Celulares y tablets

Producción:

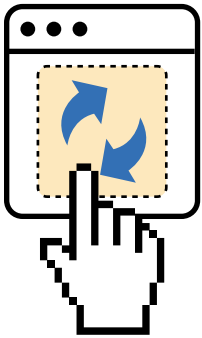
cert.br nic.br cgi.br

PROTECCIÓN Y SEGURIDAD DONDE SEA QUE ESTÉS

Los celulares y las *tablets* son dispositivos móviles que te acompañan a todas partes y su seguridad merece una atención especial.

Aquí verás cómo proteger tu celular y tu *tablet*.

PRECAUCIONES QUE DEBES TENER AL UTILIZAR TU DISPOSITIVO



INSTALA LAS ACTUALIZACIONES Y EVITA APLICACIONES INNECESARIAS

Los sistemas y las aplicaciones tienen fallas (vulnerabilidades) que se pueden aprovechar para hackear el dispositivo, capturar datos o instalar *malware*. Aplicar las actualizaciones evita que te conviertas en víctima o que seas parte de un ataque.

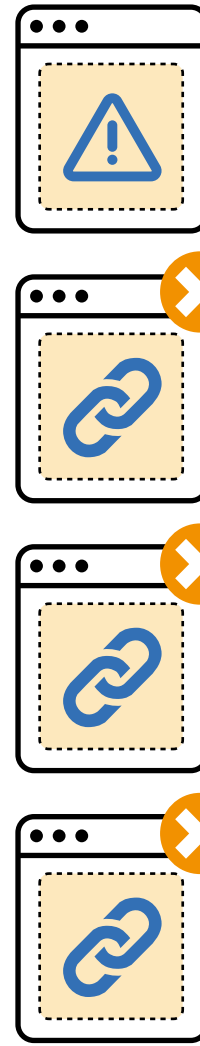
- Mantén el sistema y las aplicaciones actualizados
  - habilita la actualización automática siempre que sea posible
  - acepta siempre las actualizaciones de seguridad
  - también actualiza los relojes, auriculares y otros accesorios "inteligentes" conectados al dispositivo
- Solo mantén instaladas las aplicaciones que realmente usas

SOLO DESCARGA APLICACIONES DE LAS TIENDAS OFICIALES

Desafortunadamente, hay aplicaciones que se crean con fines maliciosos y las tiendas oficiales suelen tener políticas más estrictas y mecanismos más rápidos para eliminarlas una vez detectadas.

- Usa solo la tienda oficial del fabricante del sistema o del dispositivo
  - nunca instales aplicaciones recibidas a través de mensajes o enlaces
- Aun así, ten cuidado con las aplicaciones falsas
  - antes de instalarla, confirma el nombre de la aplicación y que el desarrollador sea quien debería ser

NO HAGAS CLIC EN TODOS LOS ENLACES QUE RECIBES



Los enlaces maliciosos se usan para dirigir a los usuarios hacia páginas falsas o con *malware*. Los atacantes intentan engañar a los usuarios para que hagan clic en estos enlaces utilizando trucos como enviarlos desde cuentas falsas o hackeadas para aprovechar la confianza entre personas conocidas.

- Antes de hacer clic, intenta analizar el contexto y observar los detalles
  - si dudas, no hagas clic
- Desconfía de los mensajes que recibas, aunque vengan de una persona conocida
  - de ser necesario, contacta a quien supuestamente envió el mensaje usando otro medio de comunicación
- Solo lee un código QR si confías en la fuente

BLOQUEA LA PANTALLA DE INICIO DE TU DISPOSITIVO

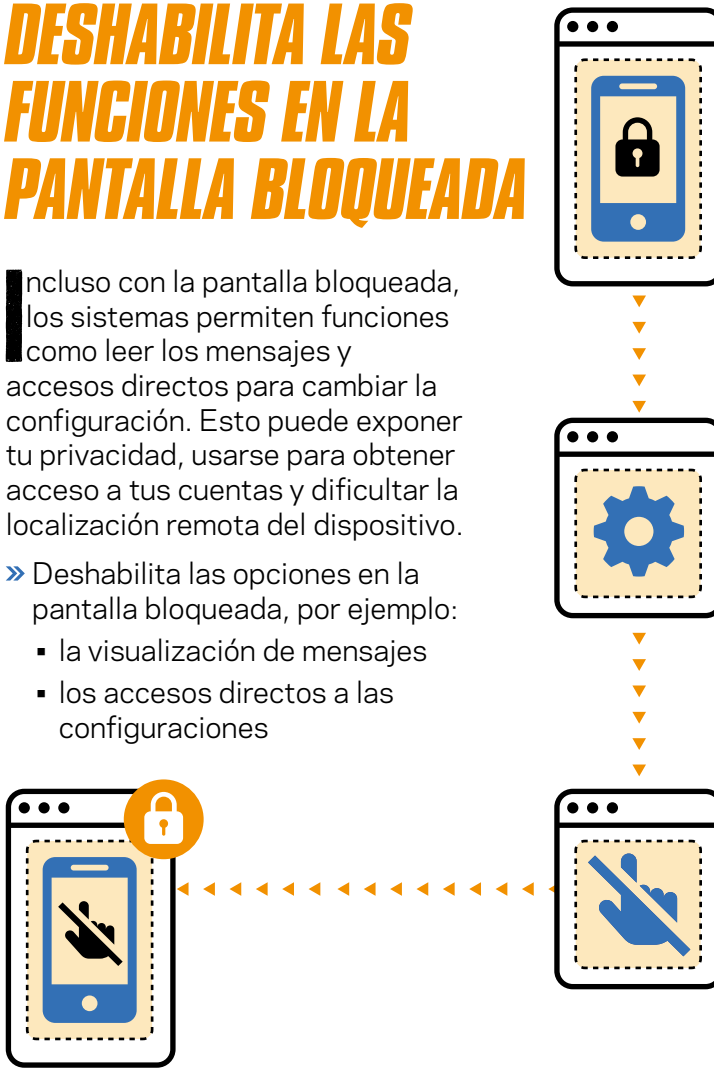
Si alguien toma tu dispositivo desbloqueado, puede acceder al contenido y usar las aplicaciones haciéndose pasar por ti para enviar mensajes, publicar en las redes sociales o realizar transacciones en las aplicaciones bancarias y de comercio electrónico.

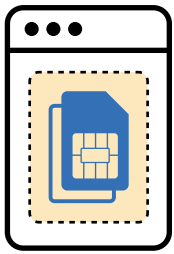
- Configura un método de autenticación en la pantalla de inicio
  - usa contraseñas largas, en lo posible alfanuméricas
  - evita usar un patrón de desbloqueo con pocos puntos o de diseño muy simple, como las letras
- Activa el bloqueo automático de la pantalla en el menor tiempo disponible

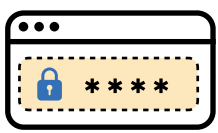
DESHABILITA LAS FUNCIONES EN LA PANTALLA BLOQUEADA

Incluso con la pantalla bloqueada, los sistemas permiten funciones como leer los mensajes y accesos directos para cambiar la configuración. Esto puede exponer tu privacidad, usarse para obtener acceso a tus cuentas y dificultar la localización remota del dispositivo.

» Deshabilita las opciones en la pantalla bloqueada, por ejemplo:
- la visualización de mensajes
- los accesos directos a las configuraciones







PROTEGE EL CHIP CON UNA CONTRASEÑA

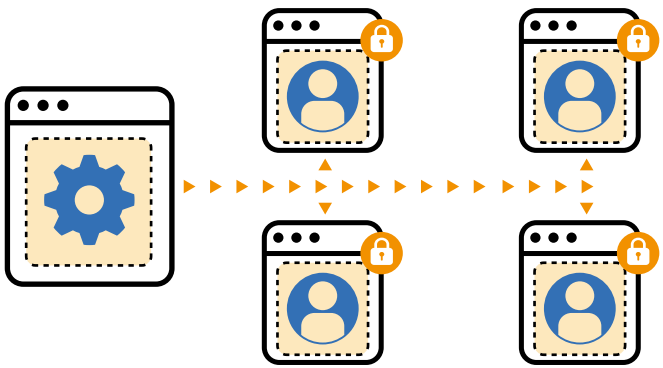
El *chip* conecta tu dispositivo a la red de telefonía móvil. Proteger el *chip* con una contraseña evita su uso indebido en otro aparato, impidiendo que otra persona reciba mensajes con códigos de verificación que podría usar para acceder a tus cuentas y/o cambiar tus contraseñas.

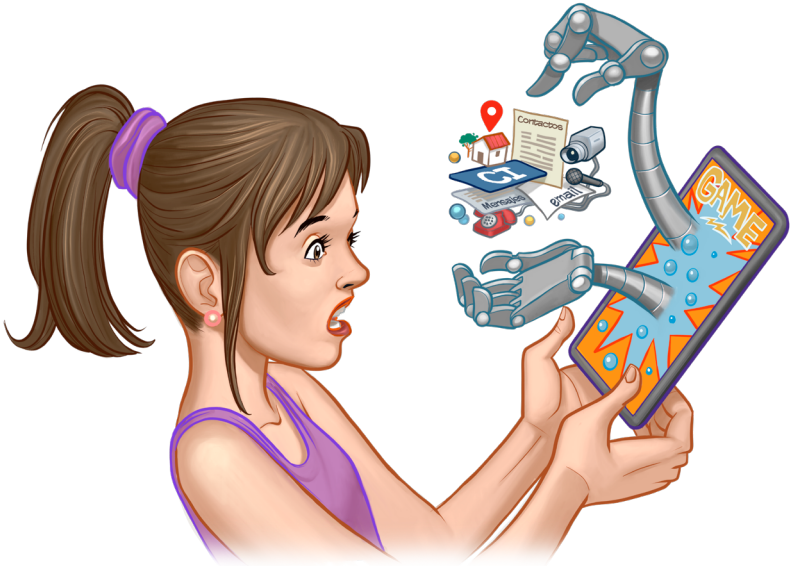
- Activa el bloqueo del *chip*
- Cambia el PIN predeterminado
  - verifica el de tu operadora

LIMITA EL ACCESO SI OTRA PERSONA UTILIZA TU DISPOSITIVO

Compartir o tomar prestado un dispositivo puede exponer tu privacidad o tener consecuencias no deseadas, incluso en forma accidental.

- Siempre que sea posible, crea perfiles separados para cada usuario o invitado
- Para permitir que alguien use una aplicación específica, bloquéala en la pantalla
  - función "Acesso guiado" en iOS o "Fijar pantalla" en Android
- Si el dispositivo es usado por niños, usa controles parentales
  - recuerda hablar con ellos sobre el uso seguro y responsable de internet





AJUSTA LOS PERMISOS DE LAS APLICACIONES SEGÚN SU USO

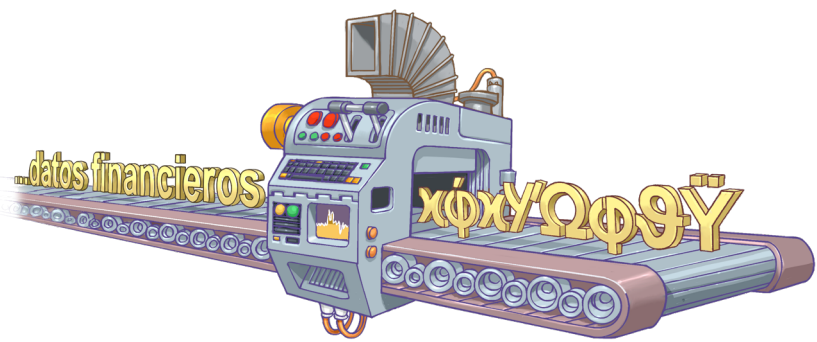
Para funcionar, muchas aplicaciones solicitan permisos, como acceso a la cámara, el micrófono, la geolocalización y la lista de contactos. Algunos accesos son esenciales, pero hay otros que son abusivos y pueden comprometer tu privacidad y seguridad.

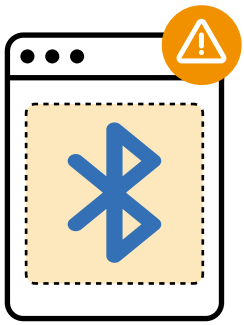
» Cuando instales y uses una aplicación, solo autoriza los accesos que tengan sentido teniendo en cuenta el uso

TEN CUIDADO AL USAR REDES WI-FI PÚBLICAS

Las redes Wi-Fi públicas pueden presentar riesgos, como exponer tu privacidad o redirigir tus conexiones a sitios maliciosos. A pesar de ser muy prácticas, no hay forma de garantizar que estén correctamente configuradas y protegidas.

- Antes de conectarte, asegúrate de que la red sea legítima
  - busca indicaciones de que hay una red disponible, como letreros y carteles
  - si tienes dudas, confirma con el establecimiento
- Usa conexiones seguras, como https para acceder a los sitios web
- Considera usar una red privada virtual (VPN)
- Para tus transacciones financieras, elige una red en la que confíes

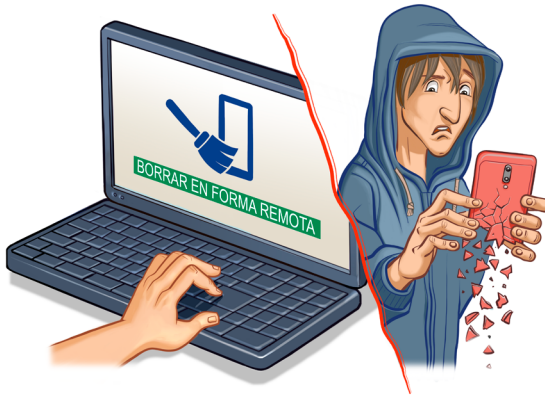




TEN CUIDADO AL UTILIZAR LA COMUNICACIÓN DE PROXIMIDAD

Los dispositivos móviles cuentan con funciones de conexión de proximidad, como *bluetooth* y NFC, para conectar accesorios, transferir y compartir datos, y realizar pagos. Los atacantes pueden abusar de estas funciones para robar datos, realizar pagos fraudulentos y hackear el dispositivo.

- Ten cuidado con las solicitudes de emparejamiento
  - solo acepta si estás seguro de que son tus propios accesorios
- Exige autenticación para autorizar los pagos por aproximación (NFC)
- Activa la función de compartir solo cuando sea necesario
  - función “Compartir con Nearby” en Android o “AirDrop” en iOS
- Reduce la exposición desactivando las funciones que normalmente no usas
  - ten cuidado con el *bluetooth* porque suele venir habilitado de fábrica



TEN CUIDADO CON TUS DISPOSITIVOS EN LUGARES PÚBLICOS

Los dispositivos móviles son pequeños, se usan constantemente, y son fáciles de perder y olvidar. Suelen ser objetos codiciados por los ladrones, tanto por el precio del dispositivo como por la información que contienen y los accesos que permiten.

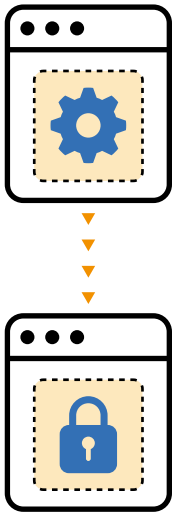
- Activa la localización remota del aparato
  - función “Encontrar mi dispositivo” en Android y “Buscar iPhone” en iOS
  - intenta localizar, bloquear o borrar el dispositivo según sea necesario
- Anota el IMEI del celular y guárdalo en un lugar seguro
- En caso de robo, consulta el fascículo “Robo de celular” para ver qué hacer

RESPALDA TUS DATOS

Los datos almacenados en tu dispositivo pueden perderse por fallas, pérdida o robo del aparato. Tener copias de los datos permite recuperarlos.

» Haz copias periódicas de tus datos

- selecciona la opción más conveniente, como la nube, otros equipos o memorias USB específicas
- programa tus respaldos para que se hagan en forma automática



EXPLORA LAS CARACTERÍSTICAS DE SEGURIDAD DE TU DISPOSITIVO

El sistema de tu dispositivo cuenta con diferentes opciones de seguridad y privacidad que no siempre vienen activadas o configuradas de fábrica. Además, si deseas características de seguridad adicionales, hay distintas aplicaciones que puedes instalar.

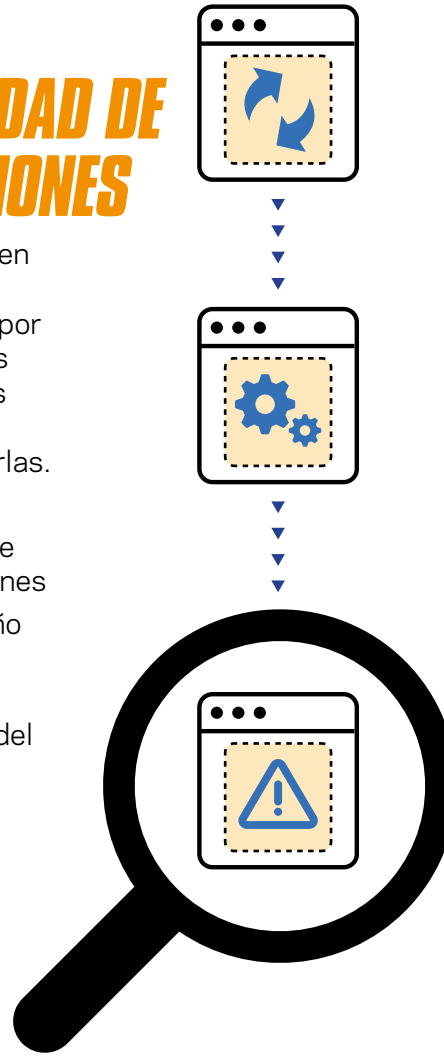
- Verifica las opciones de seguridad y privacidad que ofrece tu dispositivo
  - configúralas según tus necesidades y mejores prácticas
- Instala otras aplicaciones de seguridad si deseas características de seguridad adicionales

PRECAUCIONES QUE DEBES TENER AL COMPRAR UN DISPOSITIVO

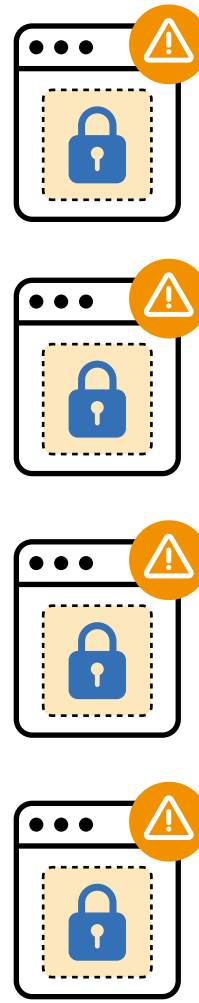
EVALÚA LA DISPONIBILIDAD DE ACTUALIZACIONES

Los fabricantes ofrecen actualizaciones y corrección de fallas por un tiempo limitado. Los celulares muy antiguos quedan sin protección porque dejan de recibirlas.

» Prefiere los modelos actuales, con soporte para las actualizaciones
  - ten en cuenta el año de lanzamiento o de fabricación
  - verifica la versión del sistema operativo

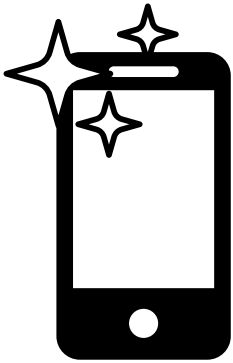


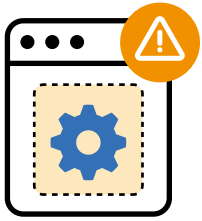
EVALÚA LAS CARACTERÍSTICAS DE SEGURIDAD

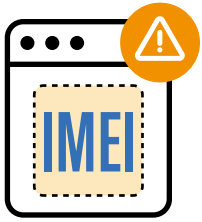


Diferentes fabricantes, sistemas y modelos ofrecen diferentes características de seguridad, entre ellos la biometría, la opción de múltiples perfiles de usuario, la autenticación para autorizar pagos y la política de la tienda de aplicaciones.

» Investiga las funciones de seguridad ofrecidas
  - escoge el modelo que mejor se adapte a tus necesidades







EVITA PROBLEMAS AL COMPRAR UN CELULAR USADO

Al comprar un celular usado hay que tener especial cuidado, ya que no siempre es posible garantizar su procedencia. El teléfono podría estar en situación irregular (IMEI bloqueado), vinculado a la cuenta del propietario anterior o infectado con *malware*.

» Verifica la situación del dispositivo
  - asegúrate de que el dispositivo esté desvinculado de la cuenta del propietario anterior
  - solicita el código IMEI del dispositivo al vendedor y consulta su situación en **https://www.gov.br/anatel/pt-br/assuntos/celular-legal/** si estás en Brasil o con la autoridad competente del país donde te encuentres

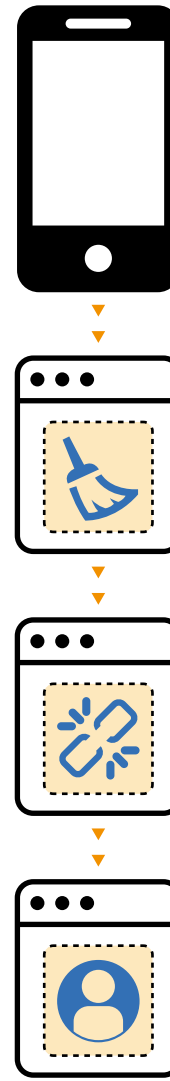
» Restablece las configuraciones originales (“de fábrica”) antes de usarlo

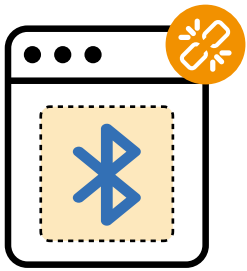
PRECAUCIONES QUE DEBES TENER AL DESECHAR O ENTREGAR UN DISPOSITIVO

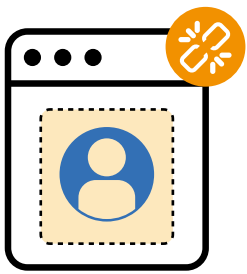
BORRA LOS DATOS DEL DISPOSITIVO Y DESVINCÚLALO DE TU CUENTA

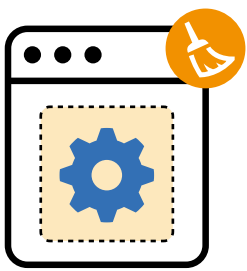
Si no los borras, los datos de tu dispositivo pueden caer en manos de otras personas. Antes de desconectar el dispositivo de tu cuenta y que el próximo propietario pueda usarlo, hay que desconectar el ID de sistema.

- Desconecta la cuenta de tu ID de sistema
  - opción “Eliminar cuenta” en Android o “Finalizar Sesión” en iOS
- Restablece la configuración original (“de fábrica”)
  - asegúrate de borrar todo el contenido y la configuración
- Elimina el dispositivo de la lista de dispositivos confiables en la cuenta de tu ID de sistema





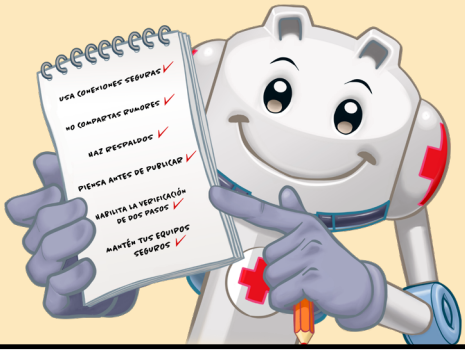




ELIMINA LAS ASOCIACIONES AL CELULAR ANTERIOR

Es posible que tengas varias cuentas de aplicaciones y accesorios conectados, por ejemplo por *bluetooth*, autenticados de forma permanente en el celular. Es necesario eliminar de las cuentas y los accesorios las autorizaciones asociadas al celular anterior.

- Elimina de tus cuentas en las aplicaciones los accesos concedidos al celular
- Elimina de tus accesorios las autorizaciones o emparajamientos asociados al celular



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.

octubre de 2022