



Manual de buenas prácticas y prevención de ciberincidentes

Índice



[01 - Diferencia entre ciberdelito y ciberincidente.](#)

[02 - Mitos y realidad sobre ciberseguridad.](#)

[03 - Resguardo de evidencia.](#)

[04 - ¿Cómo reportar un incidente en el BACSIRT?](#)

[05 - Antivirus.](#)

[06 - Tips para verificar si un sitio web es legítimo.](#)

[07 - Phishing y sus variables.](#)

[08 - Cómo cuidar tus cuentas.](#)

[09 - Activar el MFA.](#)

[10 - Qué hacer si perdés el celular.](#)

[11 - Finanzas y Ciberseguridad.](#)

[12 - Llamadas no deseadas.](#)

[13 - Protección de datos personales.](#)

[14 - Tutoriales varios.](#)

[15 - Radares Digitales](#)



Diferencia entre ciberdelito y ciberincidente



1

Diferencia entre ciberdelito y ciberincidente

Índice

Ciberincidente

Suceso que **arriesga la confidencialidad, integridad y disponibilidad de información** que se encuentre alojada en dispositivos y/o sistemas informáticos.

Ciberdelito

Acción realizada en o a través de medios digitales, que afecte datos y/o sistemas informáticos (y, consecuentemente, a sus titulares) y que **esté contemplada en el Código Penal Argentino**.

1

Diferencia entre ciberdelito y ciberincidente

Índice

Diferencia

Todos los delitos informáticos son incidentes, pero **no todos los incidentes son delitos***.

*Podés consultar el listado completo de delitos informáticos en el [sitio oficial del Ministerio de Justicia y Derechos Humanos de la Nación](#).



| Mitos y realidad sobre ciberseguridad



2 Mitos y realidad sobre ciberseguridad

Índice

Derribando mitos

Desmitificar los mitos que existen en ciberseguridad es importante para comprender sus desafíos.

Por eso les mostramos 5 ejemplos concretos.



| Resguardo de **evidencia**



3 Resguardo de evidencia

Índice

¿Cómo debo resguardar la evidencia?

No borres ni modifiques la evidencia que poseas en los dispositivos relacionados al incidente. La integridad de los procesos es vital en los procesos judiciales.

Para más información:

[¿Cómo resguardar la evidencia?](#),

[Resguardo de evidencia,](#)

[¿Cómo resguardar correctamente la evidencia digital?](#)

[Parte 1 y Parte 2](#)



| ¿Cómo **reportar un incidente** en el BACSIRT?



4

¿Cómo reportar un incidente en el BACSIIRT?

Índice

Paso a paso e información que no puede faltar



Correo electrónico:

ciberseguridad@ba-cisrt.gob.ar



Teléfono:

+54 (011) 4323 – 9362.



Redes sociales:



También podés comunicarte por BOTI.

Escribí al 11 5050-0147

Y Chateá con un/a operador/a de
lunes a viernes 10 a 17hs.

Para más información:

[¿Qué es un CSIRT?](#)

[¿Cómo reportar un incidente en el BACSIIRT?](#)

[¿Qué y cómo reportar?](#)



| Antivirus



5 Antivirus

Índice

¿Me descargo un antivirus?

La respuesta es ¡SÍ! Siempre debemos contar con una solución de protección para todos nuestros dispositivos.



Tips para **verificar** si un sitio web es legítimo



6 Tips para verificar si un sitio web es legítimo

Índice

¿Cómo puedo verificarlo?

Una forma de evitar fraudes al navegar por Internet es **prestando atención y asegurándonos de estar en el sitio legítimo** de la empresa o entidad en cuestión.



| Phishing y sus variables



7 Phishing y sus variables

Índice

PHISHING: ¿Qué es y cómo prevenirlo?

Técnica de ingeniería social donde la persona **atacante se hace pasar por una entidad conocida o persona de confianza para robar información confidencial.**

Para más información:

[Phishing](#)

[Mails a la pesca](#)

[Alertas falsas: así roban tu dinero rápidamente](#)

[¿Mails patrocinados de “Mercado Libre” en Gmail?](#)

[QRishing: el peligro que se esconde en un QR](#)

7 Phishing y sus variables

Índice

VISHING: ¿Qué es y cómo prevenirlo?

Es un engaño realizado a través de “ingeniería social”, y **llevado adelante por medio de una comunicación telefónica.**

Para más información:

[Vishing](#)

[¡Cuidado estafa del espejito roto!](#)



| Cómo cuidar tus cuentas



8

Cómo cuidar tus cuentas

Índice

Protegé tus cuentas en dispositivos digitales

En nuestros dispositivos móviles, ya sea Android o iOS, guardamos nuestras cuentas: correos electrónicos, redes sociales, bancos y más. **Proteger esta información es vital para resguardar tus datos personales y financieros.**

Para más información:

[Protegé tus cuentas en dispositivos digitales](#)

8

Cómo cuidar tus cuentas

Índice

Contraseñas

Siempre sugerimos generar y resguardar nuestras claves de forma consciente y responsable. **Tengamos en cuenta que la contraseña es nuestro primer escudo para proteger nuestra información** y nuestra identidad digital.

Para más información:

[Contraseñas](#)

[Gestores de contraseñas](#)

8

Cómo cuidar tus cuentas

Índice

Reforzá la seguridad de tu cuenta de WhatsApp

- **Evitá compartir el código** de activación de 6 dígitos que te llega por SMS.
- **Agregale un pin personal** a tu cuenta para aumentar la seguridad: Ingresá a Ajustes – Configuración – Cuenta – **Verificación en dos pasos – Activar.**
- **Tu foto de perfil solo la deben poder ver tus contactos.** Clikeá Ajustes/Config – Cuenta – Privacidad – Foto de perfil – Mis contactos.
- Si un familiar o amigo te hace un pedido inusual o extraño por WhatsApp, **llamalo para verificar su identidad.**
- **Prestá atención si decidís compartir pantalla** por videollamada de WhatsApp.

Para más información:

[Cómo cuidar tu cuenta de WhatsApp](#)

[Mensajes urgentes](#)

[¿Qué hacer si perdés el acceso a tu cuenta de WhatsApp?](#)

1

[Riesgos de compartir pantalla por videollamadas de WhatsApp](#)

[¿Qué hacer si perdés el acceso a tu cuenta de WhatsApp?](#)

2

8

Cómo cuidar tus cuentas

Índice

Reforzá la seguridad de tu Buzón de voz

El servicio de llamadas tradicionales cada vez se usa menos, sin embargo, **los buzones de voz son puntos de alta vulnerabilidad** si no están bien configurados.

8

Cómo cuidar tus cuentas

Índice

Reforzá la seguridad de tu cuenta de Telegram

Telegram, con el tiempo, se ha vuelto cada vez más utilizada por los usuarios.

Siempre debemos revisar las opciones de “privacidad y seguridad” para proteger nuestra cuenta y privacidad.



| Activar el **MFA**



9

Cómo cuidar tus cuentas

Índice

Múltiple Factor de Autenticación

El Doble Factor de Autenticación o Múltiple Factor de Autenticación es una técnica que tiene como finalidad sumarle seguridad a tu perfil, más allá del nombre de usuario y la contraseña.

Para más información:

[MFA - Android](#)

[MFA](#)



| Qué hacer si **perdés el celular**



Extravié mi dispositivo móvil ¿Qué hago?

Te brindamos algunos consejos que pueden ayudarte si te robaron y/o perdiste tu dispositivo móvil.

Pero recordá que lo más importante es prevenir.



| Finanzas y ciberseguridad



¿Transferencia por error?

Estafa en la que un comprador online “paga” con un cero de más y después **reclama que le devuelvan ese dinero que, en realidad, nunca se acreditó.**

Ciberseguridad en billeteras virtuales

Ciberdelincuentes **utilizan técnicas de ingeniería social y/o software malicioso para intentar vulnerar estas billeteras**. Pero esto puede prevenirse.

Alerta: descubriendo fraudes financieros

Informate sobre las distintas **maniobras de fraude vigentes**.

Para más información:

[Alerta jubilados](#)

[Top 3 de estafas \(Parte I\)](#)

[Top 3 estafas \(parte II\)](#)

[Los consumos y débitos no autorizados](#)

[Préstamos online: lo que nadie te cuenta](#)

[Fallos contra bancos por estafas digitales](#)

Skimming

Los ciberdelincuentes obtienen datos de tarjetas de crédito o débito de otras personas copiando la banda magnética con un dispositivo llamado “skimmer”.



| Llamadas no deseadas



Registro NO LLAME

¿Sabías que hay una forma de **registrar nuestro número para ya no recibir llamadas no deseadas?**

Ingresa en Registro NO llame .

Bloquear llamadas entrantes desde números desconocidos

Tanto Android como iOS les brindan a sus usuarios/as la posibilidad de **bloquear llamadas entrantes desde números desconocidos y/u ocultos**, sin necesidad de descargar ninguna aplicación.



| Protección de **datos personales**



Ley de protección de datos personales

Según la Ley 25.326 de Protección de Datos Personales, para que una base de datos personales -ya sea analógica, digital, pública o privada- sea lícita debe estar debidamente registrada en [Datos personales](#).

¿Quiénes tienen autorización para pedirnos foto de nuestro DNI?

- Tu empleador.
- Prepagas.
- Aseguradoras.
- Bancos y plataformas/apps que se consideren entidades financieras.
- Los organismos policiales, las fuerzas armadas y de seguridad.

Para más información:

[DNI](#)

[Protección de datos personales](#)

[Ciberseguridad en el trabajo](#)

[Derecho a la imagen de niñas, niños y adolescentes \(NNYA\)](#)



| Tutoriales varios



Encontrá el paso a paso de procesos, configuraciones, y más

- [Extraer cabeceras de un correo electrónico](#)
- [Google Ads y parámetros de búsqueda avanzada en Google](#)
- [¿Cómo activar alertas de Google?](#)
- [¿Cómo saber si fui hackeado?](#)
- [Atajos de teclado para Windows 10](#)
- [Owasp TOP 10](#)
- [Introducción a Windows Defender](#)
- [Comandos de CMD - Windows 10](#)
- [¿Sabías que Google puede guardar tu voz?](#)



| Radares Digitales



Encontrá las tendencias en ciberincidentes

- [Estafas online en Instagram](#)
- [Cobros duplicados en tarjetas de crédito](#)
- [La estafa de los “likes pagos”](#)
- [Mail falsos en nombre de Correo Argentino](#)



Muchas gracias.



Vamos por más