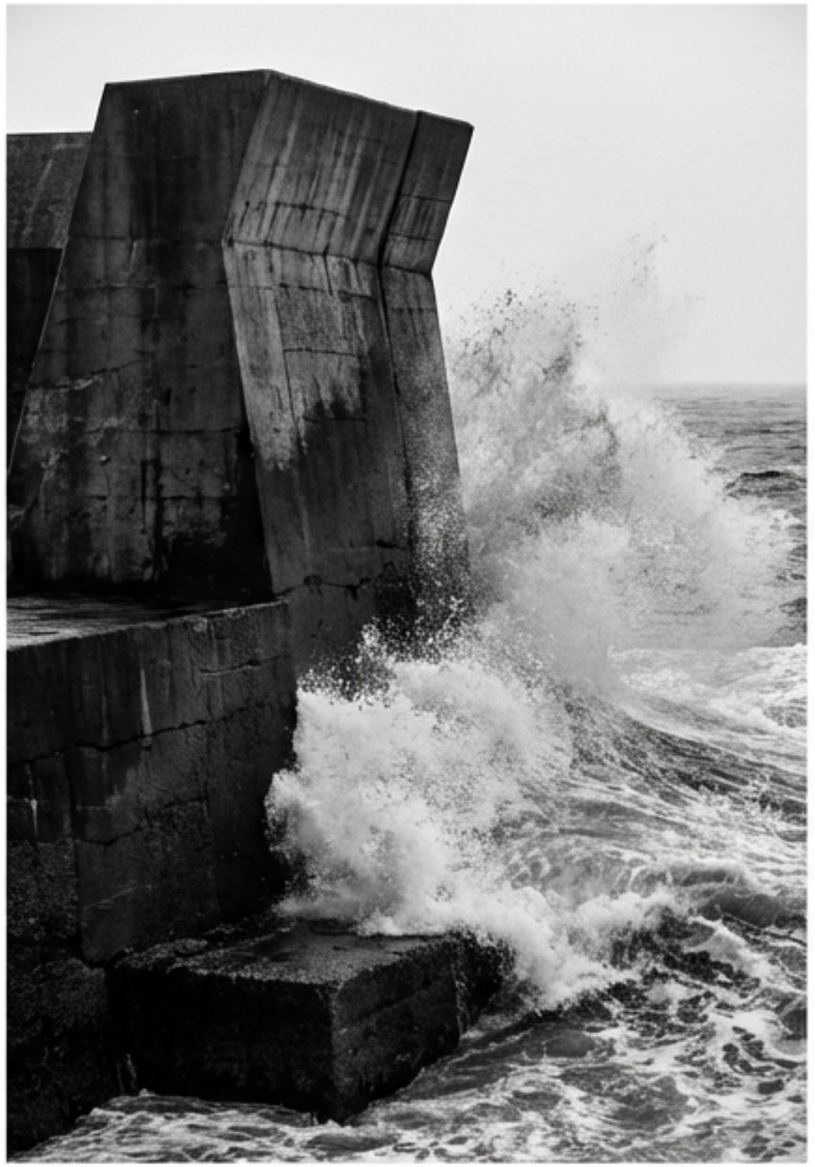
UN PODCAST DE ALGERISK CORPORATION:
GENERANDO CULTURA DE RIESGOS

Ciberresiliencia vs. Ciberseguridad

Por qué proteger ya no es suficiente.



Una transición estratégica de "construir muros más altos" a "operar bajo fuego".

Documento de Lectura Ejecutiva.

PROFESSIONAL EXECUTIVE SUMMARY

La prevención falla. La recuperación define el éxito.

Durante años, el enfoque ha sido evitar que el incidente ocurra. La realidad actual demuestra que no todas las amenazas pueden ser evitadas. La diferencia entre una organización vulnerable y una resiliente no es la ausencia de ataques, sino la capacidad de responder, recuperarse y continuar operando.

EL CAMBIO

De una lógica defensiva (Seguridad) a una lógica adaptativa (Resiliencia).

LA AMENAZA

Ransomware 3.0 y ataques a la cadena de suministro que evaden controles técnicos.

LA SOLUCIÓN

Adoptar el NIST CSF 2.0 e integrar el riesgo ciber al Gobierno Corporativo.

Hoy, proteger ya no es suficiente. La ciberresiliencia no es un proyecto tecnológico, es una decisión estratégica.

La Gran Diferencia: Seguridad vs. Resiliencia

Ciberseguridad (Defensiva)

Objetivo: Proteger sistemas.

Acciones: Prevenir accesos no autorizados, proteger confidencialidad, controles técnicos.

Mentalidad: "Evitar que el incidente ocurra."

Ciberresiliencia (Adaptativa)

Objetivo: Proteger el negocio.

Acciones: Anticipar disrupción, limitar impacto, recuperar servicios, aprender del evento.

Mentalidad: "El incidente va a ocurrir. Debemos seguir operando."

Las organizaciones que solo invierten en protección técnica fallan cuando el ataque supera sus defensas.

La premisa incómoda: El incidente va a ocurrir.

La ciberresiliencia parte de un supuesto realista: **la brecha es inevitable**. Incluso organizaciones con altos niveles de madurez han sido comprometidas porque el atacante siempre va un paso adelante.

- **Viejo Paradigma:** Invertir recursos en creer que somos invulnerables.
- **Nueva Realidad:** Invertir en planes de continuidad digital, respaldos probados y protocolos de comunicación.

"¿Qué pasa cuando los muros fallan? Si su estrategia termina en la prevención, su organización está desprotegida ante la crisis real.

Lecciones del Ransomware 3.0: De incidente técnico a crisis corporativa.

El enemigo ha evolucionado. Ya no es solo un virus, es un modelo de negocio criminal.

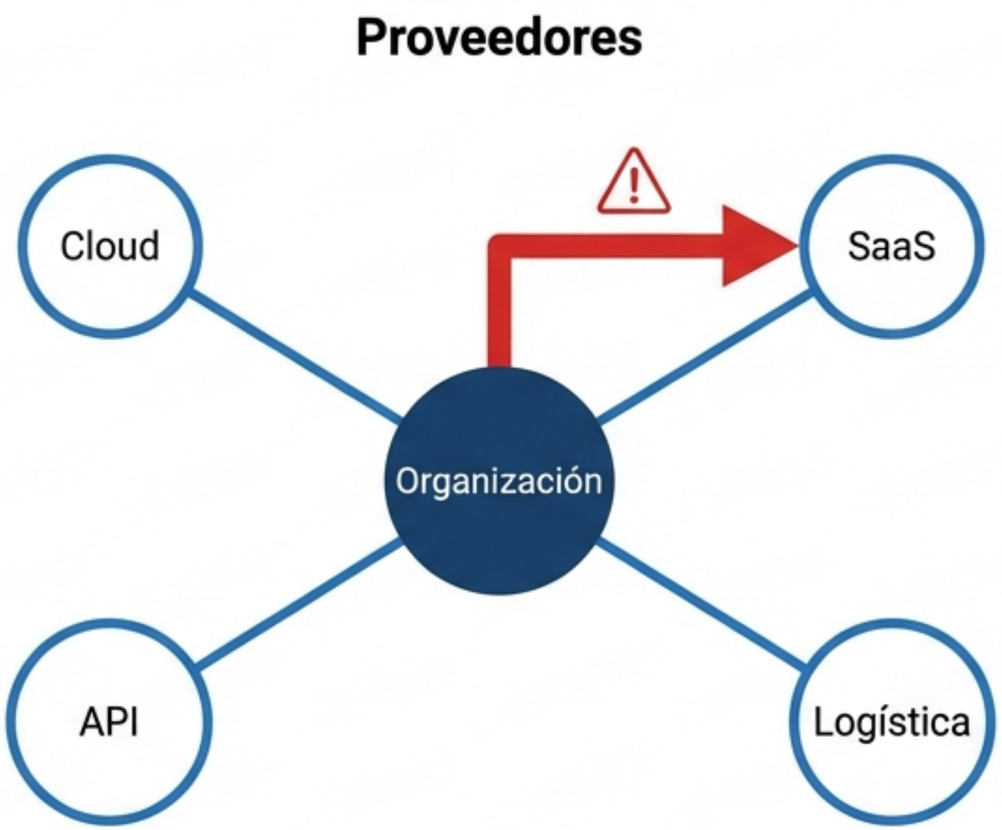
- **Doble y triple extorsión**: Cifrado + Publicación + Presión externa.
- **Robo previo**: Exfiltración de información sensible antes del bloqueo.
- **Impacto Transversal**: Afecta operaciones, reputación, proveedores y valor de mercado.

Las organizaciones sin planes de continuidad digital y roles claros de decisión terminan pagando rescates, prolongando la interrupción y amplificando el daño reputacional.

PROFESSIONAL EXECUTIVE SUMMARY

El riesgo que TI no controla: **La Cadena de Suministro**

Gran parte de la infraestructura crítica depende de terceros (Cloud, SaaS, APIs). Un ataque a un **proveedor puede paralizar múltiples** organizaciones y evadir controles internos.



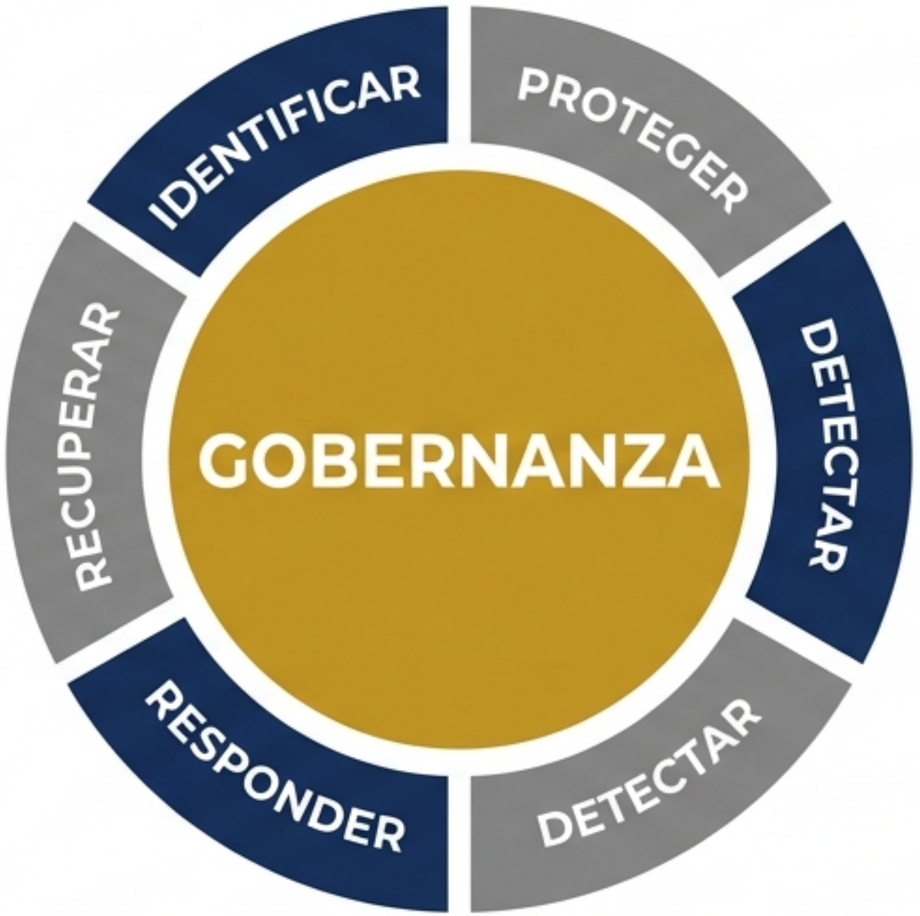
Requisito de Resiliencia

- Gestión integral del riesgo de terceros.
- Evaluación de ciberpostura de proveedores.
- Cláusulas contractuales de continuidad y pruebas conjuntas de recuperación.
- Planes de salida y sustitución definidos.

> “No se trata solo de proteger lo propio, sino de **resistir la disrupción del ecosistema digital**.”

NIST CSF 2.0: El nuevo estándar de Resiliencia Operacional.

- **Gobernanza al centro**: Refuerza que la ciberseguridad es responsabilidad de la alta dirección.
- **Integración ERM**: Los riesgos cibernéticos deben integrarse a la Gestión de Riesgos Empresariales.
- **Continuidad**: Alinea la seguridad técnica con la resiliencia operacional del negocio.



NIST ahora habla el lenguaje del negocio, no solo de la tecnología.

Integrando el Ciberriesgo en la Estrategia de Negocio.

Reporte Directo
La ciberseguridad debe reportarse al Directorio, no quedarse en el departamento de TI.

Apetito de Riesgo
Deben definirse tolerancias claras al riesgo cibernético (¿cuánto tiempo podemos estar fuera de línea?).

Responsabilidad Ejecutiva
La resiliencia deja de ser una tarea técnica para convertirse en una obligación fiduciaria.

PROFESSIONAL EXECUTIVE SUMMARY

El Rol del Directorio ante una Cibercrisis.

Decisiones críticas que no pueden recaer en el equipo de TI.

Operaciones: ¿Quién decide detener la planta o desconectar los servicios para contener el ataque?

Finanzas: ¿Quién evalúa el impacto financiero y decide si se paga o no un rescate?

Reputación: ¿Quién autoriza la comunicación pública a clientes, reguladores y prensa?

Un Directorio que solo recibe reportes técnicos (KPIs de antivirus) no está preparado para tomar estas decisiones estratégicas bajo presión.

De Proyecto Técnico a Estrategia Corporativa.

La ciberseguridad por sí sola es insuficiente. La ciberresiliencia es el nuevo estándar para mantener la confianza del mercado.

Perfil de una Organización Resiliente:

- Detectan rápido.
- Responden con orden.
- Continúan operando.
- Se recuperan con disciplina.
- Aprenden del incidente.

Exija pruebas de resiliencia y participe en simulacros de crisis.

La resiliencia se construye antes del ataque, no durante.