CIBERSEGURIDAD PARA
PEQUEÑOS NEGOCIOS

Qué es y cómo funciona

EL MARCO DE CIBERSEGURIDAD DEL NIST

Es posible que haya escuchado hablar del Marco de Ciberseguridad del NIST, ¿pero qué es exactamente?

¿Y es aplicable para usted?

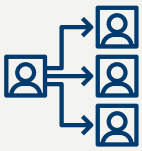
NIST es el acrónimo de Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, en inglés) dependiente del Departamento de Comercio de EE. UU. El Marco de Ciberseguridad del NIST ayuda a los negocios de todo tamaño a comprender mejor sus riesgos de ciberseguridad, administrar y reducir sus riesgos, y proteger sus redes y datos. Este Marco es voluntario. Le brinda a su negocio una reseña de las mejores prácticas para ayudarlo a decidir dónde tiene que concentrar su tiempo y su dinero en cuestiones de protección de ciberseguridad.

Usted puede implementar el Marco de Ciberseguridad del NIST en su negocio en estas cinco áreas: identificación protección, detección, respuesta y recuperación.

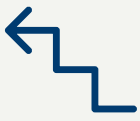
1. IDENTIFICACIÓN

Haga una lista de todos los equipos, programas software y datos que use, incluyendo computadoras portátiles, teléfonos inteligentes, tablets y dispositivos utilizados en puntos de venta.

Elabore y comparta una política de ciberseguridad de la compañía que cubra los siguientes puntos:



Funciones y responsabilidades de los empleados, proveedores y todo aquel que tenga acceso a datos delicados.



Pasos a seguir para protegerse contra un ataque y limitar el daño si se produce un ataque.

2. PROTECCIÓN

- Controle quiénes acceden a su red y usan sus computadoras y otros dispositivos.
- Use programas de seguridad para proteger los datos.
- Codifique los datos delicados, tanto cuando estén almacenados o en tránsito.
- Haga copias de seguridad de los datos con regularidad.
- Actualice los programas de seguridad con regularidad, en lo posible, automatice estas actualizaciones.
- Implemente políticas formales para la eliminación segura de archivos electrónicos y dispositivos en desuso.
- Capacite sobre ciberseguridad a todas las personas que usen sus computadoras, dispositivos y redes. Usted puede ayudar a los empleados a comprender su riesgo personal además de la función crucial que cumplen en el lugar de trabajo.

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

3. DETECCIÓN

Monitoree sus computadoras para controlar si detecta acceso de personal no autorizado a sus computadoras, dispositivos (soportes de almacenamiento de datos de tipo USB) y software.

Revise su red para controlar si detecta usuarios o conexiones no autorizados.

Investigue cualquier actividad inusual en su red o por parte de su personal.

4. RESPUESTA

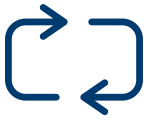
Implemente un plan para:

- Notificar a los clientes, empleados y otros cuyos datos pudieran estar en riesgo.
- Mantener en funcionamiento las operaciones del negocio.
- Reportar el ataque a los encargados del cumplimiento de la ley y otras autoridades.
- Investigar y contener un ataque.
- Actualizar su política y plan de ciberseguridad con las lecciones aprendidas.
- Prepararse para eventos inadvertidos (como emergencias climáticas) que puedan poner en riesgo los datos.

Ponga a prueba su plan con regularidad.

5. RECUPERACIÓN

Después de un ataque:



Repare y restaure los equipos y las partes de su red que resultaron afectados.

Mantenga informados a sus empleados y clientes de sus actividades de respuesta y recuperación.

Para más información sobre el Marco de Ciberseguridad del NIST y los recursos para los pequeños negocios, visite nist.gov/CyberFramework y nist.gov/programs-projects/small-business-corner-sbc.

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