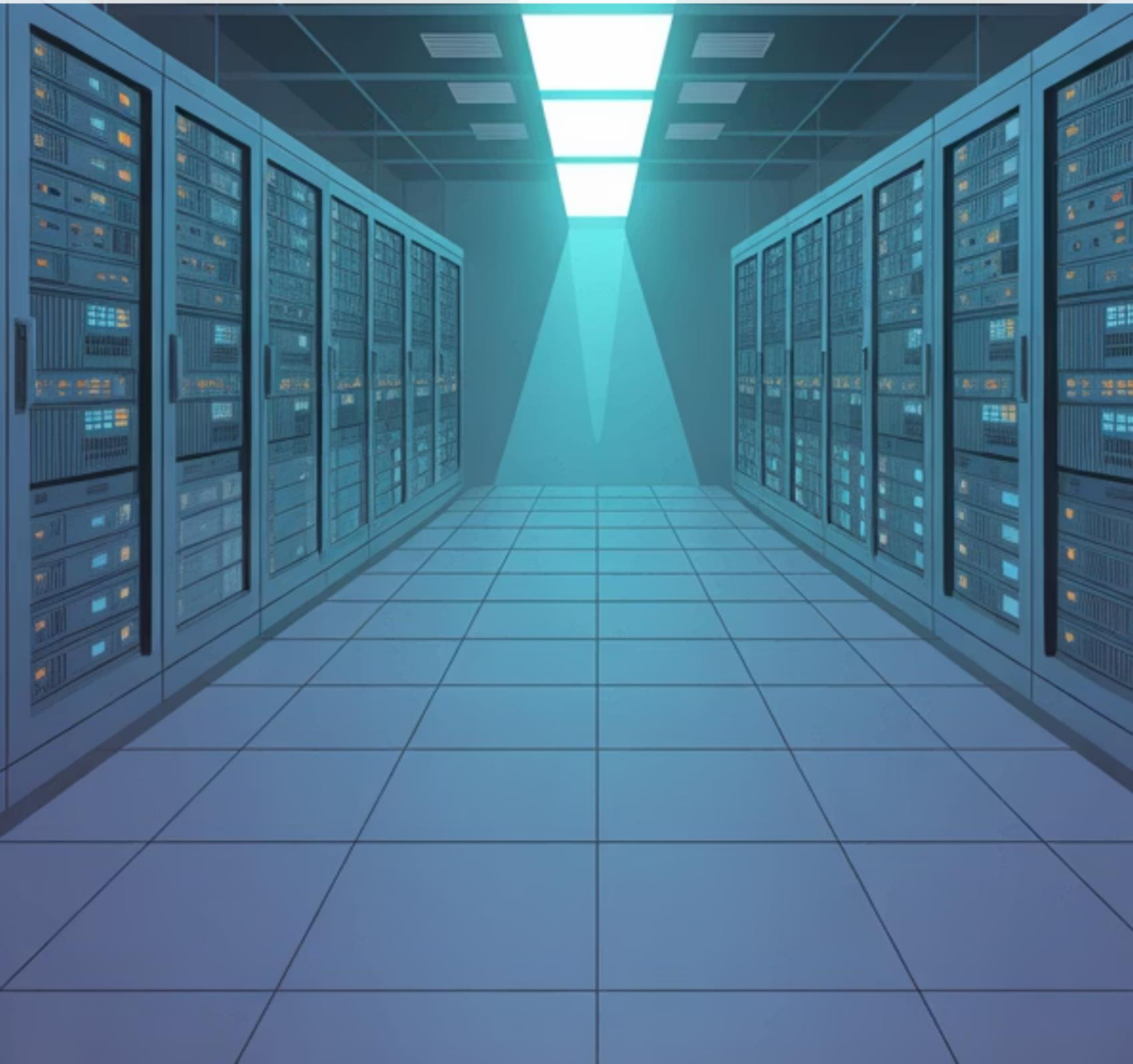
Infraestructura: Checklist inicial del área

Guía rápida para empezar a ordenar el tema y detectar quick-wins

> **Infra ordenada = menos caídas, menos sustos, menos urgencias.**

Mimetic Advisory · Diagnósticos para PyMEs

Mimetic Advisory



¿Para qué sirve este checklist?

Tu punto de partida

Una herramienta práctica para identificar rápidamente dónde estás parado y qué podés mejorar ya.

Estabilidad operativa

Menos cortes inesperados y servicios más confiables

Continuidad del negocio

Capacidad de recuperarte rápido ante problemas

Seguridad básica

Protección mínima contra amenazas comunes

Trazabilidad mínima

Saber qué pasó cuando algo falla

Punto de referencia: Si marcás menos de 60% en este checklist, estás en zona de quick wins. Hay oportunidades claras de mejora inmediata.

Checklist 1: Inventario y mapa (base)

Lo primero es saber qué tenés. Sin inventario claro, cualquier problema te toma de sorpresa y cada decisión es a ciegas.

Inventario mínimo actualizado

Qué mirar: Equipos físicos, servidores, red, nube, licencias críticas

Acción hoy: Crear planilla con marca/modelo/ubicación/función de cada activo

Evidencia: Documento compartido con equipo, actualizado en último mes

Diagrama de red simple

Qué mirar: Flujo desde internet hasta cada servicio crítico

Acción hoy: Dibujar esquema: ISP → router/firewall → switches → Wi-Fi/servidores

Evidencia: Diagrama físico o digital guardado y accesible

Servicios críticos identificados

Qué mirar: Correo, ERP, archivos compartidos, VPN, apps de negocio

Acción hoy: Listar 5-10 servicios que si fallan, paran la operación

Evidencia: Lista priorizada con responsable y horario de disponibilidad

Impacto: ALTO — Sin esto, no sabés qué proteger ni cómo recuperarte

Esfuerzo: BAJO — 2-4 horas de relevamiento inicial

Checklist 2: Perímetro y conectividad

Tu primera línea de defensa. El perímetro mal configurado es la puerta abierta más común en PyMEs.

Firewall con reglas revisadas

Qué mirar: Reglas activas, puertos abiertos innecesarios

Acción hoy: Auditar reglas y cerrar lo que no se usa activamente

Evidencia: Captura de configuración actual + justificación de cada regla

Acceso remoto controlado

Qué mirar: VPN o método de acceso remoto + autenticación

Acción hoy: Activar MFA en accesos remotos críticos

Evidencia: Usuario de prueba con MFA funcionando

Plan B de conectividad

Qué mirar: Backup de enlace (4G/segundo ISP) si operación es crítica

Acción hoy: Evaluar costo-beneficio de redundancia según criticidad

Evidencia: Decisión documentada (con o sin plan B, y por qué)

Impacto: ALTO — Compromiso del perímetro = compromiso total

Esfuerzo: MEDIO — Requiere revisar configuración y activar MFA

Checklist 3: Red interna y segmentación

No toda tu red debería estar mezclada. Una segmentación mínima previene que un problema en un área afecte todo lo demás.

1	### Wi-Fi separado **Qué mirar:** Redes para huéspedes, empleados, dispositivos IoT **Acción hoy:** Crear SSID diferente para invitados, sin acceso a recursos internos **Evidencia:** Prueba de conectividad desde red de invitados sin llegar a archivos
2	### VLANs o separación mínima **Qué mirar:** Segmentación por criticidad (servidores/usuarios/huéspedes) **Acción hoy:** Planificar al menos 2-3 VLANs básicas si tu infraestructura lo permite **Evidencia:** Configuración documentada de VLANs activas
3	### Puertos y switches documentados **Qué mirar:** Qué está conectado en cada puerto del switch **Acción hoy:** Etiquetar físicamente los puertos críticos **Evidencia:** Planilla o diagrama con asignación de puertos actualizada

Errores típicos que vemos

- Todo en la misma red plana sin segmentación
- Wi-Fi de invitados con acceso a servidores internos
- Switches sin documentar, "enchufar y rezar"

Impacto: MEDIO-ALTO — Limita propagación de problemas

Esfuerzo: MEDIO — Configuración de VLANs y redes Wi-Fi

Checklist 4: Servidores y virtualización

Tus servidores son el corazón de la operación. Conocer su estado y tener roles claros evita sorpresas en el peor momento.

01

Roles claros y backups configurados

Qué mirar: Active Directory, archivos, aplicaciones con backup automático

Acción hoy: Verificar que cada servidor crítico tiene backup activo y funcionando

Evidencia: Log de último backup exitoso (menos de 24hs)

02

Espacio en disco y salud hardware

Qué mirar: Uso de disco, alertas de hardware (temperatura, discos)

Acción hoy: Configurar alerta cuando disco supera 80% de uso

Evidencia: Dashboard o mail de alerta configurado

03

Cuentas admin separadas y auditadas

Qué mirar: Accesos con privilegios elevados, quién tiene qué

Acción hoy: Listar usuarios admin y validar que sigan siendo necesarios

Evidencia: Lista actualizada de admins con justificación de cada uno

Impacto: ALTO — Servidores son críticos para continuidad

Esfuerzo: MEDIO — Configuración de alertas y auditoría de accesos

Checklist 5: Backups y recuperación

El backup que nunca probaste es el que va a fallar cuando lo necesites. Este punto es no negociable: sin backup confiable, estás jugando a la ruleta rusa.

Backups automatizados

Qué mirar: Servidores físicos, VMs, SaaS (Google/Microsoft 365 si aplica)

Acción hoy: Confirmar que todos los servicios críticos tienen backup diario automático

Evidencia: Registro de backups exitosos de última semana

Regla 3-2-1

Qué mirar: 3 copias, 2 medios diferentes, 1 offsite/nube

Acción hoy: Verificar que al menos una copia está fuera del sitio principal

Evidencia: Ubicación física o cloud de backup externo confirmada

Prueba de restore mensual

Qué mirar: Capacidad real de recuperar datos o sistemas

Acción hoy: Agendar y ejecutar restore de prueba este mes

Evidencia: Documento con fecha, qué se probó, resultado, tiempo de restore

> "Un backup sin restore probado es una *esperanza*, no un plan."

Impacto: CRÍTICO — Sin backup funcional, cualquier incidente es catastrófico

Esfuerzo: BAJO-MEDIO — Automatización inicial + prueba mensual

Checklist 6: Parches y cambios

Los parches no aplicados son una de las causas más comunes de brechas de seguridad. Y los cambios sin control son una fuente constante de problemas inesperados.

Ventana de mantenimiento definida

Qué mirar: Día y horario fijo para aplicar actualizaciones

Acción hoy: Definir ventana mensual (ej: 2do domingo 22-24hs)

Evidencia: Calendario compartido con equipo y usuarios clave

Parches con frecuencia mínima

Qué mirar: Actualización mensual + parches críticos inmediatos

Acción hoy: Revisar parches pendientes en sistemas operativos y aplicaciones

Evidencia: Reporte de último patcheo exitoso (fecha y sistemas)

Cambios registrados

Qué mirar: Ticket o planilla que documente cambios de configuración

Acción hoy: Crear plantilla simple (qué/cuándo/quién/rollback)

Evidencia: Últimos 3 cambios documentados con plan de rollback

Impacto: ALTO — Vulnerabilidades sin parchear = ventana abierta

Esfuerzo: BAJO — Disciplina de proceso, no complejidad técnica

Checklist 7: Monitoreo y logs (mínimo viable)

No podés arreglar lo que no sabés que está roto. El monitoreo básico te avisa ANTES de que los usuarios te llamen gritando.

Alertas configuradas

Qué mirar: Caídas de servicio, disco lleno, backup fallido, accesos remotos anómalos, reinicios inesperados

Acción hoy: Activar al menos 5 alertas críticas vía mail/SMS

Evidencia: Mail de alerta de prueba recibido correctamente

Retención mínima de logs

Qué mirar: Logs de autenticación, firewall, servidores críticos

Acción hoy: Configurar retención de 30-90 días en sistemas clave

Evidencia: Configuración de retención verificada en 3 sistemas críticos

Canal de incidentes claro

Qué mirar: A quién llamar, qué hacer cuando "se cayó todo"

Acción hoy: Documentar procedimiento de escalamiento y contactos

Evidencia: Doc de 1 página: "Qué hacer si..." con teléfonos y pasos

Monitoreo básico NO es complejo: herramientas gratuitas o incluidas en equipos son suficientes para empezar. Lo importante es usarlas.

Impacto: MEDIO-ALTO — Detección temprana previene catástrofes

Esfuerzo: BAJO — Configuración inicial de 2-3 horas

Quick-wins en 7 días + Plan 30/60/90

Quick-wins (7 días)

- Crear inventario básico de activos
- Dibujar diagrama de red simple
- Revisar reglas de firewall activas
- Activar MFA en accesos remotos
- Separar Wi-Fi de invitados
- Hacer prueba de restore de backup
- Configurar 5 alertas críticas
- Definir ventana de mantenimiento
- Crear plantilla de registro de cambios
- Auditar usuarios admin activos

Roadmap 30/60/90

30 días - Base: Inventario completo, backups con restore probado, reglas de firewall limpias, Wi-Fi segmentado

60 días - Disciplina: Parches mensuales funcionando, registro de cambios activo, segmentación básica (VLANs), monitoreo operativo

90 días - Madurez: Logs retenidos, métricas de disponibilidad, plan DR básico documentado, revisión de accesos de terceros

---

¿Querés aplicarlo en tu empresa?

Convertimos este checklist en un plan ejecutable adaptado a tu realidad, prioridades y presupuesto. **Hablemos.**

Contacto: Formulario web / LinkedIn · *Mimetic Advisory — Diagnósticos para PyMEs*

> "Orden práctico = operación estable y recuperable. Sin humo, con evidencia."

Mimetic Advisory