Guía de Buenas Prácticas
de Ciberseguridad

PyMEs, emprendimientos y comercios electrónicos

Buenos Aires Ciudad

Vamos por más

1 INTRODUCCIÓN

¿Alguna vez te preguntaste si tu PyME debería preocuparse por la ciberseguridad?

Es común pensar *"a mí no me va a pasar"* o "*protegerse es demasiado caro"*. Pero la realidad es otra: los ciberataques no tienen que ver con la suerte, sino con el tiempo.

Según datos del Microsoft Security Blog (investigación Microsoft + Bredin, 2024), **1 de cada 3 PyMEs sufrió un ciberataque en 2024**, y el costo promedio por incidente puede superar los 250.000 USD, una cifra que para muchas empresas significa cerrar definitivamente.

La buena noticia es que empezar a proteger tu negocio no requiere grandes inversiones. **Desde BA-CSIRT desarrollamos esta guía con buenas prácticas simples, accesibles y de muy bajo costo -por no decir gratuitas- para que puedas implementar medidas efectivas de ciberseguridad hoy mismo.**

2 CULTURA DE LA CIBERSEGURIDAD

Muchas veces se piensa que la seguridad depende únicamente de herramientas técnicas, como tener el mejor antivirus o el firewall más avanzado. Sin embargo, la parte más importante -y **la base de toda estrategia de ciberseguridad son las personas.**

Podés tener la puerta más segura del mundo, con la cerradura más resistente. Pero si alguien se la abre a un desconocido que dice ser el cartero, ni la puerta ni la cerradura sirven de nada. En el mundo digital pasa exactamente lo mismo. Por eso, antes de hablar de medidas técnicas, **es clave entender la importancia de construir una cultura de seguridad dentro de la empresa**.

2.1 ¿Qué es una cultura de seguridad?

No es algo técnico, sino un hábito: incorporar la protección en la rutina de trabajo. Del mismo modo que seguís procedimientos diarios, la idea es que cuidar la seguridad de la empresa también sea una costumbre. **La ciberseguridad no se hace una sola vez: es un esfuerzo constante, consciente y compartido.**

2.2 ¿Cómo creamos esta cultura?

1. Dar el ejemplo desde arriba

Si los líderes no cumplen las prácticas, el resto del equipo tampoco lo hará. Todos, sin importar su rol, deben seguir las mismas reglas.

2. Explicar y enseñar, no imponer

No alcanza con decir “a partir de ahora todos tienen que hacer esto”. Es necesario mostrar cómo hacerlo y para qué es importante.

- Cómo: capacitaciones prácticas, guías simples, demostraciones.
- Para qué: entender los riesgos reales y los beneficios de aplicar buenas prácticas.

Cuando el equipo entiende el cómo y el para qué, la adopción se vuelve mucho más fácil.

3. Fomentar la cultura del reporte y del “cero culpa”

El tiempo es crítico para resolver un incidente. Si alguien comete un error (por ejemplo, hace clic en un enlace malicioso), debe sentirse seguro para reportarlo sin miedo a sanciones.

- “Cero culpa”: promover un entorno donde el error se corrige, no se castiga.
- Canales claros: crear medios simples (correo, formulario interno, chat, etc.) para informar problemas.

4. Practicar la desconfianza saludable

En el mundo digital, no todo lo que parece confiable lo es. Los ciberdelincuentes utilizan técnicas de ingeniería social para engañar y lograr que alguien les facilite información o realice acciones riesgosas.
Por eso, adoptar el hábito de verificar antes de confiar es importante. Algunas señales de alerta comunes:

- Correos, mensajes o llamadas con pedidos inusuales, como transferencias o solicitud de datos sensibles.
- Urgencias o presiones para actuar rápido, especialmente cerca del cierre de jornada o en horarios críticos.

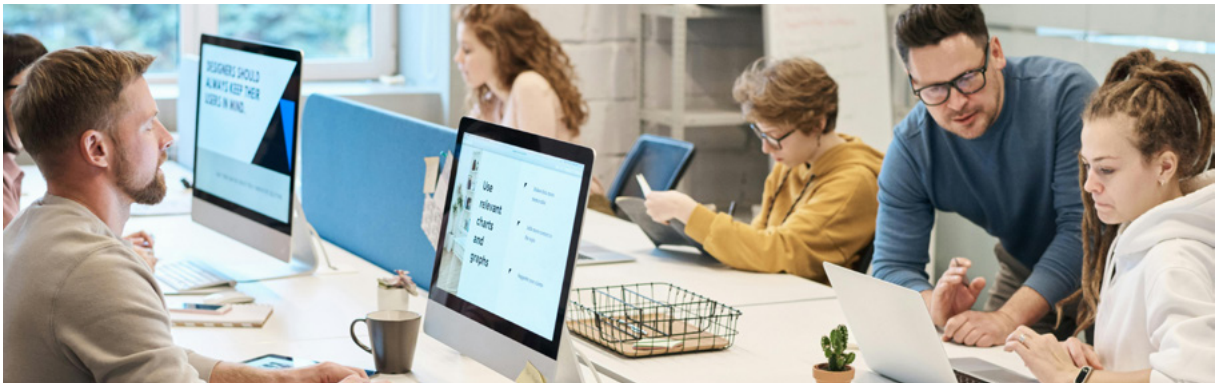
¿Qué hacer ante la duda?

Verificar la solicitud por otro medio. Por ejemplo, si recibís un correo sospechoso de un proveedor, contáctalo por teléfono o mensaje directo antes de realizar cualquier acción. **Esta simple verificación puede evitar un ciber incidente.** Mejor tardar un poco más que exponerse a un ataque cibernético.

5. Habito de preguntar

Muchas veces, alguien no sabe cómo hacer una tarea y por vergüenza o miedo prefiere no preguntar. Esto puede traer consecuencias. Por eso, es importante mostrar que siempre es mejor consultar y aprender bien que avanzar con dudas.

En resumen, **la clave de una buena cultura de ciberseguridad es lograr que cada persona incorpore estos hábitos en su día a día. Que se sienta segura y cómoda para preguntar o reportar algo sin temor.** Y eso se construye brindando lineamientos claros, explicando su importancia y acompañando esas prácticas con capacitación y buen ejemplo.



3. CONTRASEÑAS SEGURAS

3.1 ¿Qué son y por qué importan?

Las contraseñas **son como llaves digitales que protegen tus cuentas e información. Si es débil o cae en manos de un ciberdelincuente, puede tener consecuencias** como pérdida de datos, daño reputacional, problemas financieros e incluso interrupción de las actividades de tu empresa.

Igual que en la vida real no brinda la misma seguridad la llave de un candado de juguete que la de una bóveda, con las contraseñas pasa lo mismo. **Depende de vos elegir si usas una "llave" débil o una realmente segura.**

3.2 ¿Qué es una contraseña segura?

Para que una contraseña sea segura, debe ser:

1.Robusta

Evitá contraseñas fáciles de adivinar. No es lo mismo usar “el nombre de tu negocio” que “em-esc,lamnp2pqmapyvplJ.PshhSs24”.
La primera puede ser vulnerada en cuestión de segundos; la segunda tardaría muchísimo más en ser vulnerada.

2.Única

¿Usarías la misma llave para todas las puertas de tu casa y tu trabajo? No, ¿verdad? **Repetir contraseñas es una mala práctica:** si un ciberdelincuente obtiene una, accede al resto. Por eso, cada cuenta debe tener una propia.

3.Secreta, personal e intransferible

En muchas PyMEs es común “pasarse la contraseña” para resolver algo rápido, pero esto genera riesgos innecesarios.

La contraseña debe ser utilizada únicamente por su dueño. Compartirla -aunque sea con alguien de confianza o “solo por un momento”- aumenta el riesgo y dificulta saber quién realizó cada acción dentro de una cuenta o sistema.

Si otra persona necesita acceder, lo correcto es crearle un usuario propio o asignarle permisos temporales, aunque lleve un minuto más.

4.Almacenada de forma segura

Evitá anotarlas en cuadernos, post-its, lugares visibles o guardarlas en el navegador sin protección.

La opción más segura es usar gestores de contraseñas confiables que permiten crear, guardar y completar claves de manera segura.

3.3 Contraseñas robustas: qué hacer y qué no hacer

Qué NO hacer

- Dejar el usuario y contraseña que vienen por defecto.
- Usar datos personales (nombre, dirección, fecha de nacimiento, club favorito, etc.).
- Usar contraseñas comunes como “1234”, “qwerty”, “7777”.
- Seguir patrones obvios, como reemplazar siempre “a” por “4” o “s” por “5”, poner solo la primera letra en mayúscula o repetir un formato predecible.

Que SÍ hacer

- Usar métodos para crear contraseñas robustas, como:
- Frase de contraseña (passphrase):
- Convertí una frase en una contraseña usando iniciales, números y caracteres especiales.
- Ejemplo: “yo tomo café en el sillón rojo, mientras mi perro ronca” → “ytc,eesr,mmpr” → “ytc95,eesr,Mmpr!?”.
- Palabras aleatorias:
- Elegí al menos cuatro palabras sin relación entre sí y unilas con caracteres especiales.
- Ej.: “casa$torre%perro&hijo=calle”.
- Generadores aleatorios:
- Muchos gestores de contraseñas permiten crear claves totalmente aleatorias y seguras.
- Asegurarte de que la contraseña cumpla estos requisitos
- Tener al menos 15 caracteres.
- Combinar minúsculas y mayúsculas.
- Incluir números y caracteres especiales.

3.4 Segundo factor de autenticación (2FA)

Hoy no alcanza con tener una contraseña segura: siempre que sea posible, **es fundamental activar el MFA o segundo factor de autenticación (2FA).**

El 2FA es una capa extra de seguridad: además de la contraseña, se requiere un segundo paso para validar la identidad. **De esta forma, aunque alguien obtenga tu contraseña, no podrá acceder a tu cuenta.**

Algunas opciones son:

- Código por SMS o correo: es fácil de usar y compatible con la mayoría de los servicios. Aunque es menos seguro que otras opciones, es mejor que no usar 2FA.
- Aplicaciones de autenticación: son más seguras que los SMS o mails y también compatibles con la mayoría de las plataformas. Ejemplos: Google Authenticator y Microsoft Authenticator.

Regla fundamental

Nunca, bajo ninguna circunstancia, compartas los códigos de verificación con nadie. Si alguien te los pide, es una señal clara de intento de estafa.

4. GESTIÓN DE SOFTWARE

Los programas que utilizás -ya sean aplicaciones, sistemas operativos o dispositivos- no son perfectos. Con el tiempo se descubren fallas de seguridad que pueden ser aprovechadas por ciberdelincuentes.

Por eso, las empresas y organizaciones que desarrollan estos sistemas publican actualizaciones y parches de seguridad de manera constante.

Tu tarea es implementarlos para proteger los equipos y reducir riesgos.

4.1 Mantener actualizaciones al día

Es fundamental actualizar regularmente todos los equipos y aplicaciones, como:

- Sistemas operativos (Windows, Android, macOS, etc.).
- Navegadores y aplicaciones, tanto móviles como de escritorio.
- Antivirus y herramientas de seguridad.
- Dispositivos como routers, switches, terminales de pago u otros equipos del negocio.

Conviene tomarte el tiempo de revisar si hay actualizaciones disponibles y, si es posible, activar las actualizaciones automáticas.

Tené en cuenta que las actualizaciones no son para siempre: llega un momento en que un programa o dispositivo queda obsoleto y deja de recibir soporte.

Si estás usando una versión antigua que ya no recibe actualizaciones, lo más recomendable es migrar a una versión más nueva que sí tenga soporte activo.

4.2 Uso de licencias de software

En muchas PyMEs y emprendimientos es habitual usar software pirata para “ahorrar” o salir del paso. A simple vista parece funcionar, pero en realidad **representa un riesgo enorme para tu negocio.**

El software pirata suele venir modificado e incluir malware, incluso sin que lo notes. Además, al no recibir actualizaciones ni soporte, queda expuesto a vulnerabilidades que los atacantes pueden aprovechar con facilidad.

A esto se suma un punto importante: usar software sin licencia es una infracción de derechos de autor y puede generarte problemas legales.

Por eso, nunca es una opción segura. **Usar software legal no es solo cumplir una norma: es proteger tu empresa.**

5. GESTIÓN DE INFORMACIÓN

La información es uno de los activos más importantes de cualquier empresa. Desde datos de clientes hasta documentos internos, todo tiene valor. Si la información se pierde, se filtra o se modifica sin permiso, las consecuencias pueden ser graves.

Para protegerla, necesitamos tener en cuenta tres aspectos clave:

- quién puede acceder y qué puede hacer
- dónde y cómo se almacena esa información
- qué medidas se implementan para evitar pérdidas o alteraciones.

5.1 ¿Quién debería acceder a la información?

En muchas PyMEs es común que, por comodidad, todos tengan acceso a todo. Pero esto es una mala práctica que abre la puerta a errores, abusos e incidentes.

Para evitarlo, podés aplicar el principio de necesidad de saber. El nombre puede sonar técnico, pero la idea es simple:

Cada persona debe acceder solo la información que realmente necesita para su trabajo.

El acceso depende del rol y área que ocupa cada persona:

- Alguien de contaduría necesita acceso a las finanzas.
- De ventas, a los datos de los clientes.
- Y así con cada función dentro de la empresa.

La forma de otorgar ese acceso depende de dónde esté almacenada la información: un archivo compartido en la nube, un servidor interno o cualquier otra plataforma utilizada por la empresa.

Además de decidir quién accede, también es importante definir qué puede hacer cada persona con esa información. A esto se lo conoce como el principio de mínimo privilegio.

No todos necesitan editar, borrar o descargar; muchas veces, con solo ver es suficiente.

Asignar únicamente los permisos necesarios para cada rol ayuda a evitar errores, cambios no deseados e incidentes derivados de accesos excesivos.

Aplicar necesidad de saber y mínimo privilegio reduce riesgos sin afectar el trabajo diario.

5.2 ¿Dónde la almacenamos?

Para decidir dónde almacenar la información de tu empresa, debés considerar dos aspectos clave:

1. Seguridad

La información debe almacenarse en un entorno seguro, no al alcance de cualquiera. Para lograrlo, es importante aplicar medidas básicas, como:

- Usar contraseñas robustas,
- Establecer permisos de acceso adecuados,
- Y, si está en un dispositivo físico, mantenerlo resguardado en un lugar apropiado y seguro.

2. Disponibilidad

La información tiene que estar accesible cuando se la necesite y no depender de un único dispositivo ni de una sola persona.

Si todo está guardado en la computadora de un empleado, un pendrive o un disco externo, perder ese dispositivo significa también perder la información.

Una solución práctica es usar servicios en la nube que permiten subir archivos, compartirlos y definir permisos (ver, editar, comentar).

Si elegís esta opción: usá cuentas empresariales o, si no es posible, cuentas separadas de las personales. Esto protege la información del trabajo y facilita la gestión ante renuncias, despidos o licencias.

Si la información se almacena en medios físicos (computadoras, discos externos, USB), recordá que, si ese dispositivo se daña, se pierde o es robado, también se pierde su contenido.

Por eso es tan importante el siguiente punto: *las copias de seguridad.*

5.3 Copias de seguridad

Una copia de seguridad (o backup) es un respaldo adicional de la información importante, guardado en otro lugar. Esto permite recuperarla si la original se pierde, se altera o queda inaccesible por algún incidente.

La idea es tener la información protegida en más de un lugar para poder restaurarla sin complicaciones. **Un backup sencillo y frecuente puede evitar pérdidas y demoras innecesarias.**

Algunas recomendaciones:

- Si usás la nube, muchos servicios guardan versiones anteriores o incluyen opciones de recuperación. Igualmente, conviene tener un backup independiente por si hay problemas con el proveedor o la conexión.
- Si no usás la nube, es aún más importante hacer respaldos en un dispositivo externo, ya que estos medios no cuentan con protección automática.
- Guardá la copia en un lugar distinto al de la información original.
- Definí una frecuencia fija (diaria, semanal o mensual) para evitar copias desactualizadas.

Usá la regla 3-2-1:

Una buena práctica es aplicar la regla 3-2-1 al hacer copias de seguridad. **Esta regla indica que debés contar con tres copias de tu información: la original y dos respaldos adicionales.**

Esos respaldos deberían guardarse en dos tipos de soportes diferentes, por ejemplo, un disco externo y un servicio en la nube.

Además, al menos uno debe estar en un lugar físico distinto al de la información original, para protegerlo ante robos, incendios u otros incidentes que afecten el mismo espacio.

Mantener respaldos actualizados garantiza que, ante cualquier incidente, la información pueda recuperarse sin afectar la continuidad del negocio.

6 PAGOS Y TRANSFERENCIAS DIGITALES

Hoy en día, muchas PyMEs y emprendimientos reciben pagos a través de transferencias bancarias, billeteras virtuales y códigos QR. **Estos métodos son prácticos y rápidos, pero también pueden ser objetivos de fraudes.**

A continuación, te presentamos las situaciones más comunes y buenas prácticas para protegerte.

6.1 Transferencias y billeteras virtuales

Comprobantes de pago falsos:

Algunas personas utilizan comprobantes editados para simular un pago que nunca se realizó. Esto puede derivar en dos tipos de estafa:

- **Entrega del producto o servicio sin recibir el pago:** El "cliente" muestra un comprobante falso para retirar el producto o acceder a un servicio sin haber pagado.
- **Solicitud de reintegro por "monto mayor":** El comprobante falso indica un pago superior al real. Luego, el "cliente" pide que le devuelvas la diferencia. Como el pago nunca existió, terminás entregando dinero propio.

Siempre verificá la acreditación del pago dentro de la app o homebanking antes de entregar productos, brindar servicios o devolver dinero.

Cambio de CBU o alias mediante mensajes:

Otro fraude muy común ocurre cuando **un ciberdelincuente se hace pasar por un proveedor y pide que realices un pago a un CBU o alias distinto al habitual.**

Si recibís un pedido de pago inusual, confirmalo por otro medio (por ejemplo, por teléfono o mensaje directo).

Acceso no autorizado a la cuenta:

Los ciberdelincuentes buscan ingresar a cuentas bancarias o billeteras virtuales para pedir préstamos, mover dinero o vaciar fondos.

Por eso, es fundamental aplicar las prácticas mencionadas en esta guía:

- contraseñas robustas,
- MFA activado,
- no compartir usuarios,
- utilizar cuentas empresariales en lugar de personales.

Buenas prácticas para proteger tu negocio:

1. Verificar cualquier pedido de pago inusual
Si un proveedor, contador u organización solicita un pago urgente, fuera de lo habitual o a un CBU diferente, confirmalo por otro medio.

2. Confirmar que los pagos estén realmente acreditados
Nunca te guíes por capturas o mensajes. Revisá la acreditación dentro de la app o desde el homebanking antes de entregar productos, brindar un servicio o devolver dinero.

3. Evitar usar cuentas personales para el negocio
Separar las cuentas personales de las laborales evita confusiones, mejora el control y reduce riesgos.

4. Activar alertas de movimiento
La mayoría de las apps financieras notifican ingresos y egresos en tiempo real, lo que ayuda a detectar actividades sospechosas.

5. No compartir claves ni códigos de verificación
Si más de una persona necesita operar, cada una debe tener su propio usuario (si la plataforma lo permite).

6.2 Códigos QR

Los códigos QR se utilizan cada vez más para cobrar, compartir menús, dirigir a redes o compartir información. Justamente por este uso frecuente, también pueden convertirse en un objetivo de fraude.

Un riesgo común es el reemplazo del QR original por uno falso (QRishing), ya sea pegando otro por encima o sustituyéndolo por completo.

¿Por qué es un problema?

Un QR manipulado puede provocar:

- Desvío de pagos a cuentas ajenas
- Redirección a sitios fraudulentos que impersonan a tu negocio
- Robo de datos personales
- Descarga de archivos o aplicaciones maliciosas (malware).

Esto puede generar pérdidas económicas, afectar la confianza de tus clientes y dañar la reputación del negocio.

¿Cómo prevenir la manipulación de tus QR?

- **Revisar el QR de manera regular**
  Asegurate de que no esté tapado, reemplazado o modificado.
- **Ubicar el QR en un lugar seguro**
  Colocalo donde no sea fácil reemplazarlo sin que lo notes.
- **Reemplaza el QR si tenés dudas**
  Si sospechás que fue manipulado, generá uno nuevo de inmediato.
- **Generar el QR únicamente desde plataformas confiables**
  Usá siempre aplicaciones oficiales, especialmente para cobros.

7. TIENDA ONLINE

Muchos emprendimientos y PyMEs venden a través de Mercado Libre, Facebook Marketplace, Instagram u otras plataformas. **Son herramientas útiles, pero también pueden ser explotadas por estafadores.**

A continuación, algunas señales de alerta y buenas prácticas para proteger tu negocio.

7.1 Señales de alerta y cómo actuar

Pedido con urgencia

Los estafadores suelen presionarte para que actúes con urgencia -como enviar un producto, hacer un reembolso, ingresar a un enlace fraudulento o realizar cualquier otra acción riesgosa-. Esa urgencia es intencional: buscan que no tengas tiempo de pensar con claridad y tomes decisiones apresuradas que te dejen expuesto al fraude.

Buena práctica: no te apures. Siempre verificá antes de actuar. Recordá que todo puede esperar unos segundos para ser verificado.

Solicitud de cambiar la dirección de entrega

Si piden cambiar la dirección por mensaje y no desde de la app oficial, quedás sin respaldo ante reclamos.

Buena práctica: aceptá únicamente cambios realizados desde la plataforma oficial, son los únicos válidos.

Perfiles nuevos o con poca actividad

Los estafadores suelen usar cuentas recién creadas o con poco historial para evitar utilizar sus perfiles reales. Encontrar una cuenta así no significa necesariamente que sea una estafa, pero sí es una señal para estar más atento.

Buena práctica: ante perfiles nuevos, revisá que no haya señales de fraude como urgencias, pedidos inusuales o links externos.

Perfiles reales comprometidos (hackeados)

Un perfil legítimo puede estar siendo controlado por un tercero. Señales: cambios de nombre, publicaciones borradas, mensajes fuera de contexto.

Buena práctica: si ves comportamientos inusuales, no interactúes.

Pedidos para continuar la operación por fuera de la plataforma

Los estafadores buscan que interactúes fuera de la plataforma con excusas como “evitar comisiones” o “es más rápido”, para dejarte sin las medidas de seguridad que brinda el sitio.

Buena práctica: nunca realicés operaciones fuera de la plataforma. Allí estás protegido; afuera, no.

Links externos enviados por “alguien de confianza”

Pueden simular ser un cliente o proveedor y enviarte enlaces falsos.

Buena práctica: no abras enlaces sospechosos.

Pagos no acreditados o comprobantes falsos

Te envían capturas editadas o comprobantes falsos para que creas que ya te pagaron, cuando no es así.

Buena práctica: verificá siempre la acreditación del pago en la plataforma oficial.

Insistencia en hacer una “excepción”

Muchos fraudes ocurren cuando se acepta “una excepción por esta vez”.

Buena práctica: mantené siempre el proceso habitual, sin desviarte.

Recordá
Estas señales son indicadores de riesgo, no pruebas absolutas de una estafa. Estar atentos y aplicar buenas prácticas reduce significativamente las posibilidades de caer en un fraude.

Contactanos a través de Boti o llamando al 147

buenosaires.gob.ar/ciberseguridad

Buenos Aires Ciudad

Vamos pormás