Gobierno de TI: Errores comunes y cómo evitarlos

Patrones típicos en PyMEs + acciones concretas para reducir riesgo

"La mayoría de incidentes no vienen de hacks sofisticados. Vienen de hábitos repetidos."

MIMETIC ADVISORY | DIAGNÓSTICOS DE SEGURIDAD PARA PYMES

Mimetic Advisory

¿Por qué pasa en PyMEs?

Crecimiento rápido

Las prioridades cambian cada semana y la infraestructura crece sin planificación

Recursos limitados

No hay equipo dedicado a seguridad ni tiempo para procesos formales

Apagar incendios

Se resuelve lo urgente, no lo importante. La prevención queda para después

Dependencia de terceros

Proveedores externos con accesos permanentes y sin control

La solución: Controles simples, repetibles y con evidencia mínima. No hace falta ser grande para estar ordenado.

ERROR #1

Todo el mundo es admin

Impacto

ALTO

Esfuerzo

MEDIO

01

Síntoma

Cualquier usuario puede instalar software, cambiar configuraciones o acceder a carpetas sensibles

02

Riesgo

Ransomware se propaga sin límite, datos críticos expuestos, cambios no autorizados que rompen sistemas

03

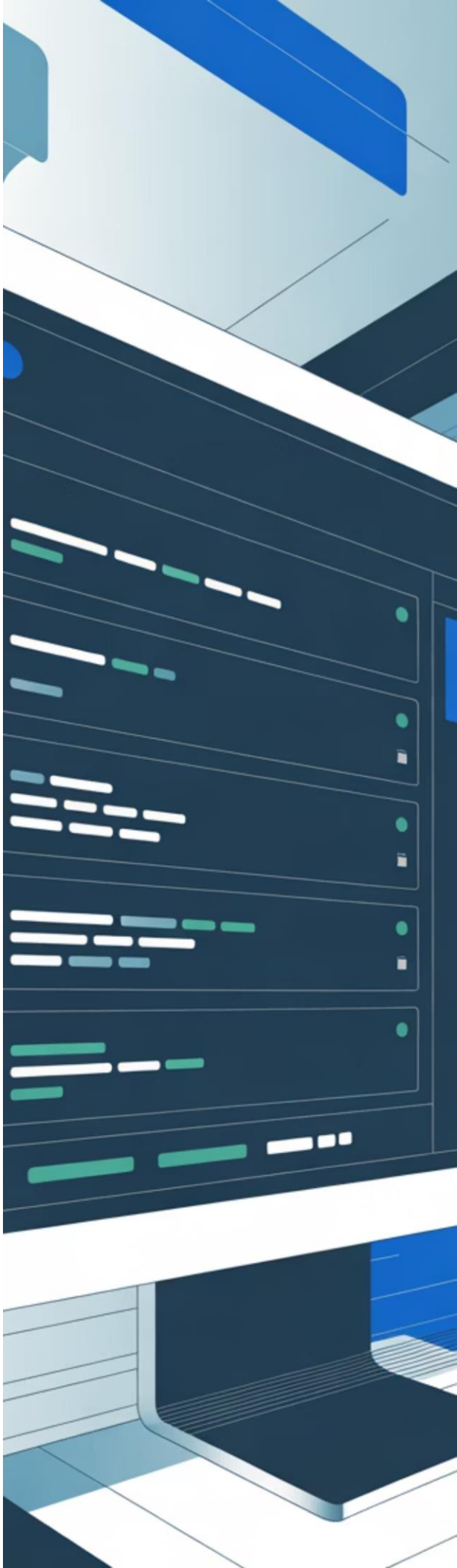
Acción concreta

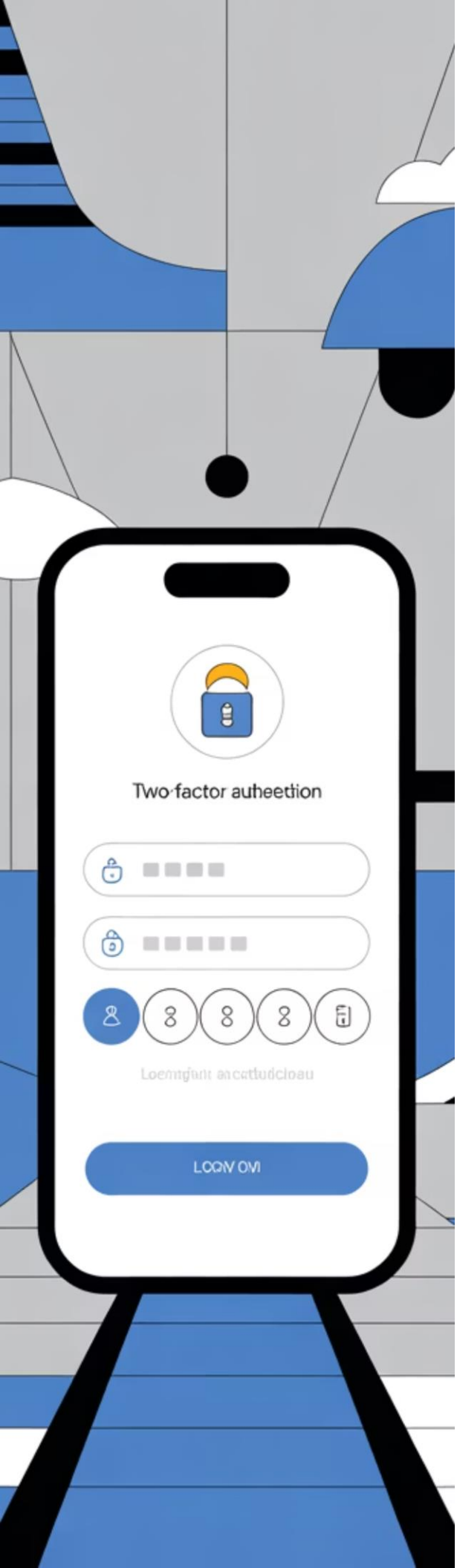
Crear cuentas de usuario estándar para trabajo diario. Cuentas admin separadas solo para tareas específicas

04

Evidencia mínima

Listado de usuarios con permisos actuales + captura de política de accesos implementada





ERROR #2

MFA ausente en correo y accesos remotos

Síntoma

El correo corporativo y la VPN solo piden usuario y contraseña. Sin segundo factor de autenticación.

Riesgo

Una contraseña filtrada = acceso total. Email comprometido permite atacar clientes, pedir transferencias, robar información sensible.

Acción concreta

Activar MFA en todas las cuentas de correo y portales de acceso remoto. Registrar dispositivos autorizados. Separar cuentas admin con MFA obligatorio.

Evidencia mínima

Captura de configuración MFA activa + listado de cuentas críticas con segundo factor habilitado + política documentada.

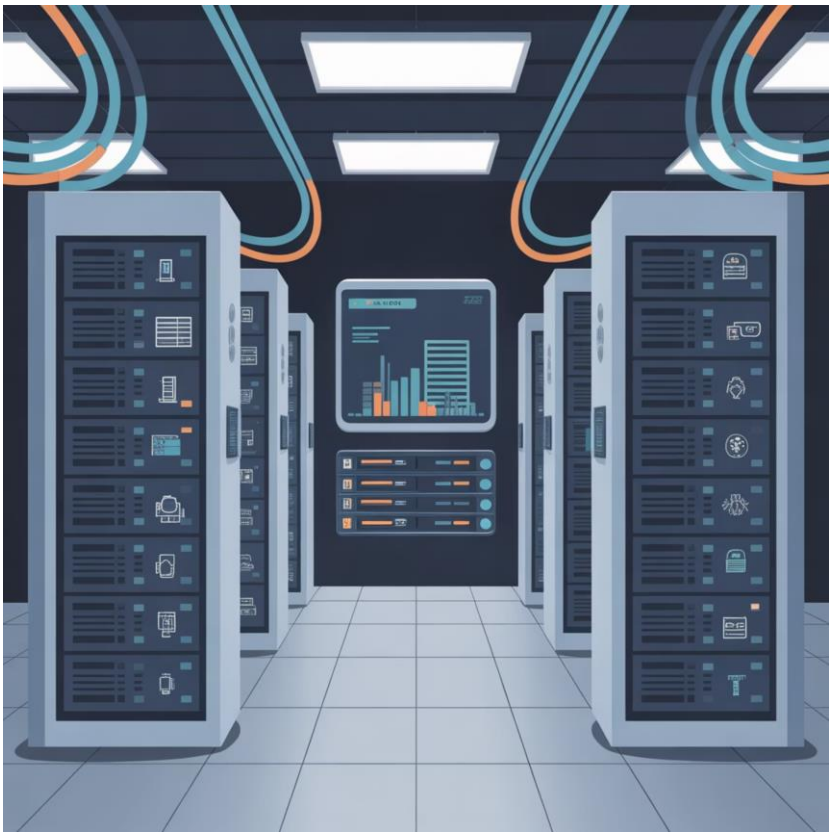
Impacto: ALTO

Esfuerzo: BAJO

Mimetic Advisory

ERROR #3

Backups que existen pero nunca se prueban



Impacto

ALTO

Esfuerzo

MEDIO

Síntoma

Hay backup configurado, pero nadie verificó en meses si realmente funciona o si se puede restaurar

Riesgo

Cuando llegue el incidente (ransomware, falla de disco), descubrís que el backup estaba corrupto o incompleto

Acción concreta

Prueba de restore mensual de al menos un sistema crítico. Aplicar regla 3-2-1: 3 copias, 2 medios diferentes, 1 offsite

Evidencia mínima

Acta corta de prueba con fecha + captura de restore exitoso + registro de ubicación de las 3 copias

ERROR #4

Parches "cuando hay tiempo" y activos sin inventario

Síntoma

Nadie sabe exactamente qué equipos hay en la red, qué versiones de software corren, ni cuándo fue el último parche aplicado. Se actualiza solo cuando algo falla.

Riesgo

Vulnerabilidades conocidas y explotables durante meses. Sistemas con soporte terminado (EOL) expuestos. Incidentes evitables se convierten en crisis.

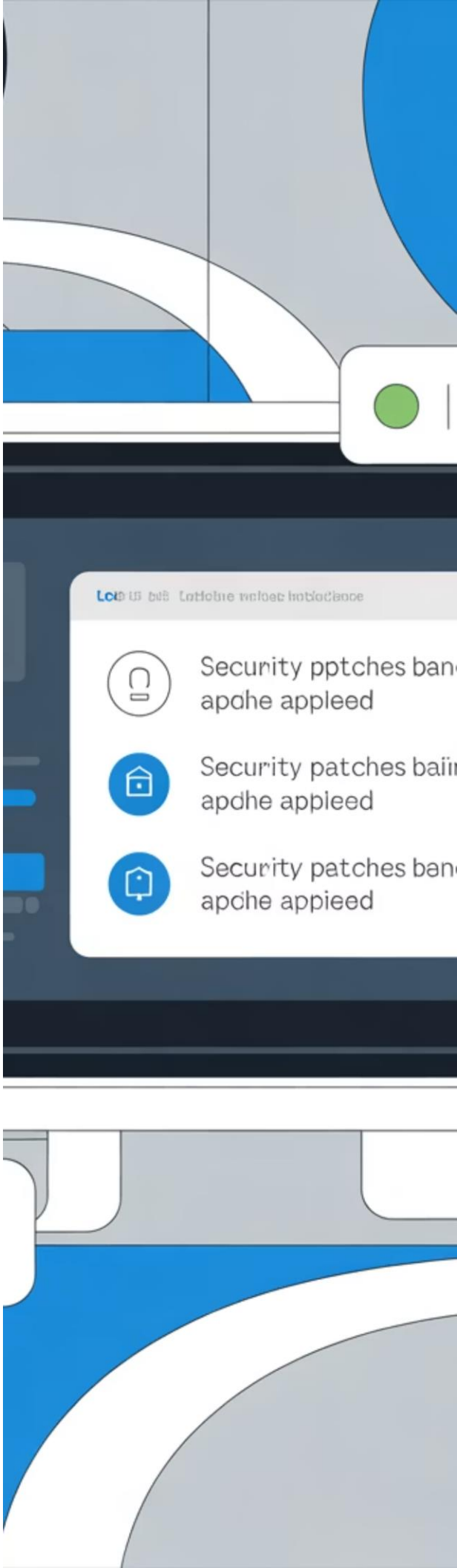
Acción concreta

Crear inventario mínimo: dispositivo, sistema operativo, versión, responsable. Calendario mensual de parches críticos. Identificar y priorizar sistemas EOL para reemplazo.

Evidencia mínima

Planilla con inventario actualizado + reporte de parches aplicados último mes + lista de sistemas EOL con plan de acción.

Impacto: ALTO **Esfuerzo:** MEDIO



ERROR #5

Cambios sin registro

Y después nadie sabe qué pasó

Síntoma

Se tocan servidores, se cambian configuraciones, se agregan reglas de firewall... sin avisar ni documentar

Riesgo

Sistema cae y nadie sabe por qué. Conflictos entre cambios simultáneos. Imposible hacer rollback

1

Acción concreta

Todo cambio requiere ticket o correo de aprobación. Bitácora simple: qué, quién, cuándo, por qué. Definir ventana de mantenimiento semanal para cambios no urgentes.

2

Evidencia mínima

5 tickets o registros de cambios del último mes con información completa y aprobación visible.

Impacto: MEDIO | Esfuerzo: BAJO

ERROR #6

Proveedores con acceso "para siempre"

Impacto

ALTO

Esfuerzo

BAJO

El proveedor que instaló el ERP hace 2 años todavía tiene VPN activa. El soporte remoto nunca se deshabilitó. Terceros entran cuando quieren, sin registro ni control.

Riesgo real

Fugas de información, accesos no autorizados, compromiso de credenciales de terceros que afecta tu empresa

Acción concreta

Lista actualizada de terceros con acceso. MFA obligatorio. Caducidad automática (30-90 días). Principio de mínimo privilegio: solo lo necesario.

Evidencia mínima

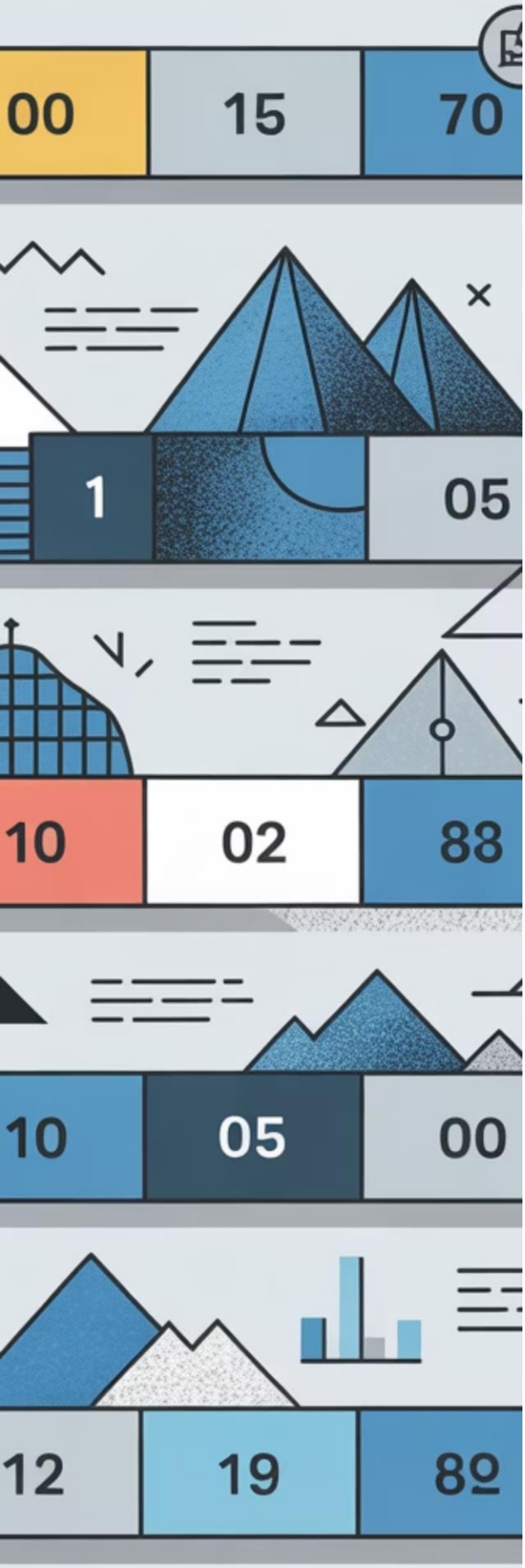
Listado de proveedores con fecha de última revisión + accesos temporales configurados + log de ingresos de terceros

Quick-wins en 7 días

Acciones rápidas de alto impacto que podés implementar esta semana

Acción	Impacto	Esfuerzo
Activar MFA en correo corporativo	Alto	Bajo
Separar cuentas admin de usuario diario	Alto	Medio
Inventario mínimo de activos críticos	Medio	Bajo
Revisar y cerrar accesos de terceros inactivos	Alto	Bajo
Prueba de restore de un backup crítico	Alto	Medio
Revisar puertos expuestos a Internet	Medio	Bajo
Implementar política básica de contraseñas	Medio	Bajo
Crear canal de reporte de incidentes	Medio	Bajo

Priorizá según tu contexto. Empezar por MFA y accesos siempre es una buena jugada.



Roadmap 30/60/90 días

1

30 días: Ordenar la base

- Inventario de activos y usuarios
- MFA en correo y accesos remotos
- Separación de cuentas admin
- Prueba de backups
- Revisión de accesos de terceros

2

60 días: Establecer procesos

- Gestión de cambios con registro
- Calendario de parches críticos
- Control de proveedores con caducidad
- Escaneo básico de vulnerabilidades
- Definir roles y responsables

3

90 días: Madurar y sostener

- Centralización de logs críticos
- Métricas básicas de cumplimiento
- Capacitación recurrente del equipo
- Políticas mínimas documentadas
- Revisión trimestral de controles

¿Querés identificar estos patrones en tu empresa y convertirlos en un plan 30/60/90?

Diagnóstico inicial + quick wins personalizados para tu contexto.

MIMETIC ADVISORY

Mimetic Advisory