viva
TECNOLOGÍA QUE CONECTA

GUÍA PRÁCTICA · 2026

Checklist contra ransomware

15 controles que toda empresa debería tener

El ransomware cifra la información de una empresa y exige un pago para recuperarla. La mayoría de los ataques no aprovechan fallas sofisticadas, sino controles básicos ausentes. Usa esta lista para revisar, en pocos minutos, qué tan preparada está tu organización.

Cómo usar esta guía

1. Revisa cada control con tu equipo de TI y marca la casilla solo si se cumple por completo.
2. Cuenta las casillas marcadas y consulta el resultado en la última página.
3. Empieza por los controles sin marcar de la sección “Prevenir”: son los que más reducen el riesgo.

> **Las tres etapas**
>
> **Prevenir:** cerrar las puertas de entrada. **Detectar:** ver el ataque a tiempo. **Responder:** contenerlo y recuperarse sin pagar rescate.

PREVENIR

Cierra las puertas de entrada

- [ ] **Autenticación multifactor (MFA)** 01
  Activa en el correo, la VPN, los accesos remotos y las cuentas de administrador. Una contraseña robada no debe bastar para entrar.

- [ ] **Parches al día** 02
  Las actualizaciones críticas de sistemas, firewalls y VPN se aplican en plazos definidos, priorizando lo que está expuesto a internet.

- [ ] **Respaldos aislados** 03
  Existe al menos una copia de respaldo fuera de la red o inmutable, que un atacante no pueda cifrar ni borrar.

- [ ] **Protección avanzada de equipos (EDR/XDR)** 04
  Computadoras y servidores cuentan con detección de comportamiento, no solo con un antivirus tradicional.

- [ ] **Filtrado del correo** 05
  Se analizan adjuntos y enlaces, y se bloquean los correos sospechosos antes de llegar al usuario.

- [ ] **Mínimo privilegio** 06
  Los usuarios no son administradores de sus equipos, y las cuentas de administrador son separadas y controladas.

- [ ] **Red segmentada** 07
  Servidores, usuarios e invitados están en redes separadas, para que un equipo infectado no alcance todo lo demás.

- [ ] **Acceso remoto seguro** 08
  No hay escritorio remoto (RDP) expuesto a internet; el acceso es por VPN con MFA o con un modelo Zero Trust.

- [ ] **Colaboradores entrenados** 09
  Se capacita de forma periódica para reconocer el phishing, con simulaciones y reportes.

DETECTAR

Ve el ataque a tiempo

- [ ] **Monitoreo 24/7** 10
  Alguien vigila los eventos de seguridad de día, de noche y en fines de semana, que es cuando suelen ejecutarse los ataques.

- [ ] **Registros centralizados** 11
  Los registros de firewalls, servidores y accesos se guardan en un solo lugar y se conservan para investigar.

- [ ] **Inventario de activos** 12
  Se conoce qué equipos, servidores y servicios existen y quién es responsable de cada uno.

RESPONDER

Contén y recupérate sin pagar

- [ ] **Plan de respuesta a incidentes** 13
  Está escrito, con roles, contactos y decisiones clave definidas antes de que ocurra un incidente.

- [ ] **Restauración probada** 14
  Se prueba periódicamente que los respaldos se pueden restaurar y en cuánto tiempo.

- [ ] **Simulacro anual** 15
  Al menos una vez al año, el equipo practica la respuesta ante un ataque simulado.

Tu resultado

Cuenta cuántas casillas marcaste:

13 a 15
POSTURA SÓLIDA

Tienes las bases. El reto es sostenerlas: revisa esta lista cada seis meses y mide la respuesta con simulacros.

8 a 12
CON BRECHAS

Un atacante podría aprovechar los controles que faltan. Prioriza los de la sección “Prevenir”.

0 a 7
RIESGO ALTO

Tu empresa está expuesta a los ataques más comunes. Conviene actuar de inmediato, empezando por MFA, respaldos aislados y acceso remoto seguro.

Si sufres un ataque: primeros pasos

01
Aísla
Desconecta de la red los equipos afectados, pero no los apagues.

02
Conserva
No borres archivos ni registros: son evidencia para la investigación.

03
No pagues
Pagar no garantiza recuperar los datos y financia nuevos ataques.

04
Pide ayuda
Contacta a especialistas en respuesta a incidentes cuanto antes.

VIVA SOLUTIONS · NOC Y SOC 24/7 DESDE PANAMÁ

¿Quieres cerrar las brechas con especialistas?

viva
TECNOLOGÍA QUE CONECTA

Diseñamos, implementamos y operamos 24/7 los controles de esta lista. Conoce tu nivel en 3 minutos con nuestra autoevaluación gratuita o habla con un ingeniero.

Autoevaluación: vivaconecta.com/autoevaluacion
¿Bajo un ataque?: vivaconecta.com/incidente
(507) 216-9004
webforms@vivaconecta.com

Guía orientativa de buenas prácticas. No sustituye una evaluación profesional de tu entorno.