Autenticación

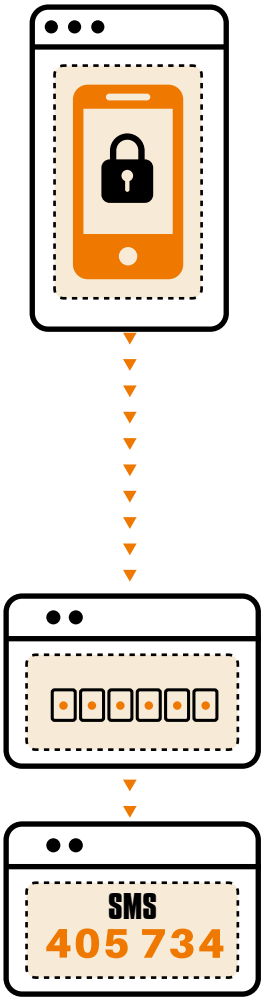
Producción:

cert.br nic.br cgi.br

PROTEGE TU VIDA DIGITAL: USA UNA AUTENTICACIÓN FUERTE

La autenticación ayuda a proteger el acceso a tus cuentas al evitar que alguien se haga pasar por ti. Pero con tantos ataques y filtraciones de datos, usar solo contraseñas puede no ser suficiente protección. Hay que reforzarlas con un segundo paso de verificación. Aquí te presentamos las precauciones que debes tener para que tus cuentas sean más seguras.

CUIDADOS FUNDAMENTALES PARA PROTEGER TUS CUENTAS



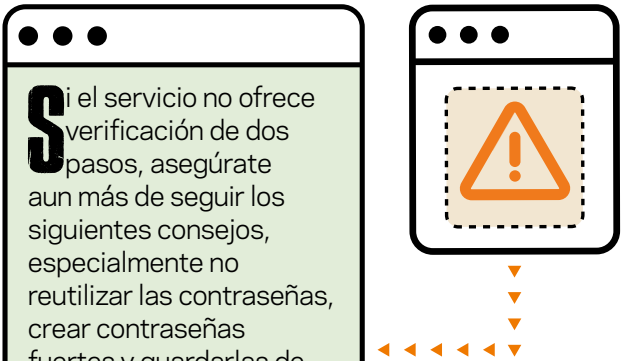
ACTIVA LA VERIFICACIÓN DE DOS PASOS

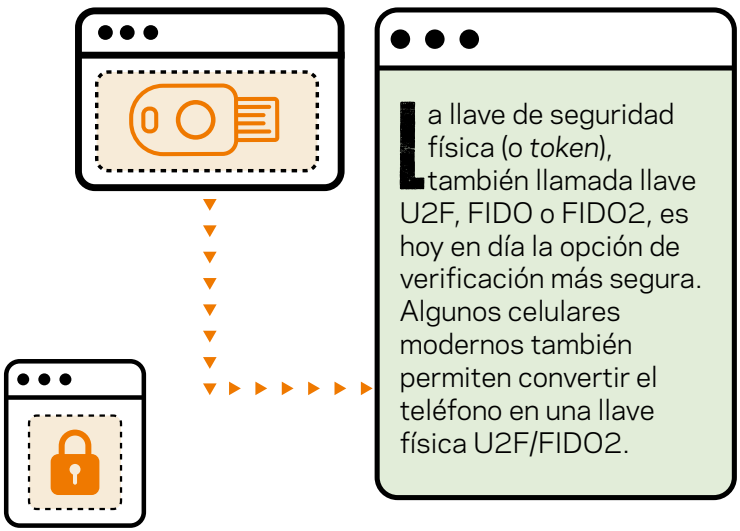
La verificación de dos pasos agrega una segunda capa de protección para acceder a tus cuentas. Cuando está activada, aunque un atacante descubra tu contraseña, necesitará otros datos para ingresar a tu cuenta.

» Elige el método que te parezca más práctico y seguro, por ejemplo:

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

Si el servicio no ofrece verificación de dos pasos, asegúrate aun más de seguir los siguientes consejos, especialmente no reutilizar las contraseñas, crear contraseñas fuertes y guardarlas de forma segura.





La llave de seguridad física (o *token*), también llamada llave U2F, FIDO o FIDO2, es hoy en día la opción de verificación más segura. Algunos celulares modernos también permiten convertir el teléfono en una llave física U2F/FIDO2.

USA LA VERIFICACIÓN DE DOS PASOS DE FORMA SEGURA

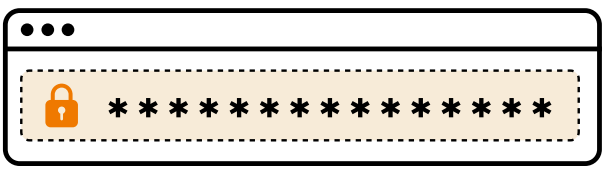
Para que la verificación de dos pasos realmente proteja tus cuentas, hay algunos otros consejos que debes seguir.

- Prefiere las llaves de seguridad físicas o las aplicaciones generadoras de códigos de verificación para celulares
  - usa SMS solo si no tienes otras opciones
- Rechaza todas las solicitudes de autorización de inicio de sesión si no estás intentando acceder a tu cuenta
- Genera códigos de respaldo para usar cuando no haya otras opciones de autenticación disponibles
  - guárdalos en un lugar seguro

USA UNA CONTRASEÑA DIFERENTE PARA CADA CUENTA

Reutilizar las contraseñas, es decir, usar la misma contraseña en distintos sitios, es arriesgado, ya que alcanza con que un atacante descubra la contraseña de una cuenta para que pueda acceder a las otras cuentas donde la has usado.

» Si sospechas que han descubierto una contraseña que has usado en varios lugares, cámbiala inmediatamente en todos los lugares donde la utilizas

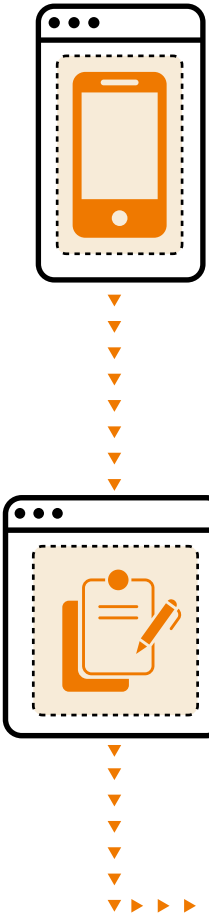


CREA CONTRASEÑAS FUERTES

Si tus contraseñas son fáciles de descubrir (débiles), tus cuentas y dispositivos de acceso pueden ser fáciles de vulnerar.

- Crea contraseñas largas
  - escoge, por ejemplo, tres palabras aleatorias
- Agrega diferentes caracteres para hacerlas aún más fuertes
  - mezcla números, caracteres especiales y letras mayúsculas y minúsculas
- Evita usar secuencias del teclado
- No utilices datos personales como nombres, apellidos, fechas u otros datos que publiques en las redes sociales

¿Te resulta difícil recordar tantas contraseñas? Mira el siguiente consejo sobre cómo guardarlas de forma segura.



GUARDA TUS CONTRASEÑAS DE FORMA SEGURA

Son tantas las contraseñas que es imposible acordarse de todas. Para evitar el uso de contraseñas débiles, escoge el método de gestión que te resulte más práctico y seguro.

» Puedes, por ejemplo:

- utilizar aplicaciones de gestión de contraseñas,
- anotarlas en un papel y guardarlo en un lugar seguro o
- grabarlas en un archivo cifrado

CAMBIA LAS CONTRASEÑAS EXPUESTAS EN UNA FILTRACIÓN

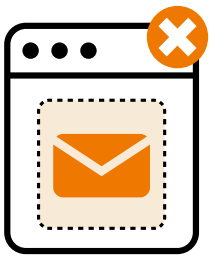
Lamentablemente, las filtraciones de datos ocurren y tus contraseñas pueden verse afectadas. Si te enteras de que una de tus contraseñas ha sido expuesta, es importante que la cambies de inmediato.

- Presta atención a las noticias sobre filtraciones de datos en los servicios que utilizas
- Utiliza los servicios de monitoreo de contraseñas que incluyen algunos sistemas y navegadores

TEN ESPECIAL CUIDADO CON LAS CUENTAS MÁS IMPORTANTES

Cuanto más "valiosa" tu cuenta, más atractiva es para los atacantes. Por ejemplo: una cuenta bancaria hackeada puede generar perjuicios financieros, mientras que una cuenta de correo electrónico hackeada se puede usar para recuperar contraseñas de otras aplicaciones.

- Evita guardar las contraseñas de tus cuentas importantes en los navegadores, por ejemplo, las contraseñas para acceder a tu banco, correo electrónico o ID de sistema
- No permitas el inicio de sesión automático para tus cuentas importantes



NO COMPARTAS TUS CONTRASEÑAS Y CÓDIGOS DE VERIFICACIÓN

Si obtiene tus contraseñas y códigos de verificación, un atacante podría ingresar a tus cuentas, robar tu identidad y estafar en tu nombre, perjudicándote a ti y a tus contactos.

» Nunca compartas tus contraseñas o códigos de verificación en mensajes, correos electrónicos o llamadas

CONFIGURA TUS DISPOSITIVOS PARA QUE SOLICITEN AUTENTICACIÓN EN LA PANTALLA DE INICIO

Alguien que tiene acceso físico a un dispositivo desbloqueado puede acceder fácilmente a ellos.

- Bloquea la pantalla de tu computadora de escritorio o portátil, tu *tablet* y tu celular antes de alejarte de ellos
- Configura tu celular y tu *tablet* para que te avise al usar reconocimiento facial
- Si usas un patrón de desbloqueo:
  - evita usar pocos puntos o diseños muy simples, como las letras
  - configúralo para que el trazo no sea visible

Patrón de desbloqueo es como se llaman las contraseñas que se "dibujan" en la pantalla al unir distintos puntos.

ESCOGE PREGUNTAS Y CONSEJOS DE SEGURIDAD DIFÍCILES DE ADIVINAR

Las preguntas y los consejos de seguridad son recursos útiles que te ayudan a recordar o recuperar tus contraseñas, pero los atacantes pueden abusar de ellos para hackear tus cuentas.

- Selecciona preguntas de seguridad cuyas respuestas sean difíciles de adivinar
- Escoge consejos de seguridad que sean lo suficientemente vagos como para que nadie los descubra y lo suficientemente claros para que los entiendas
- Registra un correo electrónico de recuperación al que accedas con frecuencia, para no olvidar esa contraseña también

TEN MUCHO CUIDADO CON LAS CUENTAS QUE USAS COMO LOGIN SOCIAL

Algunos servicios te permiten usar una cuenta externa para autenticarte, en general tu red social o servicio de correo electrónico. Si tus accesos están centralizados en una sola cuenta, cuando la contraseña correspondiente queda expuesta, todos los servicios que la usan estarán en riesgo.

» Verifica las opciones que te ofrece la cuenta que usas como *login* social
  - limita la información y los servicios a los que puede acceder
  - elimina los accesos concedidos si ya no son necesarios o si desconfías que puede ser un servicio malicioso

NO IGNORES LOS AVISOS NI LAS ALERTAS DE INICIO DE SESIÓN

Prestar atención a los avisos y alertas que envían los sistemas indicando que hubo un intento de acceso a tus cuentas ayuda a detectar los usos indebidos.

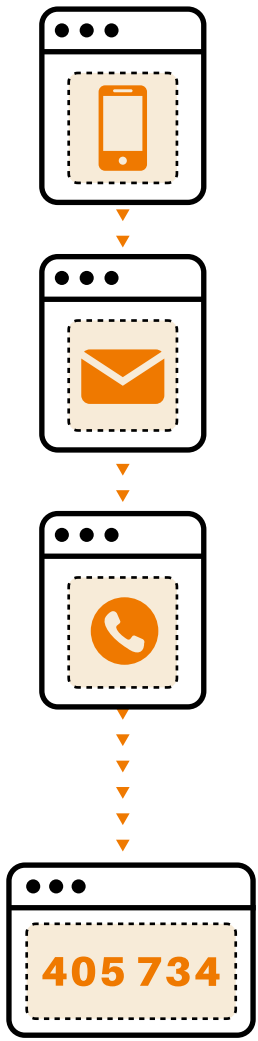
- Observa la información para ver desde dónde y cuándo se produjeron los últimos accesos a tu cuenta y verifica si efectivamente fuiste tú
- Si te das cuenta de que alguien accedió a tu cuenta de forma indebida:
  - accede a la cuenta directamente, sin hacer clic en ningún enlace
  - cambia la contraseña
- Si aún no lo has hecho, activa inmediatamente la verificación en dos pasos en tus cuentas

TEN CUIDADO DE NO COMPROMETER TU CONTRASEÑA

Para comprometer tus contraseñas, los atacantes pueden observarte cuando las digitas, convencerte de hacer clic en enlaces maliciosos (*phishing*) o infectar los dispositivos que usas.

- No abras todos los enlaces y archivos que recibas
  - solo lee un código QR si confías en la fuente
- Mantén sus dispositivos y aplicaciones actualizados
- Evita digitar tus contraseñas en dispositivos de terceros
- Usa conexiones seguras, como https para acceder a los sitios web
- Asegúrate de que no haya personas ni cámaras a tu alrededor cuando digites tus contraseñas

OTRAS PRECAUCIONES CON VERIFICACIÓN DE DOS PASOS



MANTÉN ACTUALIZADOS LOS DATOS QUE USAS PARA VERIFICAR TU IDENTIDAD

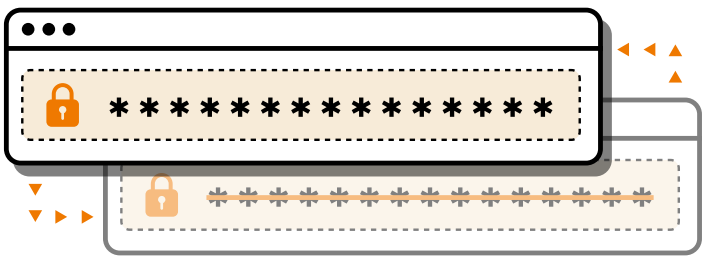
Algunos mecanismos de verificación se basan en algo que sólo tú tienes para confirmar tu identidad, por ejemplo, tu teléfono celular. Esto puede convertirse en un problema si tu teléfono no está disponible o si has cambiado de número.

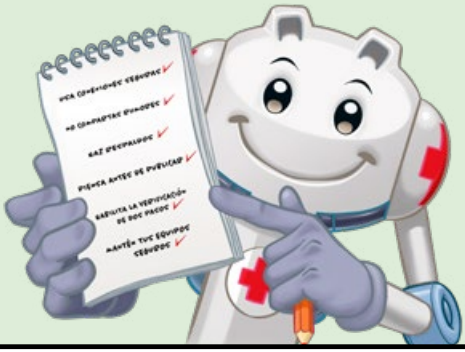
- Mantén actualizados los datos para recibir los códigos de verificación
- Registra correos electrónicos y números de teléfono alternativos para recibir los códigos de verificación en caso que los principales no estén disponibles

TEN CUIDADO DE NO PERDER TUS MECANISMOS DE AUTENTICACIÓN

Si pierdes el mecanismo configurado como segundo factor de autenticación, otra persona puede usarlo para intentar hacerse pasar por ti.

- Si pierdes o cambias un dispositivo registrado como de confianza, elimínalo de los servicios donde esté configurado
- Guarda tu llave de seguridad física en un lugar seguro
  - si la pierdes, notifica inmediatamente al servicio donde la utilizas
- Si los pierdes o sospechas que alguien ha accedido a ellos, revoca y genera nuevamente tus códigos de respaldo





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.

noviembre de 2022