DIGITALMENTESEGURO.COM.AR • EDICIÓN ESPECIAL 2026

Escudo Digital 2026: Cómo evitar estafas virtuales, phishing y robos con IA en tu negocio o empresa

Manual estratégico y práctico de prevención, detección y respuesta frente a fraudes digitales, suplantación con inteligencia artificial y secuestro de datos para PyMEs y equipos de trabajo.

Editorial: digitalmenteseguro.com.ar

Público: Dueños de PyMEs, directivos, administración y equipos

Alcance: Argentina y Latinoamérica

INTRO El fin del mito "somos chicos, no nos van a atacar"

Durante décadas, la ciberseguridad fue vista como una preocupación reservada para bancos, operadoras de telecomunicaciones y corporaciones multinacionales. En 2026, esa creencia no solo quedó obsoleta: se convirtió en la mayor brecha de seguridad de las pequeñas y medianas empresas. El cibercrimen actual opera como una industria automatizada que no selecciona objetivos por prestigio, sino por facilidad de entrada, falta de controles internos y rapidez para convertir un acceso en dinero.

Los indicadores regionales muestran la magnitud del escenario. En Argentina se registran aproximadamente 42 intentos de ciberataque por minuto contra organizaciones locales, y el *phishing* concentra el 31% de todos los incidentes reportados, con un crecimiento interanual del 300% que duplica el promedio latinoamericano **(Análisis Sectorial Argentina, 2026)**. En el plano global, el *Data Breach Investigations Report 2025* de Verizon confirmó que las PyMEs sufrieron casi cuatro veces más incidentes que las grandes corporaciones, y que el *ransomware* estuvo presente en el 88% de las brechas sufridas por empresas pequeñas frente al 39% en grandes organizaciones **(Verizon, 2025)**.

A esto se suma el impacto sobre la continuidad comercial. Según relevamientos del sector, el 60% de las empresas atacadas gravemente cierra en los seis meses posteriores al incidente **(Perfil / Canal E, 2026)**, mientras que el 80% de las organizaciones afectadas debe invertir meses en reconstruir la confianza perdida con clientes y proveedores **(Infobae, 2026b)**. Sin embargo, el panorama tiene una contracara alentadora: cerca del 90% de los ataques exitosos se podrían prevenir con controles simples, hábitos claros y una inversión muy inferior al costo de una sola crisis **(Develop Argentina, 2026)**.

Qué vas a dominar en este ebook

Sección	Contenido principal	Aplicación inmediata en tu empresa
Capítulo 1	El mapa de las estafas virtuales en 2026	Reconocer phishing local, fraude BEC, secuestro de WhatsApp Business y engaños por QR.
Capítulo 2	Inteligencia Artificial: Deepfakes y clonación de voz	Aplicar pruebas de detección audiovisual y la Regla de Oro Anti-IA antes de autorizar pagos.
Capítulo 3	Ransomware, doble extorsión y costo real	Dimensionar el impacto financiero de una parálisis frente al retorno de la prevención.
Capítulo 4	Los 6 pilares del Escudo Digital PyME	Implementar inventario, MFA, backup inmutable 3-2-1-1-0, parches, controles financieros y cultura.
Capítulo 5	Autodiagnóstico y Plan de Acción en 30 Días	Medir la exposición actual y ejecutar una hoja de ruta semanal con responsables claros.
Capítulo 6	Protocolo de los primeros 60 minutos	Contener un ataque, preservar evidencia legal, denunciar y restaurar sin pánico.
Capítulo 7	Glosario esencial para equipos no técnicos	Unificar el lenguaje de seguridad en toda la organización sin tecnicismos innecesarios.

CAP. 01 El mapa de las estafas virtuales en 2026

La gran mayoría de los incidentes que sufren los negocios no comienzan con un código sofisticado que atraviesa un servidor blindado, sino con un mensaje convincente dirigido a una persona ocupada. Esta disciplina se denomina **ingeniería social**: el uso de presión temporal, autoridad aparente o miedo a una pérdida para lograr que un colaborador haga clic, comparta un código o autorice una operación irregular **(Ministerio de Justicia / BCRA, 2026)**.

Las estadísticas de comportamiento confirman por qué funciona tan bien: un estudio regional de Kaspersky demostró que el **66% de los empleados en América Latina hizo clic al menos una vez en un correo falso**, abriendo la puerta a intrusiones en redes corporativas **(Kaspersky, 2026)**. Asimismo, el *ESET SMB Cyber Readiness Index 2026* reveló que el 45% de las PyMEs globales experimentó al menos un incidente de seguridad durante el año anterior **(ESET, 2026)**.

Las seis modalidades más activas contra negocios y empresas

- **Phishing masivo y Spear-Phishing dirigido:** En Argentina, los señuelos más efectivos imitan notificaciones urgentes de **ARCA/AFIP** por supuestas deudas fiscales, avisos bancarios de "bloqueo preventivo" que piden ingresar clave y token, alertas falsas de pagos rechazados en **Mercado Pago** o correos de proveedores habituales que adjuntan un archivo malicioso disfrazado de factura PDF **(Develop Argentina, 2026)**. Cuando el atacante investiga previamente a la víctima en LinkedIn o Instagram para redactar un mensaje a medida, se trata de *spear-phishing*.
- **Compromiso del Correo Empresarial (BEC) y Whaling:** Es una de las estafas más rentables del mundo. El atacante accede a una casilla real (o registra un dominio casi idéntico cambiando una letra) y se hace pasar por el dueño, el gerente general (*whaling*) o un proveedor de confianza para solicitar una transferencia confidencial o informar un falso "cambio de CBU/alias por auditoría". Solo en Estados Unidos, el FBI registró pérdidas por 2.770 millones de dólares por esta modalidad en 2024 **(Infobae, 2026a)**.
- **Secuestro de cuentas de WhatsApp Business:** En mercados donde gran parte de las ventas y cobranzas pasan por WhatsApp, perder el control de la línea comercial es devastador. El engaño clásico consiste en llamar o escribir simulando soporte técnico, un banco o un cliente para pedir el código de verificación de 6 dígitos que llegó por SMS. Una vez robada la cuenta, los estafadores escriben a toda la cartera de clientes ofreciendo promociones falsas o pidiendo adelantos a cuentas de terceros **(Develop Argentina, 2026)**.
- **Smishing, Vishing y Quishing (códigos QR):** El *smishing* utiliza mensajes de texto con enlaces acortados sobre envíos retenidos o multas; el *vishing* recurre a llamadas telefónicas con guiones de soporte técnico; y el fraude por códigos QR reemplaza códigos legítimos en facturas, mostradores o correos para llevar al usuario a formularios clones de pago.
- **Robo de credenciales y accesos en la nube:** El uso de contraseñas repetidas entre plataformas personales y laborales permite que una sola filtración externa exponga el correo corporativo, el panel de facturación o carpetas compartidas. Según relevamientos citados por Surfshark, Argentina figura entre los diez países con mayor volumen de credenciales filtradas, concentrando el 3,04% del total mundial **(Infobae, 2026a)**.
- **Infección vía dispositivos personales (BYOD) y software pirata:** Descargar programas sin licencia, conectarse a redes Wi-Fi públicas sin cifrado o mezclar el teléfono personal con accesos laborales multiplica la superficie de ataque. Según una encuesta de Samsung citada por ESET, el 48% de las organizaciones que permiten dispositivos personales presenció la entrada de malware desde el celular de un empleado **(ESET, 2026)**.

Anatomía de un intento de fraude: cómo leer las señales

Modalidad	Canal frecuente	Señales de alerta inmediatas	Daño principal en la PyME
Phishing / Spear-Phishing	Correo corporativo, mensajería	Urgencia extrema ("en 2 horas"), dominio alterado (ej. *empresa-arg.com.ar.xyz*), enlace externo para "validar clave".	Robo de credenciales bancarias, correo o instalación de malware.
Fraude BEC / Proveedores	Email y WhatsApp	Pedido inusual de confidencialidad, cambio repentino de CBU/alias, presión para pagar antes del cierre bancario.	Desvío directo de fondos operativos muy difícil de recuperar.
Secuestro de WhatsApp	Telefonía y WhatsApp Business	Solicitud de reenviar un código de 6 dígitos recibido por SMS o llamada automática; intentos en horario nocturno.	Estafas a clientes bajo tu marca y pérdida del canal comercial.
Accesos remotos y Cloud	VPN, escritorio remoto (RDP), Nube	Inicios de sesión desde horarios o países atípicos, repositorios con permisos públicos o sin doble factor.	Exfiltración de bases de clientes y acceso lateral a servidores.

CAP. 02 Inteligencia Artificial al servicio del fraude: Deepfakes y clonación de voz

Durante años, las capacitaciones de seguridad enseñaron a desconfiar de correos con mala ortografía, redacción robótica o diseños mal hechos. La masificación de la Inteligencia Artificial Generativa dejó obsoletas esas reglas. Hoy los modelos de lenguaje redactan comunicaciones impecables en español rioplatense, imitan el tono de un ejecutivo real analizando sus publicaciones en redes y adaptan las respuestas en tiempo real mediante chatbots maliciosos **(Ministerio de Justicia / BCRA, 2026)**.

En Argentina, el 47% de los especialistas en ciberseguridad confirma que los atacantes ya utilizan herramientas de IA de forma habitual para optimizar sus engaños **(Análisis Sectorial Argentina, 2026)**. A escala internacional, los fraudes corporativos que incorporan *deepfakes* —audios o videos sintéticos hiperrealistas— registraron un crecimiento del 3.000% **(Infobae, 2026a)**.



Figura 1. La nueva frontera del engaño: Los algoritmos de síntesis vocal y facial permiten replicar identidades de directivos y familiares a partir de fragmentos mínimos publicados en redes sociales o audios reenviados.

Tres segundos bastan para clonar una voz

Una investigación de McAfee demostró que las herramientas actuales necesitan apenas **tres segundos de audio** —obtenidos de una historia de Instagram, un reel corporativo, un podcast o un mensaje de voz— para generar una clonación vocal con un 85% de coincidencia. El mismo estudio reveló que el 70% de las personas admite no estar segura de poder diferenciar una voz humana real de una generada por inteligencia artificial **(100% Seguro / McAfee, 2026)**.

No se trata de ciencia ficción ni de ataques lejanos. A nivel corporativo global, un empleado financiero de la firma de ingeniería Arup transfirió 25 millones de dólares tras participar en una videollamada donde todos los supuestos directivos presentes eran *deepfakes* creados con IA **(Infobae, 2026a)**. En Argentina, la Fiscalía N°1 de Quilmes comprobó en diciembre de 2025 que los audios de WhatsApp empleados para engañar a una víctima y obtener una transferencia urgente habían sido generados con inteligencia artificial imitando el timbre y la cadencia de un conocido **(100% Seguro / McAfee, 2026)**.

Lista de verificación para detectar audios y videollamadas falsas

- **Anomalías en la cadencia y respiración:** Los audios clonados suelen presentar pausas demasiado uniformes entre frases, ausencia de respiraciones naturales o una entonación emocional que no coincide con la supuesta emergencia narrada.
- **Imperfecciones en videollamadas:** Observá si el parpadeo resulta mecánico, si la piel luce excesivamente suavizada, si existe un microdesfase entre labios y audio o si los bordes del rostro, el cabello y los anteojos vibran al moverse.

- **La prueba física en vivo:** Si una videollamada resulta sospechosa, pedí a tu interlocutor que gire la cabeza de perfil o pase la mano abierta frente a su rostro. Los modelos en tiempo real suelen delatarse con distorsiones visibles ante oclusiones rápidas.
- **Evaluación del contexto operativo:** Como advierten los especialistas, el fraude con IA no explota fallas tecnológicas sino la urgencia cotidiana **(Infobae, 2026a)**. Que una voz suene idéntica jamás valida por sí sola una transferencia fuera de procedimiento.

> **REGLA DE ORO ANTI-IA (CRITERIO ALINEADO CON EL BCRA)**
>
> Ante cualquier pedido urgente de transferencia, modificación de cuenta bancaria, envío de claves fiscales o entrega de códigos de verificación —aunque la voz o el rostro parezcan completamente auténticos—, **cortá la comunicación de inmediato** y confirmá la solicitud por un canal alternativo y preacordado, llamando al número habitual agendado de la persona o utilizando una palabra clave interna definida por tu empresa **(Ministerio de Justicia / BCRA, 2026)**.

CAP. 03 Ransomware, doble extorsión y el costo real de la parálisis

Si el *phishing* y la ingeniería social son la llave de entrada, el *ransomware* es el ataque capaz de detener por completo la facturación de una empresa en cuestión de minutos. Una vez que el programa malicioso logra ejecutarse —por un adjunto contaminado, una contraseña filtrada o un servidor sin actualizar—, se propaga por la red interna, cifra documentos, bases de datos y sistemas de gestión, y deja una nota exigiendo un pago en criptomonedas.

Hacia mediados de 2026, los incidentes de secuestro de datos crecieron un 48% interanual en América Latina **(Análisis Sectorial Argentina, 2026)**. Peor aún, el modelo criminal evolucionó hacia la **doble y triple extorsión**: antes de bloquear los archivos, los atacantes copian información confidencial (balances, contratos, datos personales de clientes y nóminas) y amenazan con publicarla en la *Dark Web* o extorsionar directamente a clientes y socios comerciales si no se abona el rescate.



Figura 2. Resiliencia frente al secuestro de datos: La combinación de defensas perimetrales, protección de endpoints y copias de seguridad inmutables transforma un ataque potencialmente terminal en un incidente recuperable.

Por qué pagar el rescate casi nunca resuelve el problema

Ante la desesperación de ver el negocio paralizado, muchos empresarios consideran pagar el rescate como la salida más rápida. Sin embargo, los datos demuestran lo contrario: el informe *State of Ransomware* de Sophos reveló que el 59% de las empresas argentinas víctimas terminó pagando el rescate exigido, pero **apenas el 8% logró recuperar la totalidad de sus datos (Sophos, 2023)**. Pagar no elimina la puerta trasera que dejó el atacante, no garantiza la destrucción de los datos robados y marca a la empresa como un objetivo rentable para futuros ataques.

El retorno financiero de prevenir en Argentina

Postergar la inversión en seguridad suele justificarse con la frase "nunca nos pasó nada". No obstante, al contrastar el costo directo de un incidente grave en Argentina frente al presupuesto anual de protección integral para una PyME de aproximadamente 10 personas, la conclusión económica es indiscutible **(Develop Argentina, 2026)**:

Concepto de impacto económico y operativo	Estimación de referencia (ARS, 2026)
Recuperación técnica, limpieza forense y reinstalación tras ransomware	$1.500.000 – $5.000.000
Parálisis operativa y lucro cesante (promedio de 7 días sin operar con normalidad)	Variable según facturación diaria
Sanciones por filtración de datos personales (marco Ley 25.326)	Hasta $2.000.000

Concepto de impacto económico y operativo	Estimación de referencia (ARS, 2026)
Honorarios legales, notificaciones y gestión de reclamos de terceros	$500.000 – $3.000.000
Impacto directo total estimado por un solo incidente grave	**$5.000.000 – $15.000.000+**
Inversión preventiva anual integral (antivirus empresarial/EDR, gestor de contraseñas, backup en nube y capacitación básica)	**$500.000 – $1.200.000 / año**

Más allá del balance inmediato, el cumplimiento normativo ya es una exigencia comercial. En Argentina, la **Ley 25.326 de Protección de Datos Personales** obliga a garantizar la seguridad y confidencialidad de la información de clientes y empleados; y para las PyMEs que exportan servicios o integran cadenas de suministro de grandes compañías, estándares internacionales como el RGPD europeo o la LGPD brasileña se volvieron requisitos para sostener contratos **(Perfil / Canal E, 2026)**.

CAP. 04 Los 6 Pilares del Escudo Digital para tu negocio

Construir una empresa segura no requiere comprar tecnología compleja que nadie sabe administrar. El enfoque más efectivo para una PyME es la **defensa en profundidad**: combinar seis capas básicas y coordinadas para que, si un eslabón falla —por ejemplo, un empleado hace clic en un enlace fraudulento—, las capas siguientes bloqueen el robo de identidad o permitan recuperar toda la información sin pagar rescates **(Kaspersky, 2024)**.



Figura 3. Arquitectura de defensa en profundidad: El factor humano capacitado, el control estricto de accesos y los respaldos distribuidos conforman el núcleo de un Escudo Digital sostenible para cualquier PyME.

Pilar 1: Inventario de activos críticos y Principio de Mínimo Privilegio

Para identificar qué debe protegerse primero, aplicá una pregunta directa: *"¿Qué pasaría si mañana no pudiéramos acceder a esto?"* **(ESET, 2026)**. Documentá en una planilla centralizada todas las notebooks, computadoras de escritorio, teléfonos corporativos, casillas de correo, accesos a homebanking y billeteras, sistemas de facturación, sitio web, redes sociales y carpetas en la nube. Aplicá el **Principio de Mínimo Privilegio**: cada empleado o proveedor debe tener su propio usuario con acceso únicamente a lo que necesita para su función, y sus credenciales deben revocarse el mismo día en que finaliza la relación laboral o comercial **(Kaspersky, 2026)**.

Pilar 2: Gestión profesional de contraseñas y Autenticación Multifactor (MFA / 2FA)

Usar la misma clave en el correo, el banco y las redes sociales convierte una filtración menor en un desastre generalizado. Adoptá un gestor de contraseñas empresarial (como Bitwarden o 1Password) para crear claves únicas de al menos 12 caracteres sin obligar al personal a memorizarlas. En paralelo, activá la **autenticación multifactor (MFA/2FA)** en todos los servicios críticos —preferentemente mediante aplicaciones autenticadoras o llaves de seguridad en lugar de SMS—. Esta única medida reduce en un 99,9% el riesgo de compromiso de cuentas por robo de credenciales **(Análisis Sectorial Argentina, 2026)**.

Pilar 3: Copias de seguridad inmunes al ransomware (Regla 3-2-1-1-0)

Un disco externo enchufado permanentemente a la computadora de administración no es un backup seguro: si entra un *ransomware*, cifrará también ese disco. El estándar moderno recomendado para negocios es la regla **3-2-1-1-0 (ESET, 2026)**:

- **3 copias** de todos los datos críticos (el original en uso más dos respaldos).
- **2 medios distintos** de almacenamiento (por ejemplo, servidor local y almacenamiento en la nube).
- **1 copia fuera de sitio** (en una ubicación física distinta o servicio cloud independiente de la oficina).
- **1 copia inmutable u offline** (desconectada de la red o configurada para impedir borrado y cifrado).
- **0 errores de restauración:** realizar pruebas periódicas abriendo archivos respaldados para verificar que realmente sirven en una emergencia.

Pilar 4: Actualizaciones automáticas, protección EDR y redes segmentadas

El 85% de los ataques de ransomware explota vulnerabilidades conocidas que ya tenían un parche de seguridad publicado **(Develop Argentina, 2026)**. Mantené activas las actualizaciones automáticas en Windows, macOS, celulares, navegadores, routers y plugins del sitio web (como WordPress). Reemplazá antivirus gratuitos domésticos por soluciones empresariales con **EDR (Endpoint Detection & Response)** que monitorean comportamientos sospechosos, separá la red Wi-Fi de invitados de la red administrativa y exigí conexión por VPN cuando el personal trabaje desde hogares, cafés u hoteles.

Pilar 5: Protocolos financieros anti-fraude y segregación de funciones

Las herramientas técnicas no pueden frenar una transferencia voluntaria hecha por engaño. Por eso toda PyME necesita dos controles administrativos por escrito **(Infobae, 2026a)**: primero, **segregación de funciones**, garantizando que quien carga un nuevo proveedor o solicita un pago no sea la misma persona que lo aprueba y libera en el banco; segundo, **doble validación obligatoria** mediante llamada a un número previamente verificado cada vez que un proveedor informe un cambio de CBU/alias o un directivo solicite un pago urgente fuera de agenda.

Pilar 6: Cultura digital, capacitación y blindaje de WhatsApp Business

Las malas prácticas y el error humano están presentes en el 82% de las violaciones de datos **(Kaspersky, 2024)**. Dedicá 15 a 30 minutos por trimestre a revisar ejemplos reales de estafas locales con todo el equipo y promoví una cultura de **"reportar sin vergüenza"**: es preferible que un empleado consulte diez veces antes de hacer clic a que oculte un error por miedo a represalias. Para **WhatsApp Business**, activá obligatoriamente la verificación en dos pasos con PIN de 6 dígitos y correo de recuperación, desactivá el buzón de voz si no se utiliza y establecé como norma estricta que nadie jamás entrega códigos recibidos por SMS.

CAP. 05 Autodiagnóstico Rápido y Plan de Acción en 30 Días

Antes de comprar software o contratar servicios externos, evaluá el estado real de tu negocio. Marcá cuántas de estas diez afirmaciones se cumplen hoy en tu empresa; cada respuesta negativa señala una prioridad inmediata.

Checklist de diagnóstico inicial para tu PyME

#	Control esencial de ciberseguridad	Sí / No
01	Todas las cuentas críticas (correo, banco, ARCA/AFIP, Mercado Pago, redes) tienen 2FA/MFA activo.	[ ]
02	Cada colaborador usa su propio usuario y nadie comparte contraseñas administrativas.	[ ]
03	Las contraseñas son únicas, robustas y se administran con un gestor corporativo.	[ ]
04	Existen copias de seguridad automáticas con al menos una copia offline o inmutable, probada recientemente.	[ ]
05	WhatsApp Business tiene PIN de verificación en dos pasos activo y política estricta sobre códigos SMS.	[ ]
06	Los sistemas operativos, navegadores y sitio web se actualizan automáticamente.	[ ]
07	Los equipos cuentan con protección empresarial (antivirus gestionado / EDR), no solo versiones gratuitas.	[ ]
08	Los cambios de CBU/alias de proveedores y pagos urgentes se confirman siempre por llamada telefónica.	[ ]

#	Control esencial de ciberseguridad	Sí / No
09	Se revocan de inmediato todos los accesos cuando un empleado o proveedor deja de trabajar con la empresa.	[ ]
10	El equipo sabe exactamente a quién avisar y qué hacer en los primeros 60 minutos ante un incidente.	[ ]

Hoja de Ruta de Implementación en 30 Días

Transformá el diagnóstico en resultados concretos ejecutando un bloque por semana. Imprimí este tablero y asigná un responsable por cada entrega.

Etapa	Acciones prioritarias	Responsable	Listo
Semana 1 Blindaje de accesos	Activar MFA/2FA en correo, bancos, billeteras, ARCA/AFIP y redes sociales. Configurar PIN en WhatsApp Business y eliminar claves compartidas.		[ ]
Semana 1 Gestor de claves	Implementar Bitwarden o 1Password en el equipo, migrar todas las credenciales críticas y reemplazar contraseñas débiles o repetidas.		[ ]
Semana 2 Respaldos 3-2-1-1-0	Completar inventario de activos críticos, configurar backups automáticos en nube + copia offline/inmutable y realizar la primera prueba de restauración.		[ ]
Semana 2 Equipos y redes	Activar actualizaciones automáticas en PCs, celulares y sitio web. Instalar protección empresarial de endpoints (EDR) y separar Wi-Fi de invitados.		[ ]
Semana 3 Finanzas anti-IA	Documentar protocolo de pagos: segregación de funciones, validación telefónica de cambios de CBU/alias y palabra clave interna para urgencias.		[ ]
Semana 3 Auditoría cloud	Revisar permisos en Google Workspace, Microsoft 365, CRM y carpetas compartidas; revocar accesos de exempleados y terceros inactivos.		[ ]
Semana 4 Equipo y protocolo	Dictar taller interno de 45 minutos sobre phishing, deepfakes y WhatsApp. Completar la tabla de contactos de emergencia y agendar revisión trimestral.		[ ]

CAP. 06 Protocolo de Emergencia: Los Primeros 60 Minutos

Incluso en organizaciones bien protegidas puede ocurrir un incidente. Cuando sucede, la improvisación agrava el daño: apagar equipos sin criterio puede destruir evidencia clave, y demorar el aviso a bancos o clientes multiplica las pérdidas económicas. Seguí esta secuencia ordenada durante la primera hora:

1. **Minutos 0 a 10 — Contener y aislar sin apagar:** Si detectás archivos encriptándose, ventanas extrañas o un clic en un archivo malicioso, desconectá de inmediato el equipo afectado de la red (retirá el cable Ethernet y desactivá el Wi-Fi) para frenar la propagación hacia servidores y otras PCs **(Develop Argentina, 2026)**. No apagues el equipo de golpe salvo indicación de un especialista, ya que la memoria puede contener evidencia útil.
2. **Minutos 10 a 20 — Proteger credenciales desde un equipo limpio:** Utilizando otro dispositivo que no haya sido afectado, cambiá de inmediato las contraseñas de correo corporativo, banca online, billeteras virtuales y paneles administrativos, y ejecutá el cierre remoto de todas las sesiones activas.
3. **Minutos 20 a 35 — Frenar movimientos y alertar a terceros:** Si hubo una transferencia fraudulenta o secuestro de WhatsApp Business, comunicáte de inmediato con el área de fraude del banco o billetera virtual para solicitar el bloqueo preventivo. En paralelo, avisá a tus clientes y proveedores por un canal alternativo (correo oficial, redes o teléfono) para evitar que sean estafados en nombre de tu empresa.
4. **Minutos 35 a 50 — Preservar evidencias legales:** No elimines correos, chats ni registros. Guardá capturas de pantalla, encabezados completos de los emails sospechosos, números telefónicos, enlaces recibidos, comprobantes de transferencia y la línea de tiempo exacta de lo ocurrido **(Federación Patronal, 2026)**.
5. **Minutos 50 a 60 — Activar soporte técnico y denuncia formal:** Contactá a tu proveedor de tecnología o especialista en respuesta a incidentes. No pagues rescates bajo presión. En Argentina, realizá la denuncia formal ante la **Unidad Fiscal Especializada en Ciberdelincuencia (UFECI)** o la fiscalía correspondiente **(Develop Argentina, 2026)**.
6. **Post-incidente — Limpieza, restauración y cumplimiento:** Restaurá tus sistemas desde la copia de seguridad offline/inmutable únicamente cuando el especialista confirme que el vector de entrada fue cerrado. Si se comprometieron datos personales de clientes o empleados, evaluá con asesoramiento legal las obligaciones bajo la Ley 25.326.

Directorio interno de respuesta rápida (para completar e imprimir)

Rol o entidad clave	Contacto asignado / Canal oficial	Teléfono / Guardia 24 hs
Responsable interno de incidentes		
Soporte técnico / Proveedor IT		

Rol o entidad clave	Contacto asignado / Canal oficial	Teléfono / Guardia 24 hs
Oficial de cuenta / Fraude bancario		
Asesoría legal / Cumplimiento		

CAP. 07 Glosario Esencial de Ciberseguridad para No Técnicos

Compartí esta guía rápida de términos con todo tu personal para que las alertas internas sean comprendidas al instante por cualquier área de la empresa.

Término	Significado práctico en el día a día de la empresa
Phishing / Spear-Phishing	Engaño por correo o mensaje que imita a una entidad real para robar claves o instalar malware. El *spear-phishing* es su versión personalizada contra una persona específica.
BEC (Business Email Compromise)	Fraude en el que un atacante suplanta o toma el correo de un directivo o proveedor para desviar pagos y transferencias comerciales.
Vishing / Smishing	Estafas de ingeniería social ejecutadas mediante llamadas telefónicas (*vishing*) o mensajes SMS (*smishing*).
Deepfake	Audio, imagen o video generado o manipulado con inteligencia artificial para imitar la voz o el rostro de una persona real.
Ransomware	Software malicioso que cifra los archivos y sistemas de una empresa para impedir su uso y exigir un rescate económico.
MFA / 2FA	Autenticación multifactor o en dos pasos: exige una segunda verificación (código temporal en app o llave física) además de la contraseña.
EDR	*Endpoint Detection & Response*: protección empresarial avanzada para computadoras y servidores que detecta y detiene conductas sospechosas en tiempo real.
Zero Trust / Mínimo Privilegio	Modelo de seguridad que verifica siempre cada acceso y otorga a cada usuario únicamente los permisos estrictamente necesarios para su tarea.
Backup 3-2-1-1-0	Estándar de respaldo: 3 copias, 2 medios distintos, 1 fuera de sitio, 1 copia offline/inmutable y 0 errores verificados al restaurar.

Construí una cultura de seguridad con digitalmenteseguro.com.ar: Proteger una empresa en 2026 no depende de la suerte, sino de decisiones simples ejecutadas a tiempo. Compartí este manual con tus socios y colaboradores, colgá el Protocolo de los Primeros 60 Minutos en un lugar visible de la administración y visitá **digitalmenteseguro.com.ar** para acceder a alertas actualizadas, nuevas guías prácticas y herramientas pensadas para cuidar tu negocio todos los días.

REF. Fuentes y Referencias

1. Verizon (2025). *Data Breach Investigations Report (DBIR) 2025*. Datos sobre incidencia de brechas y ransomware en PyMEs frente a grandes organizaciones.
2. ESET Latinoamérica (2026). *ESET SMB Cyber Readiness Index 2026* y *Ciberseguridad para pymes: guía práctica para proteger tu negocio* (regla 3-2-1-1-0 y política BYOD / encuesta Samsung).
3. Kaspersky (2024). *PyMEs de América Latina registran cerca de 300 millones de intentos de ciberataque* (los seis pilares de ciberseguridad para PyMEs y peso del factor humano).
4. Kaspersky (2026). *Ciberataques golpean el bolsillo de las PyMEs en Latinoamérica* y estudio regional sobre tasa de clic en correos falsos (66% de empleados).
5. Noriega, P. (2026). *Fraudes corporativos con IA: así copian voces y rostros de directivos para cometer estafas*. Infobae (datos del FBI sobre BEC, caso Arup, crecimiento de deepfakes y credenciales filtradas en Argentina según Surfshark).
6. Infobae (2026b). *Los ciberdelitos podrían costar 15.6 billones de dólares si las pymes no fortalecen su ciberseguridad* (impacto en la reconstrucción de confianza con clientes y socios).
7. 100% Seguro (2026). *Voces clonadas con IA: crecen las estafas por WhatsApp que suplantan la identidad de familiares y empresas* (estudio McAfee de 3 segundos de audio y caso judicial de la Fiscalía N°1 de Quilmes).
8. Ministerio de Justicia de la Nación — Con Vos en la Web y Banco Central de la República Argentina (BCRA) (2026). *Recomendaciones oficiales sobre ingeniería social, phishing, vishing y estafas con inteligencia artificial*.
9. Develop Argentina (2026). *Seguridad Informática para PyMEs en Argentina 2026: Guía Esencial* (señuelos locales, costos estimados de incidentes, denuncia ante UFECI y marco Ley 25.326).
10. Sophos (2023). *State of Ransomware* (tasas de pago de rescate y recuperación completa de datos en empresas argentinas).
11. Perfil / Canal E (2026). *Ciberataques: el 60% de las empresas atacadas cierran en seis meses* y análisis sobre cumplimiento normativo (Ley 25.326, RGPD y LGPD).
12. Federación Patronal Seguros (2026). *Ciberseguridad para empresas: medidas básicas para reducir el riesgo de fraude digital y preservación de evidencias*.
13. Relevamiento Sectorial de Ciberseguridad en PyMEs Argentinas (2026). *Indicadores de incidentes por minuto, crecimiento interanual de phishing (+300%), ransomware (+48%), efectividad del MFA (99,9%) y uso de IA en ataques*.