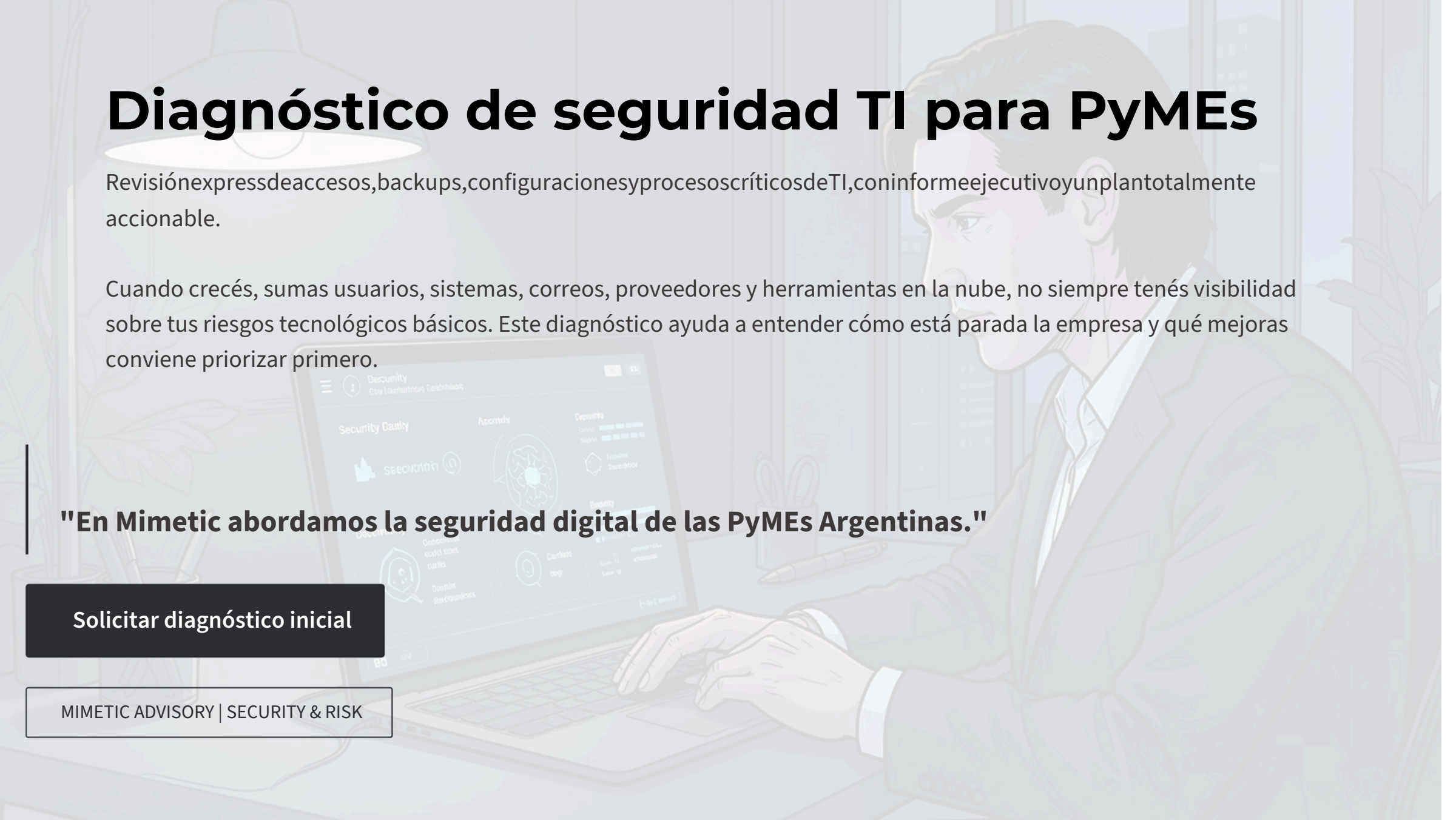
Diagnóstico de seguridad TI para PyMEs

Revisiónexpressdeaccesos,backups,configuracionesyprocesoscríticosdeTI,coninformeejecutivoyunplantotalmente accionable.

Cuando crecés, sumas usuarios, sistemas, correos, proveedores y herramientas en la nube, no siempre tenés visibilidad sobre tus riesgos tecnológicos básicos. Este diagnóstico ayuda a entender cómo está parada la empresa y qué mejoras conviene priorizar primero.



"En Mimetic abordamos la seguridad digital de las PyMEs Argentinas."

Solicitar diagnóstico inicial

MIMETIC ADVISORY | SECURITY & RISK

¿Qué revisamos y qué entregamos?

Esteservicioestá pensado para empresasque nuncatuvieronuna revisión formalde seguridad,dependen de una sola persona técnica o no saben por dóndeempezar.Esespecialmente útilpara empresas en crecimiento, estudios contables, jurídicos o profesionales, comercios con varias sucursales, hoteles, clínicas, distribuidoras, empresas de servicios y cualquier organización que use Microsoft 365, Google Workspace, sistemas de gestión, servidores o proveedores externos de TI.

Revisamos los puntos que más suelen generar riesgos en PyMEs

Accesos y usuarios

- Usuarios activos y permisos de administrador
- Bajas no realizadas y cuentas compartidas
- MFA en cuentas críticas

Backups y recuperación

- Qué se respalda, frecuencia y lugar de almacenamiento
- Pruebas de restauración
- Riesgo ante ransomware o pérdida de datos

Correo, nube y herramientas críticas

- Microsoft 365, Google Workspace y correo corporativo
- Cuentas administrativas y compartición de archivos
- Configuraciones básicas de seguridad

Equipos, parches y protección

- Antivirus o EDR y actualizaciones
- Equipos antiguos e instalación de software
- Notebooks, PCs o servidores críticos

Procesos mínimos de TI

- Altas y bajas de usuarios, gestión de proveedores
- Cambios en sistemas y administración de claves
- Responsables definidos y documentación mínima

Entregables

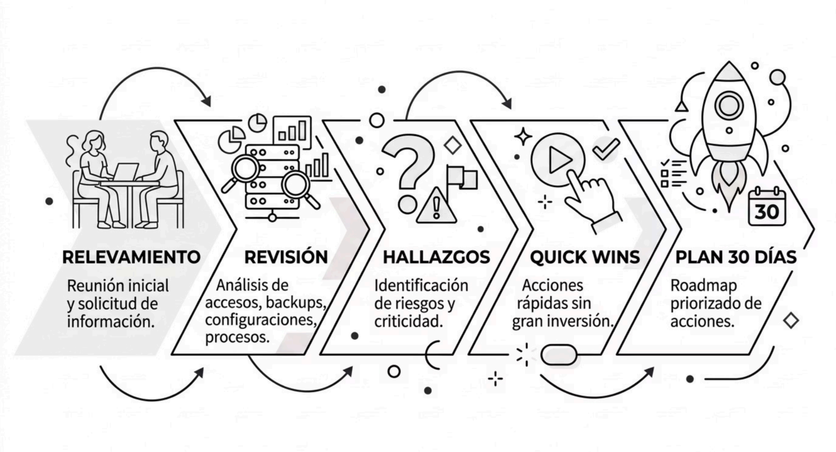
Informe ejecutivo
Resumen claro para dirección o socios, con situación general, principales riesgos, impacto y prioridades.

Matriz de hallazgos
Tabla con riesgos detectados, criticidad, impacto y recomendaciones

Quick wins
Acciones rápidas para reducir riesgo sin grandes inversiones.

Roadmap
Plan priorizado para saber qué hacer primero.

Reunión de cierre
Explicación de resultados, dudas y próximos pasos.



El proceso completo se completa en **5 a 7 días hábiles**, de forma remota según el alcance.

Situaciones comunes que este diagnóstico ayuda a ordenar

"No sabemos quién tiene permisos de administrador."

"Nunca probamos restaurar un backup."

"Hay usuarios activos que ya no trabajan en la empresa."

"El proveedor de TI maneja todo, pero no tenemos visibilidad."

"Queremos mejorar seguridad, pero no sabemos por dónde empezar."

"Tenemos herramientas en la nube, pero no sabemos si están bien configuradas."

"La empresa creció y los controles quedaron informales."

Modalidad, beneficios y próximo paso

Modalidad y duración

Duración estimada: 5 a 7 días hábiles.

Modalidad: Remota.

Proceso:

1. Reunión inicial de 20 a 45 minutos
2. Solicitud de información básica
3. Revisión de accesos, backups, configuraciones y procesos
4. Reuniones específicas de entendimiento
5. Preparación del informe
6. Reunión de cierre

Información que normalmente se solicita:

- Cantidad aproximada de usuarios
- Principales sistemas utilizados
- Plataforma de correo
- Esquema general de backups
- Responsable o proveedor actual de TI
- Políticas o procedimientos existentes, si los hubiera
- Principales preocupaciones actuales

> No siempre se requiere acceso directo a los sistemas. Muchas revisiones pueden hacerse mediante entrevistas, capturas, reportes exportados y evidencia provista por la empresa.

Alcance acotado para mantenerlo simple y accesible

Este diagnóstico **no incluye**:

- Escaneo de vulnerabilidades
- Análisis de seguridad perimetral
- Implementación técnica de los hallazgos
- Auditoría integral de los procedimientos

Si durante la revisión se detectan necesidades adicionales, pueden proponerse como una etapa posterior.

¿Qué obtiene la empresa?

Visibilidad real

Entender su situación actual de seguridad TI con evidencia concreta.

Riesgos identificados

Identificar riesgos antes de que se conviertan en incidentes.

Orden y prioridades

Ordenar accesos, backups y responsabilidades. Priorizar mejoras sin gastar de más.

Informe ejecutivo

Contarconuninformeclaro para dirección. Tener una base para futuras auditorías, certificaciones o proyectos de seguridad.

Decisiones con evidencia

Tomardecisionesinformadassobreseguridad tecnológica.

Precio de lanzamiento

Desde USD 300

Elvalorfinaldepende deltamañodela empresa, cantidad de usuarios, sistemas involucrados y reuniones realizadas, aunque este precio suele cubrir una revisión estandar.

Próximo paso

Coordinemos una llamada de 20 minutos para validar si el diagnóstico aplica a tu empresa.

> "Primero entendemos el riesgo. Después priorizamos acciones concretas."

Coordinar llamada de 20 minutos

Mimetic Advisory | Security & Risk
mimeticadvisory.com.ar
Contacto: Juan Unfuhrer