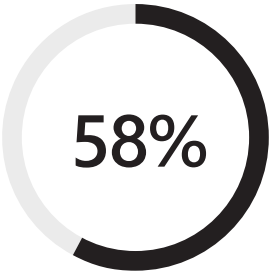
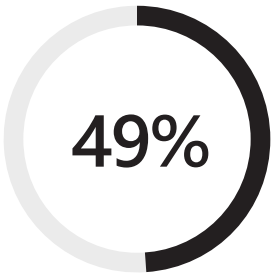
10 cosas que las pequeñas empresas no deben hacer en materia de seguridad

Microsoft

En general, solo escuchamos sobre violaciones de seguridad cuando le ocurren a gente famosa o en casos de ataques dirigidos a grandes compañías multinacionales. Pero la realidad es que las pequeñas y medianas empresas corren exactamente el mismo riesgo. ¿Cuánto valen para ti los datos acerca de clientes, transacciones y operaciones?



de las violaciones afectan a las pequeñas empresas.



se valen del malware.

Informe de investigación sobre violación de datos de Verizon 2018

Aprende qué cosas no debes hacer y mejora la seguridad digital. Aquí hay 10 reglas de seguridad para proteger y defender tu organización.

01

No hagas los clics primero y las preguntas más tarde

Los delincuentes cibernéticos son cada vez más astutos. Pueden usar bots para escribir e implementar estafas de phishing. Puede ser difícil diferenciar las comunicaciones falsas de las genuinas. Permanece alerta y busca las señales. Entrénate a ti mismo y a tu personal para ser cauteloso y evitar:

- Apertura de archivos adjuntos desconocidos
- Respuestas a solicitudes aleatorias de información
- Clics en enlaces sospechosos

54%

de las pequeñas empresas han sufrido violaciones que implicaran información de clientes y empleados en los últimos 12 meses.

Estado de ciberseguridad en pequeñas y medianas empresas en 2017, según Ponemon

59%

de las empresas no tienen visibilidad sobre las prácticas de contraseña de los empleados, como usar contraseñas débiles o compartirlas.

Estado de ciberseguridad en pequeñas y medianas empresas en 2017, según Ponemon

02

No uses contraseñas fáciles

Que todavía funcione no significa que sea seguro. De hecho, confiar en un dispositivo antiguo o en un software obsoleto puede ponerte en riesgo. Tu equipo de TI tiene mejores cosas para hacer que comprobar software para buscar virus o recuperar archivos perdidos.

Si tu empresa aún ejecuta Windows 7 o una versión anterior de Office, tu empresa es vulnerable. Actualiza tu versión a Windows 10 y Office 365, que tienen características de seguridad integradas.

03

No confíes en la tecnología obsoleta

Que todavía funcione no significa que sea seguro. De hecho, confiar en un dispositivo antiguo o en un software obsoleto puede ponerte en riesgo. Tu equipo de TI tiene mejores cosas para hacer que comprobar software para buscar virus o recuperar archivos perdidos.

Si tu empresa aún ejecuta Windows 7 o una versión anterior de Office, tu empresa es vulnerable. Actualiza tu versión a Windows 10 y Office 365, que tienen características de seguridad integradas.

¡Reemplaza esas máquinas antiguas! Las PC antiguas experimentan problemas casi dos veces más a menudo que las nuevas.

Estudio sobre PC de empresas pequeñas y medianas de Techaisle, 2018

04

04

No ignores los dispositivos

Si has equipado a tus empleados con dispositivos móviles, genial. Simplemente no olvides los dispositivos personales que ellos usan mientras trabajan. Protege con contraseña todos los teléfonos, tabletas y computadoras portátiles. Además, aumenta la seguridad aprovechando la administración de dispositivos móviles para Office 365 integrada de Microsoft, que te permite bloquear, borrar y restablecer un dispositivo perdido o robado de forma remota.

05

05

No uses la TI solo

Aprovecha la enorme inversión que Microsoft hace en seguridad. Almacena, protege y unifica tus datos de forma segura con los firewalls en nuestra nube. SharePoint acelera en gran medida el uso compartido de archivos y evita que los equipos usen unidades de memoria y otros dispositivos que pueden perderse o sufrir robos. Usa OneDrive, el servicio de almacenamiento en la nube de Office 365, para hacer una copia de seguridad automática de tus archivos y restringir el acceso a los documentos y archivos como otra capa adicional de protección para los datos.

06

06

No pases por alto el cifrado

Muchos correos electrónicos contienen datos confidenciales y es fácil cifrar los correos electrónicos confidenciales con Outlook y Office 365. ¿Estás buscando una solución con un solo clic? OneDrive para empresas permite proteger con contraseña los archivos guardados en la nube.

07

No asumas que las aplicaciones son seguras

Las copias de seguridad de los archivos son un aspecto clave, pero las aplicaciones son igual de importantes. Muchas pequeñas empresas confían en los sistemas de inventario y el software de contabilidad para funcionar todos los días. Para las aplicaciones críticas para la misión, recomendamos alojar y optimizar aplicaciones con los servicios de Azure, como Microsoft Cloud Toolkit for Business.

08

No olvides los arreglos y las actualizaciones

Windows 10 y Office 365 pueden actualizarse automáticamente, pero ¿qué pasa con el otro software que utilizas? No confíes en aplicaciones, sistemas operativos ni navegadores desactualizados. Ignorar las actualizaciones pone en riesgo a tu negocio.

09

Planificar para los mejores casos no alcanza

Incluso los propietarios de pequeñas empresas deberían invertir el tiempo y los recursos para desarrollar una estrategia de recuperación ante desastres que garantice la continuidad de su negocio, pase lo que pase. Por suerte, el servicio de recuperación de sitios de Azure automatiza el proceso para las empresas. Al aprovechar la red global de centros de datos de Microsoft para crear redundancia, Azure puede garantizar que tu empresa tendrá acceso seguro e ininterrumpido a las aplicaciones y los datos. Sin duda alguna.

La nube de Microsoft abarca más de 100 instalaciones altamente seguras en todo el mundo, todas ellas conectadas por una de las redes más grandes de la tierra, y monitoreadas en forma permanente.

Microsoft

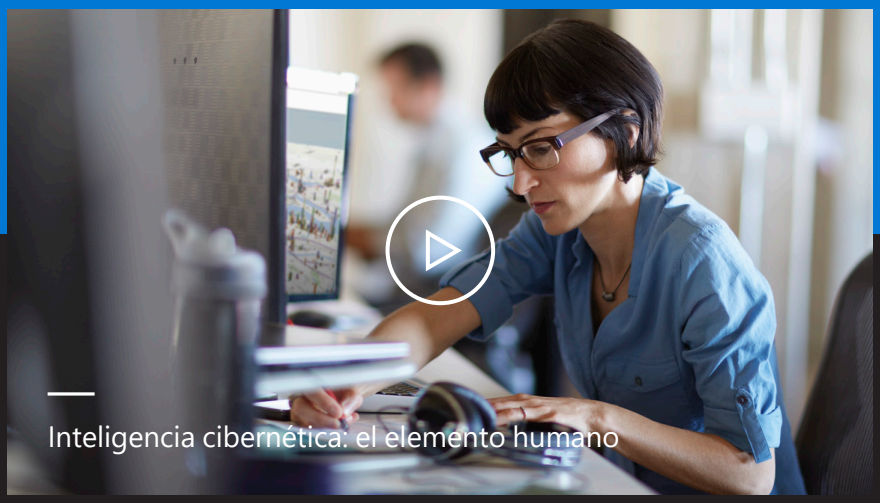
10

No solo hables sobre el tema

Se necesitará más que un solo correo electrónico para capacitar a los empleados en la comprensión de los riesgos y el reconocimiento de los signos de estafas y posibles infracciones. Explícales por qué es importante y qué puede suceder si se produce una violación a la seguridad. El equipo cumple un rol crucial en el éxito de tu negocio. Haz de la seguridad parte de su cultura corporativa.

Mira el webinar

Descubre cómo motivar a tu equipo para ayudar a prevenir una brecha de seguridad. Este video de la serie Modern Workplace se centra en el elemento humano y en lo que tú y tu equipo pueden hacer.



Obtén ayuda de expertos

¿Ya estás trabajando con un socio de Microsoft? Pregúntales cómo puedes mejorar tu seguridad digital. Si no estás trabajando con un socio de Microsoft, permítenos presentarte a algunos en tu comunidad. Visita la página de proveedores de soluciones de Microsoft para encontrar uno cerca de ti.