CIBERSEGURIDAD PARA
PEQUEÑOS NEGOCIOS

# CONCEPTOS BÁSICOS DE CIBERSEGURIDAD

**Los delincuentes cibernéticos atacan a compañías de todo tamaño.**

El hecho de conocer algunos conceptos básicos de ciberseguridad lo ayudará a proteger su negocio y reducir los riesgos de sufrir un ataque cibernético.

## PROTEJA
### SUS ARCHIVOS Y SUS DESPOTIVOS

#### Actualice sus programas

Esto incluye aplicaciones, navegadores web y sistemas operativos. Configure las actualizaciones para que se activen automáticamente.

#### Proteja sus archivos

Haga copias de seguridad fuera de internet de todos los archivos importantes en un dispositivo externo o en la nube. Asegúrese de almacenar sus archivos impresos de manera segura.

#### Exija usar contraseñas

Todas las computadoras portátiles, tablets y teléfonos inteligentes deben usar contraseñas. No deje estos dispositivos sin vigilancia en lugares públicos.

#### Codifique los dispositivos

y otros soportes de datos que contengan información personal delicada. Esto incluye computadoras portátiles, tablets, teléfonos inteligentes, discos extraíbles, cintas de copias de seguridad y soluciones de almacenamiento en la nube.


#### Use un sistema de autenticación de múltiples factores

Exija una autenticación de múltiples factores para acceder a las áreas de su red que contengan información delicada. Esto requiere seguir algunos pasos adicionales además de iniciar la sesión con una contraseña – por ejemplo, una contraseña temporaria en un teléfono inteligente o una llave que se inserta en una computadora.

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

## PROTEJA SU RED INALÁMBRICA

### Resguarde su enrutador

Cambie el nombre y contraseña predeterminados, desactive la administración remota del aparato y desconéctese como administrador del enrutador cuando ya esté configurado.

### Para codificarlo, use como mínimo el acceso protegido WPA2

Asegúrese de que su enrutador le ofrezca una codificación tipo WPA2 o WPA3, y verifique que esté activada. La codificación protege la información que se envía a través de su red para que las personas ajenas a su negocio no puedan leerla.

## USE HABITUALMENTE UNA SEGURIDAD INTELIGENTE EN SU NEGOCIO

### Exija contraseñas sólidas

Una contraseña sólida tiene por lo menos 12 caracteres con una combinación de números, símbolos y letras mayúsculas y minúsculas.

Nunca reutilice las contraseñas y no las comparta por teléfono, mensajes de texto ni por email.

Limite el número de atentos de acceso para así limitar los ataques que tratan de averiguar la contraseña.

### Capacite a todo el personal

Cree una cultura de seguridad implementando un programa regular de capacitación para sus empleados. Actualice la capacitación de sus empleados a medida de que se entere de nuevos riesgos y vulnerabilidades. Si hay empleados que no participan en la capacitación, considere bloquearles el acceso a la red.

### Tenga un plan

para guardar los datos, seguir adelante con su negocio y notificar a los clientes en caso que sufra un incidente de seguridad de datos. La guía para negocios de la FTC *Data Breach Response: A Guide for Business* (disponible en inglés) le brinda los pasos que puede seguir.

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