Guía de ciberseguridad para pequeñas empresas y emprendimientos

Fecha de creación
29/07/2021

Tipo de publicación
Guía técnica

Resumen

Cómo mejorar la ciberseguridad de una pequeña empresa o emprendimiento.

La ciberseguridad no tiene por qué ser un desafío abrumador para las pequeñas empresas. En esta guía se describen 5 claves que permiten adoptar medidas básicas de ciberseguridad, y establecer un entorno de negocio digitalmente más seguro.

Es importante que las medidas que se tomen persistan y mejoren a lo largo del tiempo. Para poder apoyar en este proceso, Agesic pone a disposición además de esta guía, el Marco de Ciberseguridad, un documento que aborda de manera integral los riesgos de ciberseguridad en las empresas y cuenta con una guía de implementación para mejorar la madurez de las medidas adoptadas.

Introducción

Esta guía permitirá

- Tomar medidas básicas de seguridad para establecer un entorno de negocio digitalmente más seguro.
- Preservar aspectos claves de la información que maneja una empresa o emprendimiento, cuidando su veracidad, su disponibilidad y siendo accesible solo para quienes debe serlo.
- Reducir las posibilidades de sufrir un incidente de ciberseguridad, y el impacto que este pueda tener, en caso de que ocurra

5 claves para mejorar la ciberseguridad

1: Usar contraseñas para proteger los datos

2: Realizar copias de seguridad

3: Mantener seguros los dispositivos móviles

4: Proteger la empresa o emprendimiento de malware

5: Prevenir ataques de phishing

Obtener plan de acción de ciberseguridad

Respondiendo algunas preguntas se obtiene una lista personalizada de acciones para ayudarte a ti, a tu empresa o emprendimiento a mejorar la ciberseguridad.

Cuestionario para pequeñas empresas y emprendimientos

Recursos

Firma digital e Identificación electrónica

Glosario de términos de ciberseguridad

Guía de gestión de vulnerabilidades

Marco de Ciberseguridad

Medios de pago

Redes sociales

Usar contraseñas para proteger los datos

Las contraseñas, cuando se implementan correctamente, son una forma fácil y eficaz de evitar que alguien acceda sin autorización a los dispositivos y a la información que se encuentra almacenada en ellos o en sitios web a los que se accede usualmente.

Esta sección contiene 5 consejos a tener en cuenta al usar contraseñas

Consejo 1: Activar la protección por contraseña

Establecer una contraseña de bloqueo de pantalla, un PIN u otro método de autenticación como huella digital o desbloqueo facial. Si se utiliza principalmente el desbloqueo de huellas dactilares o facial, la contraseña se usará con menos frecuencia, por lo que se recomienda elegir una contraseña larga, con caracteres variados, que sea difícil de adivinar y simple de recordar.

Para obtener más información sobre bloqueo en: Android, Iphone

Consejo 2: Evitar el uso de contraseñas predecibles

Es importante que las personas que trabajan en la empresa o emprendimiento reciban información útil sobre cómo establecer contraseñas que sean fáciles de recordar y que eviten las contraseñas más comunes, que los ciberdelincuentes pueden adivinar fácilmente.

Recordar que el equipo de tecnologías de la información o quienes se encargan del soporte técnico no soliciten al resto de las personas que trabajan en la empresa o emprendimiento que se le compartan cuentas o contraseñas para hacer su trabajo. Asegurarse que cada usuario tenga acceso personal a los sistemas y de que el nivel de acceso proporcionado sea siempre el mínimo necesario para hacer su trabajo, reduciendo de esta forma, la exposición innecesaria a los sistemas a los que no necesitan acceder.

Consejo 3: Usar doble factor de autenticación

La autenticación permite demostrar que un usuario es realmente quién asegura ser. La contraseña o clave no autentica a una persona.

Una identificación exitosa garantiza que la persona conoce la clave, pero no hay forma de diferenciar un usuario legítimo de un intruso que ha podido acceder a la clave.

Si existe la opción de utilizar el doble factor de autenticación para cualquiera de las cuentas, se debería hacer.

Existen 4 maneras de autenticarse:

- Por algo que se sabe: clave o contraseña.
- Por algo que se tiene: tarjeta de coordenadas, token o celular.
- Por algo que es: patrón único huella, patrón único iris, reconocimiento del habla, etc.
- Dónde se está: usando una terminal particular.

Doble factor de autenticación significa, que se deben utilizar dos métodos diferentes para "probar" la identidad antes de poder utilizar un servicio, generalmente una contraseña y alguna de las opciones comentadas. Este podría ser un SMS que se envía al celular o un código que se genera a partir del lector de tarjetas de un banco que se debe ingresar, además de la contraseña.

Consejo 4: Ayudar al personal a gestionar y generar buenas contraseñas

En la empresa, se deben recordar muchas contraseñas, relacionadas o no con el trabajo, así que:

- Aplicar el acceso con contraseña a un servicio solamente si realmente lo necesita.
- No aplicar cambios de contraseña regulares, las contraseñas solo necesitan cambiarse cuando sospechas que las credenciales de inicio de sesión están comprometidas.
- Asegurarse que el personal pueda cambiar y restablecer sus propias contraseñas fácilmente, ya que con seguridad las olvidará.

Considerar usar gestores de contraseñas (herramientas que pueden crear y almacenar contraseñas) a las que se accede a través de una contraseña "maestra". Dado que la contraseña maestra protege todas las demás contraseñas, asegurarse de que sea segura, por ejemplo, utilizando una frase. Probar la seguridad de la contraseña en este enlace.

Consejo 5: Cambiar todas las contraseñas predeterminadas

Uno de los errores más comunes es no cambiar las contraseñas predeterminadas de los fabricantes con las que se emiten los celulares, notebooks y otros tipos de equipos o aplicaciones.

Cambiar todas las contraseñas predeterminadas antes de que los dispositivos se distribuyan a quienes trabajan en la empresa o emprendimiento.

Acceder a la infografía: Usá contraseñas para proteger los datos de tu empresa o emprendimiento

Realizar copias de seguridad

Independientemente del tamaño de la empresa u emprendimiento, es importante realizar copias de seguridad (respaldos) de datos importantes. Estos respaldos deben hacerse de manera semanal. Esto permitirá que el comercio o negocio pueda seguir funcionando después de un incidente como, por ejemplo, robo, o lo que es cada vez más usual, un ciberataque.

Las empresas generan información valiosa que es importante preservar y así utilizarla de forma correcta, tanto por el personal como por terceros.

No sería posible mantener un negocio sin datos, como información de los clientes, ingresos, costos, los pedidos o los detalles de pago.

Tener copias de seguridad que se puedan recuperar rápidamente permite, por ejemplo, evitar ataques de*ransomware*.

En esta sección, se describen tres aspectos a tener en cuenta para realizar una copia de seguridad de los datos más importantes de una empresa**.**

Consejo 1: Identificar qué datos es necesario respaldar

El primer paso es identificar los datos esenciales, aquella información sin la que la empresa no podría funcionar. Puede incluir documentos, fotos, correos electrónicos, contactos, calendarios, la mayoría de los cuales se guardan en unas pocas carpetas comunes en tu computadora, teléfono, tableta o red.

Consejo 2: Mantener un respaldo de seguridad separado de su ubicación original

La restricción del acceso a las copias de seguridad ya sea a través de una red, o físicamente, es fundamental para que, en caso de sufrir un incidente, la copia no se vea afectada.

El *ransomware* u otros tipos de *malware* a menudo pueden pasar al almacenamiento adjunto automáticamente, lo que significa que cualquier respaldo local también podría estar infectado, siendo imposible recuperarlo.

Para respaldar, se puede utilizar una memoria USB, disco extraíble, o una computadora separada; sin perder de vista que no deben estar conectados, ya sea físicamente o a través de una red local, al dispositivo que contiene la copia original.

También podrías evaluar el uso de almacenamiento en la nube donde un proveedor de servicios almacena tus datos en su infraestructura y de esta manera también quedan físicamente separados de su ubicación original.

Consejo 3: Generar una rutina de respaldos semanal

Hacer una copia de seguridad es una tarea que se debe mantener en el tiempo, para lograrlo de forma práctica, lo mejor es automatizarla, garantizando la última versión de los archivos en caso de que los necesites.

La mayoría de las soluciones de almacenamiento en red o en la nube permiten hacer copias de seguridad automáticamente.

Para elegir una solución hay que considerar cuántos datos hay que respaldar y qué tan rápido es necesario acceder a los mismos en caso de un incidente.

Acceder a la infografía: Realizá copias de seguridad en tu empresa o emprendimiento

Mantener seguros los dispositivos móviles

La tecnología móvil es una parte esencial en la actividad de la empresa. Estos dispositivos son ahora muy potentes y necesitan incluso más protección que los equipos de "escritorio".

Compartimos 4 consejos rápidos que pueden ayudar a mantener seguros los dispositivos móviles y la información almacenada en ellos**.**

Consejo 1: Activar la protección por contraseña y cifrá tu dispositivo

Un PIN o contraseña adecuadamente complejas, evitará que el atacante acceda al teléfono. No utilizar una simple, o que se pueda deducir o extraer fácilmente de perfiles de redes sociales, por ejemplo.

Muchos dispositivos ahora incluyen reconocimiento de huellas dactilares para bloquear tu dispositivo, sin la necesidad de una contraseña. Sin embargo, estas funciones no siempre están habilitadas "listas para usar", por lo que se deberá verificar que estén activas.

Para obtener más información sobre bloqueo: Android o Iphone

Para notebooks o PC, es recomendable utilizar un producto de cifrado como BitLocker para Windows usando cifrado de dispositivo, o FileVault en macOS.

La mayoría de los dispositivos modernos tienen cifrado integrado, pero es posible que el cifrado deba activarse y configurarse.

Consejo 2: Activar rastreo, bloqueo y borrado remoto

La mayoría de los dispositivos incluyen funciones que permiten:

- Rastrear la ubicación.
- Bloquear de forma remota el acceso (para evitar que alguien más lo use).
- Borrar de forma remota los datos almacenados.
- Recuperar una copia de seguridad.

Para configurar estas funciones en todos los dispositivos de la empresa, se pueden utilizar los siguientes enlaces:

- Android: Cómo borrar, encontrar o bloquear un dispositivo.
- iPhone: Si perdés o te roban el iPhone, el iPad o el iPod touch

Consejo 3: Actualizar dispositivos y aplicaciones

Todos los fabricantes (por ejemplo, Windows, Android, iOS) publican periódicamente actualizaciones de seguridad críticas para mantener el dispositivo protegido.

Independientemente de los dispositivos y aplicaciones que se utilicen en la empresa, es importante que se actualicen en todo momento y se hayan configurado para que se haga de manera automática, siempre que sea posible.

Asegurarse que el personal sepa lo importantes que son estas actualizaciones y se debe explicar cómo hacerlas, si fuera necesario.

Consejo 4: Utilizar únicamente redes wifi conocidas

Cuando se utilizan puntos de acceso wifi públicos, por ejemplo, en hoteles o cafeterías, no hay forma de averiguar fácilmente quién controla el punto de acceso o de demostrar que pertenece a quien crees que pertenece. Si se establece conexión con estos puntos de acceso, otra persona podría acceder a:

- Lo que se está trabajando mientras se utilice la conexión.
- Los datos de inicio de sesión de aplicaciones y servicios web.

La precaución más simple es no conectarse a internet utilizando wifi desconocidas y, en su lugar, utilizar su red móvil que tendrá seguridad incorporada. Esto significa que también puedes compartir tu conexión de datos del teléfono con otro dispositivo.

Conocer cómo hacerlo:

- Android: Cómo compartir una conexión mediante un hotspot o un dispositivo móvil en Android
- iOS: Cómo configurar Compartir Internet en el iPhone o iPad

Consejo 5: Utilizar siempre los sitios oficiales para la descarga de tus aplicaciones

Es importante que se descarguen aplicaciones para teléfonos móviles y tabletas de tiendas aprobadas por el fabricante (como *Google Play* o *Apple App Store*). Estas aplicaciones se comprueban para proporcionar un cierto nivel de seguridad.

Es recomendable, además:

- Mirar el número de descargas que tiene la aplicación.
- Analizar los comentarios y valoraciones de la aplicación antes de descargarla.
- Comprobar quién ha creado la aplicación.
- Revisar los permisos que solicita la aplicación al instalarse, no los permita sino son necesarios para su funcionalidad.

- Más información sobre sitios oficiales en: Android, iPhone, iPad y iPod touch

Acceder a la infografía: Mantené seguros los dispositivos móviles de tu empresa o emprendimiento

Prevenir ataques de phishing

Se denomina *Phishing* al conjunto de técnicas que persiguen el engaño de una persona, imitando la identidad de un tercero de confianza, como podría ser un banco, una institución pública, empresa o red social, con el fin de manipularla y lograr que brinde información (por ejemplo, revelar información confidencial, hacer clic en un enlace a una página fraudulenta brindando información personal como el usuario o la contraseña, o descargar archivos infectados con malware).

Generalmente puede consistir en un mensaje que se recibe por correo electrónico, pero también podría ser por SMS, Whatsapp u otra red social. Los correos electrónicos que imitan la identidad son cada vez más difíciles de detectar y suele ser el medio más común por el que se recibe malware. Mediante esta práctica los ciberdelincuentes pueden hacerse de información valiosa con la que podrían realizar otro tipo de fraude a las mismas personas. Sea cual sea el negocio, por grande o pequeño que sea, se recibirán ataques de *phishing* en algún momento.

Esta sección contiene 4 pasos sencillos para ayudarte a identificar los ataques de *phishing* más comunes.

Consejo 1: Revisar la configuración de las cuentas

Configurar las cuentas de las personas que trabajan en la empresa o emprendimiento, utilizando el principio de "menor privilegio". Esto significa otorgar al personal el nivel más bajo de derechos de usuario necesarios para realizar su trabajo, por lo que, si es víctima de un ataque de *phishing*, el daño potencial se reduce.

Una cuenta de administrador es una cuenta de usuario que le permite realizar cambios que afectarán a otros usuarios. Los administradores pueden cambiar la configuración de seguridad, instalar *software* y *hardware* y acceder a todos los archivos de la computadora. Por lo tanto, un atacante que tenga acceso no autorizado a una cuenta de administrador puede ser mucho más perjudicial que acceder a una cuenta de usuario estándar. Para reducir aún más el daño que puede causar el *malware* o la pérdida de los datos de inicio de sesión, evitar o minimizar el uso por parte del personal de una cuenta con privilegios de administrador.

Utilizar el doble factor de autenticación en las cuentas importantes, como el correo electrónico o redes sociales. Esto significa que incluso si un atacante conoce las contraseñas, no podrá acceder a esa cuenta fácilmente.

Consejo 2: Concientizar al personal

Considerar las formas en que alguien podría dirigirse a la empresa y asegurarse de que todo el personal comprenda las formas normales de trabajo, especialmente en lo que respecta a la interacción con otros emprendimientos, para que estén alertas para detectar solicitudes fuera de lo común.

Los ataques más frecuentes incluyen enviar una factura por un servicio que no has utilizado, por lo que cuando se abre el archivo adjunto, el *malware* se instala automáticamente sin tu conocimiento en la computadora. Otra forma es engañar al personal para que transfiera dinero o información mediante el envío de correos electrónicos que parecen auténticos.

Es bueno pensar en las prácticas laborales habituales y en cómo ayudar a que estos ataques tengan menos probabilidades de éxito.

Por ejemplo:

- ¿El personal sabe qué hacer con solicitudes inusuales y dónde obtener ayuda?
- Si alguien que se hace pasar por una persona importante (un cliente o gerente) por correo electrónico, cómo verificar su identidad antes de cumplir con lo que pide.
- Quienes estafan, a menudo envían correos electrónicos de *phishing* de grandes organizaciones como entidades financieras, o de cualquier otra entidad pública con la que se acostumbre hacer gestiones, con la esperanza de que algunos de los destinatarios del correo electrónico tengan una conexión con esa empresa y poder engañarlos. Nunca van a solicitar datos sobre usuarios y contraseñas, es bueno verificar con una llamada a la organización remitente si esto ocurre. Si se recibe un correo electrónico de una organización con la que no hay negocios, se debe tratar con sospecha.
- Pensar en cómo alentar y apoyar al personal para que cuestione solicitudes sospechosas o simplemente inusuales, incluso si parecen ser de personas importantes. Tener la confianza para preguntar “¿es esto genuino?” puede ser la diferencia entre mantenerse a salvo o un percance costoso.

También es importante observar cómo se ven tus comunicaciones salientes a los proveedores y clientes. Por ejemplo, ¿se envían correos electrónicos solicitando dinero o contraseñas? Los correos electrónicos ¿se confundirán con *phishing* o dejarán a las personas vulnerables a un ataque que ha sido diseñado para parecerse a un correo electrónico de la empresa? Hay que considerar decirle a los proveedores o clientes que "*nunca le pediremos su contraseña*" o "*nuestros datos bancarios no cambiarán en ningún momento*".

Consejo 3: Revisar las señales de alerta

Los servicios de filtrado de correo electrónico intentan enviar los correos electrónicos de*phishing* o correo no deseado a carpetas denominadas SPAM. Sin embargo, las reglas que determinan este filtrado deben ajustarse a las necesidades de la empresa.

Es posible que se deba mantener actualizadas las reglas, para garantizar una mejor protección. Si estas reglas son demasiado abiertas y los correos electrónicos sospechosos no se envían a las carpetas de correo no deseado/SPAM, los usuarios tendrán que administrar una gran cantidad de correos electrónicos, aumentando su carga de trabajo y dejando abierta la posibilidad de acceder a ellos. Sin embargo, si las reglas son demasiado estrictas, algunos correos electrónicos legítimos podrían perderse.

Para mejorar la gestión del filtrado del servicio de correo electrónico de la empresa es fundamental que el personal conozca las señales de advertencia que le permitan identificar este tipo de correos engañosos y que sepa dónde reportarlos.

Señales de alerta:

Idioma y contenido

- Utiliza un saludo genérico

¿Se dirige por su nombre o se refiere a 'cliente valioso', 'amigo' o 'colega'? Esto puede ser una señal de que el remitente no te conoce realmente.

- Menciona algún sentido de urgencia

¿El correo electrónico contiene una amenaza o pedido de actuar con urgencia? Sospecha de palabras como "envíe estos detalles dentro de las 24 horas" o "ha sido víctima de un delito, haga clic aquí de inmediato".

- Pide información sensible, hace llamamientos humanitarios, ofertas demasiado buenas

Verificar por otro medio que sea real.

Indicador técnico

- Cuenta de correo del remitente

Muchas veces pueden mostrar un nombre de un contacto (alias) conocido, pero provenir de un correo desconocido. Ten especial cuidado si parecen provenir de una persona de alto rango dentro de la empresa, u empresa conocida, solicitando que se realice un pago a una cuenta bancaria en particular. Mirar el alias del remitente y verificar que éste coincida con la cuenta de correo.

- Contiene archivos adjuntos

Cuando se recibe un archivo adjunto en un correo, verificar que sea de un remitente real y si esperabas recibirlo. Si no se puede confirmar que se trata de un mensaje legítimo, desestimar el archivo, no abrirlo ni descargarlo.

- Contiene enlaces a un sitio en línea

Cuando se reciba un correo con un acceso a un sitio en línea como por ejemplo de e-banca, compras u una red social:

- Evitar hacerlo a través del enlace que envían o revisar la URL del enlace antes de hacer clic en él.
- Ingresar manualmente la dirección en el navegador.
- Si el navegador alerta que el sitio al que se quiere acceder no es seguro o peligroso, no intentar iniciar sesión, brindar información o realizar pagos allí.
- Corroborar que en la barra del navegador aparezca el candado que indica que la conexión es segura.
- El punto anterior no indica que el sitio es auténtico, verificar además URL, su apariencia, marcas, logos, aspecto real.

Errores

- Ortografía, gramática y puntuación

Muchos de los correos de *phishing* contienen errores ortográficos o de redacción, debido al uso de traductores automatizados. La estética también se asemeja mucho a la original, pero algún detalle siempre se escapa.

Evitar brindar información personal o confidencial por correo electrónico o por teléfono. En caso de recibir una notificación de este tipo, comunicarse con la organización para verificar su validez.

Consejo 4: Chequear qué información hay disponible en línea sobre la empresa o emprendimiento

Los atacantes utilizan información pública disponible sobre la empresa y del personal para hacer que sus mensajes de *phishing* sean más convincentes. Esto a menudo se obtiene del sitio web y cuentas de redes sociales, información conocida como "huella digital".

- Comprender el impacto de la información compartida en el sitio web y las páginas de redes sociales de la empresa. ¿Qué necesitan saber los visitantes del sitio web y qué detalles son innecesarios, pero podrían ser útiles para los atacantes?
- Ser consciente de lo que socios, contratistas y proveedores disponibilizan sobre la empresa.
- Ayudar al personal a comprender cómo el hecho de compartir su información personal puede afectarlos a ellos y a la empresa o emprendimiento. No se trata de esperar que las personas eliminen todo rastro de sí mismas de internet; es importante ayudarles a ser conscientes y gestionar su huella digital, (conformada por rastros de información sobre creencias, valores, habilidades, intereses, hobbies, ubicación e imágenes) dando forma a su perfil para que funcione para ellos y para el comercio o negocio.
- Visitar la Campaña de Ciudadanía Digital, para ayudar a las personas a realizar un uso seguro y responsable en línea.

Acceder a la infografía: Prevení ataques de phishing en tu empresa o emprendimiento

Proteger la empresa o emprendimiento de malware

El *malware*, (del inglés *malicious software*), es un *software* malicioso que puede realizar acciones dañinas en un sistema informático.

Ejemplos de *malware* que podrían infectar los dispositivos:

- Virus informático. Busca modificar el funcionamiento normal del dispositivo. Requiere la interacción de una persona para propagarse a otros archivos y sistemas.
- Gusano informático. Puede replicarse desde un dispositivo infectado a otros a través de la red, con el objetivo de lograr acceso a dispositivos de forma no autorizada.
- Troyano. Accede al sistema como un archivo o aplicación inofensiva y realiza acciones no deseadas en segundo plano.
- Spyware. Espía el dispositivo afectado. Sus funciones son recoger datos e información del dispositivo y observar la actividad del usuario sin su consentimiento.
- Adware. Rastrea el navegador y el historial de descargas del usuario con la intención de mostrar anuncios emergentes o banners no deseados para atraerlo a realizar una compra o hacer clic en un enlace.

Esta sección contiene 5 consejos para protegerse del*malware*:

Consejo 1: Instalar y activar un *software* antivirus

El *software* antivirus, que a menudo se incluye dentro de los sistemas operativos más comunes, debe usarse en todas las computadoras y dispositivos que lo permitan.

La recomendación es escanear semanalmente y de manera completa todos los equipos.

Acceder a información más detallada para Windows 10, y MacOS

Consejo 2: Activar *firewall*

Los *firewalls* crean una "zona de amortiguación" entre su propia red y las redes externas como internet. Los sistemas operativos más comunes ahora incluyen un firewall, por lo que simplemente hay que verificar que esté instalado y activado.

Acceder a información más detallada sobre como activarlos en Windows 10 y macOS.

Consejo 3: Evitar instalar *software* no autorizado o no oficial

Muchas veces, las personas usuarias en las empresas demandan productos que conocen y que tienen en sus casas para utilizarlos en el trabajo: esto ocurre con el Office, Adobe Acrobat Pro, Photoshop, entre otro.

Las consecuencias de esta práctica van mucho más allá de la evidente repercusión legal y las sanciones que pueden ser muy graves para las empresas.

Lo trataremos desde la perspectiva de la seguridad, ya que la instalación de software sin licencia es una de las principales vías de entrada de *malware*, incrementándose las posibilidades de sufrir un ciberataque. Los usuarios que instalen*software* ilegal también están expuestos a fallos críticos de sus sistemas y una pérdida de datos.

Por ello es importante:

- Utilizar siempre software legal, en particular el sistema operativo.
- Actualizar semanalmente el sistema operativo y software de tus dispositivos.
- Descargar software solo de sitios webs del fabricante.
- Analizar el programa descargado con el antivirus antes de instalarlo.

Al navegar por la web, es posible verificar la seguridad de cualquier sitio que resulte dudoso enGoogle, FireFox, Microsoft Edge.

Consejo 4: Mantener actualizado el *software* y *firmware* de los dispositivos

Las actualizaciones (parches) son modificaciones o complementos que se realizan en los sistemas operativos o aplicaciones instalados en los equipos, con el objetivo de mejorar tanto aspectos de funcionalidad como de seguridad.

Asegurarse de que el *software* y el *firmware* de los equipos, ya sean tabletas, celulares, notebooks o PC, estén siempre actualizados con las últimas versiones y siempre que sea posible, activar la actualización automática.

En algún momento, estas actualizaciones ya no estarán disponibles (cuando el producto llegue al final de su vida útil), momento en el que se debe considerar su reemplazo por una alternativa moderna.

Acceder a información más detallada sobre como activar actualizaciones automáticas enIOS para Mac y Microsoft Store.

Consultar la Guía de gestión de vulnerabilidades para conocer más sobre la aplicación de actualizaciones.

Consejo 5: Controlar el uso de las unidades USB, discos extraíbles y tarjetas de memoria

Cuando las unidades USB, discos extraíbles o tarjetas de memoria se comparten abiertamente, resulta difícil rastrear lo que contienen, dónde han estado y quiénes las han utilizado.

Se puede reducir la probabilidad de infección:

- Bloqueando el acceso a los puertos físicos para la mayoría de los usuarios.
- Usando herramientas antivirus.
- Permitiendo que solo las unidades, discos o tarjetas aprobadas se utilicen dentro de tu empresa.

También es recomendable pedirle al personal de la empresa u emprendimiento que, al transferir archivos, utilice medios alternativos como el correo electrónico o almacenamiento en la nube.

Acceder a la infografía: Protegé a tu empresa de malware