Cómo proteger la empresa frente a un ciberataque

Recoletos
Consultores | Broker

PABEMAR
CONSULTORÍA EMPRESARIAL

Medidas básicas de prevención, organización de la respuesta, continuidad de la actividad y papel del ciberseguro dentro de una estrategia de protección eficaz.

La ciberseguridad ya no es un asunto solo técnico; es una cuestión de continuidad de negocio, confianza y capacidad de recuperación.

El riesgo cibernético ya es riesgo de negocio

No se trata solo de “evitar ciberataques”. Se trata de poder seguir operando, facturando y atendiendo a clientes cuando un incidente afecta a sistemas, datos o proveedores.

1 Operación

Paradas, retrasos, dependencia del correo, ERP o accesos remotos.

2 Finanzas

Pérdida de ingresos, costes de recuperación y presión sobre caja.

3 Reputación y cumplimiento

Clientes, confianza, contratos y posibles obligaciones de notificación.

Visión de dirección: priorizar, decidir y asignar recursos.

Las medidas básicas siguen siendo las más rentables

La mayoría de las empresas mejora mucho su exposición cuando hace bien lo esencial y lo mantiene en el tiempo.

Autenticación multifactor	Especialmente en correo, VPN, paneles y cuentas con privilegios.
Actualizaciones y parcheo	Reducen puertas de entrada conocidas y vulnerabilidades explotables.
Copias de seguridad seguras	Protegidas, separadas y probadas periódicamente.
Menos privilegios	Cada persona accede solo a lo que necesita para trabajar.
Concienciación frente al phishing	El usuario debe saber detectar, parar y escalar.
Control de proveedores	La seguridad también depende de terceros con acceso o servicios críticos.

La prevención eficaz no es sofisticación: es disciplina.

El primer vector suele ser humano o externo

Correo, credenciales, accesos remotos y terceros concentran gran parte del riesgo inicial.

Tres mensajes para dirección:

1 **Phishing mejorado**

Mensajes urgentes, creíbles y cada vez más personalizados.

2 **Credenciales críticas**

Una cuenta comprometida abre la puerta a fraude, suplantación o ransomware.

3 **Cadena de suministro**

Un proveedor con acceso o una dependencia clave puede interrumpir la actividad.

Conclusión práctica

La tecnología ayuda, pero la empresa necesita procedimientos simples: verificar antes de pagar, elevar dudas rápido, revisar accesos y exigir seguridad mínima a sus proveedores.

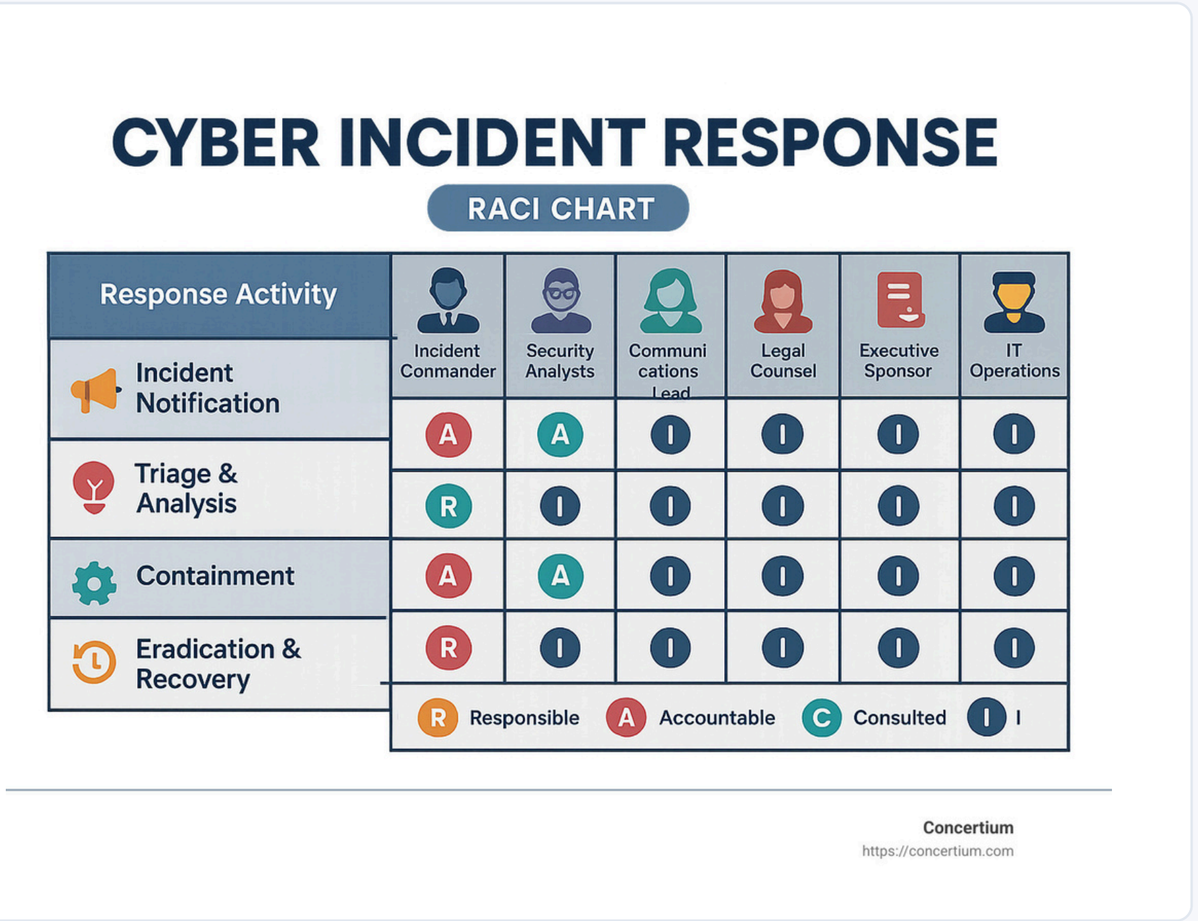
Cuando hay incidente, improvisar sale caro

La respuesta debe estar organizada antes del incidente: quién decide, quién contiene, quién comunica y quién documenta.

Primeras decisiones:

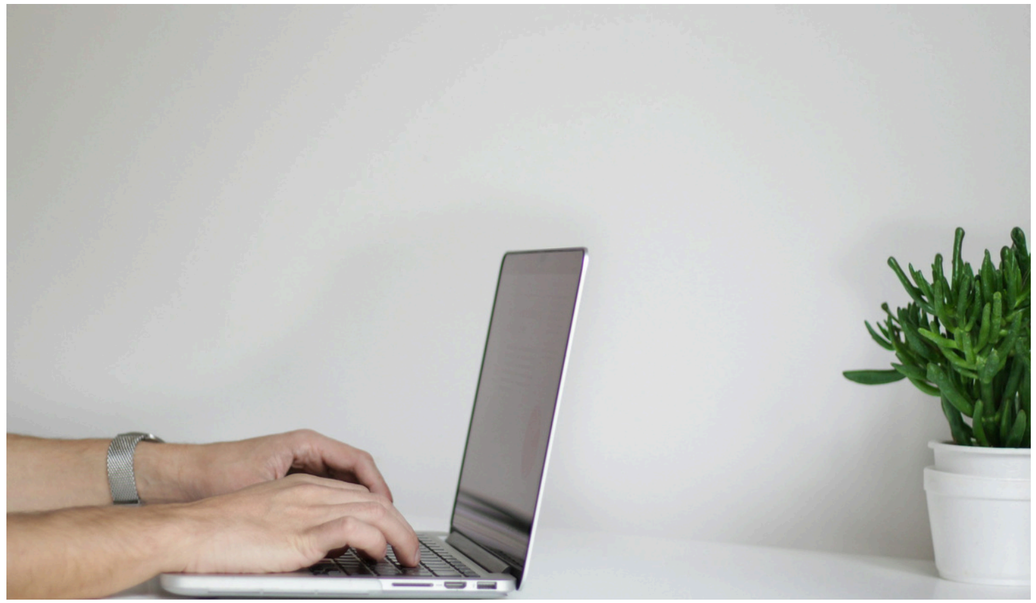
1. Confirmar el incidente y contenerlo.
2. Aislar equipos, accesos o cuentas afectadas.
3. Activar al equipo de crisis y repartir roles.
4. Preservar evidencias y registrar hechos.
5. Valorar impacto operativo, legal y reputacional.

Ransomware: la posición de partida es no pagar. Y si hay brecha de datos personales con riesgo, puede existir obligación de notificar a la AEPD en 72 horas.



Continuidad: seguir prestando servicio

La resiliencia exige saber qué procesos son críticos, cuánto tiempo pueden parar y cómo se opera mientras se recupera la tecnología.



Cuatro preguntas de continuidad

1 Qué proceso no puede parar

Ventas, atención al cliente, cobros, producción o logística.

2 Cuánto tiempo es asumible

Definir umbrales reales de parada y pérdida aceptable.

3 Cómo seguimos comunicando

Canales alternativos si el correo o los sistemas caen.

4 Cómo recuperamos y probamos

Backups, restauración y ejercicios para no descubrir fallos en caliente.

Ciberseguro: protección complementaria

Su función es ayudar a absorber impacto económico y operativo, y activar recursos especializados cuando el incidente ya se ha producido.

Qué aporta

- respuesta y coordinación de especialistas
- restauración y gastos de recuperación
- posible cobertura por interrupción de negocio
- apoyo ante reclamaciones y terceros
- una vía ordenada para gestionar la crisis

Qué no reemplaza

No evita el ataque, no arregla procesos deficientes y no elimina límites, condiciones o exclusiones de póliza.

COBERTURAS

- GESTIÓN DE INCIDENTES
- PROTECCIÓN DE DATOS
- RESPONSABILIDAD CIVIL
- EXTORSIÓN CIBERNÉTICA
- FRAUDE CIBERNÉTICO
- INTERRUPCIÓN DE NEGOCIO
- DAÑOS PROPIOS AL HARDWARE

Una estrategia eficaz combina prevención + respuesta + continuidad + seguro

Hoja de ruta sugerida para 90 días

0–30 días

MFA en accesos críticos
Inventario mínimo de activos y proveedores
Backups revisados y protegidos

30–60 días

Plan de respuesta simple
Roles de crisis y comunicación
Formación contra phishing y fraude

60–90 días

Prueba de restauración
Revisión de continuidad
Análisis de encaje del ciberseguro

“La pregunta correcta no es si mi empresa puede sufrir un ciberataque. La pregunta correcta es si estamos preparados para resistirlo, responder y seguir adelante.”

PABEMAR

CONSULTORÍA EMPRESARIAL

Recoletos

Consultores | Broker

Av. de la Azucarera 2, 28500 - Arganda del Rey (Madrid)

692 121 927

info@pabemar.es

www.pabemar.es

C. de la Montera, 24, 2º F, 28013 Madrid

910 91 03 25

informacion@recoletosconsultores.com

www.recoletosconsultores.com