CIBERSEGURIDAD PARA
PEQUEÑOS NEGOCIOS

SEGURIDAD FÍSICA

La ciberseguridad comienza con una sólida seguridad física.

Los fallos de la seguridad física pueden poner en riesgo datos delicados de su compañía que podrían usarse para el robo de identidad. Por ejemplo:

Un empleado deja accidentalmente un dispositivo de almacenamiento de datos en la mesa de una cafetería. El dispositivo – que contiene cientos de números de tarjetas de crédito de los clientes – desapareció.

Otro empleado tira viejos registros bancarios de la compañía al cesto de la basura, y un delincuente los encuentra.

Un ladrón entra a su oficina por una ventana abierta y roba archivos y computadoras.

CÓMO PROTEGER LOS EQUIPOS Y LOS ARCHIVOS DE PAPEL

Estas son algunas recomendaciones para proteger la información contenida en archivos de papel y en los discos duros, dispositivos de almacenamiento de datos, computadoras portátiles, dispositivos utilizados en puntos de venta y demás equipos.

Guarde todo de manera segura

Cuando los archivos de papel o los dispositivos electrónicos contengan información delicada, guárdelos en un gabinete o en un lugar cerrado con llave.

Limite el acceso físico

Cuando los registros o dispositivos contengan información delicada, permita el acceso únicamente a aquellos que lo necesiten.

Envíe recordatorios

Recuérdeles a los empleados que deben guardar los archivos de papel en gabinetes con llave y desconectarse de su red y aplicaciones. Recuérdeles que nunca deben dejar al descuido un archivo ni un dispositivo que contenga datos delicados.

Controle su inventario

Lleve un control y proteja todos los aparatos que recolecten información delicada de los clientes.

APRENDA MÁS EN
FTC.gov/PequeñosNegocios

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology
U.S. Department of Commerce

SBA U.S. Small Business Administration

CIBERSEGURIDAD PARA PEQUEÑOS NEGOCIOS

CÓMO PROTEGER LOS DATOS DE SUS DISPOSITIVOS

Cualquier cosa puede suceder. Pero hay menos probabilidades que se produzca un incidente de seguridad de datos en aquellos dispositivos que están protegidos. Estas son algunas maneras de hacerlo:

Exija contraseñas complejas

Exija que se establezcan contraseñas extensas, complejas y únicas. Y asegúrese de que esas contraseñas se guarden de manera segura. Considere usar un programa de administración de contraseñas.

Use un sistema de autenticación de múltiples factores

Exija autenticación de múltiples factores para acceder áreas de su red que contengan información delicada. Esto requiere pasos adicionales además de iniciar la sesión con una contraseña – como un código temporario en un teléfono inteligente o una llave que se inserta en una computadora.

Limite la cantidad de intentos de inicio de sesión

Limite la cantidad de intentos incorrectos de inicio de sesión para desbloquear los dispositivos. Esto lo ayudará a protegerse de los intrusos.

Codificación

Codifique los dispositivos portátiles, incluyendo las computadoras portátiles y pequeños dispositivos de almacenamiento de datos que contengan información delicada. Codifique todos los datos delicados que envíe fuera de la compañía, por ejemplo, a un contador o a un servicio de despacho y entrega.

CAPACITE A SUS EMPLEADOS

Incluya el tema de la seguridad física en sus sesiones de capacitación y comunicaciones regulares. Recuérdeles a los empleados que:

Trituren los documentos

Siempre deben triturar documentos que con datos delicados antes de tirarlos a la basura.

Borren correctamente los datos

Deben usar un programa para borrar los datos antes de donar o descartar computadoras, dispositivos móviles, fotocopiadoras digitales y dispositivos de almacenamiento de datos en desuso. No deben confiar únicamente en la función “eliminar”.

Promuevan prácticas de seguridad en todos los lugares

Se deben mantener prácticas de seguridad incluso cuando se trabaja remotamente desde sus casas o durante un viaje de negocios.

Estén al tanto del plan de respuesta

Todo el personal debe saber qué hacer en caso de una pérdida o robo de los equipos o archivos de papel, incluidos el nombre de las personas a las que deben notificar y los pasos a tomar. Busque información sobre cómo crear un plan de respuesta en *Data Breach Response: A Guide for Business* (disponible en inglés). Puede consultar esta guía en ftc.gov/databreach.

APRENDA MÁS EN FTC.gov/PequeñosNegocios

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration