Copias de seguridad

Producción:

cert.br nic.br cgi.br

¡HAZ COPIAS DE SEGURIDAD!

¿Te imaginas lo que sucedería si perdieras todos tus datos, tus fotos y documentos? Ya sea en tu celular, *tablet* o computadora, no esperes a que pase lo peor para darte cuenta de lo importante que son tus datos.

Aquí te damos algunos consejos para que no pierdas tus datos.

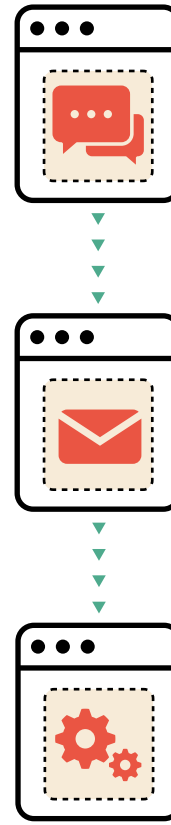
RESPALDA TUS DATOS

Puedes perder tus datos en cualquier momento, ya sea por accidente, por robo, por una falla del sistema, una actualización incorrecta o un defecto de tu dispositivo. Si tienes copias de seguridad, podrás recuperarlas, minimizando así los problemas.

» Utiliza una o más opciones, como por ejemplo:

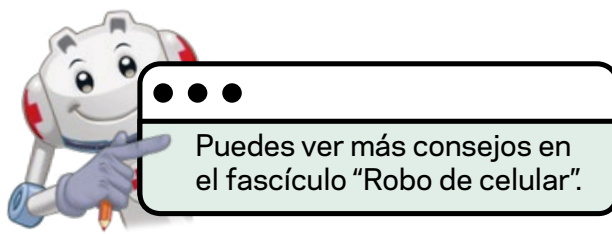
- servicios en la nube
- sincronización con otro dispositivo
- un disco externo o un *pendrive*

NO TE OLVIDES DE CREAR COPIAS DE SEGURIDAD DE TU CELULAR



Los celulares pueden ser objeto de robo y son fáciles de perder o dañar. Una copia de seguridad permite restaurar las fotos, los *mails*, los mensajes, las aplicaciones y las configuraciones, e incluso hacen que sea más fácil cambiar de aparato.

- Habilita la opción de copia de seguridad nativa del sistema
  - si no tienes un plan de datos, configúralo para que solo use Wi-Fi
- También busca otras alternativas, como un *pendrive* o la sincronización con una computadora

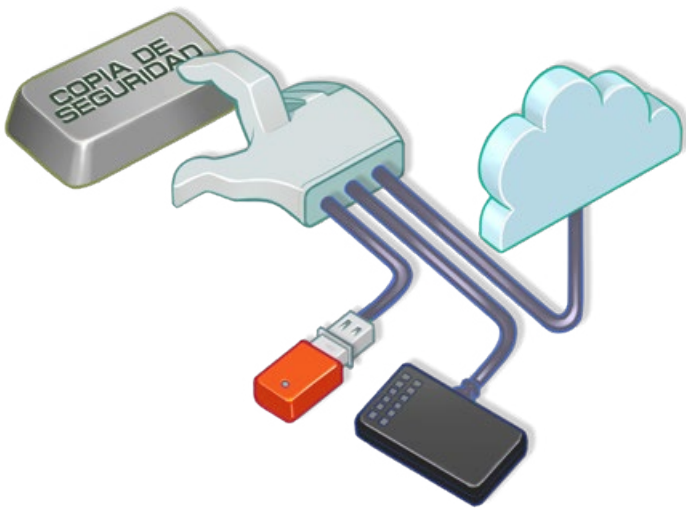


Puedes ver más consejos en el fascículo “Robo de celular”.

HABILITA LAS COPIAS DE SEGURIDAD AUTOMÁTICAS

Las copias de seguridad automáticas son menos propensas a errores y olvidos, lo que ayuda a mantener copias actualizadas y a restaurar los datos si cambiamos o perdemos el teléfono o la computadora.

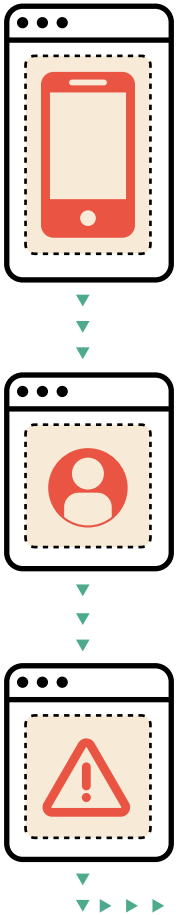
- Selecciona la frecuencia de acuerdo con tus necesidades, por ejemplo, una vez por hora, por día o por semana
- Si usas discos externos o *pendrives*, recuerda conectarlos para que se pueda crear la copia de seguridad



EN CASOS ESPECIALES, HAZ RESPALDOS MANUALES

En situaciones de riesgo, como viajes, actualizaciones del sistema, mantenimiento o reemplazo de un dispositivo, debemos complementar las copias de seguridad automáticas con copias manuales. Esto garantiza que también se copien los archivos importantes o los que se han modificado recientemente.

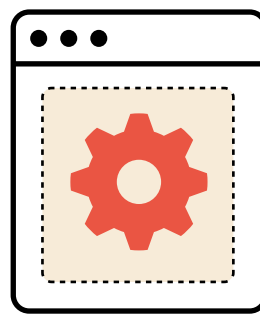
» Usa opciones como “Crear copia de seguridad ahora” para asegurar que tus copias de seguridad estén actualizadas

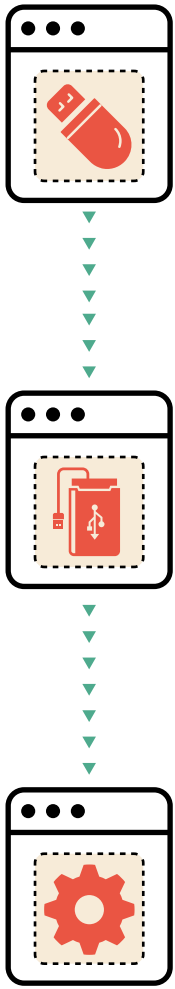


NO COPIES DATOS INNECESARIOS

Los datos ocupan lugar y pueden requerir espacios de almacenamiento cada vez más grandes. Seleccionar qué datos copiar ayuda a reducir los costos y mejora las velocidades de copia y restauración.

- De ser posible, selecciona los elementos que no se deben incluir en las copias de seguridad, como archivos o directorios específicos
- Verifica en cuáles aplicaciones están activadas las copias de seguridad y deshabilita las que no necesites





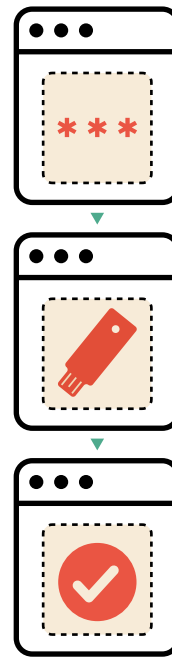
HAZ MÁS DE UNA COPIA DE SEGURIDAD

La expresión "Quien tiene una, no tiene ninguna" refuerza la importancia de tener varias copias de seguridad, ya que si precisas restablecer una copia de seguridad y esta no funciona, tendrás otra a la cual recurrir.

- Ten al menos 2 copias de tus datos
- Guarda las copias en lugares diferentes
  - por ejemplo: una en la nube y otra en un *pen drive*

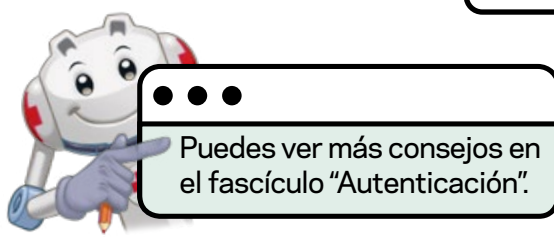
ACTIVA LA VERIFICACIÓN DE DOS PASOS EN LOS SERVICIOS EN LA NUBE

Los atacantes buscan los servicios en la nube por la gran cantidad de datos que almacenan. El uso exclusivo de contraseñas no alcanza para garantizar la seguridad, por lo que las contraseñas deben reforzarse con otras formas de autenticación.



» Elige la opción disponible que te parezca más práctica y segura, por ejemplo:

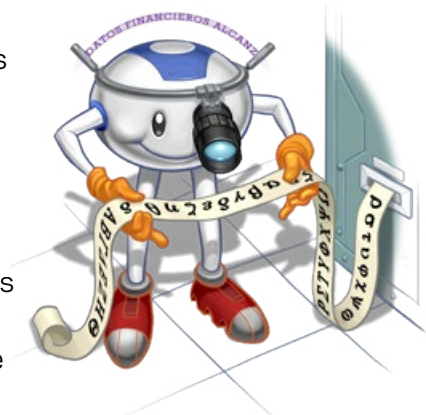
- usar una llave de seguridad física
- usar una aplicación en tu celular para generar códigos de verificación
- recibir códigos por mensaje de texto o de voz



PROTEGE LAS COPIAS DE SEGURIDAD CONTRA ACCESOS INDEBIDOS

Si los medios físicos no están protegidos, alguien podría acceder a tus archivos. Tus datos también podrían estar en riesgo si se transmiten a través de conexiones que no son seguras.

- Habilita el cifrado siempre que sea posible
  - tanto para las copias de seguridad en la nube como en los medios físicos
- No dejes los medios físicos —los dispositivos donde guardas tus copias de seguridad— conectados todo el tiempo
  - conéctalos periódicamente para crear tus copias de seguridad
- Guarda esos dispositivos en un lugar seguro
- Elije servicios en la nube donde los datos viajen a través de canales seguros (https) y que ofrezcan verificación de dos pasos



PRESTA ATENCIÓN A LAS NOTIFICACIONES Y PRUEBA TUS COPIAS

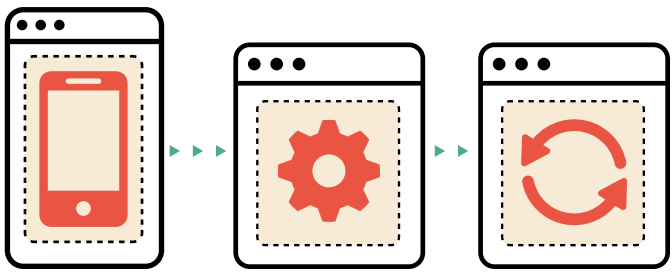
Prestar atención a las notificaciones del sistema y acceder de vez en cuando a tus copias de seguridad evita sorpresas, como archivos dañados, opciones mal configuradas, dispositivos defectuosos o áreas de almacenamiento llenas.

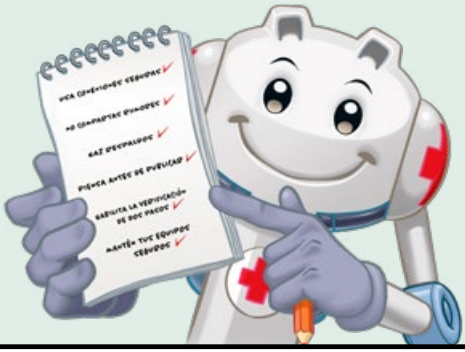
- Verifica que haya espacio disponible en las áreas de almacenamiento
- Si se están llenando:
  - borra las copias de seguridad más antiguas
  - elimina los archivos innecesarios
  - aumenta el tamaño del área destinada al almacenamiento
- Reemplaza los medios físicos defectuosos
- Haz un respaldo manual para garantizar que tengas una copia de seguridad actualizada

MANTÉN LOS SISTEMAS Y LAS APLICACIONES ACTUALIZADOS

Corregir las vulnerabilidades de los sistemas y las aplicaciones evita que sean explotadas por el *malware*, por ejemplo, el *ransomware* que cifra los datos y borra las copias de seguridad de manera que no puedas recuperarlas.

- Instala actualizaciones de forma regular
  - habilita la actualización automática siempre que sea posible
- Instala mecanismos de seguridad como un antivirus y un *firewall* personal, y mantenlos actualizados





MÁS INFORMACIÓN

» Para obtener más información sobre este y otros asuntos relacionados con los cuidados que debes tener en Internet, consulta los demás Fascículos de la Cartilla de Seguridad para Internet, disponibles en: **https://cartilla.cert.br/**

cert.br

CERT.br **(https://cert.br/)** es un Grupo de Respuesta a Incidentes de Seguridad (CSIRT) con jurisdicción nacional y de último recurso, mantenido por NIC.br. Además de la gestión de incidentes, también trabaja en la sensibilización en temas de seguridad, conciencia situacional y transferencia de conocimiento, siempre respaldado por una fuerte integración con las comunidades de los CSIRT nacionales e internacionales.

nic.br

El Núcleo de Información y Coordinación del Punto BR - NIC.br **(https://nic.br/)** es una entidad civil de derecho privado y sin fines de lucro, encargada de la operación del dominio .br, así como de la asignación de números IP y del registro de Sistemas Autónomos en Brasil. Lleva adelante acciones y proyectos que benefician la infraestructura de Internet en Brasil.

cgi.br

El Comité Gestor de Internet en Brasil **(https://cgi.br/)** es responsable por el establecimiento de directrices estratégicas relacionadas con el uso y el desarrollo de Internet en Brasil. Coordina e integra todas las iniciativas de servicios de Internet en Brasil, promoviendo la calidad técnica, la innovación y la difusión de los servicios ofrecidos.

mayo de 2023