Gobierno de TI: Checklist inicial del área

Guía rápida para ordenar el tema y detectar quick-wins

Orden ≠ burocracia. Orden = decisiones claras y trazables.

Mimetic Advisory — Diagnósticos de seguridad para PyMEs

¿Qué es Gobierno de TI?

El Gobierno de TI es el conjunto de prácticas que te permiten tomar decisiones claras sobre tu tecnología, reducir riesgos y asegurar que tus inversiones en TI generen valor real. No se trata de burocracia innecesaria, sino de crear estructuras que te den visibilidad y control.

Reduce riesgos

Previene brechas de seguridad, pérdida de datos y caídas de sistemas críticos

Optimiza costos

Evita duplicar licencias, comprar equipos innecesarios o contratar servicios redundantes

Facilita auditorías

Cumplís con requisitos legales (Ley 25.326) y exigencias de clientes o certificaciones

Transmite confianza

Tus proveedores, clientes y partners confían más cuando ven que tenés control sobre tu TI

En PyMEs, el Gobierno de TI no tiene que ser complejo. Se trata de implementar lo básico que te da tranquilidad y te permite crecer sin arrepentimientos.

Checklist 1: Roles & Responsabilidades

Antes de pensar en tecnología, necesitás gente que sepa qué hacer. Definir quién es responsable de qué es el primer paso para que nada se caiga.

1

Responsable identificado

Tenés una persona (aunque sea part-time) que es el referente de TI o seguridad. No hace todo, pero coordina.

2

Matriz simple de responsabilidades

Sabés quién aprueba, quién ejecuta, quién consulta y quién informa. RACI liviano, sin sobrecargar.

3

Canal de decisiones definido

Sabés a quién consultar cuando hay un problema de TI y cómo se toman las decisiones importantes.

4

Escalamiento claro

Si el responsable no está disponible, sabés quién lo reemplaza o a quién avisar en caso de urgencia.

Errores típicos

- Delegar todo a un solo proveedor externo sin supervisión
- No documentar quién tiene permisos de administrador
- Asignar responsabilidades vagas como "TI lo arregla"

Qué evidencia pedir

Documento con nombres, roles, canales de contacto y decisiones clave tomadas en los últimos 3 meses.

Impacto: Alto | **Esfuerzo:** Bajo

Checklist 2: Inventario & Activos

Si no sabés qué tenés, no podés protegerlo ni gestionarlo. Un inventario básico es tu mapa de batalla para cualquier decisión futura.

01

Listado mínimo de activos

Equipos de escritorio, laptops, servidores, servicios en la nube, licencias de software y dispositivos de red

02

Clasificación por criticidad

Dividí entre crítico (sin esto no funciona el negocio), importante (afecta operaciones) y resto (básico)

03

Dueño asignado

Cada activo tiene una persona responsable, aunque sea el área o el cargo, no solo el nombre

04

Ubicación y estado

Sabés dónde está físicamente cada cosa y si está activa, en reserva o descontinuada

Impacto: Alto | **Esfuerzo:** Medio | **Qué evidencia:** Planilla de inventario actualizada en los últimos 3 meses con responsables y criticidad marcada

Checklist 3: Accesos & Identidades

Los accesos son tu primera línea de defensa. Si no controlás quién entra y qué puede hacer, cualquier medida de seguridad es inútil.

Altas, bajas y cambios con registro

Tenés un proceso (aunque sea un mail o ticket) para cuando alguien se suma, se va o cambia de rol

MFA obligatorio en correo y accesos remotos

El doble factor de autenticación es barato y te protege el 99% de los ataques de phishing

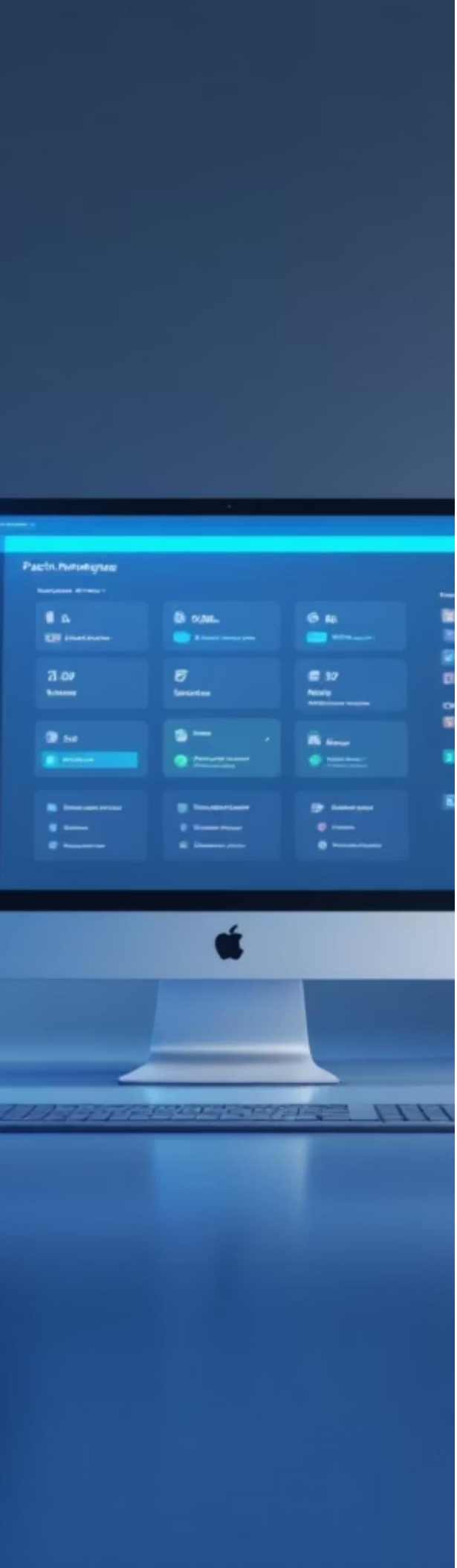
Usuarios de administrador separados

Nadie usa su usuario de admin para navegar o abrir mails. Hay uno para trabajo diario y otro solo para tareas técnicas

Revisión periódica de accesos

Cada 3 meses revisás quién tiene permisos de admin o acceso a datos sensibles y los revocás si ya no son necesarios

Impacto: Alto | **Esfuerzo:** Bajo-Medio | **Qué evidencia:** Listado de usuarios con permisos de admin, configuración de MFA activa, registro de altas/bajas del último mes



Checklist 4: Cambios, Parches y Vulnerabilidades

Cambiar cosas sin control es un camino directo al desastre. Pero tampoco podés quedarte con sistemas obsoletos que nadie mantiene.

Cambios aprobados

Antes de modificar un sistema crítico, alguien valida que no rompa nada

Ventana definida

Cambiás cosas fuera de horario de operación, no a las 11 AM de un día lunes

Parches regulares

Sistemas operativos y aplicaciones se actualizan cada 2-3 semanas como mínimo

Chequeo de vulnerabilidades

Usás herramientas gratuitas para escanear fallas de seguridad conocidas

Impacto: Alto | **Esfuerzo:** Medio | **Qué evidencia:** Historial de cambios (tickets o mails), calendario de mantenimiento, reporte de parches aplicados, resultado de escaneo de vulnerabilidades

Mimetic Advisory

Checklist 5: Backups, Logs y Monitoreo

Los backups son inútiles si no podés restaurar. Y los logs sin monitoreo no te sirven cuando pasa algo. Acá está la diferencia entre reaccionar y prevenir.

Backups con prueba de restore

No solo respaldás, sino que probás que podés recuperar archivos o sistemas completos en menos de 24hs

Regla 3-2-1 activa

Tenés 3 copias, en 2 tipos de medio diferente (disco externo + nube), con 1 copia fuera de sitio

Logs centralizados o retenidos

Guardás registros de acceso, cambios y errores de sistemas críticos por al menos 30 días

Alertas mínimas configuradas

Recibís aviso por mail cuando falla un backup, alguien accede fuera de horario o un sistema se cae

Impacto: Alto | **Esfuerzo:** Medio-Alto | **Qué evidencia:** Resultado de prueba de restore, configuración de retención de logs, regla 3-2-1 documentada, ejemplos de alertas recibidas

Checklist 6: Proveedores y Terceros

Tus proveedores pueden ser tu punto más débil. Un servicio en la nube mal configurado o un técnico de soporte con acceso ilimitado son riesgos que podés reducir con simplezas.

1

Lista de terceros con acceso

Tenés un listado de quiénes tienen acceso a tus sistemas: soporte técnico, proveedores de nube, software como servicio

2

Condiciones mínimas de seguridad

Encontrás en contratos o mails que el proveedor se compromete a mantener ciertos controles básicos

3

Accesos con MFA y caducidad

Tus proveedores usan doble factor y sus claves caducan automáticamente cuando terminan el trabajo

4

Plan de salida documentado

Sabés cómo recuperar tus datos y configuraciones si cambiás de proveedor o te deja sin aviso

Impacto: Medio | **Esfuerzo:** Bajo-Medio | **Qué evidencia:** Lista de terceros con accesos, cláusulas de seguridad en contratos, configuración de MFA en servicios externos, copia de datos clave

Quick-wins en 7 días

Estas son las acciones que podés implementar casi de inmediato y que te dan el mayor retorno en el menor tiempo. Son ideales para empezar a generar confianza y mostrar resultados rápidos.

✅ Activar MFA en correo y VPN

Impacto: Alto | **Esfuerzo:** Bajo | En 2 horas tenés implementado con apps gratuitas como Google Authenticator

✅ Verificar que los backups funcionan

Impacto: Alto | **Esfuerzo:** Medio | Pedí al proveedor que haga un restore de prueba de un archivo

✅ Separar usuarios de administrador

Impacto: Alto | **Esfuerzo:** Bajo | Creá cuentas separadas para cada técnico en menos de 1 hora

✅ Inventario mínimo de activos

Impacto: Alto | **Esfuerzo:** Medio | Planilla simple con equipos, servidores y servicios críticos

✅ Cerrar puertos abiertos innecesarios

Impacto: Medio | **Esfuerzo:** Bajo | Tu proveedor de red puede hacerlo en 30 minutos

✅ Revocar accesos de ex empleados

Impacto: Alto | **Esfuerzo:** Bajo | Listado de usuarios y fecha de baja, revocá todo lo que tenga más de 30 días

✅ Documentar responsable de TI

Impacto: Medio | **Esfuerzo:** Bajo | Mail simple donde digas quién es el contacto y quién lo reemplaza

✅ Instalar parches críticos

Impacto: Alto | **Esfuerzo:** Medio | Actualizá Windows, macOS, navegadores y software de facturación en un fin de semana

Roadmap 30/60/90 días

Una vez que implementaste los quick-wins, acá está el plan para consolidar el Gobierno de TI en tu empresa. Seguí este orden para que cada paso se apoye en el anterior sin abrumarte.

Primeros 30 días: Ordenar la base

Completá el inventario completo, activá MFA en todos los servicios críticos, verificá backups con restore, separá usuarios de admin, y documentá responsables y procesos básicos de decisiones

60 días: Implementar procesos

Establecé ventana de cambios y aprobaciones, definí frecuencia de parches, instalá herramientas de escaneo de vulnerabilidades, revisá accesos de terceros y documentá contratos de seguridad mínimos

90 días: Construir madurez

Centralizá logs y configurá alertas automáticas, creá métricas de desempeño del área TI, simulá un incidente para probar respuestas, y redactá políticas de uso aceptable y aceptación de riesgos

---

¿Listo para empezar?

Si querés que evaluemos el estado actual de tu Gobierno de TI y te armemos un plan personalizado 30/60/90, **contactanos** para un diagnóstico inicial sin cargo. En 2-3 horas de entrevista podemos identificar tus riesgos críticos y priorizar acciones según tu presupuesto.

🔍 Diagnóstico inicial

Entrevista con dueños, gerentes y responsables de TI para entender estado actual

📋 Plan 30/60/90 personalizado

Checklists priorizados según tu industria, tamaño y presupuesto

🎯 Seguimiento opcional

Reuniones mensuales para validar avances y ajustar el rumbo

Mimetic Advisory — Diagnósticos de seguridad para PyMEs

Mimetic Advisory