IDPROTECTHOR

Lista de verificación gratuita · Edición octubre 2026

15 controles de identidad que toda empresa debe revisar

Dos de cada tres incidentes empiezan por una cuenta comprometida. Marque cada control que ya tiene; los que queden vacíos son su lista de pendientes.

67%
de los incidentes investigados tuvo origen en ataques a la identidad

59%
de los casos ocurrió en organizaciones sin MFA donde hacía falta

340+
empresas con Microsoft 365 afectadas por phishing de "código de dispositivo" que evade el MFA

Fuentes: Sophos, Active Adversary Report 2026; Cloud Security Alliance, nota de investigación del 25 de marzo de 2026.

Cuentas y contraseñas

- [ ] **Inventario de administradores.** Sabe exactamente quién es administrador y por qué. Nadie usa su cuenta de administrador para el correo diario.
- [ ] **Cuentas de exempleados deshabilitadas.** Cada baja de personal desactiva sus cuentas el mismo día.
- [ ] **Contraseñas largas, sin rotación forzada absurda.** Mínimo 14 caracteres y bloqueo de contraseñas ya filtradas.
- [ ] **Contraseña de administrador local única por equipo.** Con Windows LAPS, para que una sola contraseña robada no abra todos los equipos.

Acceso y autenticación

- [ ] **MFA para todos, sin excepción.** Empezando por administradores, correo y acceso remoto (VPN).
- [ ] **MFA resistente a phishing para administradores.** Llaves FIDO2 o passkeys en lugar de SMS.
- [ ] **Flujo de "código de dispositivo" bloqueado.** Con acceso condicional en Entra ID, salvo los equipos que realmente lo necesitan.
- [ ] **Autenticación heredada desactivada.** Protocolos antiguos (POP, IMAP, SMTP básico) que ignoran el MFA.
- [ ] **Consentimiento de aplicaciones controlado.** Los usuarios no pueden autorizar aplicaciones de terceros sin aprobación de TI.

Active Directory

- [ ] **Grupos privilegiados al mínimo.** Domain Admins y Enterprise Admins con el menor número posible de miembros, revisados cada mes.
- [ ] **Cuentas de servicio bajo control.** Sin privilegios de dominio innecesarios, con contraseñas largas o gMSA.
- [ ] **Controladores de dominio actualizados.** El parche de octubre 2026 corrigió una falla crítica de ejecución remota de código en AD DS.
- [ ] **Equipos de administración dedicados.** Los administradores no navegan ni leen correo desde el equipo con el que administran el dominio.

Monitoreo y recuperación

- [ ] **Registros guardados al menos 90 días.** Inicios de sesión de AD y Entra ID, y firewall. Sin registros no hay forma de saber qué pasó.
- [ ] **Respaldo de AD fuera de línea y probado.** Una copia que el atacante no pueda alcanzar, y una prueba de restauración al año.

¿Cómo le fue?

Controles marcados	Qué significa
13 a 15	Buen nivel. Conviene una revisión externa una vez al año.
8 a 12	Base aceptable con huecos que un atacante sabría aprovechar. Priorice MFA y administradores.
0 a 7	Riesgo alto. Recomendamos una evaluación de seguridad de identidades cuanto antes.

Le ayudamos a cerrar los pendientes. La primera conversación no tiene costo: WhatsApp +52 55 6211 0970.

idprotecthor.com

Fuentes: Sophos Active Adversary Report 2026; Cloud Security Alliance (25-mar-2026), OAuth device code phishing en Microsoft 365; BleepingComputer (13-oct-2026), Microsoft October 2026 Patch Tuesday. Esta guía es informativa y no sustituye una evaluación profesional.