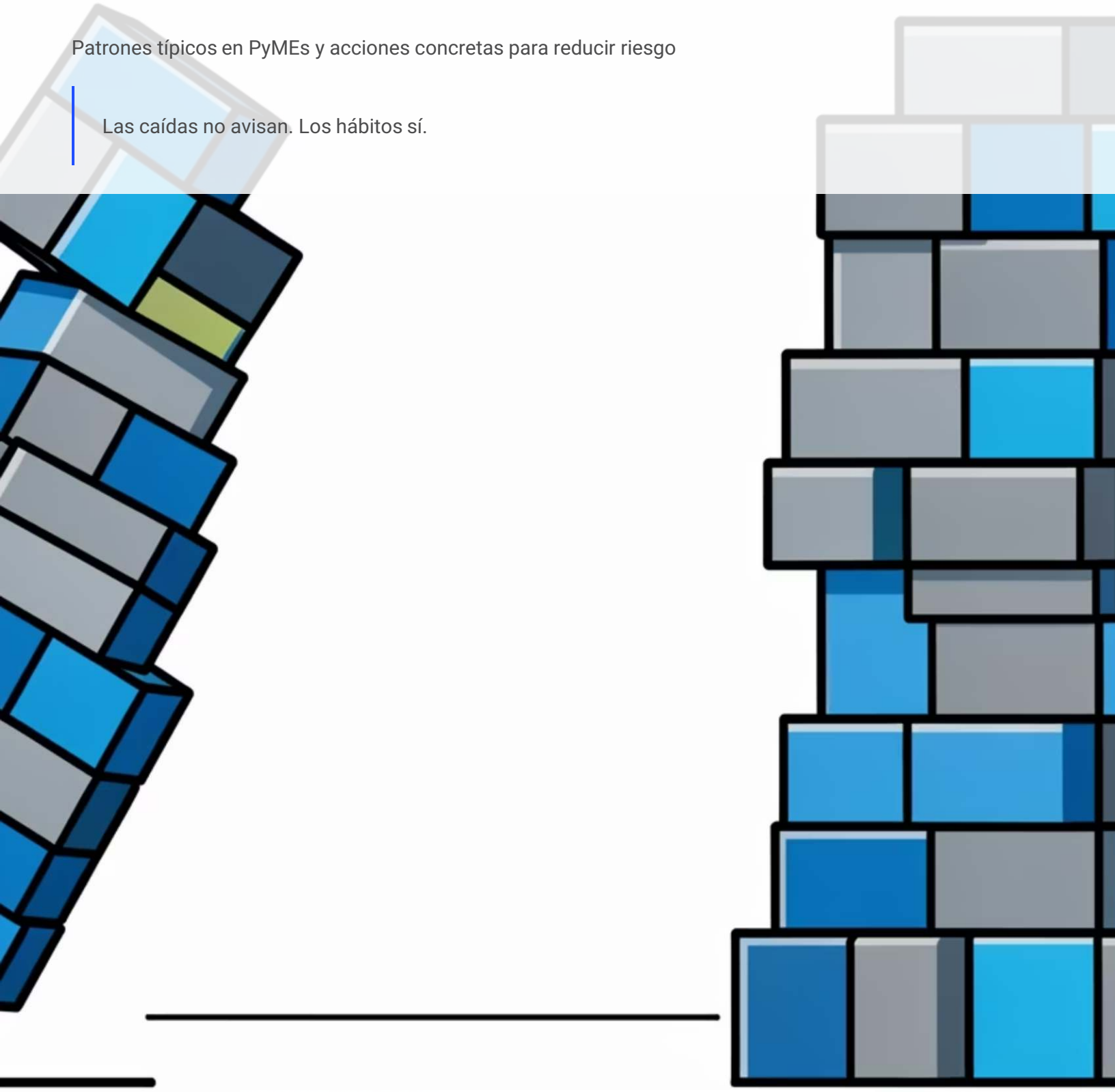
Infraestructura: Errores comunes y cómo evitarlos

Patrones típicos en PyMEs y acciones concretas para reducir riesgo

> Las caídas no avisan. Los hábitos sí.



Mimetic Advisory

Por qué pasa en las PyMEs

La infraestructura crítica termina llena de parches y deuda técnica por razones comprensibles. La urgencia del día a día, el crecimiento acelerado sin planificación, la dependencia de terceros sin controles, y la falta de registros simples crean un terreno fértil para problemas evitables.
El resultado: sistemas frágiles donde nadie tiene la foto completa. Cuando algo falla, la respuesta es reactiva y costosa. La buena noticia es que no hace falta un proyecto masivo para mejorar.

> La salida: controles simples + evidencia mínima.

Patrones recurrentes

- Urgencias que tapan la planificación
- Crecimiento sin actualizar bases
- Terceros con acceso sin control
- Falta de registro y documentación

Error #1: No hay inventario

Nadie sabe qué existe ni quién es responsable

Síntoma

Consultas recurrentes tipo "¿ese servidor qué hace?" o "¿quién maneja ese sistema?". Cuando algo falla, se pierde tiempo buscando información básica.

Riesgo

Sistemas huérfanos sin mantenimiento. Caídas por cambios no coordinados. Imposibilidad de planificar renovaciones o mejoras. Dependencia total de personas específicas.

Acción concreta esta semana

Crear una planilla con: nombre del sistema/equipo, función, dueño/responsable, criticidad (Alta/Media/Baja), ubicación. Arrancar con los 10 servicios más críticos.

Evidencia mínima

Planilla compartida actualizada + diagrama simple de red con nodos principales. Revisión trimestral en calendario.

Impacto: Alto

Esfuerzo: Bajo

Error #2: Backups en el mismo lugar

Y encima, sin probar restore nunca

Síntoma

Copias de seguridad guardadas en el mismo rack o edificio que el sistema original. Nunca se probó restaurar datos. Confianza ciega en que "funciona".

Riesgo

Incendio, robo o falla eléctrica destroye original y backups al mismo tiempo. Descubrir que los backups están corruptos o incompletos cuando ya es tarde.

1

Acción concreta esta semana

Implementar regla 3-2-1: 3 copias, 2 medios diferentes, 1 fuera del sitio. Programar restore mensual de archivos críticos para verificar integridad.

2

Evidencia mínima

Acta de restore mensual con fecha, sistema probado, resultado OK/Falló, tiempo de recuperación. Registro de ubicación de cada copia.

Impacto: Alto

Esfuerzo: Medio

Error #3: Wi-Fi invitados mezclado con red interna

Sin segmentación entre redes

Síntoma

Visitantes, proveedores o clientes conectados a la misma red que servidores, impresoras y equipos internos. Todo en un mismo segmento sin control.

Riesgo

Equipo comprometido de un invitado puede acceder a sistemas críticos. Fuga de información sensible. Imposibilidad de controlar o auditar accesos externos.

01

Acción concreta esta semana

Separar SSID y red física para invitados. Configurar VLAN o subnet diferente. Aplicar segmentación mínima: invitados solo a Internet.

02

Evidencia mínima

Diagrama de red actualizado mostrando segmentos. Captura de configuración de VLANs o subnets. Política de acceso documentada.

Impacto: Alto

Esfuerzo: Medio

Error #4: Reglas del perímetro "históricas"

Nadie las revisa, nadie sabe por qué existen

Síntoma	Riesgo	Acción concreta esta semana	Evidencia mínima
Firewall con decenas de reglas de hace años. Puertos abiertos "por las dudas". Excepciones que nadie recuerda para qué eran. Accesos remotos sin expiración.	Superficie de ataque innecesariamente grande. Accesos que ya no se usan pero siguen activos. Imposibilidad de responder "¿quién puede entrar y por dónde?"	Revisión mensual de reglas del firewall. Cerrar todo lo que no sea estrictamente necesario. Documentar excepciones con justificación, dueño y fecha de caducidad. Controlar accesos remotos con doble factor.	Snapshot mensual de reglas activas. Lista de excepciones con aprobación firmada. Reporte de accesos remotos con vencimientos claros.

Impacto: Alto

Esfuerzo: Bajo

Error #5: Parches "cuando se puede"

Equipos obsoletos sin plan de renovación

Síntoma

Actualizaciones atrasadas meses o años. Equipos fuera de soporte (EOL) aún en producción. Parches críticos sin aplicar por "miedo a romper algo".

Riesgo

Vulnerabilidades conocidas sin parchear. Fallas en equipos sin repuestos ni soporte. Incompatibilidad creciente con sistemas nuevos.

- ### Acción concreta esta semana

  Crear calendario mensual de parches por sistema. Levantar lista de equipos EOL con fecha de fin de soporte. Aplicar parches críticos de seguridad de inmediato.

- ### Evidencia mínima

  Reporte mensual de parchado con fecha, sistema, versión anterior/nueva. Planilla EOL con prioridad de reemplazo. Calendario compartido de mantenimientos.

Impacto: Alto

Esfuerzo: Medio

Error #6: Monitoreo inexistente

Te enterás por el usuario que algo está caído

Síntoma

Primera notificación de un problema viene de un usuario enojado. No hay alertas automáticas de caídas, espacio en disco, backups fallidos o enlaces saturados.

Riesgo

Problemas pequeños se vuelven crisis porque nadie detectó el síntoma temprano. Tiempo de inactividad extendido. Pérdida de confianza del negocio en TI.

Sin monitoreo básico, la infraestructura es una caja negra. No se puede ser proactivo ni medir mejoras. Cada incidente sorprende.

→ Acción concreta esta semana

Implementar alertas mínimas: caídas de servicios críticos, espacio en disco bajo, backup fallido, saturación de enlace. Empezar con herramientas gratuitas o incluidas en equipos existentes.

→ Evidencia mínima

Lista documentada de alertas configuradas con destino (mail/SMS). Reporte mensual con resumen: alertas OK vs Issues detectados. Log de respuestas a incidentes.

Impacto: Alto

Esfuerzo: Bajo

Error #7: Proveedores con acceso permanente

Sin caducidad ni control de privilegios

Es común dar accesos a terceros "por un proyecto" y olvidarse de revocarlos. Pasan meses o años con cuentas activas de gente que ya no trabaja con la empresa o cuyo alcance cambió radicalmente.

Esto multiplica vectores de ataque y complica auditorías. Nadie tiene la lista actualizada de quién puede entrar, desde dónde, y con qué nivel de privilegio.

Síntoma

Proveedores con VPN o acceso remoto sin fecha de vencimiento. Credenciales compartidas sin auditoría.

Riesgo

Accesos no autorizados. Imposibilidad de rastrear actividad. Fuga de información por canales no controlados.

1

Acción concreta esta semana

Crear lista de terceros con acceso: nombre, empresa, tipo de acceso, fecha inicio, fecha caducidad. Aplicar principio de mínimo privilegio. Revisar y renovar cada 6 meses.

Impacto: Medio

2

Evidencia mínima

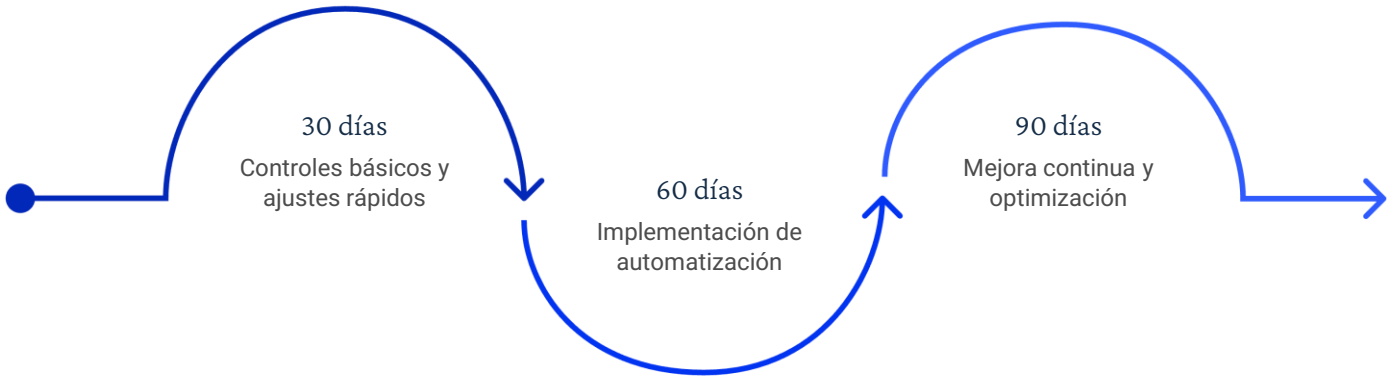
Planilla con vencimientos visibles. Calendario de revisión semestral. Log de accesos de terceros auditado mensualmente.

Esfuerzo: Bajo

Quick-wins en 7 días

Acciones de alto impacto que podés arrancar ahora mismo. No requieren presupuesto grande ni meses de proyecto, solo decisión y seguimiento.

Acción	Impacto	Esfuerzo
Inventario mínimo de sistemas críticos	Alto	Bajo
Separar red invitados de interna	Alto	Medio
Restore de prueba mensual	Alto	Medio
Revisión mensual reglas firewall	Alto	Bajo
Alertas mínimas configuradas	Alto	Bajo
Lista de equipos EOL con plan	Alto	Bajo
Control de accesos de terceros	Medio	Bajo
Calendario de parches mensuales	Alto	Medio



Este roadmap 30/60/90 te permite arrancar con lo urgente y construir bases sólidas en el primer trimestre. No hace falta transformar todo de golpe.

> ¿Querés convertir estos patrones en un plan ejecutable?
>
> Diagnóstico personalizado + quick wins priorizados + roadmap adaptado a tu contexto. Contactanos por formulario web o LinkedIn para arrancar.