Ciberseguridad en PYMES

Enfoque inicial

Jacqueline Diaz Polo
Gerente de Soluciones de Seguridad

¿Qué es la ciberseguridad y cual es su objetivo?

La **ciberseguridad** se refiere a todas las

- tecnologías,
- prácticas y
- políticas

para **prevenir** los ciberataques o **mitigar** su impacto.

A nivel empresarial la ciberseguridad es un componente clave de la estrategia de gestión de riesgos de una organización

¿Por qué es importante la ciberseguridad?

Porque pueden tener el poder de

- Interrumpir, dañar o destruir empresas
- Robar identidades, realizar extorsiones personales y corporativas

Porque podemos impulsar nuestro negocio si

- Protegemos
- Detectamos
- Respondemos

Incidentes de ciberseguridad

La Universidad de Maryland descubrió que un hacker ataca computadoras con acceso a internet

10s

Information is Beautiful

500MM de cuentas estaban a la venta en la internet oscura

Se robaron 5.2MM de cuentas de huéspedes.

Sufrieron secuestro de datos .

Las cuentas de Elon Musk y otras personas ricas fueron hackeadas

Ataque de ranswomware que pedían $5MM

En 2024, los secuestros de datos costaron a las organizaciones

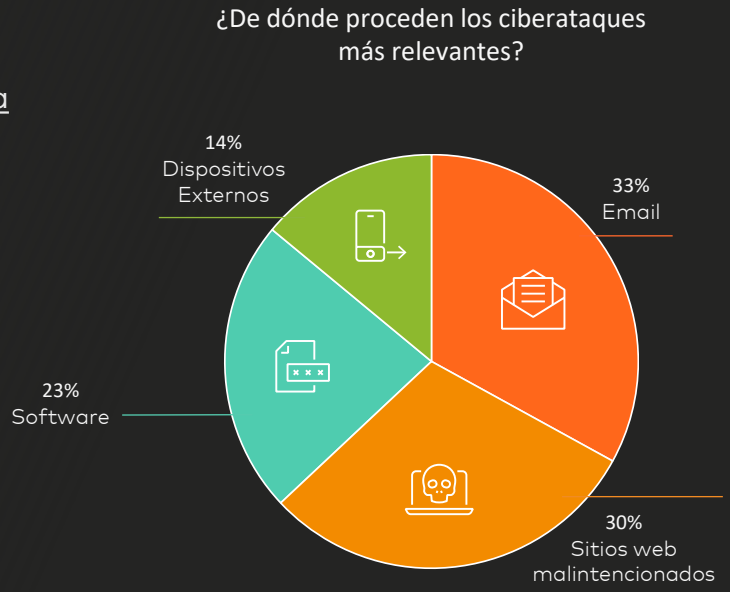
$35,000 millones

Mastercard Propriety Data. 2024

Hagamos un test

Have I Been Pwned: Check if your email has been compromised in a data breach

How Secure Is My Password? | Password Strength Checker | Security.org



Tipos de Ciberataques más comunes

Fuente: MIT Edx Cybersecure Certification Course

Impacto en las PyMEs

48%

Ataques realizados en PyMEs durante el 2024 a nivel global

1 de 321

Correos recibidos por una PyME es malicioso

43%

De las PyMEs carecen de un plan de recuperación después de un incidente

$826 a $654K

Rango del costo de un incidente de ciberseguridad

60%

De las PyMEs atacadas en los Estados Unidos tuvieron que cerrar operaciones luego de 6 meses posterior al ataque

95%

De las brechas de seguridad son atribuidas por error humano

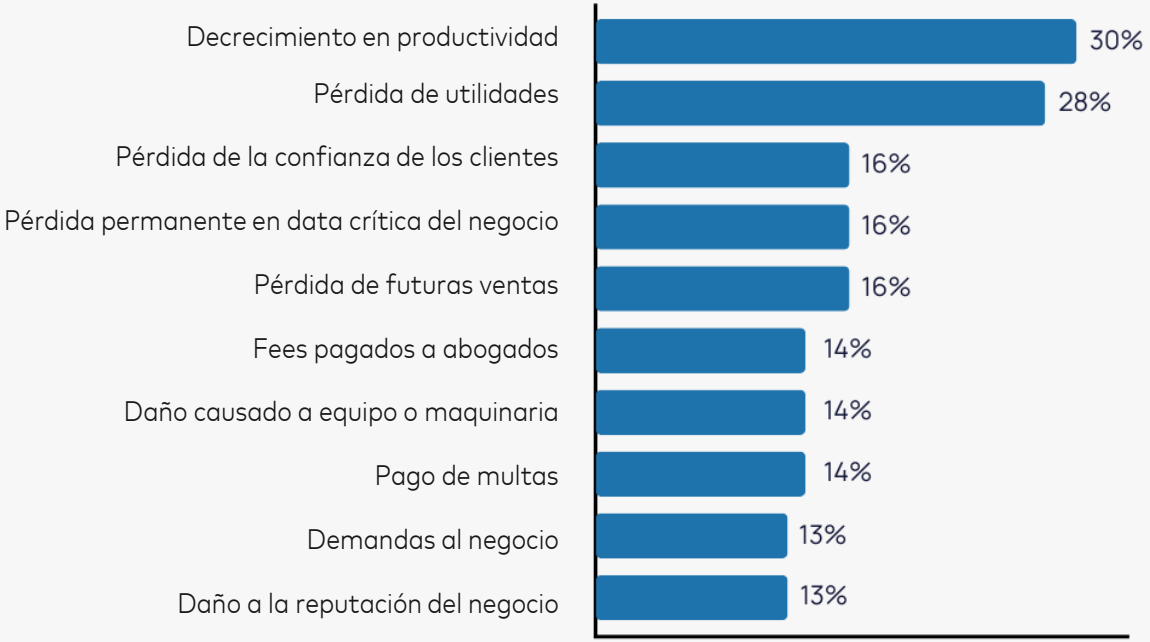
50%

De las PyMEs les toma por lo menos 24 horas en recuperarse de un incidente

Fuente: State of ransomware 2024

Impacto en las PYMES

Consecuencias más frecuentes encontradas luego de un ciberataques en PyMEs



BusinessDIT

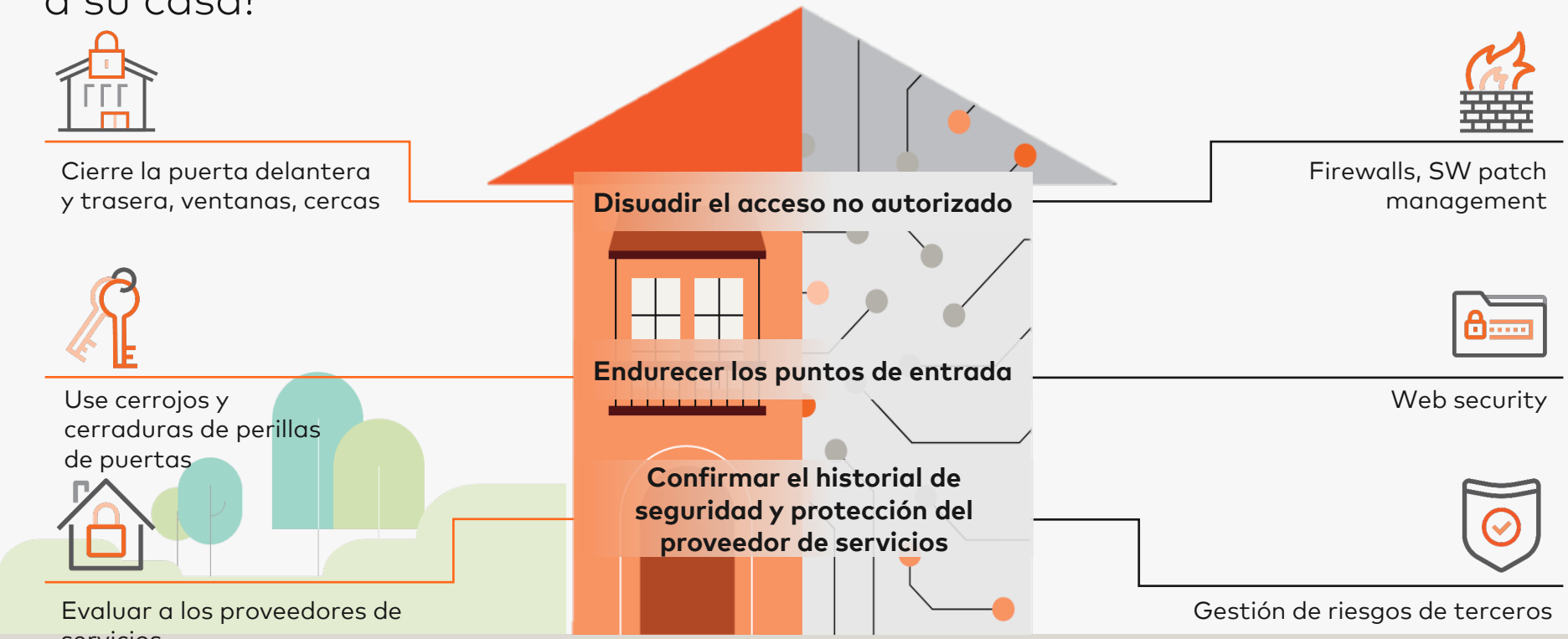
PERSPECTIVA

¿Cómo están identificando las brechas de seguridad?

Piense en sus capacidades de seguridad actuales, como piensa en proteger su casa.

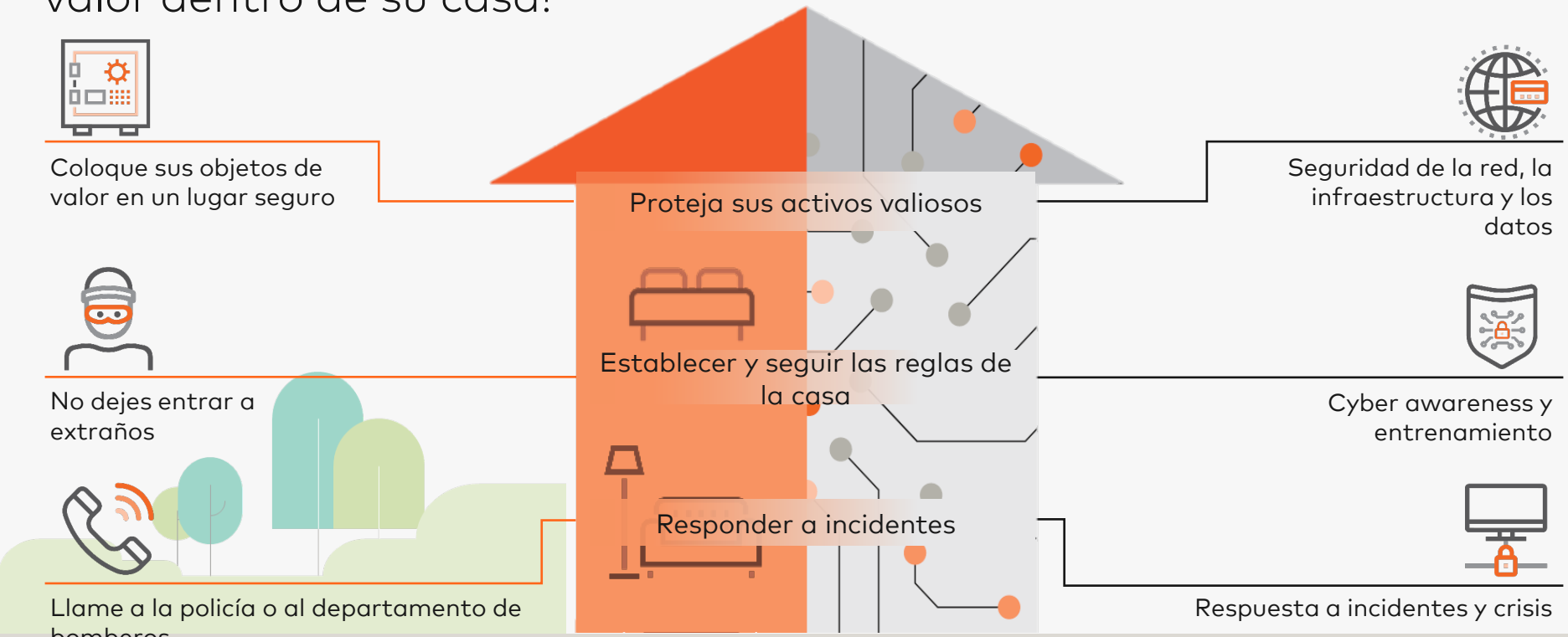
PERSPECTIVA

Un enfoque de afuera hacia adentro: ¿Están aseguradas las entradas a su casa?



PERSPECTIVA

Un enfoque de adentro hacia afuera: ¿Están asegurados los objetos de valor dentro de su casa?



¿Por donde empiezo?

¿Por donde empiezo?

Proteger

Detectar

Responder

Proteger a las organizaciones de los ciberataques

- Identificar y proteger la información de valor.
- Asegurar el acceso correcto y seguro.
- Implementar el cifrado.
- Llevar a cabo evaluaciones de manera regular para identificar y suplir las vulnerabilidades.

¿Por donde empiezo?

Proteger | **Detectar** | Responder

Detectar ciberataques

- Identificar violaciones.
- Monitorear los sistemas de seguridad constantemente.
- Mantenerse actualizado sobre las últimas infiltraciones.

¿Por donde empiezo?

Proteger

Detectar

Responder

Responder a los ciberataques y recuperarse

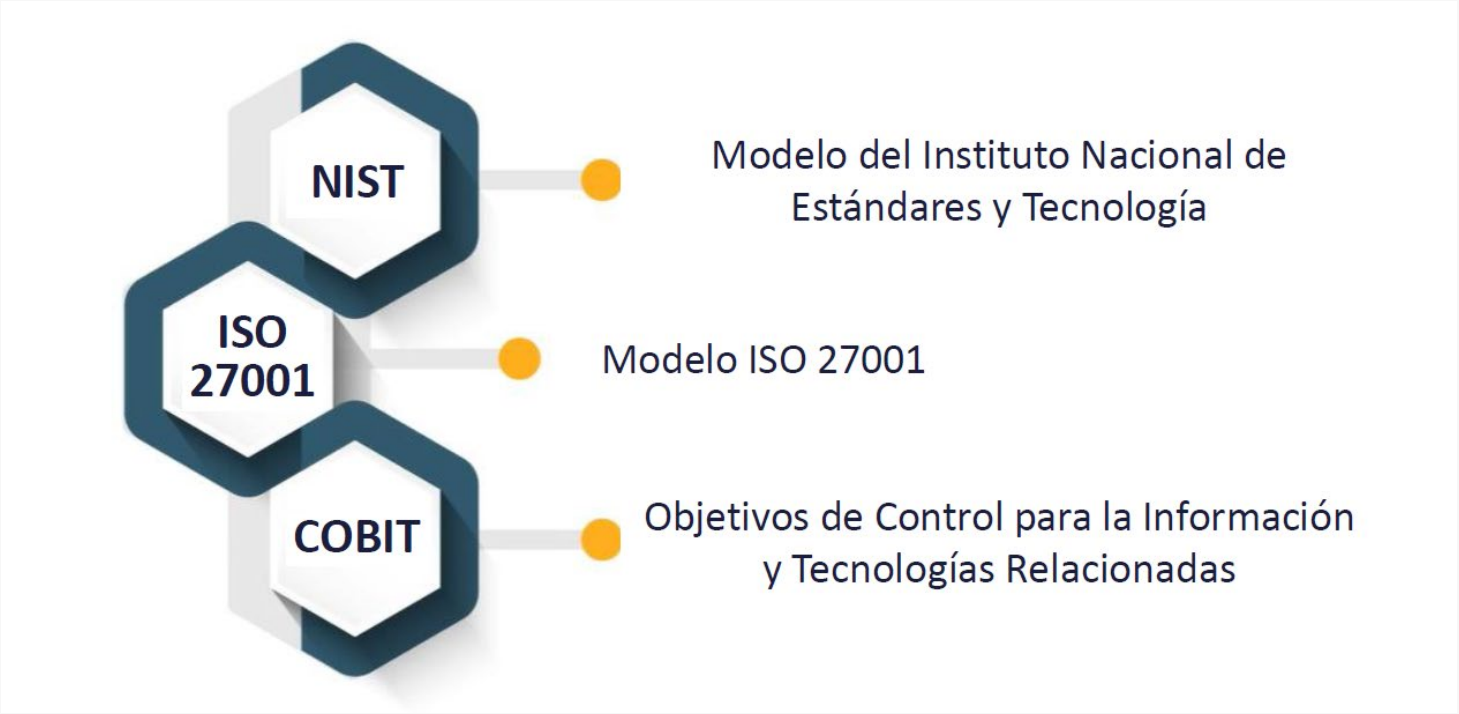
Crear un protocolo de respuesta.

Hacer una copia de seguridad de la información importante y los sistemas.

Contar con planes de continuidad del negocio que incluyan consideraciones de seguridad.

Controles de Ciberseguridad

Marcos de Control



Marcos de Control: NIST. Instituto Nacional de Estándares y Tecnología

FUENTE: NIST

5 ideas preconcebidas sobre la implementación de un programa de ciberseguridad

#1. No tengo información importante o valiosa

Las organizaciones de todos los tamaños mantienen o tienen acceso a datos valiosos que vale la pena proteger. Estos datos pueden incluir, correspondencia confidencial, sistemas de punto de venta, contratos comerciales. Todos los datos son valiosos.

Tome acción: evalúe los datos que crea, recopila, almacena, accede y transmite, y luego clasifique esos datos según su nivel de sensibilidad para que pueda tomar las medidas adecuadas para protegerlos.

#2. La ciberseguridad es sólo de la gente de TI o tecnología

No se puede confiar únicamente en la tecnología para asegurar sus datos. La ciberseguridad de una organización es responsabilidad de toda la fuerza laboral, no solo del personal de TI.

Tome acción: La ciberseguridad se aborda mejor con una combinación de **capacitación** de empleados, políticas y procedimientos claros y aceptados, e implementación de tecnologías actualizadas como software antivirus y antimalware o aplicando reglas como NIST

5 ideas preconcebidas sobre la implementación de un programa de ciberseguridad

#3. Requiere de mucha inversión

Hay muchos pasos que puede tomar que requieren poca o ninguna inversión financiera.

Tome acción:

- cree e instituya políticas y procedimientos de ciberseguridad;
- restrinja privilegios administrativos y de acceso;
- habilite la autenticación multifactor o de dos factores;
- capacite a los empleados para detectar correos electrónicos maliciosos y
- cree procedimientos manuales de respaldo para mantener los procesos comerciales críticos en funcionamiento durante un incidente cibernético.
- Aprenda más sobre cómo hacerlo utilizando la hoja de consejos "Quick Wins" de NCA

Small Business Cybersecurity "Quick Wins"

5 ideas preconcebidas sobre la implementación de un programa de ciberseguridad

#4. Si yo estoy seguro, ningún proveedor supondrá un riesgo

Externalizar el trabajo a un proveedor no exime de la responsabilidad de seguridad en caso de un incidente cibernético. Tiene sentido externalizar parte de su trabajo a otros, pero eso no significa que renuncie a la responsabilidad de proteger los datos a los que tiene acceso un proveedor. Los datos son suyos y usted tiene la responsabilidad legal y ética de mantenerlos seguros.

Tome acción: asegúrese de tener acuerdos completos con todos los proveedores, incluyendo cómo se manejan los datos de la empresa, quién posee los datos y tiene acceso a ellos, cuánto tiempo se retienen los datos y qué sucede con los datos una vez que se termina un contrato.

#5. Seguridad física y digital no van de la mano

Muchas personas asocian la ciberseguridad únicamente con software y código. Sin embargo, al proteger sus activos sensibles, no debe descartar la seguridad física.

Tome acción: incluya una evaluación de la distribución de su oficina y de lo fácil que es obtener acceso físico no autorizado a información y activos sensibles (por ejemplo, servidores, computadoras, registros en papel) en su planificación. Una vez completada la evaluación, implemente estrategias y políticas para prevenir el acceso físico no autorizado. Las políticas pueden incluir controlar quién puede acceder a ciertas áreas de la oficina y asegurar adecuadamente laptops y teléfonos mientras se viaja.


La ciberseguridad es
Priceless.
©2024 Mastercard. Proprietary and Confidential