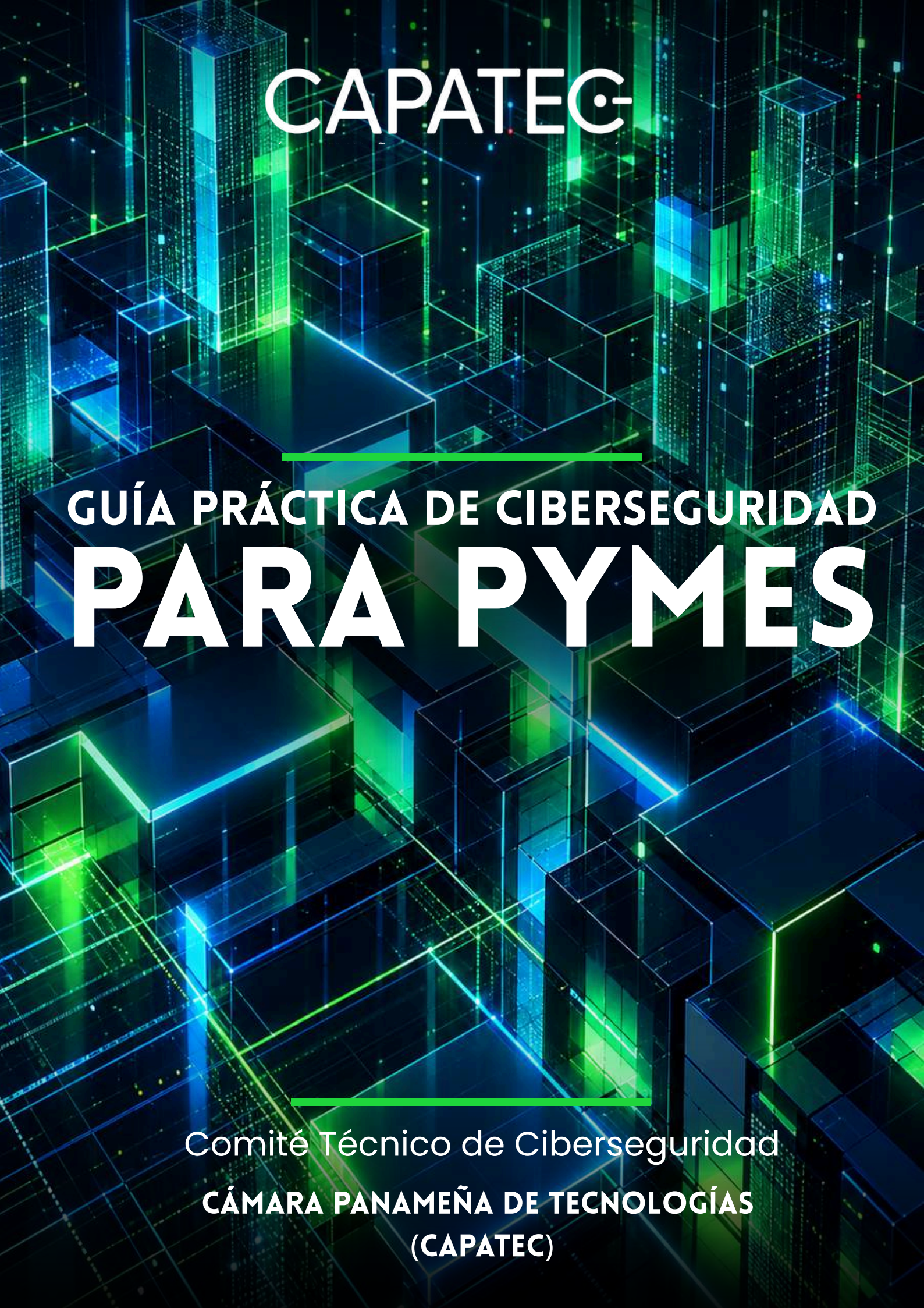



# GUÍA PRÁCTICA DE CIBERSEGURIDAD PARA PYMES

Comité Técnico de Ciberseguridad

**CÁMARA PANAMEÑA DE TECNOLOGÍAS (CAPATEC)**

# ÍNDICE


- Presentación
- Resumen ejecutivo
- Introducción
- Capítulo 1. Por qué su empresa sí es un objetivo
- Capítulo 2. Marco legal en Panamá: sus obligaciones como empresa
- Capítulo 3. El costo real de un incidente
- Capítulo 4. Las amenazas más frecuentes, explicadas en simple
- Capítulo 5. Diez áreas de protección: qué hacer y qué no hacer
- Capítulo 6. Plan de acción por fases
- Capítulo 7. ¿Y si ya ocurrió? Respuesta a incidentes paso a paso
- Capítulo 8. Autoevaluación rápida
- Capítulo 9. Recursos y lugares oficiales de consulta
- Capítulo 10. Glosario en lenguaje simple
- Conclusión. La ciberseguridad es inversión, no gasto
- Anexo A. Hoja de emergencia: si está pasando ahora
- Anexo B. Checklist mensual del dueño
- Anexo C. Reglas de oro para el personal

# PRESENTACIÓN

La Cámara Panameña de Tecnologías de Información, Innovación y Telecomunicaciones (CAPATEC), a través de su Comité Técnico de Ciberseguridad, presenta esta guía práctica dirigida a las pequeñas y medianas empresas de Panamá.

Su propósito es acercar la ciberseguridad a dueños, gerentes y colaboradores que no necesariamente son especialistas en tecnología. No se requieren conocimientos técnicos para utilizarla: cada concepto se explica en lenguaje claro y las recomendaciones se traducen en acciones concretas.

### A QUIÉN ESTÁ DIRIGIDA

A pequeñas y medianas empresas que necesitan proteger su información, sus cuentas, sus operaciones y los datos de sus clientes sin convertir la ciberseguridad en un tema inaccesible.

### CÓMO UTILIZAR ESTA GUÍA

Puede leerse de principio a fin o consultarse según la necesidad de la empresa.

- Si necesita entender sus obligaciones legales, comience por el capítulo 2.
- Si desea dimensionar el riesgo y conocer las amenazas más frecuentes, consulte los capítulos 3 y 4.
- Si quiere comenzar a actuar de inmediato, vaya al capítulo 6, donde encontrará el plan de acción, y al capítulo 8, que contiene la autoevaluación.
- Si su empresa ya sufrió un incidente, vaya directamente al capítulo 7.
- Si encuentra un concepto técnico que no conoce, consulte el glosario del capítulo 10.

Al final encontrará tres herramientas imprimibles: la hoja de emergencia, el checklist mensual del dueño y la tarjeta de reglas de oro para el personal.

**En la práctica:**

El orden sugerido es sencillo: complete primero la autoevaluación del capítulo 8.

# RESUMEN EJECUTIVO

**LA CIBERSEGURIDAD DEJÓ DE SER UN TEMA EXCLUSIVO DE BANCOS Y GRANDES CORPORACIONES.**

En Panamá se reportaron más de 4,000 millones de intentos de ciberataques durante 2024, según cifras difundidas por la industria, y el CSIRT nacional (Equipo Nacional de Respuesta a Incidentes de Seguridad Digital) registró 1,312 incidentes de seguridad en ese mismo año.

En América Latina, alrededor del 27 % de las empresas reconoce haber sufrido un ciberataque en el último año.

Las PYMES son un objetivo preferido de los delincuentes digitales precisamente porque suelen tener defensas más débiles: un solo correo fraudulento abierto por un colaborador puede derivar en el robo de la cuenta bancaria de la empresa, el secuestro de toda su información o una multa por incumplir la ley de protección de datos.

La buena noticia: la mayoría de los ataques que afectan a las PYMES se previene con medidas simples, de bajo costo y al alcance de cualquier negocio. Esta guía explica, en lenguaje no técnico:

1. Las obligaciones de las leyes panameñas (Ley 81 de 2019 y Ley 478 de 2025) y cómo cumplirlas.
2. El costo real de un incidente y por qué prevenir cuesta menos que recuperarse.
3. Las amenazas más frecuentes en Panamá y cómo reconocerlas.
4. Diez áreas de protección con acciones concretas: qué hacer y qué no hacer.
5. Un plan de acción por fases, desde la primera semana hasta el mantenimiento anual.
6. Los pasos a seguir si el incidente ya ocurrió.
7. Una autoevaluación rápida para conocer el punto de partida de su empresa.

Si solo pudiera aplicar cinco medidas de toda esta guía, serían estas: active la verificación en dos pasos (MFA) en todas sus cuentas, haga copias de seguridad automáticas y desconectadas, mantenga sus equipos actualizados, capacite a su equipo para reconocer fraudes y verifique siempre por un segundo canal antes de transferir dinero.

# POR QUÉ SU EMPRESA SÍ ES UN OBJETIVO

Muchos empresarios creen que su negocio es demasiado pequeño para interesarle a un delincuente digital. La realidad es la contraria: los atacantes automatizan sus campañas y disparan millones de correos y mensajes fraudulentos sin distinguir el tamaño de la víctima.

Para ellos, una PYME con defensas débiles es más rentable que una gran empresa bien protegida.

| Mito | Realidad |
| --- | --- |
| "Mi empresa es muy pequeña para que la ataquen" | Los ataques son masivos y automatizados; el tamaño no protege. Las PYMES concentran una parte creciente de las víctimas. |
| "No tengo nada que valga la pena robar" | Su cuenta bancaria, los datos de sus clientes, su facturación y hasta su reputación tienen valor en el mercado criminal. |
| "Con el antivirus ya estoy protegido" | El antivirus es necesario pero insuficiente: la mayoría de los fraudes actuales engaña a las personas, no a las máquinas. |
| "Eso es responsabilidad del técnico" | La ley panameña asigna responsabilidad directa a la gerencia. Además, las decisiones clave (presupuesto, políticas, cultura) son gerenciales. |
| "Si pasa algo, lo resuelvo en el momento" | Recuperarse de un incidente toma semanas o meses y cuesta varias veces más que prevenirlo; no todas las empresas lo logran. |

**La conclusión es simple:**
la pregunta no es si su empresa será blanco de un intento de ataque, sino cuándo, y qué tan preparada estará ese día.

# MARCO LEGAL EN PANAMÁ

## SUS OBLIGACIONES COMO EMPRESA

Panamá cuenta con un marco legal que impone obligaciones concretas a todas las empresas, incluidas las PYMES. Cumplirlo no es solo evitar sanciones: es una señal de seriedad frente a clientes y socios comerciales.

### 2.1 LEY 81 DE 2019 – PROTECCIÓN DE DATOS PERSONALES

La Ley 81 de 26 de marzo de 2019, vigente desde el 29 de marzo de 2021 y reglamentada por el Decreto Ejecutivo 285 de 2021, establece el régimen general de protección de datos personales.

Aplica a toda empresa, sin importar su tamaño, que:

- almacene bases de datos en territorio panameño,
- esté domiciliada en Panamá, o
- realice actividades comerciales digitales dirigidas al mercado panameño.

**¿Qué es un dato personal?** Cualquier información que identifique o permita identificar a una persona: nombre, cédula, teléfono, correo, dirección, historial de compras, datos bancarios, fotografías. Si su empresa tiene una lista de clientes, una planilla de empleados o un formulario de contacto en su sitio web, maneja datos personales y la ley le aplica.

| Principio | Qué significa para su empresa |
|---|---|
| Lealtad | No recolectar datos mediante engaño |
| Finalidad | Usar los datos solo para el propósito informado al cliente |
| Proporcionalidad | Pedir únicamente los datos mínimos necesarios |
| Veracidad y exactitud | Mantener los datos actualizados y correctos |
| Seguridad | Aplicar medidas técnicas de protección (cifrado, contraseñas, respaldos) |
| Transparencia | Informar con claridad cómo se usan los datos |
| Confidencialidad | Impedir accesos no autorizados |

### OBLIGACIONES PRÁCTICAS PARA UNA PYME

1. **Consentimiento previo:** obtenga autorización expresa antes de recopilar datos personales (por ejemplo, una casilla de aceptación en sus formularios).
2. **Almacenamiento seguro:** proteja sus bases de datos con contraseñas robustas y cifrado.
3. **Límite de tiempo:** conserve los datos solo el tiempo necesario para la finalidad informada.
4. **Derechos ARCO:** permita a sus clientes ejercer sus derechos de Acceso, Rectificación, Cancelación y Oposición sobre sus datos, y tenga un canal claro para atender esas solicitudes.
5. **Aviso de privacidad:** publique un aviso de privacidad simple y visible. Debe indicar, en lenguaje claro: quién es el responsable de los datos (su empresa y un contacto), qué datos recopila, para qué los usa, si los comparte y con quién, cuánto tiempo los conserva, y cómo la persona puede ejercer sus derechos ARCO. Puede publicarlo en su sitio web y tenerlo impreso en el local.

### SANCIONES

El incumplimiento puede acarrear multas administrativas —que pueden alcanzar los 10,000 balboas o más, según la gravedad—, suspensión de las operaciones relacionadas con datos e indemnizaciones a los afectados. La autoridad de control es la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI).

### 2.2 LEY 478 DE 2025 – MEDIDAS CONTRA LA CIBERDELINCUENCIA

La Ley 478 de 4 de agosto de 2025, publicada en la Gaceta Oficial del 5 de agosto de 2025, moderniza el marco penal panameño frente a los delitos digitales y crea nuevas obligaciones para las empresas.

## CONDUCTAS QUE LA LEY PENALIZA

- Acceso ilícito a sistemas informáticos: intrusión no autorizada a redes o servidores.
- Manipulación de datos: alteración, borrado o inserción de programas maliciosos.
- Suplantación de identidad digital: uso fraudulento de credenciales ajenas.
- Difusión de contenido íntimo sin consentimiento: compartir imágenes o videos privados de una persona sin su autorización.
- Interferencia en sistemas críticos: ataques que interrumpen servicios esenciales.

Las penas se agravan cuando los ataques afectan infraestructuras críticas: banca, salud, energía y telecomunicaciones.

## QUÉ LE EXIGE A SU EMPRESA

1. **Preservación de evidencia digital:** ante el requerimiento del Ministerio Público, la empresa debe poder conservar datos informáticos hasta por 90 días prorrogables. En la práctica, esto significa no borrar registros ni formatear equipos tras un incidente, y tener protocolos básicos de conservación.
2. **Colaboración con las autoridades:** coordinar con las autoridades judiciales y entregar la información solicitada de forma segura.
3. **Responsabilidad de la gerencia:** la alta dirección tiene responsabilidad directa por la ciberseguridad del negocio. Delegar la operación es válido; delegar la responsabilidad, no.

## TRES ACCIONES INMEDIATAS DE CUMPLIMIENTO

- Establecer un protocolo simple de conservación de datos y registros, con trazabilidad y validación de las solicitudes judiciales.
- Capacitar al personal sobre los nuevos delitos digitales.
- Actualizar el aviso de privacidad informando que los datos podrían compartirse con autoridades bajo mandato legal.

# 3. EL COSTO REAL DE UN INCIDENTE

### 3.1 LAS CIFRAS

- El costo promedio global de una violación de datos ronda los **4.44 millones de dólares**, según el informe Cost of a Data Breach Report 2025 de IBM. Una PYME no enfrenta esas magnitudes, pero incluso una fracción pequeña de esa cifra puede significar el cierre del negocio. Para dimensionarlo a escala local: para un comercio pequeño, quedar una semana sin sistema de facturación y sin acceso a sus datos, más el costo de recuperación y la pérdida de clientes, puede representar la ganancia de varios meses. Para muchos negocios, un solo incidente serio es la diferencia entre seguir abiertos o cerrar.

- El **ransomware** (secuestro de datos) es una de las amenazas más costosas: entre rescate, recuperación y costos indirectos, los incidentes se cuentan en millones de dólares, y las empresas que pagan rescate suelen desembolsar cifras cercanas al millón de dólares sin garantía de recuperar todo.

- Para una PYME, el costo de recuperarse de un ataque puede superar **1.5 veces su presupuesto anual de tecnología**.

- Más del **40 % de las PYMES de América Latina** fue víctima de intentos de phishing (suplantación por correo) en el último año, y solo una minoría cuenta con seguro contra riesgos cibernéticos.

### 3.2 LOS COSTOS QUE NO SE VEN

El golpe financiero directo es solo una parte. Considere también:

- **Interrupción operativa:** días o semanas sin facturar, sin sistema y sin acceso a la información del negocio.

- **Pérdida de confianza:** clientes que se van y no vuelven tras una filtración.

- **Daño reputacional:** la noticia de un fraude o filtración circula rápido, sobre todo en mercados pequeños como el panameño.

- **Multas y procesos:** sanciones por incumplir la Ley 81 y posibles demandas de los afectados.
- **Costos legales y periciales:** abogados, peritos informáticos, notificaciones.

- **Desgaste del equipo:** semanas de trabajo dedicadas a la emergencia en lugar del negocio.

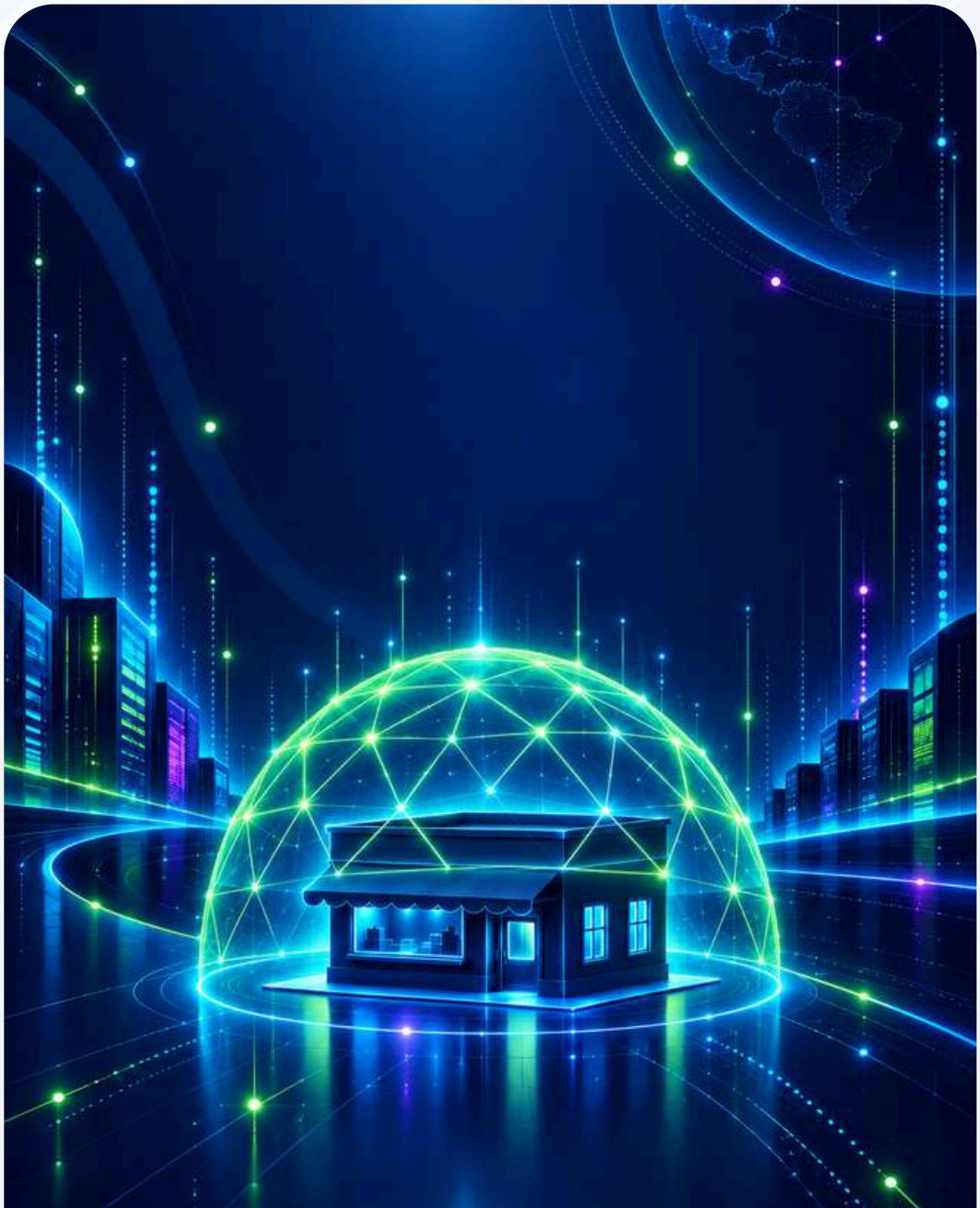
**SOBRE EL SEGURO CIBERNÉTICO.**

Existen pólizas que cubren parte de los costos de un incidente digital: recuperación de datos, honorarios de peritos y abogados, interrupción del negocio y, en algunos casos, responsabilidad frente a terceros afectados. No sustituyen a la prevención, pero pueden amortiguar el golpe.

Si lo evalúa, revise con su corredor: qué eventos cubre y cuáles excluye, si exige medidas mínimas de seguridad para que la cobertura sea válida (por ejemplo, respaldos o verificación en dos pasos), los montos máximos y el deducible, y si cubre el fraude por engaño (como el del correo empresarial comprometido), que a veces se excluye.

Las condiciones varían según la aseguradora; consúltelo con un corredor de confianza.

**La regla de oro:**
cada balboa invertido en prevención evita muchos más en recuperación. La ciberseguridad no es un gasto: es la póliza que mantiene vivo el negocio.



# 4. LAS AMENAZAS MÁS FRECUENTES EXPLICADAS EN SIMPLE

Según el CSIRT de Panamá, el phishing concentró alrededor del 42 % de los incidentes registrados en 2024, seguido por el fraude digital (22 %) y el malware (18 %). A continuación, las amenazas que toda PYME panameña debería saber reconocer.

### 4.1 PHISHING: EL ANZUELO POR CORREO

Correos que imitan a un banco, a un proveedor, a la DGI (Dirección General de Ingresos) o a una empresa de mensajería para que usted haga clic en un enlace, descargue un archivo o entregue sus contraseñas.

### CÓMO SE VE EN LA VIDA REAL:

- “Su cuenta será suspendida, verifique sus datos aquí” (supuestamente de su banco).
- Una “factura adjunta” de un proveedor que usted no esperaba.
- Un “comprobante de pago” que en realidad instala un programa espía.

**Señales de alerta:**
Remitente extraño o con letras cambiadas, errores de redacción, urgencia excesiva (“actúe ahora”), solicitudes de contraseñas o datos bancarios, enlaces que no coinciden con el supuesto remitente, archivos adjuntos inesperados.

### 4.2 FRAUDE DEL CORREO EMPRESARIAL COMPROMETIDO (FRAUDE DEL CEO)

El delincuente estudia a la empresa, suplanta o compromete el correo del gerente, de un proveedor o de un cliente, y solicita una transferencia urgente o el cambio de la cuenta bancaria donde se pagan las facturas.

Es uno de los fraudes que más dinero roba a las empresas en el mundo, y funciona sin ningún virus: solo con engaño.

**Defensa clave:**
toda instrucción de pago o cambio de cuenta bancaria se confirma por un **segundo canal** (una llamada al número ya conocido, nunca al que figura en el correo sospechoso), sin excepciones, incluso si la orden parece venir del dueño.

### 4.3 RANSOMWARE: EL SECUESTRO DIGITAL

Un programa malicioso cifra todos los archivos de la empresa y exige un rescate para devolverlos. Suele entrar por un correo con adjunto, una contraseña robada o un equipo desactualizado. Además de cifrar, los grupos criminales roban la información y amenazan con publicarla si no se paga.

**Defensa clave:**
copias de seguridad automáticas con al menos una copia desconectada de la red, equipos actualizados y verificación en dos pasos. Pagar el rescate no garantiza recuperar los datos y financia al crimen; la recomendación general es no pagar y denunciar.

### 4.3 RANSOMWARE: EL SECUESTRO DIGITAL

Un programa malicioso cifra todos los archivos de la empresa y exige un rescate para devolverlos. Suele entrar por un correo con adjunto, una contraseña robada o un equipo desactualizado. Además de cifrar, los grupos criminales roban la información y amenazan con publicarla si no se paga.

**Defensa clave:**
copias de seguridad automáticas con al menos una copia desconectada de la red, equipos actualizados y verificación en dos pasos. Pagar el rescate no garantiza recuperar los datos y financia al crimen; la recomendación general es no pagar y denunciar.

### 4.4 FRAUDES POR WHATSAPP Y REDES SOCIALES

En Panamá y la región, buena parte de los negocios opera por WhatsApp, y los delincuentes lo saben:

- **Secuestro de la cuenta de WhatsApp:** le piden "por error" el código de seis dígitos que le llegó por SMS; con él, toman su cuenta y estafan a sus contactos y clientes a su nombre.
- **Suplantación del negocio:** perfiles falsos con el logo de su empresa que ofrecen promociones y cobran por adelantado.
- **Falsos compradores o proveedores:** comprobantes de pago adulterados, enlaces de "confirmación de envío" maliciosos.

**DEFENSA CLAVE:**
active la verificación en dos pasos de WhatsApp, jamás comparta códigos recibidos por SMS y verifique los pagos directamente en el banco antes de entregar mercancía.

### 4.5 MALWARE Y PROGRAMAS ESPÍA

Programas maliciosos que roban contraseñas, espían la actividad o abren la puerta a otros ataques. En América Latina son especialmente comunes los troyanos bancarios, que se instalan sin que el usuario lo note y capturan las credenciales de la banca en línea.

### 4.6 ROBO DE CREDENCIALES Y CUENTAS

Contraseñas débiles, reutilizadas o filtradas en otros servicios permiten a los atacantes entrar "por la puerta del frente": correo, banca, redes sociales, sistemas de facturación. Con la cuenta de correo de la empresa, el atacante puede restablecer las contraseñas de casi todo lo demás.

### 4.7 INGENIERÍA SOCIAL TELEFÓNICA Y POR MENSAJERÍA

Llamadas o mensajes de texto de falsos técnicos, falsos funcionarios o falsos ejecutivos bancarios que, con pretextos convincentes, obtienen datos, códigos o accesos. La tecnología de inteligencia artificial hace estos engaños cada vez más creíbles, incluso imitando voces.

**Regla permanente**

Ninguna entidad seria le pedirá contraseñas ni códigos por teléfono, SMS o WhatsApp. Ante la duda, corte y llame usted al número oficial.

### 4.8 EL COMPROBANTE DE PAGO FALSO

En los comercios que aceptan pagos por transferencia bancaria o aplicaciones de pago móvil, un fraude muy común es el del comprobante adulterado: el cliente muestra en su teléfono una captura de pantalla de una supuesta transferencia ya realizada y se lleva la mercancía, pero el dinero nunca llega. Las capturas son fáciles de falsificar y el nombre del ordenante puede no coincidir con quien está frente a usted.

**Defensa clave**

No entregue mercancía ni servicios contra una captura de pantalla. Confirme siempre que el dinero está acreditado consultándolo usted mismo en su aplicación bancaria o esperando la notificación oficial de su banco, no la del cliente. Capacite a todo el personal de caja en la regla: sin dinero acreditado, no sale mercancía, sin importar la prisa o la insistencia del comprador.

# 5. DIEZ ÁREAS DE PROTECCIÓN

## QUÉ HACER Y QUÉ NO HACER

Este capítulo es el corazón de la guía. Cada área incluye acciones concretas en dos listas: lo que debe hacer y lo que debe evitar. Las acciones principales indican su costo aproximado: [Gratis], [Costo bajo] (unos pocos balboas al mes por equipo o usuario) o [Costo medio] (requiere contratar a un proveedor).

Si aún no lo hizo, complete primero la autoevaluación del capítulo 8: le dirá cuáles de estas diez áreas son sus prioridades.

### 5.1 CUENTAS Y CONTRASEÑAS (GESTIÓN DE IDENTIDADES)

Las contraseñas débiles y el mal manejo de credenciales son la puerta de entrada más común de los atacantes.

### QUÉ HACER

- Use contraseñas largas (mínimo 12 caracteres) y distintas para cada servicio. Una frase fácil de recordar y difícil de adivinar funciona mejor que una palabra con números.

- Adopte un **gestor de contraseñas**: una aplicación que genera y guarda contraseñas seguras para todo el equipo, cifradas y sin necesidad de memorizarlas. Existen opciones gratuitas y de pago, integradas en los navegadores o como aplicaciones dedicadas. Para empezar, elija una, cree una contraseña maestra larga y única, y cargue las cuentas del negocio a medida que las usa: no hace falta migrar todo el primer día. [Gratis o costo bajo]

- Active la **verificación en dos pasos (MFA)** en todo servicio que lo permita: correo, banca, WhatsApp, redes sociales, sistemas de la empresa. Según Microsoft, las cuentas con esta protección son 99.9 % menos propensas a ser comprometidas. Prefiera las aplicaciones de autenticación o las llaves físicas; el SMS es la opción menos segura, pero siempre mejor que nada. [Gratis]

- Cambie de inmediato toda contraseña ante la menor sospecha de compromiso, y las contraseñas predeterminadas de cualquier equipo o sistema nuevo desde el primer día.

- Mantenga un inventario de cuentas: quién tiene acceso a qué, y elimine los accesos el mismo día en que un colaborador deja la empresa. [Gratis]

- Si en el local varias personas usan la misma computadora, cree una cuenta de usuario distinta para cada quien (o al menos separe una cuenta de caja de una de administración), en lugar de compartir un único inicio de sesión. Así sabrá quién hizo qué, dará a cada persona solo los permisos que necesita y, cuando alguien se vaya, bastará con desactivar su cuenta. Configure el bloqueo automático de pantalla por inactividad. [Gratis]

**Cuando un colaborador deja la empresa (especialmente si la salida es conflictiva).**

El mismo día de la salida: cambie las contraseñas de las cuentas compartidas que esa persona conocía (correo, redes sociales, banca, sistemas del negocio); revoque su acceso al correo, a los archivos en la nube y a los grupos de mensajería del negocio; recupere los equipos y llaves entregados; y revise que no queden reglas de reenvío automático de correo creadas por esa persona. Si manejaba datos de clientes o dinero, vigile durante las semanas siguientes los movimientos o accesos inusuales. Deje constancia por escrito de la entrega de equipos y del cese de accesos.

### QUÉ NO HACER

- No reutilice contraseñas entre servicios.
- No comparta contraseñas por correo, mensajes ni notas adhesivas.
- No use datos personales (mascotas, fechas, "123456") como contraseña.
- No guarde contraseñas en archivos de texto ni en papel a la vista.
- No dependa solo de preguntas de seguridad: sus respuestas suelen ser públicas o fáciles de adivinar.

## 5.2 DISPOSITIVOS: COMPUTADORAS, TELÉFONOS Y TABLETAS

Todo dispositivo conectado a la red de la empresa es un punto de acceso potencial para un atacante.

### QUÉ HACER

- Configure **actualizaciones automáticas** en sistemas operativos, navegadores, aplicaciones de oficina y en el propio router. Muchas de las vulnerabilidades más explotadas tienen años de antigüedad y parche disponible: los atacantes cuentan con que usted no actualice. En computadoras y teléfonos, la opción está en el apartado de actualización o seguridad de la configuración; actívela para que el equipo se actualice solo, idealmente fuera del horario de trabajo. [Gratis]

- Instale **antivirus con protección contra ransomware** en todos los equipos, con escaneo en tiempo real y actualizaciones automáticas. [Costo bajo]
- Proteja los teléfonos y tabletas del negocio: bloqueo con PIN o biometría, cifrado activado, posibilidad de borrado remoto en caso de robo y aplicaciones solo de tiendas oficiales.

- Cifre los discos de las computadoras portátiles: si roban el equipo, no se llevan la información. Esta función viene incluida en los sistemas operativos modernos; búsquela en el apartado de seguridad o privacidad de la configuración, bajo el nombre de cifrado de disco o cifrado del dispositivo, y actívela. En muchos teléfonos ya está activa de fábrica cuando se usa un PIN o biometría. [Gratis]

- Separe lo personal de lo laboral: si los colaboradores usan sus propios equipos, establezca reglas mínimas (bloqueo, actualización, antivirus).

### QUÉ NO HACER

- No posponga actualizaciones: cada día sin actualizar es un día vulnerable.
- No desactive el antivirus "porque hace lento el equipo".
- No conecte a la red de la empresa dispositivos personales sin protección.
- No use memorias USB de origen desconocido.
- No ignore las alertas de seguridad del sistema o del antivirus.

### 5.3 LA RED DE LA EMPRESA E INTERNET

La red es el sistema nervioso del negocio: si un intruso entra en ella, alcanza todo lo que está conectado.

#### QUÉ HACER

- Proteja el wifi con cifrado WPA3 (o WPA2 como mínimo) y cambie la contraseña predeterminada del router, tanto la de la red como la del panel de administración. [Gratis]

- Cree una **red de invitados** separada para clientes y visitantes: nadie ajeno al negocio debe navegar en la misma red donde están sus sistemas.

- Si la empresa tiene varias áreas (ventas, administración, cámaras, impresoras), pida a su proveedor de tecnología **segmentar la red**: si un sector se ve comprometido, los demás quedan protegidos. Pídalo explícitamente y guarde constancia de que quedó configurado. [Costo medio]

- Use un **firewall** (cortafuegos): la mayoría de los routers y sistemas operativos lo incluyen; asegúrese de que esté activado.

- Desactive la función de conexión rápida del router (conocida como WPS) y, si el equipo lo permite, oculte el nombre de la red principal del negocio (SSID).

- Para trabajar desde fuera de la oficina, use una **VPN** (conexión cifrada) en lugar de exponer los sistemas directamente a internet.

#### QUÉ NO HACER

- No deje el router con las credenciales de fábrica.
- No use redes wifi públicas (aeropuertos, cafés) para operaciones sensibles sin VPN.
- No conecte cámaras u otros equipos “inteligentes” sin cambiarles la contraseña.
- No exponga a internet sistemas internos (escritorio remoto, cámaras) sin protección.

### 5.4 EL CORREO ELECTRÓNICO DE LA EMPRESA

El correo es la vía de entrada del phishing y la llave maestra de sus demás cuentas.

#### QUÉ HACER

- Use correo corporativo con dominio propio y active los filtros contra correo fraudulento que ofrece su proveedor.

- Active la verificación en dos pasos en todas las casillas, empezando por gerencia, contabilidad y quien maneje pagos.

- Configure una alerta visible en los correos que llegan desde fuera de la empresa (etiqueta de “remitente externo”).

- Pida a su proveedor de tecnología configurar las protecciones del dominio contra suplantación (conocidas como SPF, DKIM y DMARC): evitan que otros envíen correos falsos “a nombre de” su empresa. Pídalo explícitamente y guarde constancia de que quedó configurado. [Costo bajo]

- Defina la regla de oro de pagos: ningún cambio de cuenta bancaria ni transferencia se ejecuta por una simple instrucción por correo o mensaje; siempre se confirma por un segundo canal.

#### QUÉ NO HACER

- No haga clic en enlaces ni abra adjuntos de correos inesperados, aunque parezcan venir de conocidos.
- No responda correos sospechosos ni “verifique datos” desde sus enlaces.
- No use la casilla corporativa para registros personales.
- No confíe en el nombre visible del remitente: puede falsificarse; revise la dirección completa.

# 6. PLAN DE ACCIÓN POR FASES

No intente hacerlo todo a la vez. Este plan ordena las medidas por urgencia e impacto, comenzando por las que no cuestan dinero.

## SI SU NEGOCIO ES PEQUEÑO O NO TIENE PERSONAL DE TECNOLOGÍA

Gran parte de esta guía se aplica sin un técnico de planta. Donde el plan menciona TI, entienda: usted mismo o el proveedor de tecnología que contrate por horas; en negocios pequeños, todos los roles de la columna Responsable pueden recaer en el dueño.

Para un negocio de una a tres personas, concéntrese primero en cinco medidas que no requieren conocimientos técnicos: (1) active la verificación en dos pasos en su correo, su banca y sus aplicaciones de mensajería; (2) use contraseñas largas y distintas, guardadas en un gestor de contraseñas; (3) active las actualizaciones automáticas en el teléfono y la computadora; (4) haga una copia de seguridad automática en la nube y una segunda copia en un disco que mantenga desconectado; y (5) verifique todo pago por un segundo canal.

Con estas cinco medidas, aplicables en una tarde y con costo cercano a cero, su negocio queda mejor protegido que la mayoría. Para las tareas que sí requieren un técnico (segmentar la red, configurar las protecciones del dominio del correo), contrate un proveedor formal y puntual: la sección 5.10 explica cómo elegirlo.

## FASE 1 – ACCIONES URGENTES (PRIMERA SEMANA)

| # | Acción | Costo | Responsable |
|---|---|---|---|
| 1 | Activar la verificación en dos pasos en el correo de la empresa, la banca en línea y WhatsApp | Ninguno | Gerencia |
| 2 | Cambiar toda contraseña débil, repetida o compartida, empezando por correo y banca | Ninguno | Todos |
| 3 | Hacer una copia de seguridad completa de la información crítica y desconectarla de la red | **Bajo** | Gerencia / TI |
| 4 | Activar las actualizaciones automáticas en todos los equipos | Ninguno | TI / Cada usuario |
| 5 | Cambiar las contraseñas predeterminadas del router y crear red de invitados | Ninguno | TI |
| 6 | Comunicar al equipo la regla de oro: ningún pago ni cambio de cuenta sin verificación por segundo canal | Ninguno | Gerencia |
| 7 | Definir a quién se reporta cualquier correo o mensaje sospechoso | Ninguno | Gerencia |

## FASE 2 – PRIMER MES

| Área | Acción | Responsable |
|---|---|---|
| **Identidades** | Implementar un gestor de contraseñas para todo el equipo | Gerencia / TI |
| **Dispositivos** | Instalar antivirus con protección contra ransomware en todos los equipos | TI |
| **Correo** | Configurar filtros contra fraude y alerta de remitente externo; protecciones del dominio (SPF, DKIM, DMARC) | TI / Proveedor |
| **Datos** | Clasificar la información por nivel de sensibilidad | Todas las áreas |
| **Respaldos** | Establecer la rutina automática con la regla 3-2-1 | TI |
| **Personas** | Realizar la primera sesión de concientización sobre phishing y fraudes por WhatsApp | Gerencia / RR. HH. |
| **Legal** | Revisar el cumplimiento de la Ley 81: consentimientos, aviso de privacidad, canal ARCO | Gerencia / Legal |

### FASE 3 — DE TRES A SEIS MESES

**Implementaciones técnicas:** segmentación de la red por áreas, monitoreo básico de actividad sospechosa (intentos de acceso fallidos, accesos desde ubicaciones inusuales), cifrado de datos sensibles, protección específica de dispositivos móviles y control de acceso por roles.

**Procesos y políticas:** política de contraseñas y accesos, manual breve de respuesta a incidentes (capítulo 7), protocolo de preservación de evidencia digital (Ley 478), programa trimestral de capacitación con simulacros de phishing y auditoría interna de cumplimiento de la Ley 81.

**Evaluación:** prueba real de restauración de respaldos, evaluación de un seguro cibernético y, si el presupuesto lo permite, una revisión de vulnerabilidades por un tercero confiable.

### FASE 4 — MANTENIMIENTO CONTINUO

- **Cada mes:** revisar alertas y registros, verificar respaldos, enviar un recordatorio breve de seguridad al equipo.
- **Cada trimestre:** capacitación formal, prueba de restauración de respaldos, revisión de accesos y permisos, simulacro de phishing.
- **Cada año:** revisión completa de políticas, evaluación de cumplimiento legal (leyes 81 y 478), análisis de riesgos actualizado y presupuesto de ciberseguridad del año siguiente.

# 7. ¿Y SI YA OCURRIÓ?

## RESPUESTA A INCIDENTES PASO A PASO

Un incidente no manejado a tiempo multiplica el daño. Imprima esta página y téngala a mano.

## PRIMERAS HORAS

1. **Mantenga la calma y no apague todo de inmediato.** Desconecte de la red (cable y wifi) los equipos afectados, pero no los formatee ni borre nada: destruiría la evidencia que exige la Ley 478 y que necesitará el banco, el seguro o el perito.
2. **Contenga el acceso:** cambie desde un equipo limpio las contraseñas de las cuentas posiblemente comprometidas, empezando por el correo y la banca, y cierre las sesiones abiertas.
3. **Si hay dinero involucrado, llame primero al banco:** solicite el bloqueo o la retención de las transferencias; los primeros minutos son críticos.
4. **Registre todo:** hora de detección, qué se observó, capturas de pantalla, correos originales (no los reenvíe: guárdelos), números de transacción.

## PRIMEROS DÍAS

1. **Evalúe el alcance:** qué sistemas y qué datos se vieron afectados; si hay datos personales de clientes involucrados, recuerde sus obligaciones ante la ANTAI y con los afectados.
2. **Denuncie:** presente la denuncia ante el Ministerio Público y reporte el incidente al CSIRT Panamá, que orienta y coordina la respuesta.
3. **Busque apoyo técnico especializado** para erradicar la amenaza, verificar los respaldos y restaurar la operación de forma segura.
4. **Comunique con honestidad:** a su equipo y, cuando corresponda, a los clientes afectados. Ocultar un incidente que luego sale a la luz daña mucho más la reputación que informarlo con transparencia.

## DESPUÉS

1. **Restaure desde respaldos limpios** y verifique que la puerta de entrada quedó cerrada (parche aplicado, contraseñas cambiadas, accesos revisados).
2. **Aprenda del incidente:** qué falló y qué medida lo habría evitado; luego ajuste lo necesario. Un incidente bien gestionado deja a la empresa más fuerte.

**En caso de ransomware**

La recomendación general es no pagar el rescate: no garantiza recuperar la información, marca a la empresa como pagadora y financia al crimen organizado. Con respaldos fuera de línea probados, el rescate pierde su poder.

# 8. AUTOEVALUACIÓN RÁPIDA

**Responda sí o no. Cada "no" es una tarea pendiente con su capítulo de referencia.**

| # | Pregunta | Sí | No | Capítulo |
|---|---|---|---|---|
| 1 | ¿La verificación en dos pasos está activa en el correo, la banca y WhatsApp del negocio? | ☐ | ☐ | 6.1, 6.8 |
| 2 | ¿Cada cuenta importante tiene una contraseña única y robusta? | ☐ | ☐ | 6.1 |
| 3 | ¿Los equipos y el router se actualizan automáticamente? | ☐ | ☐ | 6.2, 6.8 |
| 4 | ¿Todos los equipos tienen antivirus activo con protección contra ransomware? | ☐ | ☐ | 6.2 |
| 5 | ¿Existe una copia de seguridad automática, con una copia fuera de línea? | ☐ | ☐ | 6.6 |
| 6 | ¿Se probó la restauración de esa copia en los últimos tres meses? | ☐ | ☐ | 6.6 |
| 7 | ¿El WiFi de clientes está separado del de la empresa? | ☐ | ☐ | 6.3 |
| 8 | ¿El equipo sabe reconocer un correo o mensaje fraudulento y a quién reportarlo? | ☐ | ☐ | 6.7 |
| 9 | ¿Los pagos y cambios de cuenta se verifican siempre por un segundo canal? | ☐ | ☐ | 6.8 |
| 10 | ¿Los accesos de excolaboradores se eliminan el mismo día de su salida? | ☐ | ☐ | 6.1, 6.8 |
| 11 | ¿La empresa cuenta con aviso de privacidad y canal para derechos ARCO (Ley 81)? | ☐ | ☐ | 2.1 |
| 12 | ¿Existen protocolos básicos para conservar evidencias ante un incidente (Ley 81)? | ☐ | ☐ | 2.2, 7 |
| 13 | ¿La información sensible está clasificada y cifrada? | ☐ | ☐ | 6.5 |
| 14 | ¿Los accesos de proveedores externos están limitados y controlados? | ☐ | ☐ | 6.10 |
| 15 | ¿La gerencia revisa el tema de ciberseguridad al menos una vez por trimestre? | ☐ | ☐ | 8 |

**Lectura del resultado:** de 12 a 15 respuestas afirmativas, su empresa tiene una base sólida: manténgala y profundice con la fase 3. De 7 a 11, hay avances pero quedan brechas importantes: priorice los "no" de los capítulos 5.1, 5.6 y 5.8. Menos de 7: su negocio está expuesto; comience hoy mismo con la fase 1 del plan de acción.

# 9. RECURSOS

## Y LUGARES OFICIALES DE CONSULTA

Todos los recursos de este capítulo son gratuitos, salvo indicación en contrario.
Las direcciones completas están en las notas al pie.

## INSTITUCIONES PANAMEÑAS

**ANTAI — Autoridad Nacional de Transparencia y Acceso a la Información.** Autoridad de control de la Ley 81. Difunde guías prácticas de cumplimiento, incluida una guía específica para el sector privado, y recibe denuncias por uso indebido de datos personales.

**CSIRT Panamá (AIG).** Equipo nacional de respuesta a incidentes. Reciba sus avisos de seguridad y, ante un incidente, repórtelo al correo oficial incidentes@cert.pa.

**Panamá Cibersegura.** Campaña nacional de concienciación de la AIG, con material educativo gratuito y el compendio de la legislación aplicable.

**Ministerio Público.** Orientación oficial para denunciar delitos informáticos (fraude, suplantación, extorsión); cuenta con una fiscalía especializada en seguridad informática.

**AMPYME — Autoridad de la Micro, Pequeña y Mediana Empresa.** Registro empresarial gratuito y capacitaciones sin costo para emprendedores a través de su plataforma en línea.
**INADEH.** Cursos gratuitos de informática con certificado, con preinscripción en línea.

**Superintendencia de Bancos de Panamá.** Educación financiera, prevención del fraude y canal de atención al cliente bancario.

**Su banco.** Tenga a mano el teléfono oficial de atención de fraudes: en un incidente financiero es la primera llamada.

**CAPATEC — Comité Técnico de Ciberseguridad.** Canal gremial para orientación, capacitación y vinculación con el ecosistema tecnológico panameño.

### RECURSOS INTERNACIONALES GRATUITOS EN ESPAÑOL

**Kit de Ciberseguridad para Pequeñas Empresas — Global Cyber Alliance.** Herramientas gratuitas organizadas en seis pasos, pensadas para negocios sin personal técnico.

**INCIBE (España) — Protege tu Empresa.** Más de treinta plantillas descargables de políticas de seguridad listas para adaptar, y un kit de concienciación con videos, carteles y ejercicios para capacitar al personal.

**NIST — Guía de inicio rápido del Marco de Ciberseguridad 2.0 para pequeñas empresas.** Publicación oficial en español para organizar la gestión del riesgo digital.

**OEA/CICTE — Programa de Ciberseguridad.** Publicaciones en español sobre seguridad digital para la región.

## MARCOS DE REFERENCIA

Para empresas que deseen ir más allá de lo básico: ISO/IEC 27001 (gestión de seguridad de la información), Marco de Ciberseguridad del NIST y controles CIS, cuyo grupo de implementación 1 está pensado como higiene básica para organizaciones con recursos limitados.

# 10. GLOSARIO
## EN LENGUAJE SIMPLE

**Antivirus / antimalware:** programa que detecta y bloquea software malicioso.

**Cifrado:** técnica que convierte la información en un código ilegible para quien no tenga la clave. Si roban el equipo o interceptan el mensaje, no pueden leerlo.

**Derechos ARCO:** derechos de Acceso, Rectificación, Cancelación y Oposición que la Ley 81 otorga a las personas sobre sus datos personales.

**Firewall (cortafuegos):** barrera que controla qué entra y qué sale de una red o un equipo.

**Fraude del CEO / correo empresarial comprometido:** engaño en el que el delincuente se hace pasar por un directivo o proveedor para desviar pagos.

**Gestor de contraseñas:** aplicación que crea y guarda contraseñas seguras, cifradas, para no tener que memorizarlas ni repetirlas.

**Ingeniería social:** manipulación psicológica para que una persona entregue información o realice acciones que benefician al atacante.

**Malware:** cualquier programa malicioso (virus, troyanos, espías, secuestradores).

**Pasarela de pago:** servicio que procesa los cobros con tarjeta en su tienda en línea, para que usted no tenga que guardar los datos de las tarjetas de sus clientes.

**Phishing:** correos o mensajes que suplantan a entidades legítimas para robar datos o instalar malware. Por SMS se conoce como smishing; por llamada, vishing.

**Punto de venta / datáfono:** el equipo con el que se cobran los pagos con tarjeta en el local.
**Ransomware:** malware que secuestra (cifra) la información y exige un rescate.

**Red de invitados:** red wifi separada para visitantes, sin acceso a los sistemas del negocio.

**Regla 3-2-1:** estrategia de respaldo: 3 copias, en 2 medios distintos, con 1 fuera del sitio.

**Segundo canal:** verificación de una instrucción por una vía distinta de la que llegó (por ejemplo, llamar al número conocido de un proveedor para confirmar un correo).

**SPF, DKIM y DMARC:** configuraciones técnicas del correo que impiden que otros envíen mensajes falsos a nombre de su empresa. Se solicitan al proveedor de tecnología; no necesita entender el detalle, solo pedir que estén activas.

**SSID:** el nombre con el que aparece su red wifi.

**Troyano bancario:** programa espía diseñado para robar credenciales de banca en línea.
Verificación en dos pasos (MFA): protección que exige, además de la contraseña, un segundo factor (código de una aplicación, llave física o biometría) para entrar a una cuenta.

**VPN:** conexión cifrada que protege la comunicación cuando se trabaja fuera de la oficina o en redes públicas.

**WPA2 / WPA3:** los estándares que cifran la red wifi. WPA3 es el más nuevo y seguro; WPA2 es el mínimo aceptable.

**WPS:** función de conexión rápida del router que conviene desactivar por ser insegura.

# 11. CONCLUSIÓN

## LA CIBERSEGURIDAD ES INVERSIÓN, NO GASTO

Proteger una PYME no exige presupuestos millonarios; exige decisión y constancia. Las medidas de mayor impacto de esta guía —verificación en dos pasos, respaldos fuera de línea, actualizaciones, capacitación y verificación de pagos— cuestan poco o nada, y juntas eliminan la mayoría de los riesgos que hoy golpean a las empresas panameñas.

Recuerde los puntos clave:

- **Su empresa sí es un objetivo.** Los ataques son masivos y no distinguen tamaño.
- **El cumplimiento legal es obligatorio.** Las leyes 81 y 478 imponen deberes reales, con sanciones reales, y la responsabilidad recae en la gerencia.
- **Las personas son la primera línea de defensa.** Capacite, simule, reconozca.
- **Los respaldos son su póliza de vida** frente al ransomware y las catástrofes.
- **La seguridad es un hábito, no un proyecto.** Se sostiene con rutinas mensuales, trimestrales y anuales.

**El primer paso, ahora mismo**

No espere a ser víctima. Complete la autoevaluación del capítulo 8 y ejecute esta semana la fase 1 del plan de acción. Con solo activar la verificación en dos pasos y asegurar sus respaldos, su empresa quedará mejor protegida que la mayoría.

**SU NEGOCIO, SUS CLIENTES Y SU FUTURO LO VALEN.**

# ANEXO A Hoja de emergencia: si está pasando ahora

Imprima esta hoja, complete los teléfonos y téngala visible cerca de la caja o la gerencia.

## Teléfonos que debe tener listos (complete a mano)

**Banco del negocio — atención de fraudes 24 horas:** _____

**Segundo banco (si aplica):** _____

**Proveedor de tecnología / soporte:** _____

**Responsable interno (gerente o dueño):** _____

**CSIRT Panamá:** incidentes@cert.pa | cert.pa

**Ministerio Público (denuncia de delitos informáticos):** _____

**Corredor o compañía del seguro cibernético (si tiene póliza):** _____

## Qué hacer en los primeros 30 minutos

1. Mantenga la calma. No apague ni formatee los equipos: destruiría la evidencia. Solo desconéctelos de internet (cable y wifi).
2. Si hay dinero de por medio, llame primero a su banco y pida el bloqueo o la retención de las transferencias: los primeros minutos son decisivos.
3. Desde un equipo distinto y limpio, cambie las contraseñas de las cuentas comprometidas, empezando por el correo y la banca, y cierre las sesiones abiertas.
4. Anote todo: hora de detección, qué observó, capturas de pantalla, correos originales (guárdelos, no los reenvíe) y números de transacción.

## En las horas siguientes

1. Avise al responsable interno y al proveedor de tecnología.
2. Evalúe qué sistemas y qué datos se vieron afectados. Si hay datos de clientes, prepare la comunicación a los afectados y a la ANTAI.
3. Presente la denuncia ante el Ministerio Público y reporte el incidente al CSIRT Panamá.
4. No pague ningún rescate sin buscar antes apoyo especializado: pagar no garantiza recuperar la información.

**Fecha del incidente:** _____ **Quién lo detectó:** _____ **Quién coordina:** _____

ANEXO B

# Checklist mensual del dueño

Dedique quince minutos al mes a revisar estos diez puntos. Marque cada uno.

1. ☐ Se hicieron las copias de seguridad y la última se completó sin errores.
2. ☐ Los equipos y teléfonos del negocio están actualizados, sin pendientes.
3. ☐ Revisé los accesos: nadie que se haya ido conserva cuentas activas; nadie tiene más permisos de los que necesita.
4. ☐ La verificación en dos pasos sigue activa en correo, banca y redes del negocio.
5. ☐ Revisé los movimientos bancarios del mes en busca de cargos que no reconozco.
6. ☐ No hay contraseñas anotadas a la vista ni cuentas compartidas nuevas sin control.
7. ☐ Envié al equipo un recordatorio breve de seguridad (por ejemplo, la regla del pago verificado o la del comprobante falso).
8. ☐ Revisé si aparecieron perfiles falsos de mi negocio en redes sociales.
9. ☐ El antivirus está activo en todos los equipos y no hay alertas sin atender.
10. ☐ Una vez por trimestre, además: probé restaurar una copia de seguridad; y una vez al año, revisé el cumplimiento de la Ley 81.

**Mes revisado:** _____ **Pendientes para el próximo mes:** _____

ANEXO C

# Reglas de oro para el personal

Reparta o pegue esta tarjeta en los puestos de trabajo.

1. Ante un pago o un cambio de cuenta bancaria, confirme siempre por un segundo canal (una llamada al número ya conocido), aunque la orden parezca venir del jefe. Sin verificar, no se paga.
2. Sin dinero acreditado en la cuenta de la empresa, no sale mercancía. Una captura de pantalla no es un pago.
3. Nunca comparta contraseñas ni códigos de verificación con nadie, por teléfono, mensaje o correo. Ninguna entidad seria los pide.
4. No haga clic en enlaces ni abra archivos de correos o mensajes inesperados, aunque parezcan de un conocido.
5. Use una contraseña larga y distinta para cada cuenta, y active la verificación en dos pasos.
6. Bloquee la pantalla cada vez que se aleje de su equipo.
7. Si algo le parece raro o cometió un error, repórtelo de inmediato a: _____. No hay castigo por avisar a tiempo: el silencio es lo que hace daño.

**Reportar lo sospechoso a tiempo es lo que salva a la empresa.**

## REFERENCIAS


- Ley 81 de 26 de marzo de 2019, sobre protección de datos personales. Gaceta Oficial 28743-A.
- Decreto Ejecutivo 285 de 28 de mayo de 2021, que reglamenta la Ley 81 de 2019. Gaceta Oficial 29296-A.
- Ley 478 de 4 de agosto de 2025, sobre medidas contra la ciberdelincuencia. Gaceta Oficial 30337 de 5 de agosto de 2025.
- IBM. Cost of a Data Breach Report 2025.
- CSIRT Panamá: estadísticas de incidentes 2024 (cert.pa).
- Cifras regionales de la industria de ciberseguridad sobre América Latina (encuestas sectoriales 2024-2025).


*Esta guía tiene propósito informativo y educativo, y refleja el estado del marco legal y de las amenazas a la fecha de su edición.*

*Para asesoría legal específica, consulte con un profesional especializado en derecho tecnológico y protección de datos. Documento elaborado por el Comité Técnico de Ciberseguridad de CAPATEC; se permite su distribución con fines educativos citando la fuente.*

CAPATEC
CÁMARA PANAMEÑA DE TECNOLOGÍAS DE INFORMACIÓN, INNOVACIÓN Y TELECOMUNICACIONES

## AVISO DE PROPIEDAD INTELECTUAL, USO Y PROTECCIÓN DEL DOCUMENTO

Este documento y sus contenidos originales son de titularidad exclusiva de CAPATEC y del Comité Técnico de Ciberseguridad de la Cámara. Todos los derechos quedan reservados. Los materiales de terceros que pudieran incorporarse conservan la titularidad y las condiciones de uso correspondientes.

### RESTRICCIONES DE USO.

Salvo autorización previa, expresa y por escrito de los titulares, o los usos permitidos por la legislación aplicable, queda prohibida la reproducción, distribución, publicación, comercialización, modificación o transmisión total o parcial de este documento, por cualquier medio. El acceso o la entrega de una copia no implica la cesión de derechos de propiedad intelectual ni el otorgamiento de una licencia de explotación.

### INTEGRIDAD Y ATRIBUCIÓN.

No se permite eliminar los avisos de autoría, alterar el contenido de forma que desvirtúe su sentido ni atribuir a CAPATEC o a su Comité Técnico de Ciberseguridad conclusiones o recomendaciones que no hayan aprobado expresamente.

Todo uso autorizado deberá conservar los créditos y los avisos de protección correspondientes.

### ALCANCE Y LIMITACIÓN DE RESPONSABILIDAD.

El contenido tiene fines informativos y de orientación general. No sustituye una evaluación técnica, jurídica o profesional adaptada a cada situación.

Aunque se procura su precisión, no se garantiza que la información sea exhaustiva, permanezca actualizada o resulte adecuada para todos los contextos.

Las recomendaciones no garantizan la ausencia de incidentes de ciberseguridad. Dentro de los límites permitidos por la legislación aplicable, CAPATEC y su Comité Técnico de Ciberseguridad no asumirán responsabilidad por daños derivados del uso indebido del documento o de decisiones adoptadas sin una evaluación independiente.

### RESERVA DE DERECHOS.

Cualquier uso no autorizado podrá dar lugar al ejercicio de las acciones que correspondan conforme a la legislación aplicable.

© CAPATEC y Comité Técnico de Ciberseguridad de la Cámara.

Todos los derechos reservados.