REGRESO CIBERSEGURO A CLASES 2026

¡Llevá tu mochila cargada de buenas prácticas para conectarte de forma segura!

GOBIERNO DEL PARAGUAY | MITIC

CERT-PY

Volver a clases en 2026 significa mucho más que abrir los cuadernos: significa conectarse, crear contenido con Inteligencia Artificial, compartir información y construir una identidad digital desde edades cada vez más tempranas.

En este nuevo escenario, la seguridad ya no depende solo de tener una buena contraseña. Hoy debemos aprender a reconocer contenidos manipulados, proteger nuestros datos en plataformas inteligentes, detectar intentos de suplantación y actuar con criterio frente a la información que circula en línea.

El Ministerio de Tecnologías de la Información y Comunicación (MITIC), junto al CERT-Py, presenta esta edición actualizada de "Regreso Ciberseguro a Clases", una guía diseñada para acompañar a estudiantes, familias y docentes en el uso seguro y responsable de la tecnología.
La ciberseguridad comienza con la información. Prepararnos es la mejor forma de protegernos.

Asunción, febrero 2026.

CONTENIDO

#1 LA IA ES PODEROSA, PERO... ¿ES SEGURA?

La Inteligencia Artificial (IA) es una tecnología que ya forma parte de nuestra vida diaria. Nos ayuda a estudiar, investigar, escribir, programar, traducir y crear contenidos.
Pero así como ofrece grandes oportunidades, también presenta riesgos que es importante conocer para usarla de forma segura y responsable.

¿CUÁLES SON LOS PRINCIPALES RIESGOS?

1. PRIVACIDAD DE DATOS

Las herramientas de IA recopilan y procesan grandes cantidades de información.
Todo lo que escribís, consultás o subís a una plataforma puede almacenarse en servidores externos.
Si compartís datos personales como:

- Nombre completo
- Dirección
- Número de documento
- Información bancaria
- Fotos privadas
- Trabajos escolares

esa información podría quedar expuesta o ser utilizada sin tu consentimiento.

2. SEGURIDAD DE LA INFORMACIÓN

Algunas plataformas pueden analizar los datos que ingresás para mejorar sus sistemas. Por eso, nunca debés cargar información sensible o confidencial en herramientas que no conozcas o que no sean confiables.

3. MAL USO DE LA IA

La Inteligencia Artificial también puede utilizarse con fines negativos, como:

- Creación de noticias falsas.
- Suplantación de identidad.
- Deepfakes (videos o audios falsos).
- Estafas y fraudes digitales.
- Acoso en línea.

La Inteligencia Artificial puede ser una gran aliada para estudiar y crear, pero solo si la usás con responsabilidad.
Proteger tus datos, dudar de lo que ves y pensar antes de compartir son las mejores herramientas para navegar el mundo digital de forma segura.

¿CÓMO DETECTAR CONTENIDO FALSO GENERADO POR IA?

Aprender a reconocer señales de alerta puede ayudarte a evitar engaños.

En videos e imágenes:

- Expresiones faciales poco naturales.
- Piel demasiado perfecta o sin imperfecciones.
- Ojos desalineados o parpadeo extraño.
- Movimientos de cabeza deformados.
- Desincronización entre la voz y los labios.
- Manos con dedos deformados o que cambian de forma.

⚠ **Recordá**:
Cuanto más urgente, impactante o emocional sea un contenido, más probable es que busque manipularte.
La mayoría de los deepfakes se difunden en redes sociales o aplicaciones de mensajería, no en medios oficiales.

¿CÓMO USAR LA IA DE FORMA SEGURA?

Al interactuar con herramientas de Inteligencia Artificial:

- No compartas contraseñas ni datos personales.
- No subas documentos importantes o información confidencial.
- Revisá las configuraciones de privacidad de la plataforma.
- Usá solo herramientas reconocidas y confiables.
- Mantené tus dispositivos actualizados.
- Verificá siempre la información antes de compartirla.

PENSAMIENTO CRÍTICO: TU MEJOR DEFENSA

La IA no siempre dice la verdad. Puede:

- Inventar datos.
- Confundir fuentes.
- Dar información incorrecta con mucha seguridad.

Por eso es fundamental:

- Contrastar la información con otras fuentes confiables.
- No utilizar la IA para hacer trampa en tareas escolares.
- Usarla como apoyo para aprender, no como reemplazo del pensamiento propio.

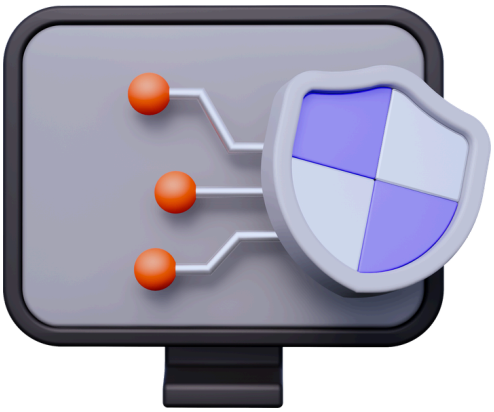
Recordá que podés reportar incidentes de seguridad al CERT-PY:
al correo **abuse@cert.gov.py** indicando la mayor cantidad de detalles.

#2 ATAQUES A CONTRASEÑAS POR FUERZA BRUTA

El ataque de fuerza bruta consiste en diferentes técnicas generalmente automatizadas de prueba y error utilizado para adivinar información de inicio de sesión: usuarios y contraseñas de acceso a sistemas. Los ciberdelincuentes prueban todas las combinaciones posibles con la esperanza de adivinar la combinación correcta.

¿CUÁL ES SU OBJETIVO?

Los ciberdelincuentes que logran acceder a las cuentas o sistemas podrían robar datos personales y realizar acciones maliciosas como transacciones financieras no autorizadas, suplantar identidades, dañar la reputación de una persona u organización y otros.



¿CÓMO ME PROTEJO?

- Usa siempre contraseñas robustas: al menos 16 caracteres combinando letras, números, mayúsculas, minúsculas y caracteres especiales.
- Usá una contraseña diferente para cada sistema.
- Aplicá la autenticación doble factor, siempre que el servicio lo permita.
- Eliminá las cuentas que ya no utilices
- Utilizá gestores de contraseñas para almacenar contraseñas de forma segura.

Recordá que podés reportar incidentes de seguridad al CERT-PY: al correo **abuse@cert.gov.py** indicando la mayor cantidad de detalles.

#3 CONTRASEÑAS SEGURAS

La mejor defensa frente a los ataques de contraseña es garantizar que tus contraseñas sean lo más seguras posible.

- A la hora de crear contraseñas combiná caracteres: Mezclá letras mayúsculas, minúsculas, números y símbolos.
  Ejemplo: ContR4$eÑAsEgUrA
- Una contraseña segura debe tener como mínimo 16 caracteres. La longitud, combinada con la mezcla de caracteres hace más difícil que un delincuente pueda adivinar las contraseñas.
- Evitá usar información conocida o fáciles de deducir como nombres, fecha de cumpleaños, documento de identidad u otros.
  Ejemplo: Carlos1998
- No repitas las contraseñas: Utiliza una contraseña diferente para cada cuenta que tengas.
- Eliminá las cuentas que ya no utilices.
- Cambiá las contraseñas al menos cada 3 meses.

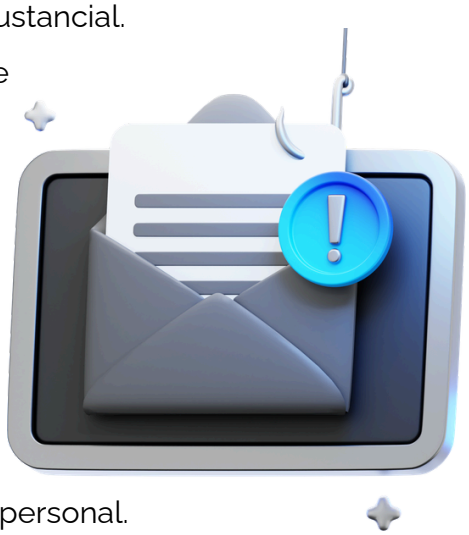
Recordá que podés reportar incidentes de seguridad al CERT-PY: al correo **abuse@cert.gov.py** indicando la mayor cantidad de detalles.

#1 ¿QUÉ ES UN CORREO MALICIOSO?

El correo malicioso es un tipo de mensaje electrónico diseñadopara engañar a la persona que lo recibe, con el fin de causar daño, robarinformación o infectar su dispositivo con software dañino.

¿CÓMO PUEDO RECONOCER UN CORREO MALICIOSO?

- Captarán nuestra atención con una oportunidad demasiado atractiva para ser verdad, como dinero fácil o una cantidad muy sustancial.
- La redacción de los mensajes suele estar llena de fallas de ortografía, errores gramaticales o una mala traducción del texto.
- Generalmente se referirán a nosotros de forma genérica, o en su defecto con alguna prueba como un correo o contraseña nuestra con la que probar su mensaje.
- En algún momento te pedirán dinero por adelantado o que compartas con ellos información personal.



¿CÓMO ACTUAR ANTE UN CORREO MALICIOSO?

- Cuando un correo te resulte sospechoso, verifica la veracidad por otros medios.
- Evitá responder.
- Si no estás seguro, evitá acceder a los enlaces o descargar archivos adjuntos sin antes confirmar su veracidad.
- Evitá realizar descargas archivos adjuntos.
- Evitá compartir correos electrónicos dudosos.

Recordá que podés reportar incidentes de seguridad al CERT-PY:
al correo **abuse@cert.gov.py** indicando la mayor cantidad de detalles.

#5 ¿TENÉS UN CELULAR NUEVO?

Seguí estos consejos para mantenerte a vos y a tu familia a salvo de los riesgos de ciberseguridad y privacidad.

- Revisá las configuraciones de seguridad del dispositivo móvil, protegélo con una contraseña segura y única. No confíes en los valores predeterminados.
- Usá contraseña segura contiene al menos 16 caracteres, letras mayúsculas, minúsculas, números y caracteres especiales.
- Siempre que sea posible, activá la función de doble factor de autenticación (2FA) para mayor seguridad en el inicio de sesión.
- Descargá aplicaciones solo en tiendas verificadas.
- Aseguráte de que todas las aplicaciones y sistemas operativos estén actualizados a la última versión. Siempre que sea posible, activá las actualizaciones automáticas.
- Revisá y ajusta la configuración del dispositivo para evitar el emparejamiento no autorizado con otros dispositivos.
- Hacé una copia de seguridad de los datos de tu dispositivo, que te ayudará rápidamente a recuperarte de en casos ransomware u otras amenazas.
- Instalá en el dispositivo un software de seguridad (Antivirus) de un proveedor de confianza.

Recordá que podés reportar incidentes de seguridad al CERT-PY:
al correo **abuse@cert.gov.py** indicando la mayor cantidad de detalles.

#6 TÉCNICA DE SIM SWAPPING

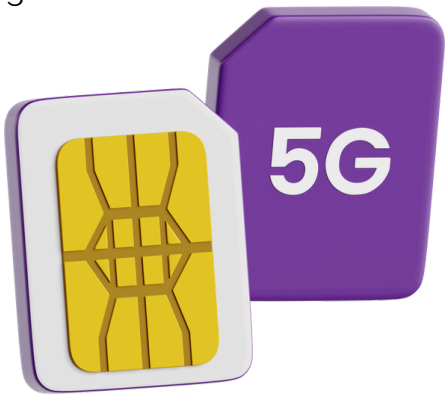
Un estafador obtiene el control de un número de teléfono asumiendo la identidad de la víctima y logra que tu proveedor de servicio móvil transfiera el número a una tarjeta SIM nueva que está en su poder. Una vez que lo logra, también podría evadir cualquier proceso de autenticación de dos factores basado en mensajes de texto de las cuentas asociadas a ese número como WhatsApp y otros, con lo que obtiene el control total sobre el teléfono y las cuentas asociadas.

En caso de que tengas sospechas de ser víctima de un ataque de SIM Swapping, o alguien está usando sin tu permiso tu dispositivo, seguí estos pasos:

- Ponete en contacto con tu compañía de telefonía para informar el caso, y seguí los pasos recomendados.
- Al tener la tarjeta SIM activa de nuevo, podrás volver a utilizar tu dispositivo y hacer el registro de WhatsApp y otras aplicaciones asociadas en tu móvil.

RECOMENDACIONES DE SEGURIDAD PARA ESTE TIPO DE INCIDENTES

- Protegé tu dispositivo con una contraseña única y segura, que combine al menos 16 caracteres con letras mayúsculas, minúsculas, números y caracteres especiales, y/o controles biométricos.
- Siempre que sea posible, activá la verificación de 2 pasos en el dispositivo y aplicaciones que utilices.
- No compartas códigos ni contraseñas con nadie por ningún motivo.
- Si recibiste un código de verificación por mensaje de texto, sin haberlo solicitado, podría significar que alguien más ingresó tu número de teléfono y solicitó el código de registro. Ignóralo y no lo compartas con nadie.
- Eliminá todas las sesiones iniciadas en ordenadores o WhatsApp Web una vez hayas concluido su uso.



Recordá que podés reportar incidentes de seguridad al CERT-PY: al correo **abuse@cert.gov.py** indicando la mayor cantidad de detalles.

#7 MALAS PRÁCTICAS DE SEGURIDAD DIGITAL QUE DEBES EVITAR

- Hacer clic en enlaces y abrir archivos adjuntos en mensajes no solicitados o no verificados.
- Omitir actualizaciones de seguridad.
- Conectar dispositivos USB de terceros sin escaneo con software antivirus.
- Uso y reutilización de contraseñas débiles, como por ejemplo nombre, secuencia de números seguidos, etc.
- No activar la autenticación en dos pasos (2FA).
- No hacer una copia de seguridad (backup).
- Usar y compartir dispositivos laborales para uso personal. No utilizar antivirus en todos los dispositivos.

Recordá que podés reportar incidentes de seguridad al CERT-PY:
al correo **abuse@cert.gov.py** indicando la mayor cantidad de detalles.

#8 ATAQUES POR MALWARE ADWARE

Se trata de un software malicioso diseñado para mostrarnos anuncios no deseados de forma masiva.

¿CÓMO SE PROPAGA/INFECTA/EXTIENDE?

Suelen instalarse junto a otros programas legítimos que, sin darnos cuenta aceptamos y terminamos por instalar en el equipo.

¿CUÁL ES SU OBJETIVO?

Los anuncios dirigidos tienen como objetivo recopilar información sobre nuestra actividad para mostrar publicidad personalizada. Aunque suelen ser molestos, su instalación también puede causar una disminución del rendimiento y problemas de funcionamiento en el dispositivo. Además, a menudo sirven como enlaces a sitios web maliciosos.

¿CÓMO ME PROTEJO?

- Evitá la descarga de aplicaciones de sitios no oficiales.
- Al momento de instalar aplicaciones, prestá atención a los pasos de la instalación, para evitar seleccionar alguna casilla que permita la instalación de programas no deseados.
- Puede ser útil hacer clic en el botón de “Instalación Avanzada” u “Opciones de instalación”.
- Mantené los programas de protección Antivirus y similares siempre activos y actualizados.
- Mantené el sistema operativo, programas utilizados como navegadores y otros siempre actualizados.
- Usá contraseña segura contiene al menos 16 caracteres, letras mayúsculas, minúsculas, números y caracteres especiales.

Recordá que podés reportar incidentes de seguridad al CERT-PY: al correo **abuse@cert.gov.py** indicando la mayor cantidad de detalles.

#9 ATAQUES POR MALWARE SPYWARE

Este malware se instala en nuestros equipos y comienza a recopilar información, como: Nombres de usuario y contraseñas, Datos bancarios, Números de tarjetas de crédito, Historial de navegación web, Mensajes de correo electrónico, Archivos personales, supervisando toda tu actividad para luego compartirla con un usuario remoto. También es capaz de descargar
otros malware e instalarlos en tu equipo.

¿CÓMO SE PROPAGA/INFECTA/EXTIENDE?

Al navegar por páginas webs no seguras, pueden aparecer mensajes en forma de anuncios que, al hacer clic, descargan este tipo de malware.
También es común que se ejecuten como programas adicionales durante la instalación de un software descargados de sitios web no oficiales.

¿CUÁL ES SU OBJETIVO?

Una vez que el malware se instala en el dispositivo, puede llevar a cabo numerosas acciones, como controlar el dispositivo de forma remota, realizar capturas del contenido de aplicaciones y servicios como el correo electrónico o redes sociales.
También es capaz de registrar y capturar el historial de navegación y llevar a cabo grabaciones utilizando la cámara o el micrófono.

¿CÓMO ME PROTEJO?

- Realizá descargas e instalación de software, solamente desde sitios web oficiales.
- Prestá atención a los anuncios y ventanas emergentes que aparezcan durante la navegación, para evitar la instalación de programas maliciosos.
- Evitá hacer clic en archivos o enlaces que provengan de un sitio poco confiable, sin antes verificar la veracidad.
- Usá contraseña segura contiene al menos 16 caracteres, letras mayúsculas, minúsculas, números y caracteres especiales.
- Mantené el sistema y las herramientas de protección (antivirus) siempre activas y actualizadas.
- Tené cuidado al compartir información personal en línea.
- Leé los términos y condiciones antes de instalar cualquier software.
- Realizá análisis periódicos del dispositivo en busca de malware.
- Mantené una copia de seguridad de tus datos importantes.

Recordá que podés reportar incidentes de seguridad al CERT-PY: al correo **abuse@cert.gov.py** indicando la mayor cantidad de detalles.

#10 ATAQUES POR MALWARE TROYANOS

Los troyanos son un tipo de malware que se disfraza de software legítimo para engañar a los usuarios para que lo instalen. Una vez instalado, el troyano puede realizar una variedad de acciones maliciosas, como robar información personal, instalar otro malware o tomar el control del dispositivo.

¿CÓMO SE PROPAGA- INFECTA - EXTIENDE?

A menudo, se propagan por medio de técnicas de ingeniería social, archivos adjuntos maliciosos en correos electrónicos o desde páginas webs poco confiables escondiéndose tras descargas de juegos, películas o aplicaciones no legítimas.

Nosotros, confiados, podríamos no ser conscientes de que nuestros equipos han sido infectados hasta que es demasiado tarde.

¿CUÁL ES SU OBJETIVO?

La mayoría de los troyanos tienen como objetivo controlar nuestro equipo, robar los datos, introducir software malicioso en el equipo y propagarse a otros dispositivos.

¿CÓMO ME PROTEJO?

- Realizá descargas e instalación de software, solamente desde sitios web oficiales.
- Prestá atención a los anuncios y ventanas emergentes que aparezcan durante la navegación, para evitar la instalación de programas maliciosos.
- Evitá hacer clic en archivos o enlaces que provengan de un sitio poco confiable, sin antes verificar la veracidad.
- Usá contraseña segura contiene al menos 16 caracteres, letras mayúsculas, minúsculas, números y caracteres especiales.
- Mantené el sistema y las herramientas de protección (antivirus) siempre activas y actualizadas.
- Tené cuidado al compartir información personal en línea.
- Leé los términos y condiciones antes de instalar cualquier software.
- Realizá análisis periódicos del dispositivo en busca de malware.
- Mantené una copia de seguridad de tus datos importantes.

Recordá que podés reportar incidentes de seguridad al CERT-PY: al correo **abuse@cert.gov.py** indicando la mayor cantidad de detalles.

#11 ATAQUES POR MALWARE RANSOMWARE

Se trata de un tipo de malware que consigue tomar el control del dispositivo para cifrar el acceso al mismo y/o nuestros archivos o discos duros. A cambio de recuperar el control y la información, generalmente estos grupos exigen el pago de un rescate.

¿CÓMO SE PROPAGA/INFECTA/EXTIENDE?

Se propagan por medio de archivos adjuntos en correos electrónicos o desde páginas webs poco fiables, escondiéndose tras descargas de juegos, películas o aplicaciones no legítimas. No somos conscientes del ataque hasta que es demasiado tarde.

¿CUÁL ES SU OBJETIVO?

Una vez que el malware se ejecuta, poco a poco va cifrando todos los archivos y carpetas del dispositivo, impidiendo el acceso a ellos sin una clave. Una vez completada su tarea, el atacante nos envía las instrucciones para el pago y el posterior envío de la clave para descifrar el equipo.

¿CÓMO ME PROTEJO?

- Realiza descargas e instalación de software, solamente desde sitios web oficiales.
- Prestá atención a los anuncios y ventanas emergentes que aparezcan durante la navegación, para evitar la instalación de programas maliciosos.
- Evitá hacer clic en archivos o enlaces que provengan de un sitio poco confiable, sin antes verificar la veracidad.
- Asegurate de utilizar contraseñas seguras y únicas para cada cuenta. Esto implica que cada contraseña contenga al menos 16 caracteres, incluyendo letras mayúsculas, minúsculas, números y caracteres especiales.
- Mantené el sistema y las herramientas de protección (antivirus) siempre activas y actualizadas.

- Tené cuidado al compartir información personal en línea.
- Leé los términos y condiciones antes de instalar cualquier software.
- Realizá análisis periódicos del dispositivo en busca de malware. Mantené
- una copia de seguridad de tus datos importantes.

¿QUÉ DEBES HACER SI CREES QUE DESCARGASTE UN SOFTWARE MALICIOSO?

- **No pagues el rescate.** Pagar el rescate no te garantiza que recuperarás tus archivos y, además, fomenta el desarrollo de este tipo de ataques.
- **Desconecta el dispositivo infectado de la red.** Esto evitará que el ransomware se propague a otros dispositivos.
- **Reportá el ataque.** Podés hacerlo enviando un correo electrónico a abuse@cert.gov.py proporcionando la mayor cantidad de detalles posible para una mejor atención y seguimiento del incidente.

Recordá que podés reportar incidentes de seguridad al CERT-PY: al correo **abuse@cert.gov.py** indicando la mayor cantidad de detalles.

#12 ATAQUES POR INGENIERÍA SOCIAL PHISHING

El phishing es un tipo de estafa en la que los atacantes se hacen pasar por una entidad legítima (como un banco, una empresa de servicios públicos o una red social) para engañar a las víctimas y que revelen información personal o financiera. Los atacantes suelen enviar correos electrónicos o mensajes de texto que parecen ser de la entidad legítima, y que incluyen un enlace o un archivo adjunto infectado. Si la víctima hace clic en el enlace o abre el archivo adjunto, se instala malware en su dispositivo o se la dirige a un sitio web falso que simula ser el sitio web legítimo. En el sitio web falso, se le pide a la víctima que introduzca sus datos personales o financieros, como su nombre, dirección, número de teléfono, contraseña o información bancaria.

¿CÓMO SE PROPAGA/INFECTA/EXTIENDE?

El principal medio de propagación es el correo electrónico donde, fingiendo ser una entidad de confianza, el atacante lanza un cebo. Generalmente suele ser un mensaje urgente o una promoción muy atractiva, para motivarnos a hacer clic en el enlace o archivo adjunto, o a compartir los datos que el atacante pide en su mensaje.

¿CUÁL ES SU OBJETIVO?

Su objetivo es obtener datos personales y/o bancarios de los usuarios, haciéndonos creer que los estamos compartido con alguien de confianza. También pueden utilizar esta técnica para que descarguemos malware con él podría infectar y/o tomar control del dispositivo.

¿CÓMO ME PROTEJO?

El principal consejo es ser precavido y leer el mensaje detenidamente, especialmente si se trata de entidades con pedidos urgentes, promociones demasiado atractivas.

ADEMÁS, OTRAS PAUTAS QUE PODÉS SEGUIR PARA EVITAR SER VÍCTIMA DE UN PHISHING SON:

- Evitá abrir correos electrónicos de remitentes desconocidos o sospechosos sin verificar la autenticidad del remitente. Además, es importante no hacer clic en enlaces ni descargar archivos adjuntos de esos correos.
- Mantené siempre actualizado el sistema operativo de tu dispositivo.
- Mantené siempre activo y actualizado el antivirus de tus dispositivos.
- Escribir directamente la URL del servicio en el navegador, en lugar de llegar a la web a través de enlaces disponibles desde páginas de terceros, en correos electrónicos o en mensajes de texto.
- Evitá facilitar tus datos personales (número de teléfono, nombre, apellidos, dirección o correo electrónico) o bancarios en cualquier página.
- Infórmate previamente y lee los textos legales de la web para descartar un posible mal uso de tus datos.
- Asegurate de utilizar contraseñas seguras y únicas para cada cuenta. Esto implica que cada contraseña contenga al menos 16 caracteres, incluyendo letras mayúsculas, minúsculas, números y caracteres especiales.
- Desconfiá de promociones online que requieran facilitar información personal.

Recordá que podés reportar incidentes de seguridad al CERT-PY: al correo **abuse@cert.gov.py** indicando la mayor cantidad de detalles.

#13 ¿POR QUÉ ES IMPORTANTE REALIZAR UN BACKUP?

La copia de seguridad, también llamada respaldo o backup, se refiere a la copia de archivos físicos o virtuales o bases de datos a un sitio secundario para su preservación en caso de falla del equipo u otra catástrofe.

CONSEJOS PARA TUS COPIAS DE SEGURIDAD:

- **Realiza backup de forma periódica.** Poco sirve tener una copia de seguridad si ésta se encuentra desactualizada ya que los datos más recientes no se podrían recuperar.
- **No retrases la realización del backup.** Es importante que se empiece a realizar este backup lo antes posible y actualizarlo periódicamente según nuestro ritmo de generación y actualización de datos.
- **Almacena tus copias de seguridad en sitios diferentes.** Es importante almacenar tus copias de seguridad en ubicaciones diferentes para mitigar el riesgo de pérdida total en caso de desastres naturales o incendios. Si ambos, los datos originales y las copias de seguridad se encuentran en el mismo lugar y se ven afectados, la utilidad de tener una copia de seguridad se reduce considerablemente.
- **Cifra toda la información confidencial.** Tanto si almacenamos nuestra copia de seguridad en un medio físico como en la nube es importante cifrar aquellos datos que sean confidenciales.

Recordá que podés reportar incidentes de seguridad al CERT-PY: al correo **abuse@cert.gov.py** indicando la mayor cantidad de detalles.

#14 SEGURIDAD PARA TELÉFONOS MÓVILES

RIESGOS EN EL USO DE DISPOSITIVOS MÓVILES

- Pérdida o robo de información
- Violación de la privacidad
- Robo de dispositivos
- Robo de credenciales (usuario y password)
- Conexión a redes inseguras
- Los datos de GPS pueden ser muy útiles para ciertas tareas, pero permiten a otros saber dónde nos encontramos en cada momento.
- Configuraciones de seguridad no revisadas.

MEDIDAS DE SEGURIDAD PARA LA PROTECCIÓN DE LA INFORMACIÓN EN DISPOSITIVOS MÓVILES

- Aseguráte de utilizar contraseñas seguras y únicas para cada cuenta que utilizás en tu dispositivo móvil. Esto implica que cada contraseña contenga al menos 16 caracteres, incluyendo letras mayúsculas, minúsculas, números y caracteres especiales.
- Protegé el dispositivo con contraseña robusta, PIN de más de cuatro caracteres o biometría cuando sea posible.
- Activá la autenticación de dos factores a las aplicaciones instaladas siempre que sea posible. Mantené actualizado el sistema operativo de tu dispositivo móvil.
- Actualizá las aplicaciones regularmente.
- Instalá las últimas actualizaciones de seguridad.

- Descargá aplicaciones solo de fuentes confiables.
- Leé las reseñas de las aplicaciones antes de descargarlas.
- Realizá copias de seguridad de tus datos regularmente.
- Encriptá tus datos si es posible.
- No almacenes información confidencial en tu dispositivo móvil.
- Desactivá la conexión Wi-Fi y Bluetooth cuando no la estés usando.
- Empareja tu dispositivo móvil solo con dispositivos Bluetooth conocidos
- Instalá una aplicación de rastreo en tu dispositivo móvil en caso de robo o pérdida.
- Instalá un software antivirus y anti-malware en tu dispositivo móvil.
- Realizá análisis regulares de tu dispositivo móvil en busca de malware.

Recordá que podés reportar incidentes de seguridad al CERT-PY: al correo **abuse@cert.gov.py** indicando la mayor cantidad de detalles.

#15 MEDIDAS DE SEGURIDAD PARA PROTEGER TU PERFIL EN REDES SOCIALES

MEDIDAS DE SEGURIDAD

- Revisáyajustá la configuración de privacidad de cada red social que uses.
- Limitálavisibilidad de tu perfil, publicaciones e información personal a tus amigosoconocidos.
- Evitácompartir información personal como tu dirección, número de teléfonoodatos bancarios.
- Asegurátede utilizar contraseñas seguras y únicas para cada cuenta. Esto implicaque cada contraseña contenga al menos 16 caracteres, incluyendo letrasmayúsculas, minúsculas, números y caracteres especiales.
- Activálaautenticación de dos factores.
- Evitácompartir información confidencial.
- Tené cuidado al hacer clic en enlaces o descargar archivos de publicaciones o mensajes en redes sociales, sin confirmar el origen.
- Evitá acceder a sitios web o aplicaciones de dudosa procedencia.
- Protegé tu dispositivo móvil con un antivirus y anti-malware.
- Mantené actualizado el software de tu dispositivo móvil y ordenador.
- Instalá las últimas actualizaciones de seguridad para las aplicaciones de redes sociales que uses.

Recordá que podés reportar incidentes de seguridad al CERT-PY: al correo **abuse@cert.gov.py** indicando la mayor cantidad de detalles.


www.cert.gov.py