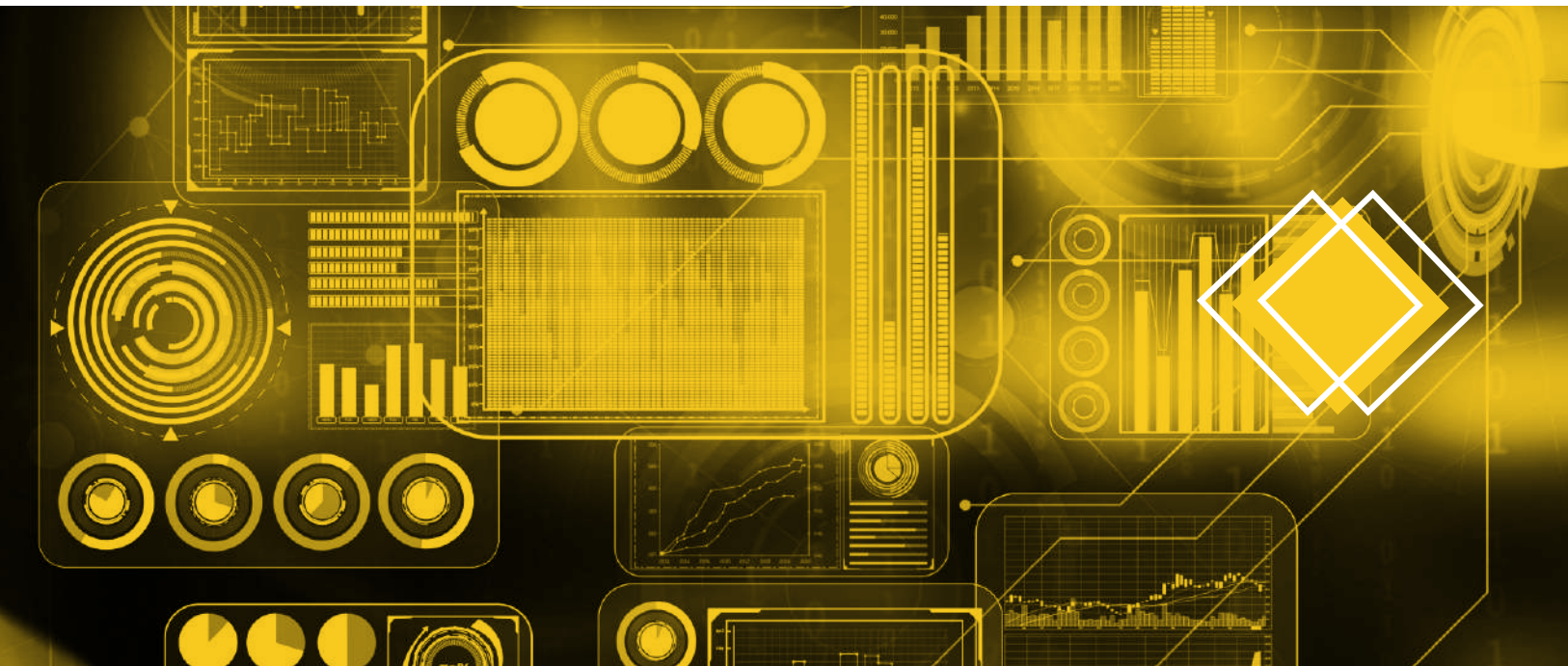
Ciberseguridad para No Tecnólogos

Decisiones inteligentes para proteger tu empresa

ÍNDICE



1.Introducción

Vivimos en una época donde la información, los sistemas y los datos de clientes son el motor de la empresa, sin importar el sector o el tamaño. Hoy, **la ciberseguridad se ha vuelto una prioridad estratégica, no solo un tema para "los de sistemas"**.

El mundo digital nos da oportunidades inéditas de crecimiento, pero también nos pone **en la mira de amenazas** cada vez más sofisticadas. La alta dirección y los responsables de negocio deben comprender estos riesgos y liderar la protección, aún si no son expertos en tecnología. **La pregunta ya no es si serán atacados, sino cuándo y cómo responderán.**

2. El panorama actual: el cibercrimen es negocio

El cibercrimen se ha profesionalizado y crece a pasos agigantados.

Grupos criminales organizados trabajan como verdaderas empresas:

- *Tienen centros de operación, estructuras jerárquicas y "afiliados" que distribuyen ataques en todo el mundo.*
- *Venden accesos, alquilan malware y ofrecen soporte para realizar ciberataques.*
- *Según estimaciones de Cybersecurity Ventures, el cibercrimen generará más de $10.5 billones de dólares al año en 2025, siendo la tercera "economía" global.*

Hoy, por menos de $100 dólares, cualquier persona puede adquirir herramientas para atacar una empresa, incluyendo instrucciones y soporte. Las empresas medianas, por su perfil y recursos limitados, se han convertido en uno de los blancos favoritos: **tienen información valiosa y, muchas veces, defensas insuficientes.**

3. La superficie de ataque en las empresas del mercado medio

La digitalización ha multiplicado los puntos vulnerables en las organizaciones. Antes, proteger la oficina era suficiente; **hoy, los empleados trabajan desde casa, acceden a sistemas desde sus celulares, y colaboran con proveedores o clientes en plataformas digitales**.

La infraestructura se ha vuelto híbrida: conviven sistemas heredados, servicios en la nube, aplicaciones móviles y dispositivos conectados a internet. Muchas empresas usan varias herramientas de ciberseguridad, pero estas no siempre se comunican entre sí.

Además, **la falta de visibilidad sobre los activos críticos y quién accede a ellos deja "puertas abiertas" que los atacantes saben explotar.** El riesgo no distingue tamaño: si tu empresa usa tecnología, tiene una superficie de ataque.

4. El costo real de los ciberataques

El impacto de un ciberataque va mucho más allá de un simple "susto":

- **Económico:** El costo promedio global por filtración de datos es de $4.45 millones de dólares por incidente, y en el caso de empresas medianas, esto puede ser la diferencia entre seguir operando o cerrar. Las pérdidas incluyen recuperación, pagos a proveedores, horas improductivas y sanciones.
- **Reputacional:** Los clientes, socios y proveedores pierden confianza cuando la empresa sufre un incidente. En la era digital, la reputación es uno de los activos más valiosos.
- **Operativo:** Un ataque puede detener la facturación, ventas, logística y atención al cliente durante días o semanas.

Con la entrada de nuevas leyes, las multas y sanciones por incumplimiento pueden ser severas y afectar la viabilidad de la empresa.

En México, más del 60% de las empresas medianas afectadas tardan semanas en recuperar su operación y muchas no lo logran.

5. Principales amenazas: ¿qué está en juego?

Las amenazas digitales evolucionan todos los días. Las más frecuentes son:

- **Ransomware:** El secuestro de datos y sistemas, pidiendo un rescate para devolver el acceso.
- **Phishing:** Correos, mensajes o llamadas que suplantan identidades para engañar a los empleados y obtener acceso a sistemas o información sensible.
- **Exploits y vulnerabilidades:** Errores o debilidades en programas y aplicaciones que permiten a los atacantes ingresar.
- **Robo de credenciales:** El 33% de los ataques exitosos comienzan por credenciales comprometidas.
- **Amenazas internas:** Desde errores accidentales hasta empleados descontentos o poco capacitados que exponen la empresa.

El 39% de las intrusiones en la nube inician por robo de credenciales, y el 35% por phishing. Nadie está exento, y un solo clic puede desencadenar una crisis.

6. Regulación y nuevas obligaciones para empresas

Las autoridades mexicanas e internacionales están endureciendo las reglas:

- **Europa:** Normas como la Directiva NIS2 y la Cyber Resilience Act exigen que las empresas (sin importar sector) prevengan, resistan y se recuperen de ciberataques, responsabilizando directamente al Consejo de Administración.
- **Estados Unidos:** La SEC obliga a las empresas públicas a reportar incidentes y sus estrategias de ciberseguridad.
- **México:** En 2023 se presentó la iniciativa de Ley Federal de Ciberseguridad, que busca regular y sancionar ataques, crear una Agencia Nacional y exigir reportes y controles en todos los sectores.

El incumplimiento puede dejar a las empresas fuera del mercado, perder certificaciones, enfrentar demandas o multas. La omisión ya no es ignorancia: es negligencia empresarial.

7. De la reacción a la prevención: cultura organizacional

Más allá de la tecnología, el mayor reto es la mentalidad:

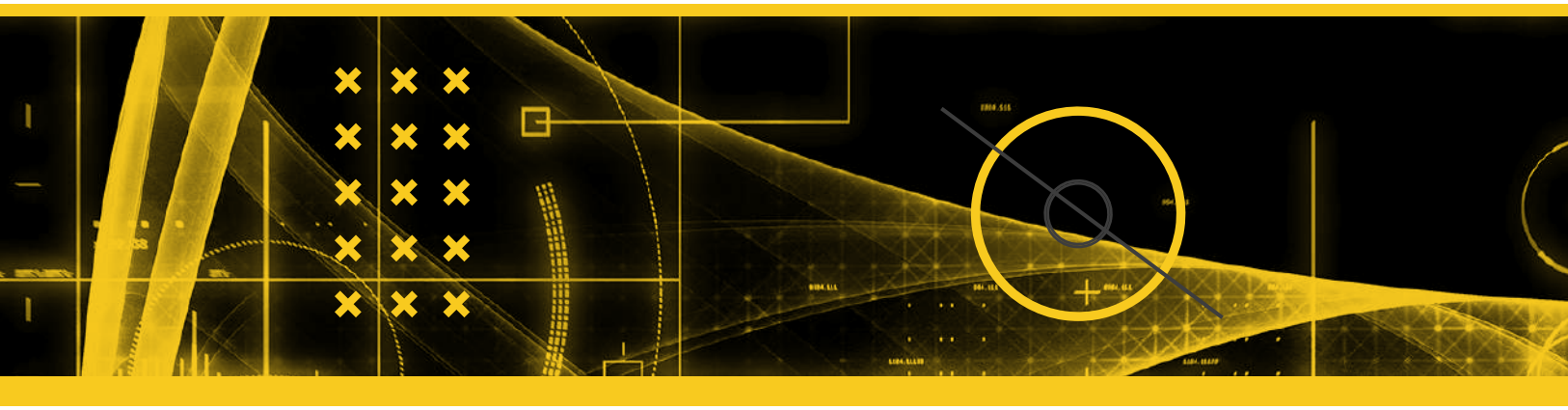
- Muchas empresas **ven la ciberseguridad como un gasto**, y la relegan solo a TI.
- **El 56% de los directivos subestiman el riesgo real** y no priorizan la prevención.
- **Falta de liderazgo y coordinación entre áreas:** cada quien cuida “su parte”, pero nadie ve el todo.
- **Hay escasez de talento en ciberseguridad** y pocas iniciativas de capacitación para todo el personal.

La resiliencia digital solo se logra cuando la seguridad es parte de la estrategia, reportes y cultura diaria. El liderazgo desde la alta dirección es clave para que todos, desde el CEO hasta el último colaborador, asuman la responsabilidad de proteger la empresa.

8. Estrategias prácticas sin tecnicismos

No necesitas ser ingeniero para fortalecer la ciberseguridad de tu empresa:

- **Gobierno corporativo:** Incluye el riesgo cibernético en tus indicadores y reuniones clave; exige reportes periódicos.
- **Adopta modelos internacionales:** Marcos como NIST o Zero Trust sirven como guía, incluso de manera simplificada.
- **Evalúa riesgos periódicamente:** Realiza diagnósticos de madurez y vulnerabilidades al menos una vez por año, con apoyo de expertos externos si es necesario.
- **Automatiza y agiliza la respuesta:** Implementa herramientas que alerten de incidentes y activen respuestas automáticas para minimizar daños.
- **Capacita a todo el personal:** La seguridad es tarea de todos. Realiza simulaciones, cursos y campañas periódicas.
- **Responsable de ciberseguridad:** Designa a un líder que tenga voz en la dirección y recursos para implementar acciones.
- **Integración total:** Busca que todas las soluciones y procesos de seguridad trabajen juntos, evitando “parches” aislados y silos de información.



9. Autodiagnóstico: checklist de seguridad para líderes

Hazte estas preguntas:

- ¿Cuánto invierte tu empresa en ciberseguridad cada año?
- ¿Sabes cuáles son tus activos y datos más críticos y vulnerables?
- ¿Existe una persona o comité en la dirección responsable de ciberseguridad?
- ¿Han sufrido incidentes en el último año? ¿Cómo respondieron?
- ¿La seguridad digital está en tus reportes y KPIs clave?
- ¿Realizan simulaciones o pruebas internas de ataque (red teaming)?
- ¿Recibes reportes claros y periódicos sobre riesgos digitales?
- ¿Tu equipo está capacitado y motivado para actuar antes, durante y después de un incidente?
- ¿Tienes una cultura de prevención o solo reaccionas ante incidentes?

Entre más “no” contestes, mayor es la urgencia de fortalecer tu estrategia.

10. ¿Por qué Grupo Scanda? Nuestra experiencia

En Grupo Scanda llevamos más de 30 años acompañando a empresas medianas y grandes en su transformación digital y en la protección de su información más valiosa.

- **Expertos en seguridad y gobierno corporativo:** Hemos implementado estrategias de ciberseguridad en sectores como finanzas, salud, retail, servicios, logística, educación y muchos otros.
- **Soluciones a tu medida:** Desde diagnósticos y planes de acción hasta la ejecución de marcos internacionales, automatización y pruebas de resiliencia.
- **Impulsamos la cultura preventiva:** Ayudamos a crear comités y responsables ejecutivos, diseñamos simulaciones de ciberataques y capacitamos a todos los niveles de la organización.
- **Visión integral:** Entendemos la relación entre tecnología, negocio y personas, traduciendo la ciberseguridad en confianza, reputación y continuidad operativa.
- **Reconocimiento y casos de éxito:** Participamos en foros internacionales, estamos a la vanguardia de tendencias y nuestros clientes avalan nuestra capacidad de proteger lo que más valoran.

Con Grupo Scanda, la ciberseguridad es un acompañamiento estratégico y humano que asegura tu presente y futuro empresarial.

11. Conclusiones

La ciberseguridad ya no es solo una función técnica, es una prioridad de negocio y una responsabilidad de liderazgo.

Las amenazas digitales no se detendrán, pero las empresas que actúan hoy estarán preparadas para cualquier reto que traiga el mañana.
La diferencia entre sobrevivir o ser noticia por el próximo incidente está en las decisiones que tomes ahora.

Proteger tu empresa es proteger tu reputación, tus clientes, tu equipo y tu legado. No lo dejes para mañana.

¿Quieres saber cómo está tu empresa?

En Grupo Scanda te ayudamos a diagnosticar, fortalecer y liderar la ciberseguridad de tu organización.

- **scanda.com.mx**
- **Grupo Scanda**
- **GrupoScanda_**
- **Grupo Scanda**
- **Grupo Scanda**
- **grupo_scanda**