segura se ha diseñado principalmente para el acceso en línea a sistemas bancarios y otros sitios web que procesan datos confidenciales. Cuando utiliza Navegación Web Segura, todos los cambios (guardar cookies, informe de sitios web visitados, etc.) van a permanecer en el ambiente seguro y no va a afectar al sistema operativo, lo cual significa que no puede ser explotada por intrusos. Si es necesario, puede limpiar todos los cambios efectuados al navegador seguro y restaurar la configuración predeterminada. Cuando estamos trabajando con servicios bancarios online, el usuario necesita una protección especial, ya que las fugas de información confidencial pueden dar lugar a pérdidas financieras.

Características mínimas necesarias en esta funcionalidad:

4.1. Navegación Web categorizada por ejemplo: Pornografía, Drogas, Phishing y Fraude etc.
4.2. Restricción Horaria Basado en el usuario y tiempo.
4.3. Filtro Web Phishing y URL Malware.
4.4. Detección de páginas web contaminadas.
4.5. Capacidad de crear nuevas categorías en base al requerimiento del usuario.
4.6. Políticas de navegación aplicables a grupos o usuarios
4.7. Bloqueo de streaming, audio y video selectivo (Java & Scripts)
4.8. Estadísticas de bloqueo por usuario y equipo.

5. Firewall (Cortafuegos).

Un Cortafuegos (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Este cortafuego se configura para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos, sobre la base de un conjunto de normas y otros criterios.

Características mínimas necesarias en esta funcionalidad:

5.1. Firewall Inteligente de doble vía (independiente a Windows) con sistema de prevención de intrusos (IPS) / sistema de detección de intrusos (IDS)
5.2. El Firewall debe trabajar bajo comunicaciones Capa 3 OSI.
5.3. Monitor de Estado de Conexiones Activas
5.4. Encriptación en puertos de comunicación Consola – Estación de Trabajo – Consola.

6. Seguridad de Punto Final.

Control de dispositivos o Seguridad de Punto final: es simplemente restringir el acceso en los volúmenes de almacenamiento, dispositivos, interfaces, etc. El Control de dispositivos es un componente importante de Endpoint Security que permite controlar y restringir el acceso a los dispositivos de entrada y salida que puedan ser administrados por ejemplo: el USB, las unidades de CD/DVD.

Características mínimas necesarias en esta funcionalidad:

6.1. Control de aplicaciones permitidas y no permitidas para su uso dentro del equipo con restricción basada en horario.
6.2. Historial de archivos copiados a USB.
6.3. Clave de activación y lectura de USB.
6.4. Exclusión de escaneo de USB basado en clave de autorización.
6.5. Bloqueo de la Cámara Web.
6.6. Bloqueo de Tarjetas SD.
6.7. Control de Bluetooth.
6.8. Bloqueo de CD o DVD.
6.9. Estadísticas de archivos bloqueados o infectados por equipo.

7. Control de Privacidad.

Su información privada es un objetivo constante para los ciberdelincuentes. Como las amenazas se han extendido a prácticamente todo el espectro de las actividades online, el correo electrónico, la mensajería instantánea y la navegación web que no estén protegidos debidamente pueden producir la fuga de información que ponga en compromiso su privacidad.

Características mínimas necesarias en esta funcionalidad:

7.1. Realiza un mantenimiento lógico del equipo donde se eliminen cookies, archivos recientes, ultimas búsquedas de equipos etc.
7.2. Debe permitir configurar diferentes directorios para su eliminación.
7.3. Mantenimiento lógico sobre archivos de Microsoft Office.

8. Seguridad en la Nube.

La Red de Seguridad basada en la nube, asegura la protección contra amenazas actuales, tales como virus, gusanos y troyanos. Identifica y bloquea nuevas amenazas antes de que se extienda y al tratarse de un nuevo malware, permite tener una respuesta rápida con un nivel avanzado de detección que proporciona una protección superior de día 0.

Un ataque de día-cero (en inglés zero-day attack o 0-day attack) es un ataque contra una aplicación o sistema que tiene como objetivo la ejecución de código malicioso gracias al conocimiento de vulnerabilidades que, por lo general, son desconocidas para la gente y el fabricante del producto. Esto supone que aún no hayan sido arregladas.

Este tipo de exploit circula generalmente entre las filas de los potenciales atacantes hasta que finalmente es publicado en foros públicos. Un ataque de día cero se considera uno de los más peligrosos instrumentos de una guerra informática

Características mínimas necesarias en esta funcionalidad:

8.1. Protección y seguridad de los dispositivos basados en la nube [Cloud Security].
8.2. Detección Día 0 basado en la nube esto vía Consola de Administración Remota y en las Estaciones de Trabajo.
8.3. Debe permitirse estar firmado a la nube de forma permanente para recibir actualizaciones críticas.
8.4. Recibir notificaciones del Cloud sobre nuevas amenazas.

9. Soporte Remoto.

Administración Remota a la funcionalidad de algunos programas que permiten realizar ciertos tipos de acciones desde un equipo local y que las mismas se ejecuten en otro equipo remoto.

Características mínimas necesarias en esta funcionalidad:

9.1. Aplicación integrada dentro de la Suite de Seguridad para poder brindar Soporte Remoto tanto externo como interno.

10. Consola de Administración Remota Centralizada o en la Nube.

La Consola de Administración es un interfaz que provee acceso a las funciones del Servidor de Administración, de manera local o remotamente a través de la red o a través de una Nube segura publicada en el Internet. También puede instalar una Consola a cualquier ordenador o equipo de cómputo en la red corporativa que satisface los requerimientos del sistema. Puede instalar cualquier número de Consolas en una red. Además hay posibilidad de instalar/actualizar la versión de la Consola de Administración de forma remota.

Características mínimas necesarias en esta funcionalidad:

10.1. Consola de Administración Remota Vía Web (HTTP y HTTPS) Publicable en la Nube con puertos encriptados.
10.2. Soporte para HIPS (Sistema de prevención de intrusiones basado en el Host) y SSL (Secure Sockets Layer es un protocolo diseñado para permitir que las aplicaciones para transmitir información de ida y de manera segura hacia atrás.), con encriptado de puertos (128 bits mínimos).
10.3. Soporte e Interacción con Active Directory y encriptación de puertos del Directorio Activo de Microsoft.
10.4. Administración y actualización de equipos y dispositivos a través de la nube (Cloud).
10.5. Resumen de los primeros diez (Top Ten).
10.6. Capacidad de manejo de múltiples consolas y servidores de actualización.
10.7. Envió y replicación de políticas desde grupos a estaciones de trabajo y viceversa.
10.8. Instalación de clientes de forma local y remota de forma automática vía grupos.
10.9. Instalación remota de software de terceros (ejemplo: Office, Adobe etc.).
10.10. Encendido remoto de estaciones de trabajo para escaneo de Malware.
10.11. Monitoreo de las Impresiones en Red.
10.12. Soporte para múltiples sistemas operativos dentro de una misma Consola de Administración Remota (Ejemplo: Windows, Linux, Mac y Android).

10.13. Gestión y captura de datos vía SNMP (protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red).
10.14. Gestión de registros de eventos vía SYSLOG (es un estándar de facto para el envío de mensajes de registro en una red informática IP) Integrada.
10.15. Plantillas de Reportes Programables (ejemplo: tipo de reporte, día, mes, año y/o rango de fechas).
10.16. Exportación de reportes en formatos de: Excel (XLS), Acrobat Reader (PDF), Archivos separados por coma (CVS) y Visualización de elementos a través de la Web vía navegador (HTML).
10.17. Alertas de eventos de infección o actualización de bases de firmas a través de un correo electrónico.
10.18. Reporte de inventario a nivel de Hardware y Software de los equipos o dispositivos administrados desde consola.
10.19. Administración de licencias de software centralizada. (Consola Principal y SubConsolas).
10.20. Historial de eventos de la impresión de documentos y archivos copiados a USB.
10.21. Capacidad para enviar tareas y configuraciones especiales a equipos administrados.
10.22. Localización remota y control de robo de dispositivos basados en Android.
10.23. Capacidad para agendar escaneos y actualizaciones mediante políticas.

INSTITUTO QUINTANARROENSE DE INNOVACIÓN Y TECNOLOGÍA
Directorio de Servidores Públicos

PARTICIPARON EN LA ELABORACIÓN

Marco Antonio Bravo Fabian
Director General
marco.bravo@qroo.gob.mx

Natividad Cauich Rivero
Coordinadora de Normatividad y Planeación
natividad.cauich@qroo.gob.mx

German Gongora
Analista Profesional
german.gongora@qroo.gob.mx

Última modificación: Junio, 2018

Carlos A. Vidal #23
Fovissste II Etapa
Chetumal, Quintana Roo, México
Tel:(983) 83 50700 ext. 25200
qroo.gob.mx/iqit