Manual de buenas prácticas

y prevención de ciberincidentes

Índice

Diferencia entre ciberdelito y ciberincidente

Diferencia entre ciberdelito y ciberincidente

Ciberincidente

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

Diferencia entre ciberdelito y ciberincidente

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.

Diferencia entre ciberdelito y ciberincidente

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.

Para más información:
Ciberseguridad: Incidente vs Delito

Mitos y realidad sobre ciberseguridad

Mitos y realidad sobre ciberseguridad

Derribando mitos

Desmitificar los mitos que existen en ciberseguridad es importante para comprender sus desafíos. Por eso hoy les mostramos 5 ejemplos concretos.

Para más información:
Mitos y realidades

Resguardo de evidencia

Resguardo de evidencia

¿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?

¿Cómo reportar un incidente en el BACSIRT?

Paso a paso e información que no puede faltar

Correo electrónico: ciberseguridad@ba-cisrt.gob.ar

Teléfono: +54 (011) 4323 – 9362.

Redes sociales:

FACEBOOK - TWITTER - INSTAGRAM - LINKEDIN - TIKTOK - YOUTUBE

Para más información:

¿Cómo reportar un incidente en el BACSIRT? y ¿Qué y cómo reportar?

Antivirus

Antivirus

¿Me descargo un antivirus?

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

Para más información:
¿Me descargo un antivirus?

Tips para verificar si un sitio web es legítimo

Tips para verificar si un sitio web es legítimo

¿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.

Para más información:
Verificar si un sitio web es legítimo, URL y Sitio seguro?

Phishing y sus variables

Phishing y sus variables

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 y Mails a la pesca

Phishing y sus variables

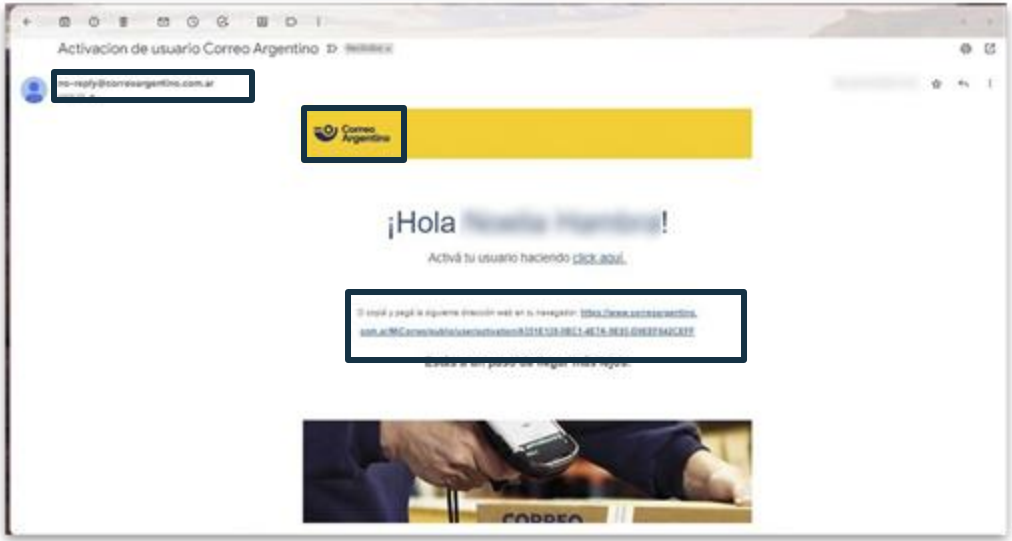
VISHING: ¿Qué es y cómo prevenirlo?

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

Para más información:
Vishing

Phishing y sus variables

¿Cómo verificar la legitimidad de un correo electrónico?



Siempre debemos ver que la dirección de correo electrónico, los elementos visuales, el tono comunicativo, y el mensaje sean coherentes con el remitente.

Cómo cuidar tus cuentas

Cómo cuidar tus cuentas

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

Cómo cuidar tus cuentas

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

Cómo cuidar tus cuentas

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? y Riesgos de compartir pantalla por videollamadas de WhatsApp

Cómo cuidar tus cuentas

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.

Para más información:
Buzón de voz resguardado y Configurá tu buzón de voz

Cómo cuidar tus cuentas

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.

Para más información:
Cuidá tu cuenta de Telegram

Activar el MFA

Activar el MFA

Multiple 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 y MFA

Qué hacer si perdés el celular

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.

Para más información:

Paso a paso y Robo o pérdida de celular

Finanzas y ciberseguridad

Finanzas y ciberseguridad

¿Transferencia por error?

Tipo de estafa en la que: comprador online “paga” con un cero de más para luego exigir al vendedor que le devuelva ese dinero que en realidad nunca se acreditó.

Para más información:
Transferencia por error

Finanzas y ciberseguridad

Ciberseguridad en billeteras virtuales

Los/as ciberdelincuentes utilizan técnicas de ingeniería social y/o softwares maliciosos, para intentar vulnerar estas billeteras. Pero esto puede prevenirse.

Para más información:
Ciberseguridad en billeteras virtuales

Finanzas y ciberseguridad

Alerta jubilados: descubriendo el fraude financiero

Recientemente, surgió una nueva modalidad de estafa mediante débitos no autorizados en cuentas bancarias y/o financieras, que se realizan de modo sistémico y masivo.

Para más información:
Alerta jubilados

Finanzas y ciberseguridad

Skimming

Los ciberdelincuentes consiguen los datos de tarjetas de crédito y débito de otras personas, ya sea mediante el copiado de sus bandas magnéticas, a través de un dispositivo denominado “skimmer”.

Para más información:
Skimming

Llamadas no deseadas

Llamadas no deseadas

Registro NO LLAME

¿Sabías que hay una forma de registrar nuestro número para ya no recibir llamadas no deseadas? Ingresá en Registro NO llame.

Para más información:
Registro NO LLAME

Llamadas no deseadas

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.

Para más información:
Bloqueo de llamadas

Protección de datos personales

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.

Protección de 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 y Protección de datos personales

Tutoriales varios

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?

¡MUCHAS GRACIAS!


BA
Buenos
Aires
Ciudad
Vamos por más