Auditoría IT: Checklist inicial del área

Guía rápida para ordenar el tema y detectar quick-wins

> Auditar no es juntar papeles. Es reducir riesgo con evidencia mínima.

Mimetic Advisory — Transparencia y practicidad para PyMEs argentinas

Mimetic Advisory

¿Para qué sirve este checklist?

Esta guía te ayuda a poner orden en el caos sin perder tiempo en burocracia innecesaria. Es el punto de partida para construir controles que funcionen de verdad.

Ordenar el alcance

Definir qué revisás y qué queda para después

Detectar gaps reales

Encontrar huecos que generan riesgo concreto

Priorizar quick-wins

Arreglar lo urgente con poco esfuerzo

Dejar trazabilidad

Evidencia simple que demuestra control

Benchmark rápido: Si marcás menos de 60% en este checklist, estás en zona de quick-wins. Hay mucho para mejorar con poco esfuerzo.

Checklist 1 — Alcance y universo auditado

Antes de auditar, definí qué revisás. Un inventario simple de procesos y sistemas críticos te da el mapa del territorio.

□ Inventario mínimo

Qué mirar: Listado de procesos/sistemas críticos para el negocio

Acción hoy: Planilla con nombre, dueño, criticidad (alto/medio/bajo)

Evidencia: Excel actualizado con fecha de última revisión

□ Definir exclusiones

Qué mirar: Qué sistemas/procesos quedan fuera del alcance

Acción hoy: Documento breve con justificación del recorte

Evidencia: Acta firmada por gerencia explicando el alcance

□ Criterio de criticidad

Qué mirar: Cómo clasificás cada activo (alto/medio/bajo)

Acción hoy: Matriz simple: impacto operativo + impacto financiero

Evidencia: Tabla con criterio claro y ejemplos por categoría

Impacto: Alto — Sin esto, no sabés qué auditar

Esfuerzo: Bajo — 2-3 horas de relevamiento

Checklist 2 — Riesgos y objetivos de control

Hablá en lenguaje de negocio, no de TI. Los riesgos tienen que entenderlos hasta los que no saben de tecnología.

□ Top 10 riesgos TI

Qué mirar: Amenazas reales para el negocio (ej: pérdida de datos, caída de sistema clave)

Acción hoy: Lista priorizada con impacto en $$ o tiempo perdido

Evidencia: Documento con riesgos + impacto estimado

□ Objetivo por riesgo

Qué mirar: Qué control mitiga cada riesgo (1 línea, sin tecnicismos)

Acción hoy: Matriz riesgo-control con responsable asignado

Evidencia: Planilla con columnas: Riesgo / Control / Dueño

□ Dueño del riesgo

Qué mirar: Quién responde por cada riesgo (nombre y cargo)

Acción hoy: Asignar responsables formalmente con mail de confirmación

Evidencia: Lista de dueños con aceptación por escrito

Impacto: Alto — Define toda tu estrategia

Esfuerzo: Medio — Workshop de 4-6 horas con líderes

Checklist 3 — Evidencia mínima y trazabilidad

La evidencia no tiene que ser perfecta, tiene que existir y ser encontrable. Estructura simple, nomenclatura consistente, y listo.

01

□ Qué se prueba

Cada control tiene descripción clara de qué evidencia lo respalda

02

□ Dónde está

Carpeta compartida con estructura lógica (Drive, SharePoint, etc.)

03

□ Nomenclatura simple

Formato: Control-Fecha-Responsable (ej: Backup-2024-01-Lopez)

Errores típicos que te van a costar caro

- Guardar evidencia sólo en la PC de una persona
- Nombres de archivo tipo "final_final_v3_definitivo.xlsx"
- No poner fecha en los documentos (¿cuándo se hizo?)

Impacto: Alto — Sin evidencia, no hay auditoría

Esfuerzo: Bajo — 1-2 horas armando carpetas

Checklist 4 — Accesos y privilegios

Este es el punto donde más duele cuando falla. Accesos mal gestionados = puerta abierta al desastre. Revisá quién tiene llaves del reino.

1

□ Lista de admins

Qué mirar: Quién tiene acceso de administrador en cada sistema crítico

Acción hoy: Planilla con usuario, sistema, fecha de otorgamiento, justificación

Evidencia: Export de configuración + mail de aprobación gerencial

2

□ Revisión periódica

Qué mirar: Accesos privilegiados revisados cada 3 meses mínimo

Acción hoy: Agendar revisión trimestral en calendario compartido

Evidencia: Acta de revisión firmada por responsable TI + gerencia

3

□ Altas/bajas/cambios

Qué mirar: Proceso documentado para cambios en accesos

Acción hoy: Formato simple: solicitud con aprobador + ticket cerrado

Evidencia: Registro de últimos 6 meses en ticketera o planilla

Impacto: Alto — Un ex empleado con acceso admin puede destruir todo

Esfuerzo: Medio — Primera vez: 4 horas. Después: 1 hora trimestral

Checklist 5 — Cambios, parches y configuración

Los cambios sin control son bombas de tiempo. No hace falta un proceso NASA, pero sí registro mínimo de qué, cuándo, quién y por qué.

□ Cambios con aprobación

Qué mirar: Todo cambio en producción tiene ticket o mail de aprobación

Acción hoy: Definir quién aprueba qué (criticidad baja/media/alta)

Evidencia: Últimos 10 tickets cerrados con OK del aprobador

□ Ventana de mantenimiento

Qué mirar: Horarios definidos para cambios (ej: sábados 8-12hs)

Acción hoy: Calendario publicado para el equipo y usuarios clave

Evidencia: Documento con ventanas + comunicación a stakeholders

□ Parches críticos

Qué mirar: Frecuencia definida para aplicar parches de seguridad

Acción hoy: Política simple: críticos en 7 días, normales en 30 días

Evidencia: Reporte de parchado del último mes (captura o export)

Impacto: Alto — Un parche no aplicado = vulnerabilidad explotable

Esfuerzo: Medio — Armado inicial: 3 horas. Después: rutina

Checklist 6 — Backups, restore y continuidad

Tener backup no sirve si no probaste que funciona. El restore es lo único que importa cuando todo se cae.



□ Backups automatizados

Qué mirar: Respaldo diario/semanal de sistemas críticos sin intervención manual

Acción hoy: Verificar logs de últimos 7 días — todos OK

Evidencia: Captura de pantalla del sistema de backup con fecha

□ Prueba de restore mensual

Qué mirar: Restore real de al menos un sistema cada mes

Acción hoy: Agendar prueba mensual con responsable asignado

Evidencia: Acta breve: qué se restauró, cuánto tardó, funcionó OK

□ Evidencia de restore

Qué mirar: Registro de todas las pruebas del último trimestre

Acción hoy: Carpeta con capturas + acta firmada post-prueba

Evidencia: Archivo con fecha, resultado, tiempo de recuperación

Impacto: Crítico — Sin restore, un ransomware te funde

Esfuerzo: Bajo — 1 hora mensual para la prueba

Checklist 7 — Incidentes y monitoreo mínimo

No hace falta un SOC. Hace falta saber cuándo algo se rompe y tener registro de qué pasó. Monitoreo mínimo, pero que exista.

□ Canal de reporte

Qué mirar: Lugar único donde se reportan problemas (mail, Teams, ticketera)

Acción hoy: Comunicar canal oficial a todo el equipo

Evidencia: Comunicación con instructivo simple + responsable asignado

□ Registro de incidentes

Qué mirar: Planilla o ticketera con todos los incidentes del mes

Acción hoy: Formato mínimo: fecha, problema, solución, tiempo

Evidencia: Reporte mensual con top 5 incidentes + acciones

□ Alertas críticas

Qué mirar: Notificaciones por backup fallido, acceso remoto, caídas

Acción hoy: Configurar 3-5 alertas clave que lleguen por mail/SMS

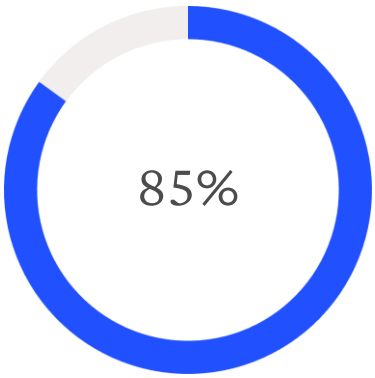
Evidencia: Captura de configuración + test de alerta funcionando

Impacto: Medio — Te permite reaccionar rápido y aprender

Esfuerzo: Bajo — Config inicial: 2 horas. Después: automático

Quick-wins en 7 días + Roadmap 30/60/90

Empezá por lo que da resultado rápido. Después construís madurez de a poco, sin pausas pero sin prisa.

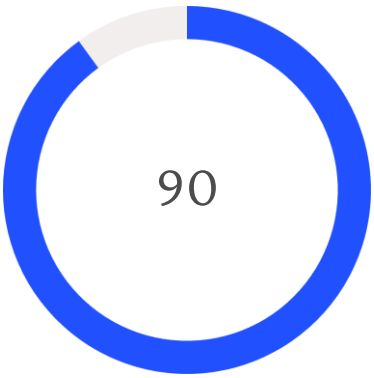


Reducción de riesgo

Con quick-wins bien ejecutados

Días promedio

Para implementar la base



Días a madurez

Proceso completo y sostenible

Quick-wins (semana 1)

- Inventario de sistemas críticos — Impacto: Alto / Esfuerzo: Bajo
- Lista de admins actuales — Impacto: Alto / Esfuerzo: Bajo
- Verificar último backup OK — Impacto: Alto / Esfuerzo: Bajo
- Estructura de carpetas evidencia — Impacto: Medio / Esfuerzo: Bajo
- Canal único de incidentes — Impacto: Medio / Esfuerzo: Bajo
- 3 alertas críticas activas — Impacto: Medio / Esfuerzo: Bajo
- Ventana de mantenimiento — Impacto: Medio / Esfuerzo: Bajo
- Matriz riesgo-control básica — Impacto: Alto / Esfuerzo: Medio

1

30 días: Base

Alcance, evidencia mínima, accesos, backups funcionando y documentados

2

60 días: Disciplina

Cambios con aprobación, parches, configuración, revisión de terceros

3

90 días: Madurez

KPIs, monitoreo continuo, pruebas periódicas, políticas formalizadas

¿Querés que lo bajemos a tu realidad y lo convirtamos en un plan ejecutable?

Agenda una sesión de diagnóstico sin costo. Revisamos tu situación actual, identificamos quick-wins específicos y armamos un roadmap a medida.

Formulario we

Conectar en LinkedI

Mimetic Advisory