DIGITALMENTESEGURO.COM.AR • EDICIÓN ESPECIAL 2026

Ciberseguridad para PyMEs sin ser experto

«El manual anti-ransomware y anti-estafas para proteger tu empresa en 1 día» — Guía de acción directa para dueños, directores y administradores en Argentina.

Editorial: digitalmenteseguro.com.ar

Público: Dueños de PyMEs, comercios y directivos

Instagram: @digitalmenteseguro.com.ar

60%	60%	2.470	99,9%
PyMEs Atacadas	**Cierre Definitivo**	**Ataques Semanales**	**Riesgo Mitigable**
en Argentina en el último año	en 6 meses tras ataque grave	promedio por empresa local	activando MFA y respaldo 3-2-1

PROPÓSITO Y ALCANCE DE ESTE MANUAL

¿Por qué existe esta guía? Las pequeñas y medianas empresas argentinas se han convertido en el blanco preferido del cibercrimen organizado: concentran el **66% de los incidentes en el país** y enfrentan más de 260 millones de intentos de ataque al trimestre. La creencia de «somos chicos y no le interesamos a los hackers» es el mito más peligroso para la continuidad del negocio.

Este manual sintetiza inteligencia de amenazas (CERT.ar, Check Point Research, Kaspersky, Sparkfound y Sophos) y establece una hoja de ruta de 24 horas para cerrar las brechas que provocan el 90% de los incidentes.

Contenido del Manual

Capítulo	Contenido y Foco de Gestión	Pág.
Capítulo 1	La Realidad del Riesgo en Argentina: Estadísticas, mortandad empresarial y la trampa del rescate.	2
Capítulo 2	Anatomía de las Amenazas: Ransomware (RaaS), estafas AFIP/ARCA, WhatsApp y banca online.	3
Capítulo 3	El Plan de Blindaje en 1 Día: Cronograma Mañana/Tarde (MFA, Bitwarden, Backup 3-2-1 y Doble Vía).	4
Capítulo 4	Economía y Marco Legal: Presupuestos reales en pesos vs. pérdidas, Ley 25.326 y sanciones AAIP.	5
Capítulo 5	Plan de Emergencia y Checklist: Primeras 2 horas ante un ataque, qué NO hacer y checklist final.	6

CAPÍTULO 1

La Realidad del Riesgo en Argentina: Desmitificando el «A mí no me va a pasar»

Existe un paradigma profundamente arraigado entre dueños y líderes de pequeñas y medianas empresas: asumir que la ciberseguridad es una preocupación exclusiva de multinacionales, bancos u organismos públicos. Los reportes locales demuestran exactamente lo contrario: las PyMEs operan en la primera línea de fuego.

El Mito de la Invisibilidad frente al Cibercrimen Automatizado

Los atacantes modernos no eligen a sus víctimas de manera manual ni artesanal. Usan bots e inteligencia artificial que escanean automáticamente millones de direcciones IP y sitios web buscando contraseñas débiles, paneles expuestos y sistemas desactualizados. Una PyME resulta el blanco predilecto porque custodia datos de clientes y dinero real pero suele carecer de auditorías preventivas.

2.470	42 / min	66%	15%
Ataques Semanales por entidad en Argentina	**Intentos de Ataque** constantes en redes locales	**Foco en PyMEs** del total de ataques del país	**Alza en Incidentes** graves reportados al CERT.ar

La Letalidad del Impacto Económico: Por Qué el 60% Cierra en Seis Meses

El **60% de las PyMEs atacadas gravemente cierra dentro de los seis meses posteriores al incidente**. El golpe financiero no se limita a un pedido de rescate, sino que desata una parálisis operativa total: días enteros sin poder facturar ni entregar mercadería, pérdida de registros contables, honorarios forenses de emergencia, reclamos de clientes y sanciones legales.

Para una empresa argentina, un incidente serio genera pérdidas directas que oscilan entre **$5.000.000 y $15.000.000+ ARS** (o entre USD 25.000 y USD 200.000 en estructuras medianas), capaces de comprometer la liquidez anual.

La Trampa del Rescate: Por Qué Pagar No Es una Solución

Frente a un sistema secuestrado, la desesperación empuja a evaluar el pago extorsivo. Las estadísticas en Argentina son categóricas: el **59% de las empresas víctimas pagó el rescate exigido, pero solo el 8% recuperó la totalidad de sus datos**. Pagar financia a las mafias, marca a la empresa como pagadora y multiplica hasta por 7 el costo colateral por lucro cesante.

> **EL RIESGO SILENCIOSO — ALERTA CLAVE**
>
> **No haber notado un ataque no significa estar seguro:** las intrusiones permanecen ocultas un promedio de **197 a 247 días** antes de detonar un secuestro o fraude. Mientras tanto, bases de clientes, precios y correos ya pueden estar siendo copiadas en silencio.

CAPÍTULO 2

Anatomía de las Amenazas: Ransomware y Estafas de Ingeniería Social

En Argentina, el 90% de los incidentes que paralizan comercios y PyMEs se concentra en dos familias principales: el secuestro extorsivo de datos (ransomware) y los fraudes psicológicos mediante suplantación de identidad (phishing e ingeniería social).

1. Ransomware Moderno: Doble y Triple Extorsión

El ransomware opera bajo el modelo *Ransomware-as-a-Service*: grupos delictivos alquilan herramientas listas para infectar redes y plataformas web. Ya no solo encriptan archivos para frenar las ventas, sino que primero copian bases de clientes y balances para amenazar con publicarlos o extorsionar directamente a tus compradores y proveedores.

2. Phishing y Estafas Locales Adaptadas a Argentina

Con inteligencia artificial generativa, los correos y mensajes fraudulentos ya no tienen errores de ortografía: replican a la perfección el tono rioplatense, los logotipos oficiales y la urgencia administrativa:

- **Suplantación de AFIP / ARCA:** Correos o mensajes por supuestas «deudas fiscales urgentes» o «verificación de CUIT» buscando robar la Clave Fiscal. *Regla inviolable: ARCA jamás solicita tu Clave Fiscal por correo o enlace.*
- **Falsas Alertas Bancarias y Billeteras (Mercado Pago / Ualá):** Avisos de «bloqueo preventivo» o «transferencia retenida» con soportes falsos que piden instalar AnyDesk o TeamViewer.
- **Compromiso de Correo (BEC) y CBU Falso:** Correos desde dominios casi idénticos avisando un «cambio urgente de cuenta bancaria» para desviar pagos de facturas.
- **Secuestro de WhatsApp Business:** Engaño telefónico para robar el código SMS de 6 dígitos y estafar a toda tu cartera de clientes usando tu marca.

Amenaza	Mecanismo de Entrada	Señal de Alarma	Impacto en la Empresa
Ransomware	Adjuntos simulando facturas (.exe, .zip), accesos remotos expuestos.	Archivos con extensiones raras y nota de rescate en pantalla.	Parálisis de operaciones (3 a 15 días) y pérdida operativa severa.
Phishing ARCA / Bancos	Emails o links con portales clonados para capturar claves.	Urgencia extrema («regularice en 2 hs») y dominio extraño.	Vaciamiento de cuentas bancarias y fraude tributario.
Fraude BEC (CBU Falso)	Suplantación de un proveedor o directivo habitual por correo.	Aviso repentino de «cambio de CBU/alias para transferir hoy».	Pérdidas financieras directas e irrecuperables por transferencia.
Robo de WhatsApp	Engaño para que un empleado reenvíe el código SMS de 6 dígitos.	Llamados de falsos clientes o soportes pidiendo códigos por teléfono.	Estafas en cadena a tus clientes y pérdida de confianza.

CAPÍTULO 3

El Plan de Blindaje en 1 Día: Protocolo de Acción Paso a Paso

No hacen falta meses de consultoría compleja para elevar drásticamente la seguridad de tu negocio. Implementando este cronograma práctico en una sola jornada laboral se neutraliza la gran mayoría de los ataques habituales:

BLOQUE MAÑANA (09:00 - 12:00) | Identidad y Control de Accesos

- **Paso 1 — Autenticación Multifactor (MFA / 2FA) Obligatoria:** Activar segundo factor en correo corporativo, bancos, Mercado Pago, ARCA y hosting web usando aplicaciones autenticadoras (Google/Microsoft Authenticator), evitando SMS cuando sea posible. Bloquea hasta el 99,9% de intrusiones con contraseñas filtradas.
- **Paso 2 — Gestor de Contraseñas Corporativo:** Eliminar claves anotadas en papel o compartidas por chat. Usar Bitwarden o 1Password para generar contraseñas únicas de 14+ caracteres.
- **Paso 3 — Principio de Mínimo Privilegio:** Cada integrante solo debe acceder a lo indispensable para su rol. Dar de baja el mismo día los accesos de exempleados y exproveedores.

BLOQUE MEDIODÍA (12:00 - 14:00) | Respaldo Inmutable con Regla 3-2-1

Si tenés un respaldo aislado que un intruso no pueda borrar, un secuestro digital deja de ser terminal:

- **3 Copias** de tus datos críticos (el sistema activo + 2 copias de resguardo).
- **2 Medios distintos** (servidor/disco local + nube independiente).
- **1 Copia fuera de la oficina u offline:** Desconectada o con versionado inmutable. Si el disco externo queda enchufado a la PC principal, el ransomware también lo cifra.
- **Prueba mensual:** Simular restaurar un archivo real cada mes para validar que la copia sirve.

BLOQUE TARDE (14:00 - 17:30) | Dispositivos, Web y Protocolo Anti-Estafa

- **Paso 4 — Parcheo Automático y Auditoría Web:** Mantener actualizados sistemas, plugins de WordPress/e-commerce y realizar una auditoría profesional periódica para detectar puertas abiertas en formularios o servidores.
- **Paso 5 — Protección de Equipos y Wi-Fi Segmentado:** Separar el Wi-Fi de invitados/celulares de la red administrativa y usar protección empresarial gestionada.
- **Paso 6 — Protocolo de Doble Vía y PIN en WhatsApp:** Activar verificación en dos pasos de 6 dígitos en WhatsApp Business y prohibir cambios de CBU o pagos urgentes sin confirmación telefónica previa al número habitual.

> **PROTOCOLO ANTI-ESTAFA EN FINANZAS**
>
> **Regla de Oro:** Ante cualquier pedido imprevisto de pago urgente o cambio de cuenta bancaria (incluso si llega por audio o mail del supuesto proveedor o director), confirmarlo por llamada telefónica directa antes de transferir.

CAPÍTULO 4

Economía de la Ciberseguridad y Marco Legal en Argentina

Postergar la prevención suele justificarse pensando que protegerse es caro. Al comparar el costo de ordenar la seguridad frente al golpe financiero y legal de una brecha o parálisis operativa, la diferencia es abrumadora:

Concepto	PyME Chica (5-10 puestos)	PyME Mediana (10-50 puestos)	Beneficio Protector
Gestor de Contraseñas	~$5.000 / mes	~$20.000 / mes	Elimina claves repetidas y filtradas.
Backup en Nube Automatizado	~$10.000 / mes	~$30.000 / mes	Recuperación sin pagar extorsiones.
Protección Endpoints + EDR	~$15.000 / mes	~$40.000 / mes	Detección y bloqueo de malware en tiempo real.
Protección Email / Cultura	Incluido en suite básica	~$25.000 / mes	Filtra phishing y entrena al equipo.
INVERSIÓN PREVENTIVA BASE	**~$30.000 / mes**	**~$115.000 / mes**	**Continuidad operativa protegida todo el año.**
IMPACTO DE UN ATAQUE GRAVE	**$5M a $15M+ ARS**	**USD 100k – USD 200k+**	**Hasta 60% de riesgo de quiebra en 6 meses.**

Marco Normativo y Responsabilidad Legal en Argentina

- **Ley N° 25.326 de Protección de Datos Personales y Decreto 1558/2001:** Obliga a toda empresa que almacene datos de clientes, pacientes, alumnos o empleados a implementar medidas técnicas de seguridad. La AAIP (Res. N° 47/2018) aplica sanciones económicas a empresas que sufren filtraciones sin medidas preventivas razonables.
- **Ley N° 26.388 de Delitos Informáticos:** Tipifica el acceso indebido, daño informático e interrupción de sistemas en el Código Penal Argentino.
- **Exigencia Comercial y Exportación:** Clientes corporativos y contratos internacionales exigen estándares auditados (OWASP / ISO / RGPD / LGPD) para trabajar con proveedores locales.

> **CUMPLIMIENTO LEGAL OBLIGATORIO**
>
> **Responsabilidad de la Empresa:** Si vulneran tu web y roban datos de terceros, la ley responsabiliza a la empresa titular del negocio —no al diseñador o proveedor freelance— bajo el Código Civil y Comercial y la Ley de Defensa del Consumidor (Ley 24.240).

CAPÍTULO 5

Plan de Emergencia: Primeras 2 Horas y Checklist de Blindaje

Si detectás archivos bloqueados, sesiones extrañas o un empleado entregó un código de acceso, las decisiones en los primeros 120 minutos definen el desenlace:

- **1. Aislamiento Físico (Minuto 0 a 15):** Desconectar cables de red y Wi-Fi de los equipos afectados. **NO apagar ni reiniciar de golpe** para no borrar evidencia de memoria volátil ni activar rutinas destructivas.
- **2. Contención Bancaria y Fiscal (Minuto 15 a 45):** Llamar a los bancos/billeteras para frenar transferencias y cambiar la Clave Fiscal de ARCA desde un dispositivo externo limpio.
- **3. NO Pagar Rescate (Minuto 45 a 90):** No negociar con atacantes; evaluar alcance de filtración con especialistas y consultar proyecto *NoMoreRansom.org*.
- **4. Denuncia Formal (Minuto 90 a 120):** Denunciar ante la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) o Delitos Tecnológicos conservando correos, capturas y registros.
- **5. Restauración Segura:** Restaurar desde backup aislado solo después de validar que la brecha de entrada fue cerrada y auditada.

Estado	Checklist Rápido de Blindaje Empresarial (10 Puntos)
[ ]	**1. Doble Factor (MFA):** Activo con app autenticadora en correo, bancos, Mercado Pago y ARCA.
[ ]	**2. Gestor de Contraseñas:** Claves únicas y robustas sin compartir por planillas ni chats.
[ ]	**3. Backup 3-2-1 Inmutable:** Copia diaria desconectada de la red principal y probada.
[ ]	**4. Parcheo Automático:** Windows, macOS, celulares, routers y sitio web actualizados.
[ ]	**5. Auditoría / Pentesting Web:** Revisión profesional sin contraseñas para detectar puertas abiertas.
[ ]	**6. Red Wi-Fi Segmentada:** Red de invitados separada de computadoras administrativas.
[ ]	**7. Regla Doble Vía:** Confirmación telefónica obligatoria antes de pagar a nuevos CBU/alias.
[ ]	**8. WhatsApp Blindado:** PIN de 6 dígitos en verificación en dos pasos en todas las líneas.
[ ]	**9. Baja de Accesos:** Revocación inmediata de credenciales de exempleados o terceros.
[ ]	**10. Protocolo de Emergencia:** Contactos de bancos, IT y UFECI impresos y visibles.



¿Querés saber qué puertas abiertas tiene tu sitio web, tienda o app HOY?

En **digitalmenteseguro.com.ar** realizamos auditorías de ciberseguridad y pentesting para PyMEs y empresas en Argentina **sin pedirte contraseñas**, bajo acuerdo legal de confidencialidad (NDA) y con **1 re-chequeo incluido**.

https://digitalmenteseguro.com.ar • Consulta inicial sin cargo vía web/WhatsApp
Instagram Oficial: @digitalmenteseguro.com.ar