




ANA CECILIA PÉREZ
Co-fundadora y Directora
Capa 8

Protege tu PyME: Estrategias esenciales de ciberseguridad para el éxito empresarial



An illustration depicting digital security and growth. A large computer monitor is the central focus, displaying a large orange padlock icon. A person is lying on their back on top of the monitor. Another person is sitting on the monitor, working on a laptop. To the left, a person is running while carrying a large orange and red credit card. To the right, a person is holding up a large gold coin with a dollar sign. The background is a light gray with faint icons of a mail envelope and a document.

"En un mundo digital, la ciberseguridad no es solo una opción, es la base que sostiene el crecimiento y la supervivencia de las PyMEs."

Objetivo

- Proporcionar un conjunto de **estrategias esenciales de ciberseguridad** para PyMEs que puedan implementar de **manera práctica, inmediata y eficiente** para proteger sus negocios y asegurar su éxito en un entorno digital cada vez más riesgoso.



Importancia de la ciberseguridad en PyMEs

Contexto



Incremento de ciberataques a PyMEs: una tendencia preocupante

- **Ciberataques en México:**
 - Según un informe de la Asociación de Internet MX, los ciberataques en México han aumentado considerablemente en los últimos años. **Cerca del 33% de las PyMEs mexicanas** reportaron haber sufrido algún ciberataque en 2023, un incremento del **20% respecto a años anteriores**.
- **América Latina en general:**
 - Según un informe de Kaspersky, **la región de América Latina ha experimentado un aumento del 24% en ataques cibernéticos** entre 2022 y 2023, con las PyMEs siendo las principales víctimas debido a su menor capacidad de implementar defensas robustas.
 - En particular, **México, Brasil y Argentina** han sido los países más afectados, representando más del **80% de los ciberataques en la región**.
 - **Datos específicos para PyMEs** indican que al menos el **50% de las PyMEs afectadas por ciberataques** terminan cerrando en un plazo de 6 meses debido a los daños financieros y reputacionales sufridos.



Estadísticas

- El **85% de los ataques exitosos** en PyMEs comienzan con phishing.
- El **20% de las PyMEs** que experimentan un ataque de ransomware nunca recuperan sus datos, incluso si pagan el rescate.
- En México, se estima que el costo promedio de un ciberataque para una PyME es de **\$1.5 millones de pesos**, según el reporte del "Cyber Readiness Report" de Hiscox (2023).
- Además, **el 60% de las PyMEs afectadas** tarda entre 6 meses y 1 año en recuperarse completamente, si es que logran hacerlo.
- El costo de los incidentes está compuesto por **pérdidas de ingresos, interrupciones en las operaciones, pérdida de confianza del cliente, y gastos en remediación** y recuperación de datos.



Factores que agravan la vulnerabilidad de las PyMEs

- **Falta de inversión en ciberseguridad:**
 - Más del **75% de las PyMEs en México** destinan menos del 1% de su presupuesto total a ciberseguridad, lo que las deja con recursos insuficientes para implementar medidas preventivas efectivas.
- **Brecha de conocimiento y capacitación:**
 - En México, **el 68% de los empleados** en PyMEs nunca ha recibido capacitación en ciberseguridad, según datos de la Asociación de Internet MX.



The image features a close-up, high-angle view of a brown printed circuit board (PCB) with intricate white circuit traces. A silver-colored metal padlock is positioned diagonally across the center-left of the frame. The padlock has a keyhole and a shackle. The background is a dense, repeating pattern of circuit traces, creating a sense of depth and complexity. The overall color palette is muted, with browns, greys, and metallic tones.

Estrategias esenciales de ciberseguridad

¿Por dónde empezar?



¿Cuál es nuestra postura de seguridad?

Diagnóstico integral

- Análisis de riesgos
- Análisis de vulnerabilidades
- Pruebas de penetración



Define tu estrategia de seguridad

Cultura organizacional

Normatividad

Componentes tecnológicos



Mide, evalúa y mejora de manera continua

Monitoreo continuo

Diagnóstico periódico

Lecciones aprendidas

Estrategia



Acciones preventivas:

Capacitación a colaboradores
Políticas de contraseñas seguras y AMF
Actualización y parches de software



Acciones detectivas

Monitoreo de red y sistemas
Auditorías de seguridad periódicas
Sistemas de detección de intrusos



Acciones correctivas

Restauración de respaldos
Aislamiento de sistemas comprometidos
Plan de respuesta a incidentes

Información clave de un diagnóstico integral

- Inventario de activos críticos
- Evaluación de vulnerabilidades
- Análisis de riesgos
- Revisión de políticas y procedimientos
- Capacitación del personal
- Cumplimiento normativo
- Capacidades de respuesta a incidentes

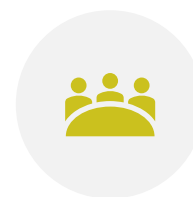
Claves para una cultura de ciberseguridad proactiva



Compromiso del liderazgo



Formación continua y concienciación



Implementación de políticas claras y accesibles



Fomentar la responsabilidad compartida



Uso de tecnologías accesibles y automatización



Preparación para lo inesperado



Monitoreo y revisión continua

95%

of Breaches are Caused



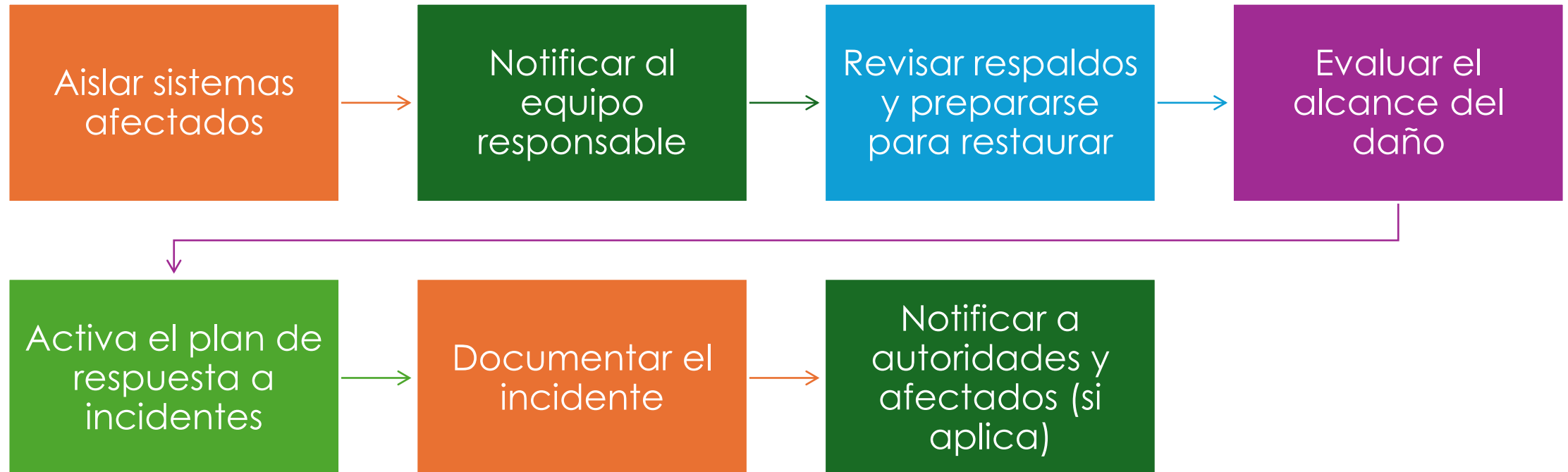
Los errores
humanos más
comunes que
comprometen
la seguridad

- **Phishing:** Los empleados que no saben identificar correos o mensajes fraudulentos son susceptibles a ser engañados, comprometiendo credenciales y acceso a información sensible.
- **Contraseñas débiles:** La reutilización de contraseñas o la falta de autenticación multifactor sigue siendo un problema importante.
- **Descuido al manejar dispositivos:** El uso de dispositivos personales en redes inseguras o dejar laptops y teléfonos sin proteger puede exponer a la empresa a riesgos.
- **Estadística relevante:** El 57% de los empleados **no detectan correos electrónicos fraudulentos** correctamente, según un estudio de KnowBe4.

Plan de respuesta a incidentes

A man in a dark blue suit and tie is shown from the chest up, interacting with a futuristic digital interface. His right hand is raised, palm facing forward, with several glowing yellow circles appearing on it. His left hand is holding a glowing orange globe with a magnifying glass over it. The background is a dark blue grid with various icons floating around: a car, a checkmark, a bar chart, a location pin, a laptop with a lock, a padlock, a telephone, and a group of people. The text "Plan de respuesta a incidentes" is overlaid in the center in a white, sans-serif font.

¿Qué hacer en caso de un ataque?



A close-up photograph of a piece of blue paper that has been torn. The tear is irregular and jagged, revealing a white surface underneath. On the white surface, the word "CONCLUSION" is printed in a black, serif, all-caps font. The blue paper is slightly curled on the left side, and the overall lighting is soft, highlighting the texture of the paper.

CONCLUSION

Cyber Security as a Core Business Function



Ciberseguridad
no es solo un
tema de TI

- Es un **asunto de toda la empresa**. No solo el equipo de tecnología debe estar capacitado en ciberseguridad, sino **todos los empleados**, desde la alta dirección hasta los trabajadores de primera línea.
- La **cultura de ciberseguridad** debe estar presente en cada nivel de la organización, con el personal actuando como la primera línea de defensa.

Inversión con alto retorno



- **Costo de los ciberataques:** En México, más del **58.3% de los ciberataques tienen éxito**, afectando gravemente a las empresas que no cuentan con medidas preventivas adecuadas.
- **Costo promedio de una brecha de seguridad:** Para PyMEs, una brecha puede significar la quiebra, ya que el 60% de las pequeñas empresas cierran seis meses después de un ciberataque.
- **Reducción del riesgo con ciberseguridad:** Las empresas que implementan medidas robustas de ciberseguridad, como autenticación multifactor y cifrado de datos, entre otros, pueden reducir el riesgo de un ciberataque hasta en un **90%**, según Cybersecurity Ventures.
- **ROI en seguridad proactiva:** Invertir en soluciones de seguridad proactiva, como firewalls, sistemas de detección de intrusos y capacitación de empleados, puede reducir los costos asociados a ataques cibernéticos en **\$1 millón USD en promedio** por incidente, de acuerdo con Ponemon Institute.

¿Qué puedes hacer hoy?

- Realiza una auditoría rápida de ciberseguridad
- Activa la autenticación multifactor
- Capacita a tu equipo sobre los riesgos más comunes
- Revisa y actualiza contraseñas
- Realiza una copia de seguridad de tus datos
- Instala y actualiza soluciones de seguridad
- Revisa los accesos y permisos de los empleados



Mensaje final



Las PyMEs en México y América Latina son el motor económico de la región, pero también son los blancos más vulnerables a los ciberataques debido a la falta de inversión, capacitación y políticas preventivas de ciberseguridad.



El contexto actual muestra un incremento alarmante de ataques, especialmente en forma de phishing y ransomware, que tienen un impacto devastador en términos económicos y operativos.



Para asegurar su supervivencia y crecimiento, las PyMEs deben adoptar un enfoque proactivo que integre la ciberseguridad en todas sus operaciones, desde la dirección hasta el personal de todos los niveles.

Preguntas y respuestas

Gracias

ANA CECILIA Pérez Rosales

Co fundadora y directora de Capa 8, Familias y Escuelas Ciberseguras



@annecpr



www.linkedin.com/in/anaceciliaperezr



contacto@capa8.com
fciberseguras@capa8.com
eciberseguras@capa8.com



capa8®





MUCHAS GRACIAS



Liderando la digitalización por México



CÁMARA DE COMERCIO
SERVICIOS Y TURISMO
CIUDAD DE MÉXICO