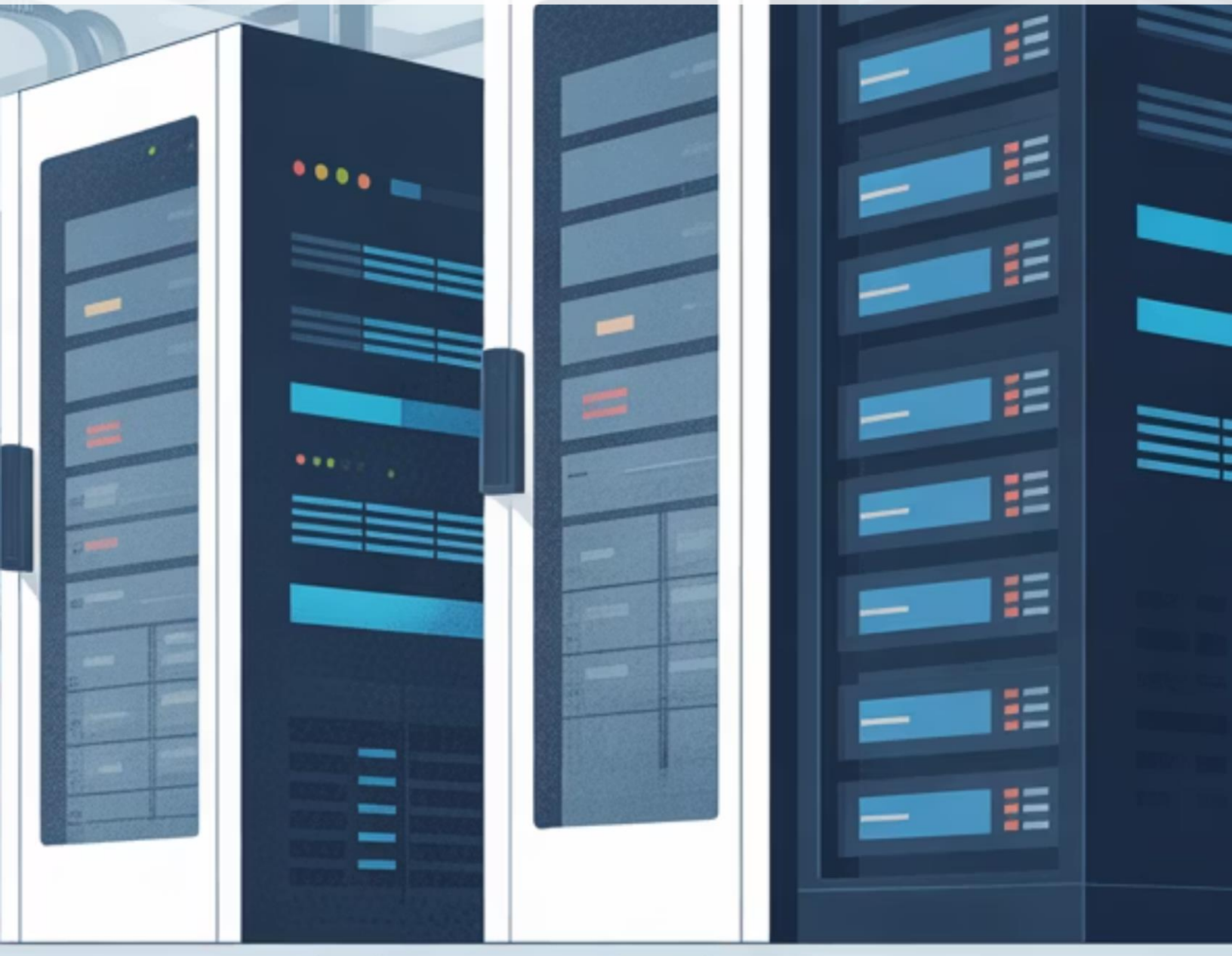
Infraestructura: Checklist inicial del área

Guía rápida para ordenar el tema y detectar quick-wins

Infra ordenada = menos caídas + menos urgencias.

MIMETIC ADVISORY | DIAGNÓSTICOS PARA PYMES



Mimetic Advisory

¿Para qué sirve este checklist?

Reducir caídas

Identificá puntos débiles antes de que exploten en horario crítico

Detectar puntos únicos de falla

Encontrá dónde un solo problema para todo

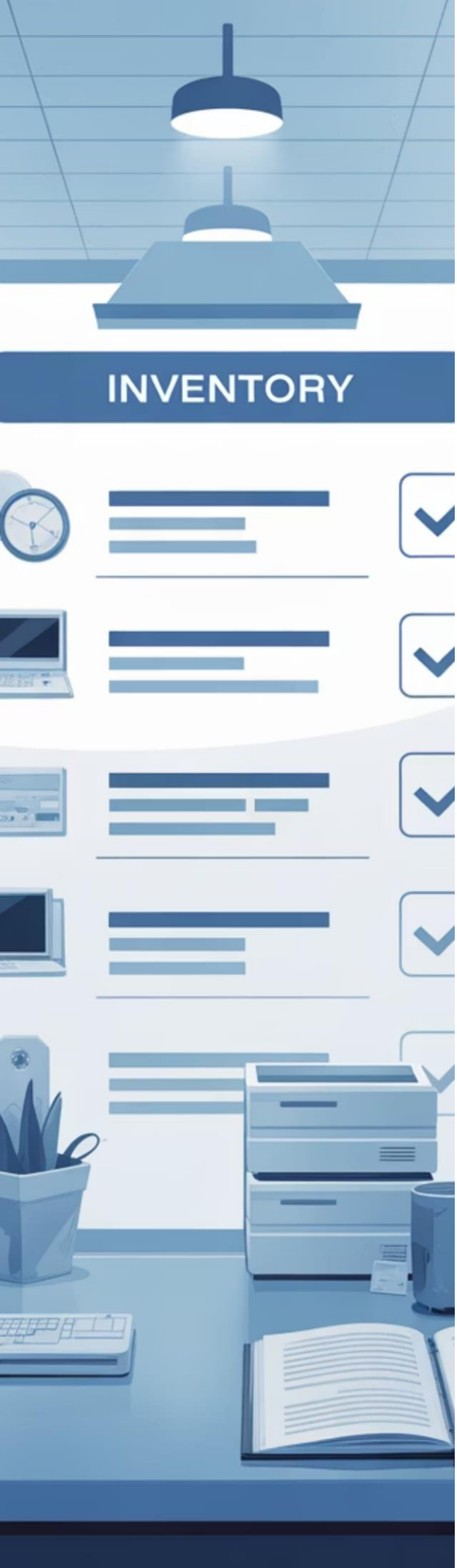
Priorizar gasto

Invertí primero donde más duele

Crear evidencia mínima

Documentación que sirve cuando hay problemas

Nota importante: Si marcás menos del 60% de los puntos, estás en zona de quick wins. Hay oportunidades claras de mejora inmediata.



Checklist 1: Inventario mínimo y criticidad

La base de todo lo demás

Qué mirar

Lista actualizada de servicios, activos críticos y quién responde por cada uno

Acción concreta hoy

Creá una planilla con: servicio/activo, criticidad (Alta/Media/Baja), dueño

Evidencia mínima

Planilla compartida con toda la info básica visible

Elementos clave

- Servicios: Internet, firewall, Wi-Fi, servidores, nube, backups
- Activos: Router, switches, APs, servidores físicos/virtuales, NAS
- Críticos para facturar: ERP, e-mail, facturación electrónica, sistema POS
- Responsables: Nombre + contacto de quién responde por cada servicio

Impacto: Alto | **Esfuerzo:** Bajo

Mimetic Advisory

Checklist 2: Conectividad e Internet

Tu dependencia #1

□ ISP y plan documentados

Qué mirar: Proveedor, plan contratado, contacto soporte, SLA básico

Acción: Guardá contrato + número de soporte en lugar accesible

Evidencia: Doc con datos del ISP + histórico de reclamos

□ Redundancia evaluada

Qué mirar: ¿Qué pasa si cae el enlace principal?

Acción: Evaluá 4G/5G corporativo o segundo enlace según criticidad

Evidencia: Plan B documentado, aunque sea básico

□ DNS y dominios controlados

Qué mirar: Quién administra dominios y DNS

Acción: Confirmá acceso admin a panel de dominio

Evidencia: Credenciales guardadas en lugar seguro

□ Registro de incidentes

Qué mirar: ¿Cuándo y cuánto duran los cortes?

Acción: Empezá planilla simple: fecha, duración, impacto

Evidencia: Log básico de caídas del último trimestre

Impacto: Alto | **Esfuerzo:** Bajo

Checklist 3: Perímetro (firewall/router)

Tu primera línea de defensa

Impacto: Alto | **Esfuerzo:** Medio

01

Acceso remoto controlado

Acción: Revisá qué servicios están expuestos (RDP, VPN, admin). Cerrá lo innecesario.

Evidencia: Lista de puertos abiertos + justificación

02

Reglas revisadas mensualmente

Acción: Agendá revisión mensual de reglas del firewall

Evidencia: Planilla con última fecha de revisión

03

Admin no expuesta

Acción: Deshabilitá acceso a panel admin desde internet

Evidencia: Captura mostrando admin solo en red interna

04

Backup de configuración

Acción: Exportá config del firewall/router, guardala versionada

Evidencia: Archivo de config con fecha

Errores típicos

- Dejar panel de admin accesible desde internet
- Abrir puertos "por las dudas" y olvidarse de cerrarlos
- No tener backup de la config del firewall

Checklist 4: Wi-Fi y segmentación mínima

1

Wi-Fi invitados separado

Qué mirar: Red de invitados aislada de la red interna

Acción: Configurá SSID separado sin acceso a recursos internos

Evidencia: Dos redes visibles + prueba de aislamiento

2

Contraseñas administradas

Qué mirar: Passwords rotadas, no escritas en post-its

Acción: Cambio trimestral mínimo, guardado en gestor

Evidencia: Fecha último cambio + proceso documentado

3

Cobertura razonable

Qué mirar: Zonas críticas sin señal débil

Acción: Mapa básico: dónde llega bien, dónde falta

Evidencia: Plano con cobertura marcada

4

Equipos críticos cableados

Qué mirar: Servidores, impresoras fiscales, POS por cable

Acción: Listá equipos críticos y asegurá conexión cableada

Evidencia: Lista de equipos críticos + tipo de conexión

Impacto: Medio | **Esfuerzo:** Bajo

Checklist 5: Servidores y nube

Donde vive tu operación

Elementos a controlar

- **Capacidad monitoreada:** Disco, RAM, CPU con alertas básicas
- **Servicios documentados:** Qué corre en cada servidor y de qué depende
- **Accesos admin controlados:** Quién tiene acceso y por qué
- **Cambios registrados:** Aunque sea en planilla o sistema de tickets básico

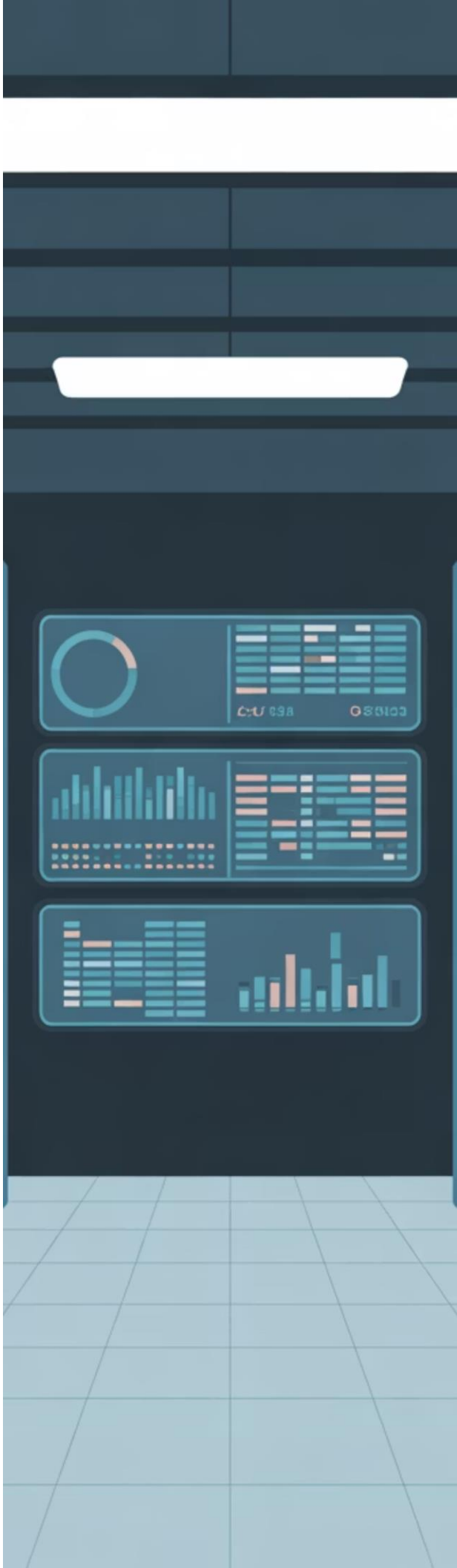
Acción inmediata

Creá un documento simple por cada servidor/servicio cloud con: nombre, función, aplicaciones, responsable y dependencias críticas.

Evidencia mínima

Planilla con inventario de servidores + alertas de capacidad configuradas (aunque sea por email).

Impacto: Alto | **Esfuerzo:** Medio



Checklist 6: Backups y recuperación

Sin esto, todo duele el doble

Backups automatizados

Programados, sin intervención manual

Regla 3-2-1

3 copias, 2 medios distintos, 1 fuera de línea

Restore mensual

Probá recuperar datos todos los meses

Copia inmutable

Al menos una copia que no se pueda borrar

Qué mirar

¿Los backups están corriendo? ¿Cuándo fue la última vez que restauraste algo? ¿Dónde están las copias?

Acción concreta hoy

Verificá log del último backup exitoso + agendá prueba de restore para esta semana

Evidencia mínima

Captura de backup exitoso + registro de última restauración de prueba

Impacto: Alto | **Esfuerzo:** Medio

Checklist 7: Monitoreo y alertas mínimas

Para enterarte antes que el usuario

□ Alertas de caída

Qué mirar: Internet y servicios críticos monitoreados

Acción: Configurá alerta por email/SMS cuando caen servicios clave

Evidencia: Probá que llega la alerta desconectando algo

□ Alertas de capacidad

Qué mirar: Disco lleno, backup fallido, memoria alta

Acción: Umbrales en 80% disco / falla backup / 90% RAM

Evidencia: Mail de alerta recibido en última semana

□ Registro simple

Qué mirar: Log de incidentes: qué pasó, cuándo, cuánto duró

Acción: Planilla compartida o ticketera básica

Evidencia: Últimos 3 incidentes documentados

□ Revisión mensual

Qué mirar: ¿Qué anduvo bien? ¿Qué falló? ¿Qué hacer?

Acción: Reunión 30 min: OK / Issues / Acciones

Evidencia: Minuta o checklist completado

Impacto: Alto | **Esfuerzo:** Bajo-Medio

Quick-wins en 7 días + Plan 30/60/90

De checklist a acción ejecutable

Quick-wins (primera semana)

- Inventario mínimo de servicios y activos
- Backup config firewall/router
- Separar Wi-Fi invitados
- Alertas de backup fallido
- Prueba de restore de un archivo
- Revisión reglas firewall básicas
- Documentación ISP + contacto
- Lista accesos admin actualizados

Plan 30/60/90 días

30 días (Base): Inventario completo, backups + restore probado, Wi-Fi segmentado, alertas mínimas funcionando

60 días (Disciplina): Control de cambios, revisión mensual de reglas, monitoreo de capacidad, auditoría de terceros

90 días (Madurez): Redundancia evaluada/implementada, métricas de disponibilidad, simulacros, hardening básico

---

¿Querés que lo apliquemos?

Convertimos este checklist en un plan ejecutable con diagnóstico, quick wins priorizados y roadmap adaptado a tu realidad.

Diagnóstico + quick wins + roadmap 30/60/90

Contacto

Formulario web o conectá por LinkedIn

MIMETIC ADVISORY

Orden práctico = operación predecible

Mimetic Advisory