CIBERSEGURIDAD

PARA TODOS:

Protege tu información en el entorno digital

Guía Educativa de Ciberseguridad

Dirigida a todo el personal no técnico
Versión 1.1 © Año 2026

CENAMEP AIP
Centro Nacional de Metrología de Panamá AIP

SENACYT
Secretaría Nacional de Ciencia, Tecnología e Innovación



Ciberseguridad para todos: protege tu información en el entorno digital. Guía educativa de ciberseguridad. *Autores:* Edwin González y Alfonso Carrión. Ciudad de Panamá, República de Panamá. 2026.

26 páginas.
Incluye textos, imágenes, tablas y referencias bibliográficas.

Centro Nacional de Metrología de Panamá (CENAMEP AIP)

Licencia:
Esta guía está bajo una Licencia de Creative Commons:
Reconocimiento-NoComercial-CompartirIgual 4.0 Internacional.

https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es

ISBN: 978-9962-8557-3-6

AGRADECIMIENTO

El Centro Nacional de Metrología de Panamá (CENAMEP AIP) expresa su agradecimiento a todas las personas e instituciones que hicieron posible el desarrollo de esta *Guía Educativa de Ciberseguridad*. Su elaboración fue posible gracias al trabajo colaborativo, el compromiso y el apoyo brindado por todos los colaboradores del Centro durante las distintas etapas de un proyecto de investigación científica desarrollado desde sus instalaciones.

De manera especial, se reconoce el valioso respaldo de la *Secretaría Nacional de Ciencia*, *Tecnología e Innovación* (SENACYT) y del CENAMEP AIP, cuyo acompañamiento y aportes fueron fundamentales para fortalecer las iniciativas orientadas a la capacitación, la mejora continua de los procesos y el desarrollo de capacidades institucionales. Especial reconocimiento se desea conferir al *Contrato de Subsidio Económico DDCCT No. 144-2024* de la SENACYT, por el apoyo económico para la generación de esta guía en el Centro.

Asimismo, se agradece al personal técnico y administrativo que contribuyó con su conocimiento, orientación y participación, así como a todas las personas que forman parte del CENAMEP AIP y de las demás empresas e instituciones colaboradoras, quienes con su compromiso diario fortalecen la cultura de ciberseguridad y promueven el uso responsable de la información y la tecnología.

Como citar este documento:
González, E. y Carrión, A. *Ciberseguridad para todos: protege tu información en el entorno digital. Guía educativa de ciberseguridad,* Ciudad de Panamá. 26 páginas. 2026.

Autores y edición:
Edwin González, Pasante del CENAMEP AIP
Mgter. Alfonso Carrión, Coordinador de TIC, CENAMEP AIP
Revisión técnica:
Dr. Jaime Estrella, Coordinador de I+D+i, CENAMEP AIP

PREFACIO

La transformación digital ha facilitado el trabajo diario de las organizaciones, pero también ha incrementado los riesgos asociados al uso de la tecnología. Hoy en día, cualquier persona que utilice correo electrónico, Internet o dispositivos digitales puede estar expuesta a amenazas de ciberseguridad, independientemente de su rol o nivel técnico.

Con el fin de fortalecer la cultura de seguridad de la información, el Centro Nacional de Metrología de Panamá (CENAMEP AIP) desarrolló esta *Guía Educativa de Ciberseguridad*, dirigida a todo el personal no técnico. Esta guía complementa los contenidos abordados en la plataforma de capacitación del Centro, donde se compartieron videos, ejemplos prácticos y simulaciones controladas de incidentes como *phishing*, correos maliciosos y otros ataques comunes. Esta guía también abarca las recomendaciones emitidas en dos talleres de planificación participativa (con el método ZOPP simplificado), enfocados a presentar soluciones a incidentes cibernéticos.

Es importante reconocer que la ciberseguridad no se aprende en una sola sesión. Por ello, esta guía ha sido diseñada como un material de apoyo y consulta, que permite reforzar conceptos clave, identificar señales de alerta y conocer las acciones correctas que deben tomarse ante una situación sospechosa o un posible incidente de seguridad.

La prevención, la atención y el reporte oportuno son responsabilidades compartidas. Cada persona cumple un rol fundamental en la protección de la información, los sistemas y la continuidad de las operaciones de su institución. A través de prácticas simples y conscientes, es posible reducir significativamente los riesgos y contribuir a un entorno digital más seguro.

Este documento busca servir como una herramienta práctica, clara y accesible, que acompañe al personal en su día a día y refuerce el compromiso institucional con la seguridad de la información. Esta guía surge en el marco de iniciativas institucionales que promueven la colaboración, el fortalecimiento de capacidades y la mejora continua de los procesos. En particular, se reconoce el apoyo y la participación de la *Secretaría Nacional de Ciencia, Tecnología e Innovación* (SENACYT) y del *Centro Nacional de Metrología de Panamá* (CENAMEP AIP), cuya contribución ha sido fundamental para el desarrollo de proyectos orientados al fortalecimiento institucional, la transferencia de conocimiento y la consolidación de buenas prácticas que impactan positivamente en la infraestructura y la cultura organizacional.

Los autores.

CONTENIDO



1. Introducción 6
2. Objetivo de esta guía 7
3. Alcance de esta guía 7
4. Glosario 8
5. ¿Qué es la ciberseguridad? 10
6. Amenazas digitales 11
- *Phishing* 12
- *Malware* 13
- *Ransomeware* 14
- Ingeniería social 15

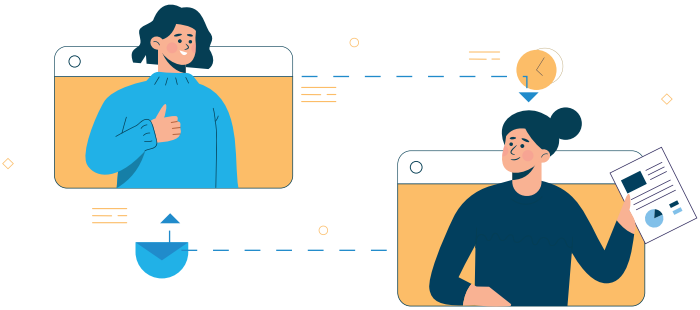
7. Buenas prácticas de seguridad 16
8. Uso seguro de contraseñas 17
- Contraseñas fuertes 17
- No las reutilices 17
- Autenticación multifactor 17

9. Dispositivos móviles y trabajo remoto 18
10. ¿Qué hacer ante un incidente cibernético? 19
11. Recomendaciones para el usuario 21
12. Recursos consultados en esta guía 22
13. Conclusiones sobre esta guía educativa sobre ciberseguridad 23
14. Recursos recomendados 24

1. INTRODUCCIÓN

La ciberseguridad es una responsabilidad compartida dentro de una organización. En la actualidad, el uso constante de herramientas digitales, plataformas en línea y correo electrónico expone a las instituciones a múltiples riesgos relacionados con la seguridad de su información. En los últimos años, los reportes de incidentes cibernéticos han ido en aumento, evidenciando que ninguna organización está completamente libre de estos riesgos digitales.

Este panorama también impacta a sectores altamente especializados como la metrología científica, legal e industrial. En este campo, los procesos están experimentando un cambio de paradigma impulsado por la transformación digital de la industria y la sociedad. Cada vez más, los laboratorios incorporan tecnologías que permiten digitalizar las mediciones, transmitir datos y automatizar los procesos de entrega de resultados a los clientes, reduciendo así la posibilidad de error humano y mejorando la eficiencia operativa.



Sin embargo, el incremento en el uso de tecnologías digitales también amplía la superficie de exposición a posibles amenazas cibernéticas. Muchos incidentes tienen su origen en errores humanos, como hacer clic en un enlace malicioso, descargar archivos sospechosos o compartir información sensible sin verificar el origen de la solicitud. Por esta razón, la concienciación del personal administrativo y técnico de una entidad se convierte en un elemento clave para la protección de la información institucional.

En este contexto, la presente guía ha sido elaborada como un documento de apoyo permanente que permita al personal identificar situaciones de riesgo y actuar de manera adecuada ante un posible incidente de ciberseguridad. Su ámbito de aplicación está dirigido al CENAMEP AIP, así como a otras AIP o entidades en Panamá que busquen fortalecer sus prácticas de seguridad digital.

2. OBJETIVO DE ESTA GUÍA

El objetivo principal de este documento es proporcionar al personal no técnico de una organización una referencia clara, práctica y accesible sobre los conceptos básicos de ciberseguridad y los procedimientos de respuesta ante incidentes que pueden implicar riesgos e incluso pérdidas (parciales o totales) de información, que podrían derivar en repercusiones económicas, legales y reputacionales.

De manera específica, esta guía busca:

- **Compartir** nuevos conocimientos de ciberseguridad, o bien, reforzar los conocimientos adquiridos en capacitaciones previas de un usuario.
- **Facilitar** a un usuario la identificación de amenazas comunes.
- **Establecer** acciones claras sobre qué hacer y qué no hacer ante un incidente de ciberseguridad.
- **Definir** los canales de reporte y comunicación internos en una entidad dada.
- **Reducir** el impacto de los incidentes mediante una respuesta temprana.

3. ALCANCE DE ESTA GUÍA

Esta guía aplica a todo el personal no técnico de una organización, independientemente de su cargo o función. Sin embargo, aplica también al personal técnico, al presentarse consejos prácticos sobre ciberseguridad. Incluye a todas las personas que utilicen:

- Equipos de cómputo institucionales.
- Correo electrónico corporativo.
- Plataformas digitales y sistemas internos.
- Dispositivos móviles utilizados para fines laborales.

El contenido de esta guía no sustituye las políticas institucionales de seguridad de la información, sino que las complementa.

4. GLOSARIO

A continuación, se presentan las definiciones de algunos términos clave utilizados a lo largo de esta guía, con el fin de facilitar su comprensión y asegurar una interpretación común de los conceptos relacionados con la ciberseguridad.

Archivo malicioso o *malware:* se trata de un *software* diseñado para interferir con el funcionamiento normal de un ordenador.

Ataque cibernético: intento de dañar, robar información digital u obtener acceso no autorizado a computadoras o redes, utilizando una o más computadoras.

Buenas prácticas: acciones para usar la tecnología de forma adecuada, asegurando la calidad de los servicios que se ofrecen a sus usuarios.

Ciberdelincuente: persona que buscará sacar beneficio de problemas o fallos de seguridad utilizando para ello distintas técnicas como son la ingeniería social o el *malware.*

Ciberseguridad: es la práctica de proteger a las personas, los sistemas y los datos de los ciberataques mediante el uso de diversas tecnologías, procesos y políticas.

Copia de seguridad: es un duplicado seguro de los datos de un usuario, que permite restaurarlos en caso de pérdida, fallo del sistema o ataque informático.

Correo fraudulento: tipo de estafa que utiliza el correo electrónico para engañar a las víctimas, a fin de que revelen información personal, permitan acceso a plataformas o para que transfieran fondos a cuentas fraudulentas.

Cracker: es un experto en informática que utiliza sus conocimientos técnicos para dañar sistemas ajenos, con el fin de extorsionar solicitando dinero o causando daño.

Enlace falso: se trata de un enlace que lleva a una página web peligrosa o clonada imitando un sitio web real.

Hacker: es alguien que tiene un profundo conocimiento de la tecnología y utiliza estas habilidades para explotar sistemas, redes y dispositivos.

Información confidencial: datos que suelen estar sujetos a normas de privacidad y seguridad, y su exposición a externos no autorizados puede tener consecuencias financieras, jurídicas o reputacionales.

Mensaje urgente: comunicación que presiona a la persona que lo recibe para actuar de manera rápida, en donde se dispone de poco tiempo para analizar la situación.

Phishing: es una táctica de ciberdelincuencia en la que los atacantes engañan a las personas para que revelen información confidencial (por ejemplo, contraseñas, datos bancarios) a través de correos electrónicos, mensajes o sitios web engañosos.

Ransomware: es un tipo de *malware* que retiene como "rehenes" a los datos confidenciales o el dispositivo de una víctima, amenazando con mantenerlos bloqueados, o algo peor, a menos que la víctima pague un rescate al atacante.

Sistema comprometido: se refiere a un dispositivo, red o infraestructura digital que ha sido infiltrado, manipulado o accedido sin autorización, por parte de actores malintencionados. Esto puede implicar la pérdida de datos, el control remoto del sistema o la interrupción de sus servicios.

Suplantación de identidad: consiste en hacerse pasar por otras personas para obtener un beneficio, y para ello, se suele cometer algún fraude, como por ejemplo, obtener datos de manera ilegal, el *ciberbullying* o *grooming* (conseguir confianza de un menor para poder abusar de él sexualmente).

Usuario no técnico: persona que utiliza un servicio o sistema sin conocimiento profundo de la tecnología detrás de dicho sistema.

Vulnerabilidad informática: es cualquier fallo o error en el *software* o en el *hardware* que hace posible a un atacante o *hacker* comprometer la integridad y confidencialidad de los datos que procesa un sistema.

El conocimiento de estas definiciones permitirá obtener una base común para interpretar correctamente los contenidos presentados al lector.

Con esto, se logra identificar con mayor claridad los riesgos asociados al entorno digital y aplicar de manera adecuada las medidas de prevención descritas en las siguientes secciones de esta guía.



5. ¿QUÉ ES LA CIBERSEGURIDAD?

Es protección digital:
Conjunto de prácticas y tecnologías que resguardan su información y sistemas.

Es responsabilidad compartida:
No es solo el técnico: cada persona es clave en la seguridad de la organización.



Usted, la primera línea de defensa

Muchos ciberataques tienen a Ud. como objetivo. Su atención es su mejor escudo, por eso es importante evitar:

- Abrir correos sospechosos o de remitentes que no conozca.
- Descargar archivos desconocidos o de sitios poco seguros.
- Compartir información sensible en redes sociales.
- Mantener el *software* actualizado, lo que ayuda a corregir vulnerabilidades que pueden ser explotadas por atacantes.
- Reutilizar la misma contraseña en varias cuentas o aplicaciones. Si una cuenta es comprometida, las demás también pueden quedar expuestas.



¡La prevención y la concienciación son las mejores herramientas de defensa!

6. AMENAZAS DIGITALES

Las amenazas digitales representan uno de los principales riesgos para la seguridad de la información en las organizaciones. Actualmente, **los ciberdelincuentes** utilizan diversas técnicas para engañar a los usuarios, acceder a sistemas o comprometer datos sensibles. Entre las más comunes se encuentran las siguientes:



Phishing
Envío de correos falsos o mensajes que aparentan ser legítimos para robar datos o información confidencial.

Malware
Son programas maliciosos que dañan dispositivos electrónicos o roban su información. Son comúnmente conocidos como virus, troyanos y gusanos, entre otros.





Ransomware
Es un tipo de *malware* que bloquea archivos y el acceso al equipo; además, exige un pago, durante un tiempo determinado, comúnmente por criptomonedas.

Ingeniería social
Se trata de un conjunto de técnicas que manipulan a las personas para obtener información confidencial o inducirlas a realizar acciones que comprometen su seguridad.



A continuación, veamos cada una de estas categorías con más detalle.

Phishing
Envío de correos falsos o mensajes que aparentan ser legítimos para robar datos o información confidencial.

El ***phishing*** es una técnica de engaño utilizada para obtener información confidencial, como contraseñas o datos personales, en donde **el ciberdelincuente** se hace pasar por una entidad legítima.

Estos ataques suelen presentarse a través de correos electrónicos, mensajes de texto o sitios web falsos. Los mensajes de *phishing* suelen ***generar urgencia*** o miedo para provocar una reacción rápida del usuario.

Señales comunes de *phishing*:

- Errores ortográficos o gramaticales presentes en el correo recibido.
- Remitentes desconocidos.
- Enlaces que no coinciden con el sitio oficial.
- Solicitudes de información confidencial.
- Baja calidad en imágenes o posiciones extrañas de las mismas, dentro del mensaje.

Siga estos consejos para evitar el *phishing*:

- Identifique los mensajes sospechosos; revise cuidadosamente la dirección del remitente y los enlaces.
- Verifique siempre la fuente; nunca proporcione información confidencial (contraseñas, números de identificación personal) a través de correos electrónicos o mensajes.
- Evite hacer clic en enlaces de correos sospechosos.
- Mantenga actualizado su sistema operativo y utilice un antivirus confiable.
- Asegúrese de que las páginas web comiencen con **"https://"**; verifique que el ícono del "candado cerrado" se muestre en su navegador (ya que esto es un protocolo seguro).

Estos consejos son esenciales para protegerse contra ataques de phishing y mantener la seguridad de sus datos personales, institucionales o financieros.



Malware
Son programas maliciosos que dañan dispositivos electrónicos o roban su información. Son comúnmente conocidos como virus, troyanos y gusanos, entre otros.

El ***malware*** (software malicioso) es cualquier programa o archivo diseñado para dañar equipos, robar información o afectar el funcionamiento normal de los sistemas **sin el consentimiento del usuario**. Su objetivo principal es comprometer la seguridad de la información y los recursos tecnológicos de la persona y/o de la organización. El *malware* puede instalarse de forma silenciosa cuando el usuario descarga archivos, abre enlaces maliciosos, o cuando conecta dispositivos de almacenamiento externos infectados (como, por ejemplo: dispositivos USB, discos duros externos, discos compactos, tarjetas SD y micro SD, y hasta teléfonos inteligentes).

El *malware* suele propagarse a través de:

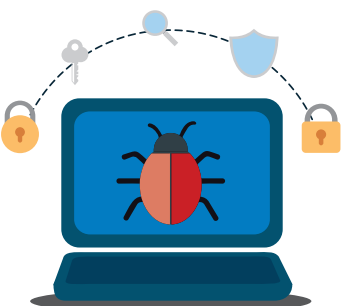
- Correos electrónicos con archivos adjuntos infectados.
- Enlaces a sitios web no seguros.
- Descarga de *software* no autorizado.
- Dispositivos USB desconocidos.
- Aplicaciones falsas o modificadas.



En muchos casos, el malware requiere de una acción del usuario para ejecutarse.

Para evitar el *malware*, puede seguir estos consejos:

- Instale un buen programa antivirus en su computadora y dispositivos móviles.
- Asegúrese de que las aplicaciones que descargue provengan de fuentes oficiales y confiables.
- Antes de descargar una aplicación, lea las descripciones escritas por el desarrollador y los comentarios de otros usuarios; sus experiencias previas son siempre de gran ayuda.
- Asegúrese de que su sistema operativo y aplicaciones estén siempre actualizados para protegerse contra vulnerabilidades.



Ransomware
Es un tipo de *malware* que bloquea archivos y el acceso al equipo; además, exige un pago, durante un tiempo determinado, comúnmente por criptomonedas.

El ***ransomware*** es un tipo de *malware* diseñado para bloquear el acceso a los archivos o sistemas de una organización, cifrando la información y exigiendo un pago ("rescate") a cambio de su recuperación. Este tipo de ataque puede paralizar completamente las operaciones y generar **pérdidas económicas, legales y reputacionales** del usuario o de la empresa. El *ransomware* suele aprovechar errores humanos, descuidos, configuraciones inseguras o sistemas desactualizados para propagarse.

Señales comunes de un ataque de *ransomware*:

- Archivos inaccesibles o con extensiones desconocidas.
- Mensajes en pantalla solicitando un pago para recuperar la información.
- Bloqueo total o parcial del equipo de cómputo.
- Imposibilidad de acceder a sistemas o aplicaciones.
- Cambios repentinos en nombres o formatos de los archivos digitales.

Siga estos consejos para evitar el *ransomware*:

- Asegúrese de hacer copias de seguridad de sus datos de forma regular y almacenarlas en un lugar seguro, preferiblemente desconectado de la red.

- Mantenga todos sus sistemas operativos y aplicaciones actualizados. Las actualizaciones suelen incluir parches de seguridad que corrigen vulnerabilidades que los atacantes pueden explotar.

- Utilice herramientas de escaneo para detectar *malware* en correos electrónicos antes de que lleguen a la bandeja de entrada de su aplicación de correos.



Ingeniería social
Se trata de un conjunto de técnicas que manipulan a las personas para obtener información confidencial o inducirlas a realizar acciones que comprometen su seguridad.

En este tipo de ataques, el **factor humano es el principal objetivo.** Los atacantes se aprovechan de la confianza, de infundir urgencia, el miedo o la curiosidad de las personas, logrando que el atacante pueda manipular a la víctima para que revele datos confidenciales, entregue credenciales de acceso, descargue archivos maliciosos, o bien, realice acciones que comprometan la seguridad de la información personal o de la organización.

¿Cómo actúa un ataque de ingeniería social?

La ingeniería social puede presentarse de distintas formas:

- Llamadas telefónicas de **ciberdelincuentes** haciéndose pasar por personal de soporte.
- Correos electrónicos que aparentan ser de jefaturas o de proveedores.
- Mensajes "urgentes" solicitando información o acciones inmediatas.
- Visitas presenciales con identidades falsas.
- Uso de información de las redes sociales para recopilar información pública de la víctima, previo al ataque del ciberdelincuente.

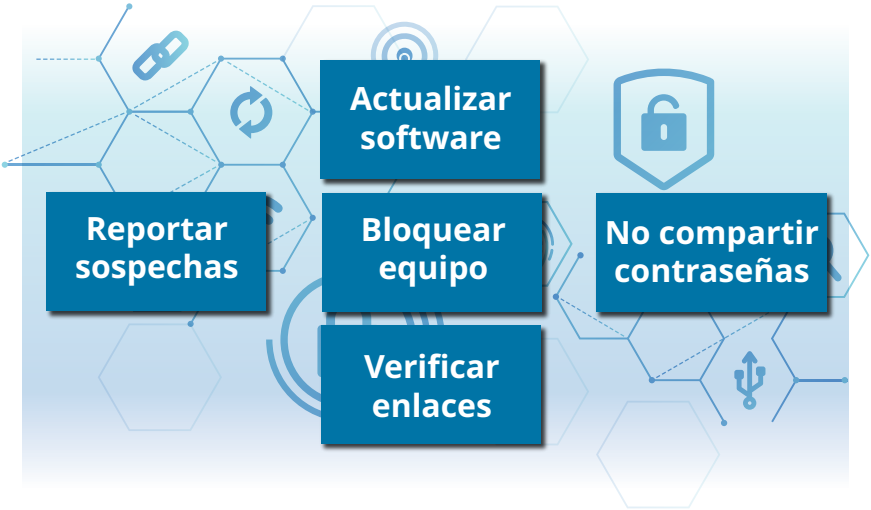


Siga estos consejos para evitar la ingeniería social:

- Si recibe Ud. un correo electrónico o mensaje sospechoso, verifique la dirección del remitente de dicho correo electrónico, el dominio o el enlace adjunto antes de hacer clic.
- Evite compartir sus credenciales de acceso en redes sociales o plataformas públicas.
- Evite colocar su información personal en foros electrónicos, redes sociales o sitios web públicos.



7. BUENAS PRÁCTICAS DE SEGURIDAD



- Las **actualizaciones** corrigen vulnerabilidades que los ciberdelincuentes podrían aprovechar para acceder a su información o a aquella de la empresa.

- Las **contraseñas son personales** y deben mantenerse en privado; compartirlas, incluso con compañeros de trabajo, puede comprometer cuentas y aumentar el riesgo de accesos no autorizados.

- Muchos ataques comienzan con **enlaces falsos**: antes de hacer clic en un enlace recibido por correo, mensaje o redes sociales, verifique que el remitente sea confiable y que la dirección web sea legítima.

- Cuando se aleje de su computadora o dispositivo, **bloquee la pantalla** para evitar que otras personas accedan a información sensible o realicen acciones sin su autorización.

- Si recibe correos, mensajes o archivos que parezcan sospechosos, **repórtelo** al área de tecnología o al responsable de seguridad informática de su entidad. Informar a tiempo puede prevenir incidentes y proteger tanto su información como la de la organización.

¡Las pequeñas acciones diarias hacen una gran diferencia en su seguridad digital!

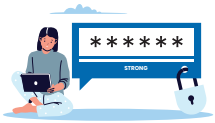
8. USO SEGURO DE CONTRASEÑAS

Contraseñas fuertes



Utilice combinaciones largas y únicas, con letras, números y símbolos para diseñar su contraseña. Evite usar información personal o contraseñas repetidas en diferentes cuentas, ya que esto aumenta el riesgo de accesos no autorizados en caso de filtración.

¡No las reutilice!



Cada cuenta o aplicación debe tener una contraseña diferente para evitar riesgos en caso de que una de ellas sea comprometida. Reutilizar contraseñas facilita que un incidente aislado se convierta en múltiples accesos no autorizados a distintos servicios o plataformas.

Autenticación multifactor

Este mecanismo requiere una segunda verificación, como un código temporal o una confirmación en un dispositivo adicional, lo que dificulta el acceso incluso si la contraseña ha sido comprometida. Actívela siempre que sea posible para añadir una capa adicional de seguridad a sus cuentas.



9. DISPOSITIVOS MÓVILES Y TRABAJO REMOTO

A continuación, unos ejemplos para mantenerse protegido durante su trabajo remoto:



¡Cuidado con el WiFi público!
Evite conectarse a redes abiertas para realizar tareas laborales o acceder a información institucional. Estas redes pueden ser utilizadas por terceros para interceptar datos, capturar credenciales o distribuir software malicioso sin que el usuario lo perciba.

Recurra al bloqueo de pantalla
Mantenga su dispositivo bloqueado cuando no lo esté utilizando, especialmente en entornos compartidos o públicos. Esta medida sencilla evita accesos no autorizados y protege la información sensible frente a potenciales usos indebidos o manipulaciones accidentales.



Separe lo personal de lo laboral
Evite instalar aplicaciones desconocidas en dispositivos utilizados para actividades laborales y no mezcle información personal con datos institucionales sensibles. Mantener esta separación reduce el riesgo de filtraciones, infecciones por *malware* y accesos no autorizados a información crítica.



10. ¿QUÉ HACER ANTE UN INCIDENTE CIBERNÉTICO?

Ante la sospecha o la presencia de un incidente cibernético, se recomienda lo siguiente:



Ante un **incidente cibernético**, es importante actuar con calma y seguir los procedimientos establecidos: se debe evitar interactuar con el posible ataque, como abrir archivos sospechosos, o responder a mensajes maliciosos; no borre ninguna evidencia que pueda ayudar a investigar y resolver lo ocurrido; el incidente debe reportarse de inmediato al responsable de la seguridad de la información. Estas acciones permitirán **contener el incidente** y reducir posibles impactos en los sistemas y la información de la organización.

Un solo clic puede generar un incidente; una buena decisión puede evitarlo.

LA CIBERSEGURIDAD:
UNA RESPONSABILIDAD COMPARTIDA



Con pequeñas acciones diarias, todos contribuimos a proteger la información, los sistemas y la continuidad de nuestro trabajo.

11. RECOMENDACIONES PARA EL USUARIO

- **No comparta sus contraseñas:** son personales y confidenciales; compartirlas puede permitir accesos no autorizados a su información (personal o institucional).
- **Desconfíe de correos extraños:** si recibe un correo inesperado, verifique siempre el remitente antes de responder o interactuar con él.
- **No haga clic en enlaces sospechosos:** un clic puede causar un problema; antes de abrir un enlace revise cuidadosamente la dirección (o el dominio).
- **No abra archivos desconocidos:** los archivos adjuntos desconocidos pueden contener *malware* capaz de comprometer su equipo y dañarlo.
- **Desconfíe de mensajes "urgentes":** la urgencia y presión pueden ser señal de engaño.
- **Bloquee su computadora al ausentarse:** proteja su información; bloquee su equipo cuando se aleje de su puesto.
- **No conecte dispositivos USB desconocidos:** pueden contener virus o programas maliciosos que infectarían su computadora.
- **Use el correo institucional o empresarial con cuidado:** evite compartir información sensible sin verificar primero la identidad de la persona que le envía un correo.
- **Reporte cualquier situación sospechosa:** ante correos, archivos o comportamientos inusuales, informe de inmediato al área responsable de tecnología o seguridad; es preferible no intentar resolver un incidente solo. ¡Recurra a apoyo!

¡La seguridad es responsabilidad de todos. Ante la duda, siempre, reportar!



12. RECURSOS CONSULTADOS EN ESTA GUÍA

Las siguientes fuentes confiables respaldan los contenidos de esta guía y le permiten a Ud. ampliar conocimientos sobre la ciberseguridad de forma segura y educativa:

Smartfense: Plataforma de concienciación en ciberseguridad

Descripción: plataforma utilizada para la formación del personal, con videos, campañas y simulaciones controladas.

https://smartfense.com/

INCIBE: Instituto Nacional de Ciberseguridad (España)

Descripción: Recursos educativos sencillos para usuarios no técnicos.

https://www.incibe.es/

NIST: National Institute of Standards and Technology

Descripción: buenas prácticas generales para la protección de la información.

https://www.nist.gov/cybersecurity

ISO/IEC 27001: International Organization for Standardization

Descripción: estándar internacional para la gestión segura de la información.

https://www.iso.org/standard/27001

CISA: Cybersecurity and Infraestructure Security Agency

Descripción: buenas prácticas e información clara sobre *phishing, ransomware* y otras amenazas comunes.

https://www.cisa.gov/cybersecurity



13. CONCLUSIONES SOBRE ESTA GUÍA EDUCATIVA

La **correcta aplicación de esta guía** ayudará al personal a reconocer situaciones de riesgo y a actuar de manera adecuada frente a posibles amenazas de ciberseguridad. A través de hábitos simples y buenas prácticas en el uso diario del correo electrónico, los equipos electrónicos y la información, se puede prevenir la mayoría de los incidentes cibernéticos que afectan a las organizaciones de distintos niveles.

Es importante comprender que **muchas amenazas digitales no explotan únicamente** fallas técnicas, sino descuidos humanos, decisiones apresuradas o desconocimiento. Por ello, adoptar conductas responsables, mantener una actitud preventiva y verificar la información antes de actuar son medidas fundamentales para reducir la exposición al riesgo.

La **ciberseguridad es un proceso de aprendizaje continuo**, en el que cada persona cumple un rol importante dentro de la organización. La atención, la prevención y el reporte oportuno ante cualquier situación sospechosa son **acciones clave** para proteger la información, preservar la continuidad operativa y fortalecer la confianza institucional en el entorno digital.



¡La información segura comienza con hábitos digitales responsables!

14. RECURSOS RECOMENDADOS

National Cybersecurity Alliance – Canal de YouTube

Descripción: canal oficial con videos educativos sobre seguridad en línea y concienciación digital para todo tipo de usuarios.

https://youtube.com/@staysafeonlinenca?si=WjLad1fmpmIt15ZP

EasyPhishing.org – Guía práctica de phishing

Descripción: portal que explica de forma clara qué es el *phishing*, cómo identificarlo y cómo responder de manera segura.

https://easyphishing.org/

Cybersecurity Awareness Month – Video oficial

Descripción: video introductorio del "Mes de Concienciación sobre Ciberseguridad", con recomendaciones básicas y estratégicas de protección en línea.

https://youtu.be/_OyQaUAcNHY?si=F1MkeHjGNjlDpfKo

NTEN – Videos de ciberseguridad básicos

Descripción: centro de recursos con videos educativos que cubren temas básicos como contraseñas seguras, comunicación segura y evaluaciones de tecnología.

https://www.nten.org/learn/resource-hubs/cybersecurity

Security Awareness Episodes (Stay Safe Online)

Descripción: serie de videos breves que cubren temas como: contraseñas, *phishing, ransomware,* medios removibles y más. Está pensada para aprendizaje general.

https://www.staysafeonline.org/es/art%C3%ADculos/episodios-de-concientizacion-sobre-seguridad

PBS NOVA – Juego interactivo y videos de concienciación

Descripción: recurso gratuito que incluye juegos y contenido audiovisual que ayuda a comprender la ciberseguridad de forma interactiva y amigable.

https://www.pbs.org/wgbh/nova/labs/lab/cyber/

NOTAS



CENAMEP AIP

Edificio 206, Calle Luis Bonilla,

Ciudad del Saber, Clayton

Ciudad de Panamá, República de Panamá

Teléfono: (+507) 517-3100

www.cenamep.org.pa



ISBN: 978-9962-8557-3-6