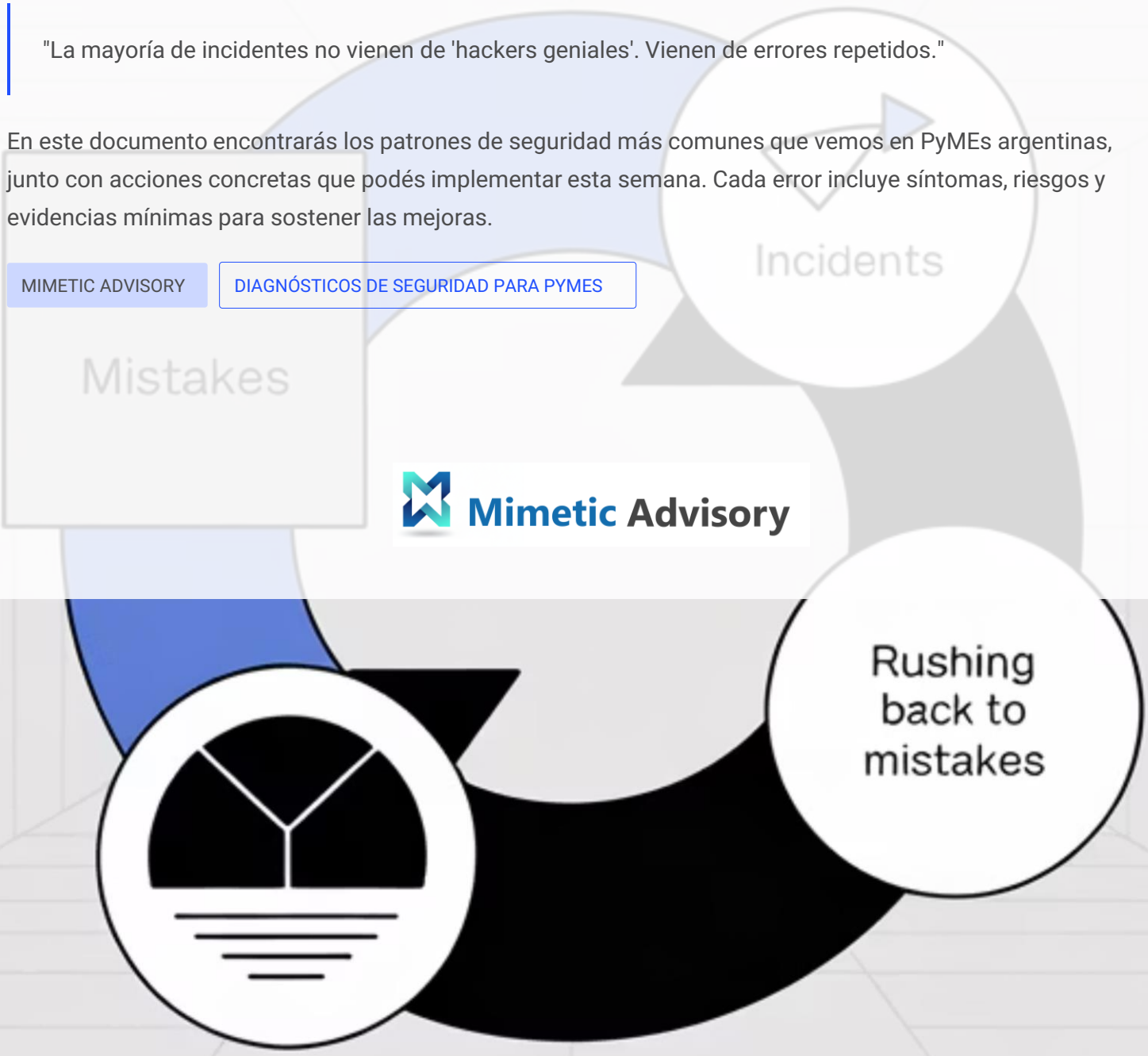
Ciberseguridad: Errores comunes y cómo evitarlos

Patrones típicos en PyMEs y acciones concretas para reducir riesgo

> "La mayoría de incidentes no vienen de 'hackers geniales'. Vienen de errores repetidos."

En este documento encontrarás los patrones de seguridad más comunes que vemos en PyMEs argentinas, junto con acciones concretas que podés implementar esta semana. Cada error incluye síntomas, riesgos y evidencias mínimas para sostener las mejoras.

MIMETIC ADVISORY | DIAGNÓSTICOS DE SEGURIDAD PARA PYMES



Por qué estos errores se repiten en PyMEs

El contexto PyME

La realidad de las empresas en crecimiento hace que ciertos patrones de riesgo se repitan una y otra vez. No es falta de intención, es falta de estructura.

Crecimiento rápido

Los equipos y sistemas crecen más rápido que los procesos

Modo apagar incendios

La urgencia operativa desplaza la prevención

Dependencia de terceros

Proveedores con acceso sin control formal

Sin dueño claro

Nadie tiene asignada la responsabilidad de seguridad

La solución: Controles simples + evidencia mínima que se puedan sostener en el tiempo. No necesitás un equipo de seguridad dedicado, necesitás hábitos repetibles.

Error #1: Contraseñas débiles o reutilizadas

Síntoma

Misma clave en correo, sistemas internos y servicios externos. Claves simples tipo "Empresa2024" o "Admin123".

Riesgo

Una filtración en cualquier servicio externo compromete todos los accesos internos. Acceso no autorizado a información crítica.

Acción concreta esta semana

Implementar gestor de contraseñas corporativo. Política mínima: 12 caracteres, sin reutilización. Rotación obligatoria en cuentas compartidas.

Evidencia mínima

Listado de usuarios con gestor activado. Captura de política de contraseñas aplicada en sistemas principales.

Alto	Bajo
Impacto	Esfuerzo

Error #2: Sin MFA en correo y accesos remotos

El correo electrónico es la puerta de entrada más común a los sistemas de una empresa. Sin un segundo factor de autenticación, una contraseña comprometida es todo lo que necesita un atacante.

01

Síntoma típico

Acceso al correo y sistemas remotos solo con usuario y contraseña

02

Riesgo real

Phishing exitoso = acceso total. Credenciales filtradas en brechas externas permiten ingreso directo

03

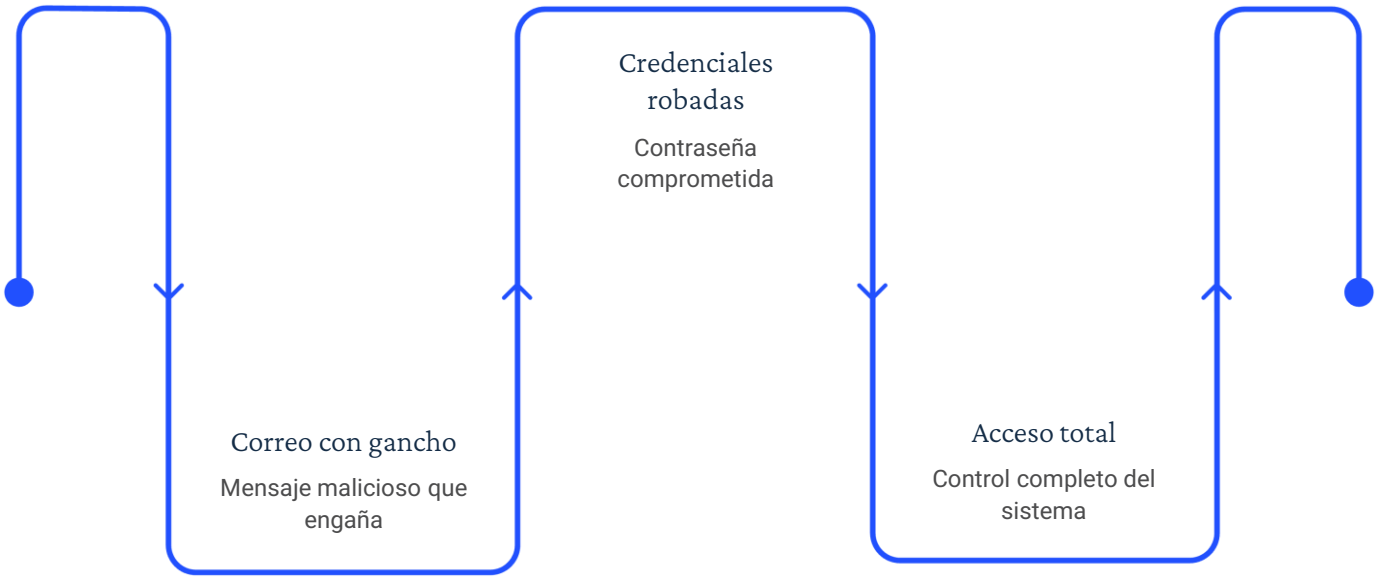
Implementá ahora

Activar MFA en correo corporativo, VPN y accesos administrativos. Priorizar app authenticator sobre SMS

04

Registrá la evidencia

Listado de cuentas críticas con MFA activado + fecha de implementación



El segundo factor bloquea el 99% de ataques automatizados basados en credenciales comprometidas.

Impacto: Alto - Previene la mayoría de accesos no autorizados

Esfuerzo: Bajo - Configuración en 1-2 días

Error #3: "Todos son admin" o privilegios excesivos

1 2 3

Síntoma

Usuarios operativos con permisos de administrador "por las dudas". Acceso a sistemas no relacionados con su función.

Riesgo

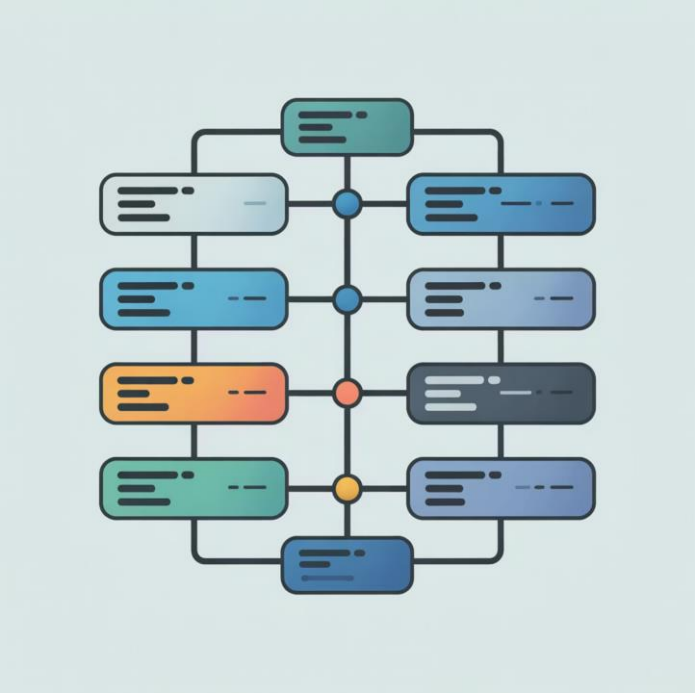
Cualquier cuenta comprometida tiene alcance total. Errores operativos pueden afectar toda la infraestructura.

Acción

Separar cuentas admin de uso diario. Aplicar mínimo privilegio por rol. Revisar permisos trimestralmente.

Evidencia mínima

- Listado actualizado de administradores (máximo 2-3 personas)
- Matriz de permisos por rol
- Fecha de última revisión trimestral
- Registro de aprobación de excepciones



> "El principio de mínimo privilegio no es desconfianza, es contención de daño. Una cuenta con permisos limitados limita el radio de un incidente."

Alto

Impacto

Medio

Esfuerzo

Error #4: Backups existen, pero nadie prueba restore

Tener copias de seguridad da tranquilidad. Pero ¿funcionan cuando realmente las necesitás? El 40% de las empresas que sufren pérdida crítica de datos descubren en ese momento que sus backups no sirven.

Síntoma	Riesgo	Acción concreta	Evidencia mínima
Backups automáticos corriendo hace meses o años sin verificación. "Debe estar funcionando".	Backup corrupto, incompleto o inaccesible descubierto durante un incidente real. Pérdida permanente de datos.	Prueba de restore mensual documentada. Copia offline cuando sea posible. Verificar que incluye todos los sistemas críticos.	Acta o captura de pantalla de restore exitoso con fecha. Checklist de sistemas incluidos.

Regla 3-2-1 explicada en una línea

3 copias de tus datos → **2** medios diferentes → **1** copia fuera del sitio (offline o cloud separado)

Impacto: **Alto**

Un restore que falla en producción puede significar el cierre de la operación.

Esfuerzo: **Bajo**

2-3 horas mensuales para verificación completa y documentación.

Error #5: Parches "cuando hay tiempo" + sistemas EOL

El problema

Los parches de seguridad quedan postergados indefinidamente por miedo a "romper algo" o falta de tiempo. Sistemas fuera de soporte (EOL) siguen en producción "porque funcionan".

Síntoma

Servidores o aplicaciones sin actualizar hace meses. Sistemas operativos o software EOL en infraestructura crítica.

Riesgo

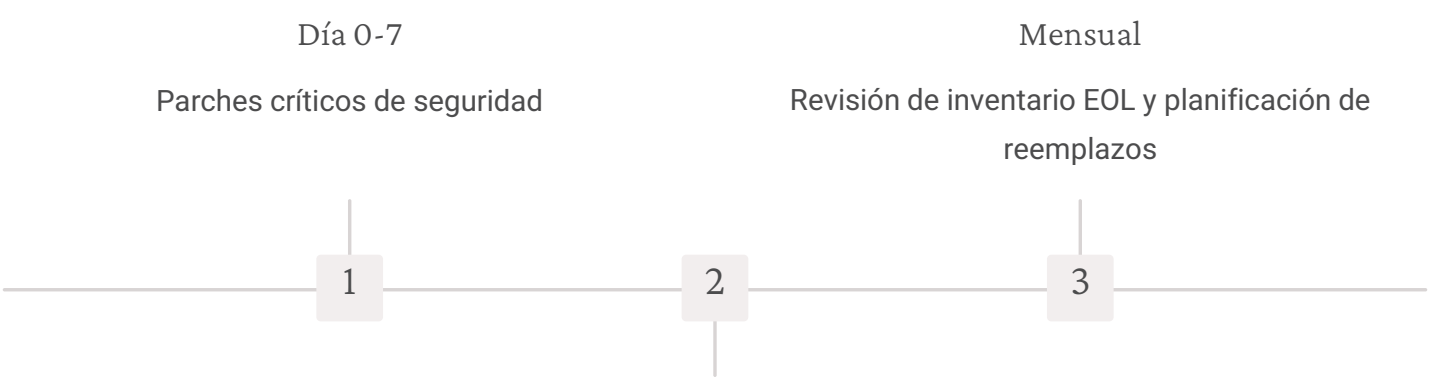
Vulnerabilidades conocidas públicamente sin corrección. Exploits disponibles que funcionan "out of the box".

Acción concreta esta semana

Crear calendario mensual de parches. Priorizar críticos (7 días). Generar inventario de sistemas EOL con fecha de reemplazo.

Evidencia mínima

- Reporte mensual de parches aplicados
- Planilla de sistemas EOL con plan de acción
- Registro de parches críticos con fecha



- **Impacto: Alto** - Vulnerabilidades públicas son la vía de entrada más común
- **Esfuerzo: Medio** - Requiere planificación pero se vuelve rutina

Error #6: Exposición innecesaria a internet

Servicios administrativos, paneles de control y protocolos internos publicados directamente a internet "para que sea más fácil acceder". Cada puerto abierto es una puerta que alguien puede intentar forzar.

1

Síntoma típico

RDP, paneles admin, FTP o bases de datos accesibles desde cualquier IP pública

2

Riesgo real

Escaneos automáticos encuentran el servicio en minutos. Intentos de fuerza bruta 24/7. Explotación de vulnerabilidades conocidas

3

Acción inmediata

Inventario de servicios expuestos. Cerrar lo no necesario. Implementar VPN o restricción por IP en lo crítico

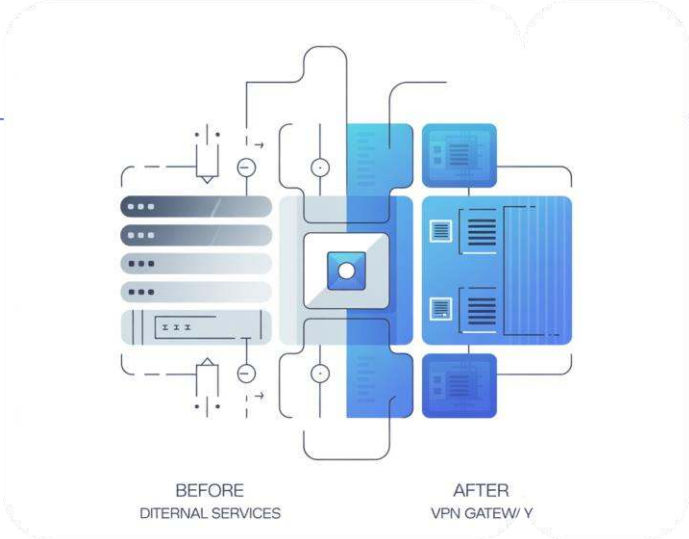
4

Documentar

Lista de servicios expuestos "aprobados" con justificación. Reglas de firewall revisadas y documentadas

Antes

Servicios internos expuestos directamente a Internet



Después

Gateway VPN protege los servicios internos

La mayoría de los servicios administrativos no deberían ser accesibles directamente desde internet. Una VPN o restricción por IP reduce drásticamente la superficie de ataque.

85%

Reducción de intentos de acceso

Al cerrar puertos innecesarios

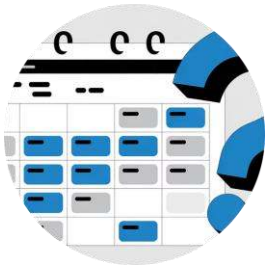
Impacto: Alto - Reduce dramáticamente intentos de intrusión

Esfuerzo: Medio - Requiere revisión de infraestructura y configuración

Error #7: Proveedores con acceso "para siempre"

Síntoma

Proveedores de soporte, desarrollo o servicios con accesos creados hace años. "Por las dudas que necesiten entrar".



Riesgo

Cuentas olvidadas sin rotación. Ex-empleados del proveedor con acceso activo. Sin MFA ni auditoría de actividad.

Acción concreta

Crear inventario de terceros con acceso. Implementar MFA obligatorio. Establecer vencimiento (30-90 días). Acceso solo a lo mínimo necesario.

Evidencia mínima

1. Planilla de terceros actualizada
2. Fecha de última revisión
3. Fecha de vencimiento por acceso
4. Alcance específico de permisos
5. MFA activado en todas las cuentas

Pregunta clave

¿Sabés quiénes tienen acceso a tus sistemas en este momento? ¿Cuándo fue la última vez que lo revisaste?

La mayoría de las empresas no tiene respuesta para esto.

Alto

Impacto en contención de incidentes

Bajo

Esfuerzo inicial de implementación

Mimetic Advisory

Quick-wins en 7 días + Roadmap 30/60/90

Acciones inmediatas (esta semana)

- **MFA en correo corporativo** - Impacto: Alto / Esfuerzo: Bajo
- **Separar cuentas admin de uso diario** - Impacto: Alto / Esfuerzo: Bajo
- **Revisar y cerrar exposición innecesaria** - Impacto: Alto / Esfuerzo: Medio
- **Prueba de restore de backup** - Impacto: Alto / Esfuerzo: Bajo
- **Inventario de accesos de terceros** - Impacto: Medio / Esfuerzo: Bajo
- **Aplicar parches críticos pendientes** - Impacto: Alto / Esfuerzo: Medio
- **Política de contraseñas implementada** - Impacto: Medio / Esfuerzo: Bajo
- **Crear checklist mensual de revisión** - Impacto: Medio / Esfuerzo: Bajo

30 días: Base

- MFA en sistemas críticos
- Backups + restore verificado
- Exposición cerrada
- Inventario de activos

60 días: Disciplina

- Calendario de parches
- Revisión de privilegios
- Control de terceros
- Protección de endpoints

90 días: Madurez

- Monitoreo y logs
- Simulacros phishing
- Métricas de seguridad
- Playbooks de respuesta

¿Querés identificar estos patrones en tu empresa?

Trabajamos con PyMEs para convertir estos errores comunes en un plan ejecutable: diagnóstico inicial + quick-wins priorizados + roadmap 30/60/90 días adaptado a tu realidad operativa.

Mimetic Advisory

Diagnósticos de ciberseguridad para PyMEs y empresas medianas

Contacto: Formulario web / LinkedIn