Ciberseguridad: Checklist inicial del área

Guía rápida para ordenar el tema y detectar quick-wins

> "No necesitás un SOC para empezar. Necesitás hábitos repetibles."

Mimetic Advisory — Diagnósticos de seguridad para PyMEs

Mimetic Advisory

¿Para qué sirve este checklist?

Tu herramienta de orden

Este checklist te ayuda a poner en blanco y negro dónde estás parado hoy en ciberseguridad, sin teoría ni certificaciones imposibles.

Reducir riesgo real

Los incidentes más comunes se evitan con controles básicos bien hechos

Priorizar inversiones

Sabés exactamente dónde poner plata y dónde solo hace falta orden

Generar evidencia mínima

Para auditorías, clientes o simplemente tranquilidad tuya

Nota clave: Si marcás menos de 60% en estos checklists, estás en zona de quick wins. Hay mucho por hacer con poco esfuerzo.

Checklist 1 — Inventario mínimo

LA BASE

Qué mirar: Qué activos existen y cuáles son críticos para el negocio

☐ Lista de equipos y servidores

PCs, notebooks, servidores físicos, instancias cloud, dispositivos móviles corporativos

☐ Sistemas críticos identificados

ERP, facturación, correo, e-commerce, CRM, sistema de pagos, RRHH

☐ Dueño/responsable asignado

Cada activo tiene un nombre y apellido a cargo

☐ Registro actualizado mensual

El inventario no es un documento de una vez, se revisa y actualiza

Acción concreta hoy

Armá una planilla con: nombre del activo, tipo (servidor/PC/cloud), responsable, criticidad (Alta/Media/Baja)

Evidencia mínima

Planilla o documento con todos los activos listados, actualizado este mes

Alto

Impacto

Sin inventario no sabés qué proteger

Bajo

Esfuerzo

2-3 horas de relevamiento inicial

Checklist 2 — Identidades y accesos

LA PUERTA DE ENTRADA

Qué mirar: Quién entra, cómo entra, y si tiene más acceso del que necesita

☐ MFA en correo y accesos remotos

Correo corporativo, VPN, RDP, portales administrativos: todos con doble factor

☐ Cuentas admin separadas

El administrador no usa su cuenta de admin para el mail del día a día

☐ Altas/bajas con registro

Aunque sea una planilla: quién entró, cuándo, qué accesos se le dieron o quitaron

☐ Revisión trimestral de accesos

Cada 3 meses revisás: ¿esta persona sigue necesitando esto?

Acción concreta hoy

Activá MFA en el correo corporativo (Google Workspace, Microsoft 365, etc.) — es gratis y tomás 30 minutos

Evidencia mínima

Captura de configuración MFA activa + planilla de altas/bajas del último mes

Alto

Impacto

90% de los ataques empiezan por credenciales débiles

Bajo

Esfuerzo

1-2 horas de configuración inicial

Checklist 3 — Perímetro y exposición externa

LO QUE VE INTERNET

Qué mirar: Qué servicios están publicados a Internet y si realmente tienen que estarlo

☐ Solo servicios necesarios expuestos

Si no tiene que estar en Internet, no lo expongas. Punto.

☐ Firewall/Router con reglas revisadas

No la config "de fábrica": reglas actualizadas y documentadas

☐ Acceso remoto con MFA y mínima exposición

VPN activa, RDP nunca directo a Internet, portales con autenticación fuerte

☐ Dominios/SSL correctos

Sin certificados vencidos, sin subdominios "de prueba" colgados hace 2 años

Acción concreta hoy

Escaneá tus IPs públicas con Shodan o similar: ¿qué ve el mundo? ¿Debería verlo?

Evidencia mínima

Documento con puertos/servicios expuestos y justificación de por qué cada uno está ahí

Errores típicos: Dejar RDP expuesto sin VPN | Tener paneles de admin sin MFA | Olvidarse subdominios de desarrollo publicados

Alto

Impacto

La superficie expuesta es donde te buscan primero

Medio

Esfuerzo

2-4 horas de auditoría + ajustes

Checklist 4 — Endpoints y hardening

PCS Y NOTEBOOKS

Qué mirar: Si las computadoras tienen protección básica y configuración de mínimo privilegio

☐ Antivirus/EDR activo y actualizado No alcanza con tenerlo instalado: tiene que estar funcionando y reportando	☐ Bloqueo de macros/scripts no necesarios Los adjuntos de correo con macros son el vector #1 de ransomware	☐ Disco cifrado en equipos críticos Notebooks de gerencia, finanzas, y cualquiera que salga de la oficina	☐ Política de bloqueo de pantalla Bloqueo automático después de 5-10 min de inactividad, siempre

Acción concreta hoy

Revisá 5 PCs al azar: ¿tienen antivirus activo? ¿Se bloquean solos? ¿Las macros están deshabilitadas?

Evidencia mínima

Captura de consola de antivirus mostrando equipos protegidos + config de bloqueo aplicada

Alto

Impacto

Los endpoints son donde empieza el ransomware

Medio

Esfuerzo

3-5 horas de config + despliegue

Checklist 5 — Parches y vulnerabilidades

MANTENIMIENTO BÁSICO

Qué mirar: Si tus sistemas están actualizados o si estás corriendo con agujeros conocidos

1

☐ Frecuencia de parches definida

Mínimo mensual, críticos apenas salen

2

☐ Sistemas EOL identificados

Si está fuera de soporte, está en la lista de reemplazo

3

☐ Escaneo básico trimestral

Vulnerabilidades conocidas chequeadas cada 3 meses

4

☐ Remediación priorizada

Críticos primero, resto según impacto/esfuerzo

Acción concreta hoy

Hacé una lista de todos los sistemas operativos y aplicaciones: ¿cuáles están actualizados? ¿Cuáles no tienen soporte?

Evidencia mínima

Planilla con versiones actuales, última fecha de parcheo, y lista de sistemas EOL con plan de reemplazo

Alto

Impacto

La mayoría de los exploits aprovechan bugs viejos ya parcheados

Medio

Esfuerzo

2-3 horas mensuales de gestión

Checklist 6 — Backups y recuperación

SIN ESTO, TODO SE VUELVE CARO

Qué mirar: Si tenés backups de verdad (probados y recuperables), no solo archivos guardados en algún lado

1

☐ Backups automatizados

Diarios para datos críticos, semanales para el resto. Sin excepciones.

2

☐ Regla 3-2-1 aplicada

3 copias, 2 medios diferentes, 1 fuera de línea (offsite o inmutable)

3

☐ Prueba de restore mensual

Un backup sin prueba es una promesa. Restore real, mensual, documentado.

4

☐ Copia fuera de línea/inmutable

Que el ransomware no pueda cifrarla. Cloud inmutable o cinta offline.

Acción concreta hoy

Programá un restore de prueba este viernes: elegí un archivo crítico y restauralo desde el backup

Evidencia mínima

Planilla con última fecha de backup exitoso + última fecha de restore probado + resultados OK/NOK

Alto

Impacto

Es tu plan B cuando todo falla. No es negociable.

Bajo

Esfuerzo

Config inicial 2-3h, pruebas 1h/mes

Checklist 7 — Incidentes, monitoreo y concientización

LA ÚLTIMA LÍNEA

Qué mirar: Si la gente sabe qué hacer cuando pasa algo raro, y si vos te enterás cuando pasa

☐ Canal de reporte claro

"Me llegó algo raro": ¿a quién aviso? ¿Cómo? Mail, ticket, teléfono. Definido y comunicado.

☐ Alertas mínimas configuradas

Login desde ubicación rara, reenvíos de correo automáticos, fallas de backup, cambios de admin

☐ Registro simple de incidentes

Planilla o ticketera: qué pasó, cuándo, quién reportó, qué hicimos, resuelto/no resuelto

☐ Capacitación anti-phishing

Corta (30 min), práctica, para recepción/administración/tesorería. Semestral como mínimo.

Acción concreta hoy

Enviá un mail a toda la empresa: "Si recibís algo sospechoso, reenvialo a seguridad@tuempresa.com inmediatamente"

Evidencia mínima

Mail/circular comunicando canal + planilla de incidentes (aunque esté vacía) + registro de última capacitación

Medio

Impacto

La gente es tu sensor más sensible

Bajo

Esfuerzo

1-2h comunicación + capacitación trimestral

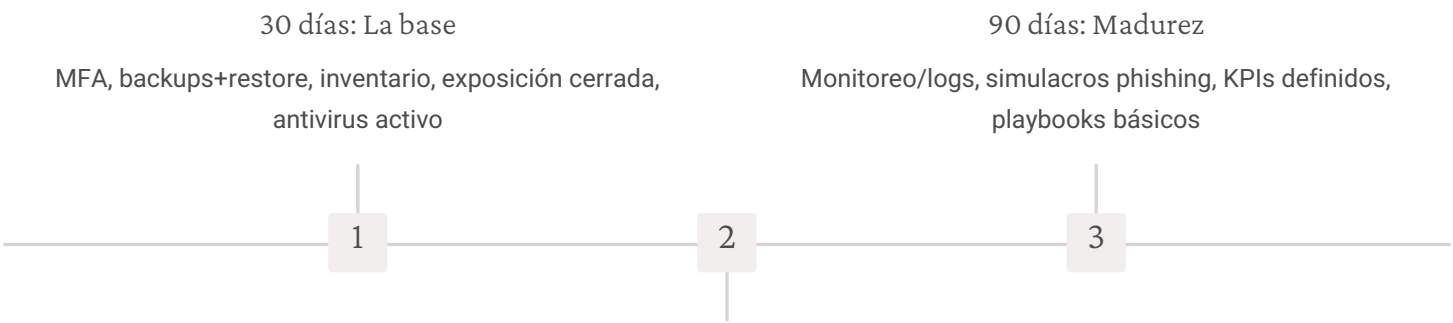
Quick-wins en 7 días + Plan 30/60/90

ACCIÓN INMEDIATA

Empezá por acá (esta semana):

- Activá MFA en correo corporativo
- Separá cuentas admin de usuarios diarios
- Armá inventario mínimo de activos críticos
- Revisá qué servicios están expuestos a Internet (cerrá lo innecesario)
- Probá restore de un backup
- Listá terceros con acceso remoto (proveedores, soporte)
- Implementá regla de pagos con doble validación
- Bloqueá macros en correo

Plan de madurez 30/60/90 días:



> "¿Querés que lo apliquemos en tu empresa y lo convirtamos en un plan ejecutable? Diagnóstico inicial + quick wins + roadmap 30/60/90."

Contacto: Buscanos en LinkedIn o completá el formulario en nuestro sitio web

Mimetic Advisory — Orden práctico = controles repetibles

Mimetic Advisory