IDPROTECTHOR

Guía gratuita para empresas · Edición octubre 2026

La primera hora ante un ciberataque

Qué hacer, en qué orden y qué evitar cuando sospecha que alguien entró a su red. Pensada para dueños de empresa y responsables de TI, no para especialistas.

3.4 h
tarda un atacante, ya dentro, en llegar al servidor de Active Directory

88%
de los ataques de ransomware se lanzan fuera del horario laboral

3 días
es la mediana de tiempo que un intruso pasa en la red antes de ser detectado

Fuente: Sophos, Active Adversary Report 2026 (661 casos de respuesta a incidentes, nov 2024 – oct 2025).

Los primeros 60 minutos, en orden

1. **Nombre a un responsable y anote la hora**
   Una sola persona coordina. Desde este momento, todo se registra: hora, quién, qué vio, qué hizo (use la hoja de la página 3).

2. **Aísle, no apague**
   Desconecte de la red (cable y Wi-Fi) los equipos afectados, pero no los apague: la memoria guarda evidencia valiosa. Si el ataque se extiende, separe la red de servidores.

3. **Proteja las identidades**
   Desde un equipo limpio, cambie las contraseñas de las cuentas de administrador y de servicio críticas, cierre las sesiones activas en Microsoft 365 / Entra ID y deshabilite cualquier cuenta sospechosa.

4. **Ponga a salvo los respaldos**
   Desconecte los respaldos que sigan en línea. No restaure nada todavía: primero hay que saber cómo entró el atacante, o volverá a cifrar lo restaurado.

5. **Preserve la evidencia**
   Tome fotos de las pantallas y notas de rescate. No borre registros (logs) ni formatee equipos.

6. **Avise a quien corresponde**
   Dirección, asesor legal y su aseguradora si tiene póliza de ciberriesgo. Valore con su abogado el aviso a clientes si hay datos personales involucrados, y presente denuncia ante la Guardia Nacional (088).

Señales de que puede estar bajo ataque

- Archivos que no abren o con extensiones extrañas
- Una nota de rescate en pantallas o carpetas
- Cuentas bloqueadas o contraseñas que "ya no sirven"
- Inicios de sesión desde países o a horas inusuales
- Cuentas de administrador nuevas que nadie creó
- Antivirus desactivado sin explicación
- Reglas de correo que reenvían mensajes a fuera
- Lentitud extrema o equipos que se reinician solos

Lo que NO debe hacer

- Pagar el rescate sin asesoría: no garantiza recuperar nada
- Apagar o reiniciar servidores afectados
- Conectar discos de respaldo a la red comprometida
- Coordinar la respuesta por el correo que puede estar comprometido
- Restaurar antes de cerrar la puerta de entrada
- Negociar o contestar al atacante por su cuenta

Si usa Active Directory y Microsoft 365, revise de inmediato

- Miembros de los grupos Domain Admins, Enterprise Admins y Administradores
- Cuentas creadas o modificadas en las últimas 72 horas
- Políticas de grupo (GPO) cambiadas recientemente
- Tareas programadas y servicios nuevos en los controladores de dominio
- Inicios de sesión de riesgo en Entra ID
- Reglas de reenvío y accesos delegados en buzones
- Aplicaciones con consentimiento OAuth recientes
- Dispositivos registrados que nadie reconoce

Hoja de registro del incidente

Hora	Quién	Qué se observó o qué se hizo

Teléfonos y contactos a la mano

Contacto	Nombre	Teléfono / correo
Responsable del incidente		
Proveedor de TI / internet		
Aseguradora (póliza cyber)		
Asesor legal		
Guardia Nacional (denuncia)		088
Respuesta a incidentes	IDProtecThor	WhatsApp +52 55 6211 0970

¿Le pasó a usted? Escríbanos por WhatsApp: le ayudamos a contener el ataque y proteger sus identidades.

idprotecthor.com