Infraestructura: Errores comunes y cómo evitarlos

Las caídas no avisan. La infraestructura ordenada sí.

Patrones típicos en PyMEs + acciones concretas para reducir riesgo

Por qué pasa en PyMEs

Crecimiento sin planificación

Se suma infraestructura según la urgencia, sin diseño ni documentación

Presión operativa

El día a día absorbe todo el tiempo, y lo urgente desplaza lo importante

Dependencia de terceros

Proveedores que configuran sin transferir conocimiento ni registros

Falta de registro histórico

Nadie documenta cambios, configuraciones quedan en cabezas que rotan

Estos patrones crean infraestructura frágil, donde cada incidente revela que nadie sabe realmente qué hay, cómo funciona, ni quién es responsable de qué.

Error #1: No hay inventario

IMPACTO: ALTO | ESFUERZO: BAJO

Síntoma

Nadie puede responder "qué servidores tenemos" o "qué aplicaciones corren dónde". Cada caída es una sorpresa.

Riesgo

Imposible evaluar impacto, planificar cambios o recuperarse ordenadamente. Cada decisión es a ciegas.

Acción esta semana

- Inventario mínimo: servidor/dispositivo + función + ubicación + dueño
- Diagrama simple con conexiones críticas
- Asignar un responsable por cada servicio

Evidencia mínima

Planilla compartida + diagrama publicado + nombres de responsables

Error #2: Backups en el mismo lugar

IMPACTO: ALTO | ESFUERZO: MEDIO

Síntoma

Los backups están en el mismo servidor, rack o edificio. Nunca se probó un restore completo.

Riesgo

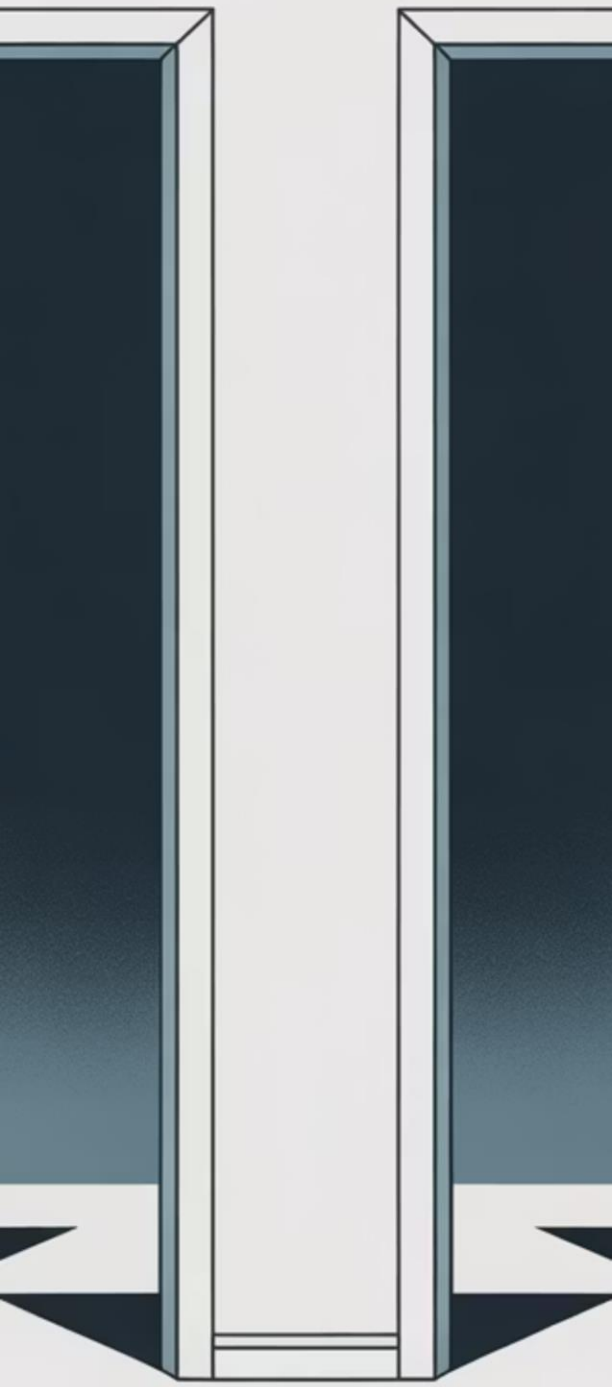
Un incendio, robo o falla física destruye producción Y backup al mismo tiempo. El restore falla cuando más se necesita.

Acción esta semana

- Implementar regla 3-2-1: 3 copias, 2 medios diferentes, 1 fuera de sitio
- Agendar prueba de restore mensual de un servicio crítico
- Documentar ubicación de cada copia

Evidencia mínima

Acta de restore exitoso + planilla con ubicación de copias + captura de logs



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

IMPACTO: ALTO

ESFUERZO: BAJO

Síntoma

Visitantes, proveedores y empleados comparten la misma red. Cualquiera puede "ver" dispositivos internos.

Riesgo

Un dispositivo comprometido de invitado accede a servidores, impresoras, NAS. Movimiento lateral sin fricción.

Acción esta semana

- Crear SSID separado para invitados con aislamiento de red
- Segmentar mínimo: invitados / usuarios / servidores
- Configurar VLAN básica si el equipamiento lo soporta

Evidencia mínima

Diagrama de red + configuración resumida + prueba de que invitado no ve red interna

Error #4: Reglas del perímetro "históricas"

IMPACTO: MEDIO | ESFUERZO: MEDIO

Síntoma

Reglas de firewall acumuladas por años sin revisión. Nadie sabe para qué sirven ni quién las pidió.

Riesgo

Puertos abiertos innecesarios, accesos remotos sin MFA, excepciones temporales convertidas en permanentes.

Acción esta semana

- Revisión mensual de reglas: quién/qué/por qué
- Cerrar puertos no utilizados en últimos 90 días
- Todo acceso remoto con MFA obligatorio
- Crear lista de excepciones con vencimiento

Evidencia mínima

Snapshot de reglas antes/después + planilla de excepciones aprobadas con fecha y responsable + política de revisión mensual

Error #5: Parches "cuando se puede"

IMPACTO: ALTO | ESFUERZO: MEDIO

Síntoma

Los parches se aplican "si hay tiempo", sin calendario ni criterio. Equipos fuera de soporte (EOL) siguen en producción.

Riesgo

Vulnerabilidades conocidas sin corregir durante meses. Equipos EOL sin actualizaciones de seguridad son puerta de entrada garantizada.

Acción esta semana

- Crear calendario mensual de parches críticos
- Inventariar equipos EOL + plan de reemplazo 6 meses
- Parchar servidores críticos este mes sin excusas
- Definir ventana de mantenimiento mensual

Evidencia mínima

Reporte de parches aplicados + lista EOL con fechas + calendario publicado

Error #6: Monitoreo inexistente

IMPACTO: ALTO | ESFUERZO: BAJO

Síntoma

Te enterás de las caídas cuando llama un usuario o cliente. No hay alertas proactivas.

Riesgo

Problemas críticos escalan sin control. Backups fallan en silencio. Discos se llenan y tumban servicios.

Acción esta semana

- Configurar alertas mínimas: caída de servicio, espacio en disco crítico, backup fallido, enlace WAN caído
- Definir responsable que recibe alertas 24/7
- Dashboard simple: verde/rojo para servicios críticos

Evidencia mínima

Lista de alertas configuradas + responsable asignado + reporte mensual "OK/Issues" compartido con gerencia

Error #7: Proveedores con acceso permanente

IMPACTO: MEDIO | ESFUERZO: BAJO

Síntoma

Proveedores configuraron infraestructura hace años y mantienen acceso VPN/admin sin caducidad ni control.

Riesgo

Ex-empleados de proveedores con credenciales activas. Accesos sin auditoría. Movimientos sin trazabilidad.

Acción esta semana

- Inventario de terceros con acceso + permisos otorgados
- Forzar MFA en todos los accesos externos
- Configurar caducidad automática 90 días
- Principio de mínimo privilegio: solo lo necesario

Evidencia mínima

Planilla con vencimientos + revisión semestral agendada + logs de acceso terceros

Tu plan de acción: 7 días y roadmap 30/60/90

Quick-wins en 7 días

1

Inventario mínimo

Alto impacto, bajo esfuerzo

2

Separar Wi-Fi invitados

Alto impacto, bajo esfuerzo

3

Alertas básicas

Alto impacto, bajo esfuerzo

4

Revisar accesos terceros

Medio impacto, bajo esfuerzo

30 días

Backup 3-2-1 + prueba restore + calendario parches

60 días

Revisión reglas firewall + inventario EOL + plan reemplazo

90 días

Segmentación red completa + monitoreo ampliado + auditoría accesos

1 2 3

> **¿Querés convertir estos patrones en un plan ejecutable?**
>
> Diagnóstico técnico + quick wins priorizados + roadmap personalizado. Dejamos tu infraestructura ordenada, documentada y con evidencia sostenible.