FASE .0
Technology Solutions
SEGURIDAD - SOPORTE - SERVICIO

CYBERSECURITY ADVISORY

MANUAL DE PROTECCIÓN

Guía Básica de Ciberseguridad

Estrategias esenciales de protección digital para usuarios & PyMEs.
Edición Octubre 2026



Octubre 2026 | Edición: 1.0

Distribución Gratuita / Guía Informativa

Título: Guía Básica de Ciberseguridad para usuarios y PyMEs.
Edición: Primera Edición Octubre 2026
Versión del documento: 1.0
Fecha de creación: 05 de octubre de 2026
Fecha de última actualización: 24 de octubre de 2026
Idioma: Español

Dirección del proyecto: Equipo de Seguridad Digital FASE .0
Redacción y desarrollo técnico: Área de Contenidos Técnicos FASE .0
Diseño visual y maquetación: Departamento de Diseño FASE .0
Sitio web oficial: **https://fasecero.solutions**
Contacto: **soporte@fasecero.solutions**

Copyright © 2026 FASE .0. Todos los derechos reservados.
Este documento se distribuye bajo el espíritu de garantizar la libertad de uso, estudio, distribución y modificación del conocimiento técnico.

El contenido de **Guía básica de Ciberseguridad para Usuarios y PyMEs 2026** © 2026 by **Fase .0** está protegido bajo la licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional **(CC BY-NC-SA 4.0)**.
Para ver una copia completa de esta licencia, visite: https://creativecommons.org/licenses/by-nc-sa/4.0/

Es libre de compartir; copiar y redistribuir el material en cualquier medio o formato; Adaptar, remezclar, transformar y construir a partir del material; modificar la guía, traducirla, extraer secciones; **bajo los siguiente términos:**

- **Atribución y reconocimiento** — Usted debe dar crédito de manera adecuada, brindar un enlace a la licencia, e indicar si se han realizado cambios. Puede hacerlo en cualquier forma razonable, pero no de forma tal que sugiera que usted o su uso tienen el apoyo de la licenciante.
- **NoComercial** — Usted no puede hacer uso del material con propósitos comerciales.
- **CompartirIgual** — Si remezcla, transforma o crea a partir del material, debe distribuir su contribución bajola misma licencia del original. **(CC BY-NC-SA 4.0)**

DESCARGO DE RESPONSABILIDAD (DISCLAIMER)

La información contenida en este documento tiene fines puramente educativos, informativos y de divulgación técnica. **FASE .0** y sus colaboradores no otorgan garantías expresas o implícitas sobre la exactitud, integridad o aplicabilidad de los protocolos descritos. El uso de las estrategias y herramientas mencionadas es responsabilidad exclusiva del usuario. **FASE .0** no se hace responsable de daños operativos, pérdida de datos, interrupciones de servicio o consecuencias legales derivadas de la aplicación, interpretación o mal uso de la información contenida en esta guía. Este documento no sustituye una **auditoría de seguridad profesional**, asesoría legal especializada ni asistencia forense.

CONTENIDO

Cómo usar esta guía

- Este documento está diseñado para usuarios independientes, microempresas y PyMEs.
- Es educativo: no sustituye auditoría, asistencia forense, asesoría legal ni obligaciones de protección de datos.
- Revíselo constantemente, y ante cambios de herramientas tecnológicas de proveedores o personales.

Esta guía está diseñada para traducir la complejidad técnica en estrategias claras, prácticas y económicas, adaptadas a las realidades de cada usuario.

Prioridades de las primeras 24 horas

Proteger el correo permite recuperar todas las demás cuentas.

- **Activa MFA** en correo, banca, nube, dominio, hosting y redes sociales
- **Activa las notificaciones** de las actualizaciones en sistemas, equipos portátiles, teléfonos, apps, routers.
- **Usa un gestor de contraseñas** como Bitwarden o 1Password para generar y guardar claves complejas de forma cifrada.
- **Crea una copia separada** de los datos críticos y restaura un archivo de prueba.
- **Verifica fuera del correo** cualquier cambio bancario o pago.

Nunca compartas contraseña, código MFA, frase de recuperación ni aprobación de inicio de sesión.

TABLA DE CONTENIDO

1	Glosario
2	Introducción: El Ecosistema Digital
3	Los 3 Pilares Fundamentales
4	Datos Biométricos
5	Identidad Digital
6	Principales amenazas
7	Estrategias de seguridad
8	Gestión de contraseñas
9	¿Cómo se crea una contraseña segura?
10	Backups & copias de seguridad

01 GLOSARIO

Deepfakes: Son contenidos audiovisuales manipulados y modificados mediante un software con Inteligencia Artificial para simular a una persona, y fabricar con su imagen contenido falso.

EDR (Endpoint Detection and Response): Software que monitorea continuamente los dispositivos finales para detectar y responder a amenazas avanzadas.

FIDO2: Estándar abierto para la autenticación de usuarios. Pretende reforzar la forma en que las personas inician sesión en servicios online para aumentar la seguridad y la confianza general.

MFA (Multi-Factor Authentication): Autenticación Multifactor que requiere dos o más pruebas de identidad.

Phishing: Intentos de engaño para robar credenciales. El Spear Phishing está altamente personalizado usando IA con datos reales de la víctima.

RaaS: “Ransomware as a Service” o “Ransomware como Servicio”, es un modelo en el que los desarrolladores venden o alquilan códigos maliciosos a otros “usuarios”, permitiendoles emplearlas para iniciar los ataques.

Ransomware: Software malicioso que cifra los datos y exige un rescate, generalmente en criptomonedas, para desbloquearlos.

TOTP: Metodo de identificación de 2 factores (2FA) que genera códigos temporales que cambian cada 30 a 60 segundos, lo que hace que sea extremadamente difícil de comprometer.

WebAuthn: Estándar web y componente fundamental del proyecto FIDO2. El objetivo es normalizar una interfaz para autenticar a los usuarios con aplicaciones y servicios basados en la web utilizando criptografía asimétrica.

Zero Trust (Confianza Cero): Modelo de seguridad que asume que la red ya está comprometida y verifica cada solicitud de acceso como si viniera del exterior.

02 INTRODUCCIÓN

EL ECOSISTEMA DIGITAL

Hoy la digitalización es más que una ventaja competitiva, es un recurso fundamental e indispensable para la operación de toda empresa. Los usuarios de Pequeñas y Medianas Empresas operan en un **entorno hiperconectado** donde la **Inteligencia Artificial Generativa** y la **automatización** son la norma. Sin embargo, esta misma tecnología ha **facilitado el ciberdelito**.



Los atacantes ya no necesitan ser genios; solo necesitan suscribirse a un servicio de "Ransomware como Servicio" (RaaS) impulsado por IA.

La ciberseguridad no es exclusiva de las grandes corporaciones.

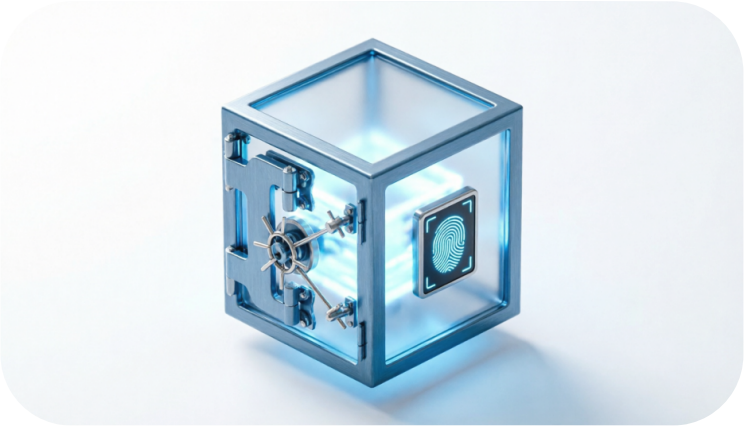
Las Pequeñas y Medianas Empresas (PYMEs), y los usuarios particulares, son hoy el blanco principal de **ataques automatizados** debido a niveles de protección más bajos.

03 Los tres pilares fundamentales

CONFIDENCIALIDAD

Proteger la información para que sea accesible solo por las personas o sistemas autorizados. Evita su divulgación.





INTEGRIDAD

Proteger la información para garantizar que sea exacta y completa. Evitar que sea modificada, alterada o destruida por usuarios, sistemas o procesos con y sin autorización.

DISPONIBILIDAD

Proteger los sistemas y la información para que estén accesibles y operativos para los usuarios autorizados cuando los requieran.



04 Datos Biométrios

En el mundo digital existen datos únicos sobre las características físicas o de comportamiento de un individuo. Información que si se compromete puede afectar gravemente la integridad de un individuo y su identidad digital, estos son los Datos biométricos.

Son cualquier tipo de **información sobre las características físicas de un individuo**. Desde la secuenciación del ADN; que es el tipo de dato biométrico más preciso; seguido de los **rasgos fisiológicos**; como los **patrones de la retina**, las **huellas dactilares** y la **estructura facial**.

Entre los datos biométricos con menor precisión técnica se encuentran la huella vocal o reconocimiento de voz, la geometría de las manos y los electrocardiogramas (ECG).



05 *Identidad Digital*



Es el conjunto total de datos, atributos, credenciales y registros de actividad que **representan a una persona o entidad en el entorno digital**. Se compone de los siguientes elementos:

Identificadores Directos
¿Quién eres en el sistema?

Son los datos que nos **vinculan** de manera única y **directa** con todos los **servicios**, **cuentas** y **dispositivos**.

- **Nombre**
- **Dirección de residencia**
- **Números telefónicos**
- **Números de Identificación Oficial**
- **DNI | Pasaporte**
- **Seguro Social**
- **Registro Tributario | RUT / RFC**
- **Correos Electrónicos**
- **Nombres de usuario y alias**

Credenciales de Autenticación

¿Cómo demuestras que eres tú?

Mecanismos que validan que el usuario que intenta acceder es el **legítimo propietario** de la **identidad**.



- Contraseñas y frases de recuperación (passwords/passphrases)
- Códigos PIN numéricos
- Claves de acceso (Passkeys) basadas en criptografía | pública/privada
- Tokens de seguridad | YubiKey | códigos TOTP
- Certificados digitales |Archivos que acreditan la identidad

06 Principales Amenazas

Phishing | Suplantación

Correos o mensajes falsos que simulan ser entidades legítimas para robar credenciales o datos bancarios.

Ransomware | Malware

Programas maliciosos que secuestran y cifran archivos o sistemas, y exigen un rescate económico para devolver el acceso. Espian, registran pulsaciones de teclas (keyloggers) y roban datos.

Ataque a la cadena de suministros

Intrusiones que atacan, aprovechando la vulnerabilidad del software, al proveedor externo de confianza para afectar a sus clientes y colarse por la puerta trasera.

Inteligencia Artificial | Ataques Deepfakes

Uso de IA para automatizar ataques, crear suplantaciones de voz e imagen (Deepfakes), así como redactar correos de Phishing hiperrealistas a gran escala.

07

Estrategias de Seguridad

1 Crear políticas de seguridad:

Muchos **minimizan la importancia de las políticas de seguridad** escritas, y ponen su atención en los controles técnicos. Estos, por lo general, se implementan sin procedimientos administrativos, y se ejecutan de una manera reactiva sin una estrategia adecuada, coherente y completa; ni con una gestión de seguridad (que se define en función del **análisis de la seguridad de la información y las políticas**). Significa que inevitablemente se invertirá en soluciones que no serán implementadas de manera efectiva, por lo que la protección será incompleta e inadecuada.

2 Identifique sus activos:

La violación de datos de Target 2013, atacantes accedieron a un sistema de mantenimiento de calefacción y aire acondicionado, para extraer la información de las tarjetas de bancarias y otros datos personales de 110 millones de clientes.

Conozca exactamente qué está protegiendo. Es importante que lleve un inventario de todo su hardware y software de TI. Esto le permitirá conocer las vulnerabilidades de su red y aplicar medidas correctivas a tiempo. Se puede comenzar utilizando **herramientas gratuitas disponibles**. Las soluciones comerciales ayudan a mantener con precisión el inventario de activos de manera continua, y ofrecen capacidades de administración remota. Reduzca la superficie de ataque para todos los activos conectados a Internet (incluyendo los dispositivos personales). Mantenga al día la protección de seguridad.

3 Conozca su postura de seguridad

Identificar las amenazas contra los activos del entorno, **implementar** las medidas adecuadas de **seguridad** y **protección** de datos.

- **Crear** una hoja de ruta o modelo para mostrar el estado o situación actual.
- **Analizar** las diferencias entre el estado actual de seguridad y el deseado.
- **Determinar** qué pasos debe seguir y dónde invertir sus recursos.

4 Clasificar todos los datos

¿Cómo afectaría una violación de datos a la **imagen** de su marca; la **lealtad** de los clientes; o incluso a la **continuidad** de su negocio?

La información y los datos confidenciales de los clientes representan los elementos más valiosos; sin embargo, protegerlos y controlarlos es complicado y poco práctico. **Identificar** los datos cuya pérdida o exposición representaría un riesgo operativo, legal o financiero severo para la organización, y que no lo dejarían dormir si se extraviaran o fueran robados. Cree y documente una **política de clasificación** de datos intuitiva para su organización, que incluya etiquetas (p.ej.: "*Solo para uso interno*" | "*Datos confidenciales*" | "*Aprobado para divulgación pública*") especificando los **requisitos de protección** de datos (*cifrado* | *copias de seguridad* | *aprobación de la versión* | *destrucción*) para los **diferentes niveles** de información.

5 Backups & Pruebas de recuperación

Probar regularmente su capacidad para **recuperar** sus sistemas y datos críticos de los Backups, no solo para **asegurarse** de que las copias de seguridad no estén dañadas, sino también para **verificar** que tanto usted como su personal **conocen** el proceso de recuperación.

Una práctica básica de seguridad es hacer Backups confiables y periódicos de sus sistemas y datos. Las buenas copias de seguridad le **garantizan** la recuperación de un archivo que se eliminó accidentalmente o de un disco rígido dañado. Puesto que el costo de los Backups basados en discos es cada vez menor y las soluciones de Backups basadas en la nube son rentables y fáciles de usar, no hay excusas para no hacer Backups. Con el rápido aumento del Ransomware en los últimos años, los Backups son la única forma de garantizar la recuperación de sus datos si llega a ser víctima de un ataque de Ransomware. Como beneficio adicional, no tendrá que pagar el rescate.

6 Planificación & Preparación

El equipo de respuesta a incidentes debe estar **capacitado** en procedimientos forenses básicos para **garantizar** que cada incidente de **seguridad** se trate como un caso legal potencial y que se **mantenga** la cadena de custodia para cualquier posible evidencia.

Tener un plan de respuesta a incidentes, de continuidad del negocio y de recuperación ante desastres. Los planes de continuidad del negocio y de recuperación ante desastres ayudan a su empresa a reanudar las operaciones comerciales normales lo más rápido posible tras una catástrofe o evento de seguridad importante. Las comunicaciones precisas y oportunas, tanto internas como externas, son un componente crítico de los planes de continuidad del negocio y de recuperación de desastres.

7 Capacitación del equipo

Los atacantes utilizan técnicas de ingeniería social para que usuarios **desprevenidos** accedan a enlaces maliciosos (spam | Phishing), **revelen** sus contraseñas y visiten sitios Web maliciosos.

Consulte la sección
¿Cómo se crea una contraseña segura?

El eslabón más débil de la seguridad siempre han sido los usuarios finales. Es poco probable que todas las personas que trabajan para la empresa hayan sido contratadas por ser expertos en seguridad. Lleve a cabo ejercicios de capacitación para la concientización sobre seguridad que sean periódicos, atractivos, relevantes y, por sobre todas las cosas, cortos, para que sus usuarios aprendan a desenvolverse ante una situación de seguridad.

8 Protección para Endpoints

Invertir en **soluciones confiables** en vez de descargar de Internet software antivirus gratuito.

Proteger todos los equipos de escritorio, dispositivos móviles y servidores con solución sólidas. Hoy en día, la información está en todas partes y ahora más que nunca todo confluye en las **Endpoints**, es por eso que es definitivamente un área en la que vale la pena **invertir**.

08 Gestión de contraseñas

En la seguridad informática el **eslabón más débil** suele ser la **autenticación**.

El uso de contraseñas débiles y/o reutilizadas facilita el acceso no autorizado.

Regla de oro:

Autenticación de Doble Factor (2FA / MFA)

Active siempre la **Autenticación Multifactor**. Utilice aplicaciones autenticadoras (como Google Authenticator | Microsoft Authenticator) en lugar de SMS, los cuales son vulnerables a duplicaciones de SIM.

Prolongar: Usar frases de más de 15 caracteres, con mayúsculas, minúsculas, números y caracteres especiales.

Delegar: Usar un gestor para generar y conservar contraseñas únicas (Protege el gestor con MFA). Usa Passkeys o llaves FIDO2/WebAuthn; resisten mejor el Phishing que los SMS.

Priorizar: Configura el **MFA** en el correo, la nube, la banca, el dominio y administración.

Asegurar: Guarda códigos de recuperación aparte del dispositivo.

Verificar: Revisa sesiones, dispositivos, apps conectadas y reenvíos de correo cada mes.

Limitar: Trabaja con cuenta estándar; reserva la cuenta administradora para cambios. Cada colaborador debe tener cuenta individual. Revoca de inmediato sesiones y accesos al terminar una relación laboral.

Buenas Prácticas | Para Credenciales Seguras

Longitud sobre complejidad: Utilice frases de contraseña (ej. "Gato.Cafe.Teclado.2026!") de más de 14 caracteres.

Gestores de Contraseñas: Implemente soluciones empresariales o personales (Bitwarden, 1Password) para almacenar claves cifradas sin memorizarlas.

Evitar reutilizar: Cada servicio o cuenta debe poseer una clave única. Si un servicio se compromete, los demás seguirán a salvo.

09 *¿Cómo se crea una contraseña segura?*

Usar palabras largas:

Las contraseñas deben tener mínimo 8 caracteres, con números, mayúsculas, minúsculas y caracteres especiales. Compruebe que su contraseña no haya sido expuesta en una violación de datos en...

https://haveibeenpwned.com/Passwords

Evitar información personal:

Las redes sociales facilitan a los delincuentes la obtención de la información personal; incluyendo segundos nombres, fecha de nacimiento, dirección, escuela, nombre de la pareja o hijo, **¡y lo que hizo el verano pasado!**

Usar frases y caracteres especiales:

Una frase que conste de 30 caracteres con números, mayúsculas y puntuación, que pueda recordar, es mucho mejor que una palabra de 8 caracteres con sustituciones comunes (como un “3” para la letra “E”).

Evitar palabras comunes:

Los programas para descifrar contraseñas usan diccionarios de idiomas; incluyendo los extranjeros; términos médicos, legales o de ingeniería. También evite caracteres repetitivos (“aaaa”), o secuenciales (“1234”), y los patrones reconocibles (“qwerty”).

Jamás compartir las contraseñas:

Trate las credenciales de acceso como información de máxima confidencialidad. Nunca comparta las contraseña, códigos MFA, frases de recuperación ni aprobación de inicio de sesión.

Evitar la misma contraseña dos veces:

Independientemente de lo buena que sea, si su contraseña resulta comprometida en un solo lugar (p. ej. la cuenta de correo), los cibercriminales intentarán usar esas mismas credenciales en otros lugares (como las cuentas bancarias).

10 Backups & Copias de seguridad



La única garantía real *contra ataques devastadores, es contar con un* ***plan sólido*** *de* ***respaldos actualizados****.*

La Regla 3-2-1 del Respaldo

Mantenga **3 copias** de sus datos, en **2 medios diferentes** (disco externo y nube), y **1 copia fuera de la empresa** (offline o nube aislada).

Pasos para una Estrategia Efectiva

Automatización

Programar respaldos diarios sin depender de la intervención humana.

Verificación

Realizar prueba de restauración de datos, para comprobar su integridad y su correcta recuperación.

Aislamiento

Mantener una versión desconectada de la red para evitar que el Ransomware la afecte.

FASE .0

Para información adicional sobre nuestros productos o servicios, por favor contáctanos:

Email: **soporte@fasecero.solutions**

Móvil: **(+52) 624 2678615**

Visita nuestro sitio para más información:

https://fasecero.solutions

Desarrollado por **FASE .0** |
Una solución elegante e inteligente.

Aviso de distribución

Este documento puede ser guardado, imprimirse y distribuirse como material educativo, No comercial.

Edición Octubre 2026 | Revisión recomendada:
cada 3 meses o después de un incidente significativo.

Guía básica de Ciberseguridad para Usuarios y PyMEs 2026 © 2026 by Fase .0 (Fase Cero) is licensed under Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International.
To view a copy of this license, visit https://creativecommons.org/licenses/by-nc-sa/4.0/

