SEGURIDAD EN EL MUNDO DIGITAL

ENACOM

primero la gente

Introducción

El acceso y uso de los medios y las Tecnologías de la Información y las Comunicaciones (TIC) requieren del desarrollo de capacidades específicas, diversas y dinámicas. La alfabetización mediática e informacional busca promover herramientas de prevención, concientización y capacitación para que las personas cuenten con recursos para un uso responsable, seguro, reflexivo, creativo y crítico de los medios de comunicación y el entorno digital.

El Ente Nacional de Comunicaciones (ENACOM), como organismo del Estado, tiene dentro de sus misiones y funciones la elaboración de políticas públicas para garantizar el acceso a la tecnología y la conectividad, pero también la responsabilidad de brindar herramientas a las y los ciudadanos para el vínculo con este entorno mediático.

En este marco, el Programa de Alfabetización en Medios y TIC, creado en la órbita de ENACOM a partir de la Resolución 1705/21, impulsa el acceso equitativo, asequible y de calidad a los medios de comunicación para todas y todos los habitantes de la Argentina.

Como parte de las iniciativas que lleva adelante este programa, se encuentra la confección de este cuadernillo, que aborda temas vinculados a la seguridad y privacidad en el mundo digital, entre ellos: huella digital, tipos de amenazas en Internet, ingeniería social, phishing, estafas bancarias digitales y compras en la web. Asimismo, este material ofrece consejos y herramientas para poder prevenir situaciones de riesgo en las cuales exista la posibilidad de que los datos y la información personal puedan ser captados y robados por terceras personas.

Seguridad y privacidad en el mundo digital

La presencia de las tecnologías ha producido grandes cambios en la sociedad, que generaron impactos significativos en los aspectos sociales, culturales, comunicacionales y educativos de las y los ciudadanos.

Para hablar de la importancia de la presencia del mundo digital, se debe conocer el concepto de inclusión digital. Y para que esta exista, deben darse varios factores: conectividad, herramientas tecnológicas y conocimiento en el uso de ellas.

Cabe señalar que en Argentina contamos con un escenario de gran desigualdad en materia de acceso a instrumentos tecnológicos y conectividad, que modifican la experiencia de cada usuaria y usuario con el ámbito digital.

La situación antes descripta da lugar a la brecha digital. A fin de lograr una mayor inclusión, existen diferentes proyectos y acciones públicas y privadas pensadas para poder revertir esta realidad –entre las que se encuentra este programa– que, a través de distintas propuestas, contribuyen a la alfabetización mediática.

Por lo expuesto, resulta necesario trabajar y hablar de la conectividad en general para poder desarrollar a fondo los diversos temas vinculados al mundo digital y, de esta manera, brindar la mayor información posible.

En aquellas personas digitalmente incluidas, las TIC han posibilitado la comunicación y la realización de actividades diarias de manera digital, que antes solo se efectuaban de manera analógica. Sin embargo, el uso de estas tecnologías trajo consigo la aparición de peligros presentes en la web, que hacen que nos encontremos expuestas y expuestos a diversas amenazas en las pantallas.

Las TIC han llegado para ofrecer múltiples posibilidades y soluciones a la vida en sociedad; sin embargo, su uso puede, de alguna manera, potenciar los distintos tipos de problemáticas existentes en el mundo físico. Por ello, es importante proceder en el desarrollo de concientización sobre las posibles amenazas digitales y cómo prevenirlas.

Existen programas digitales que permiten cuidar los dispositivos y los datos personales que se suben a Internet. A este aspecto se suman las configuraciones de las diferentes aplicaciones que protegen la privacidad de toda información personal que permita identificar a una persona, como edad, sexo, poder adquisitivo, pasatiempos, dispositivos, geolocalización, sistema operativo, gustos, etc.

Resulta necesario tener en cuenta nuestra **privacidad** y **seguridad** cuando navegamos por Internet. Es indispensable el resguardo de nuestros datos e información, por lo que debemos considerar los diversos temas que desarrollaremos en este material para poder resguardarlos.

Huella digital

Es el rastro que dejamos cada vez que navegamos e interactuamos en la red. Esta huella está conformada por nuestras actividades en el mundo digital, como compartir fotos y videos, efectuar búsquedas, realizar publicaciones, hacer comentarios, entre otras.

La huella digital se construye a través de nuestra interacción con las diferentes plataformas digitales y por las acciones de otras y otros usuarios, como por ejemplo, cuando nos citan o etiquetan en las diferentes redes sociales. Está compuesta por:

- Datos públicos: son los datos de la obra social, CUIT o CUIL, declaraciones de impuestos, domicilios en las facturas de servicios, resúmenes de tarjetas de crédito, cargos, becas, resultados de sorteos, resoluciones judiciales.
- Datos publicados por otras personas: son fotos, posteos de amigas y amigos, familiares, clubes o espacios de pertenencia en redes sociales.
- Datos generados por una o uno: posteos, comentarios, fotos en redes sociales y foros, ubicaciones y desplazamientos por geolocalización según el uso de diversas aplicaciones, así como formularios que completaste, contenidos que compartiste en plataformas como tu currículum, perfiles en redes de contactos u otros contenidos, como listas de reproducción y videos favoritos.

Esta información que se encuentra en la red asociada a nuestro nombre se convierte en la manera con la que cuentan otras personas para conocernos; conforma nuestra identidad digital.

Consejos para cuidar la huella digital:

- Pensar antes de publicar: poder razonar en el momento previo a compartir y difundir el contenido.
- Cuidar la información que se brinda a personas desconocidas.
- Configurar la privacidad de redes y aplicaciones.
- Tener actualizado el sistema operativo y utilizar antivirus originales para tener mayor resguardo.
- Usar contraseñas seguras.

Puede obtenerse más información acerca de la huella digital y otros temas que afectan a la seguridad digital de la vida familiar, como ciberbullying, sexting y grooming, en el material “Uso seguro de las TIC”, del Programa de Alfabetización en Medios y TIC, que se encuentra disponible en: https://www.enacom.gob.ar/materiales_p5493#contenedorSite

Tipos de amenazas

Para proteger la seguridad y la privacidad en el mundo digital, es importarte informarse. La prevención y la precaución constituyen pilares fundamentales, ya que debemos estar conscientes de los riesgos que circulan por la web para saber de qué manera manejarnos. A continuación, hablaremos de los diferentes tipos de amenazas en Internet.

Malware

El malware es un término general que se utiliza para mencionar a cualquier tipo de software malicioso, creado con la finalidad de infiltrarse en un dispositivo, con el objetivo de dañarlo sin el conocimiento de la persona propietaria. Existen diversos tipos de malware que circulan por computadoras, dispositivos móviles, correos electrónicos y redes sociales, que presentan características diferentes.

Los ciberdelicuentes a través del malware, se encargan de robar datos personales, obtener claves de tarjetas de crédito, adquirir contraseñas, espiar las distintas actividades que se practican en el dispositivo, cobrar rescate por la información obtenida, bloquear equipos, destruir información personal, usar las computadoras para impedir el acceso a sitios web y mostrar publicidad no deseada.

El malware, con sus diferentes características, puede acceder a la información personal, a la cámara del dispositivo, a las imágenes o videos archivados, a los contactos y conversaciones de las aplicaciones de mensajería, a las aplicaciones descargadas, a la **geolocalización**, a los archivos guardados, al historial de navegación y a las contraseñas.

Geolocalización: *consiste en obtener la ubicación geográfica de un objeto en un momento determinado.*

Tipos de malware[1]*:*

VIRUS: son programas que se dispersan por la red y que, al ejecutarlos, infectan los dispositivos.
GUSANOS: son programas que afectan a los diversos dispositivos cuando se ingresa a sitios web no seguros. No precisan ser ejecutados y utilizan Internet para propagarse.
TROYANOS: son archivos infectados que presentan características similares a las originales, pero cuando se ejecutan infectan los equipos. Los troyanos pueden crear un acceso oculto para administrar los dispositivos en forma remota.
RANSOMWARE: son programas que, al ser activados, secuestran diferentes archivos y carpetas de los dispositivos afectados, **encriptan** la información e impiden el acceso a los mismos. Los ciberdelicuentes exigen el pago de una suma de dinero como forma de rescate a cambio de la clave que permite recuperar la información que ha sido retenida.

[1] https://www.argentina.gob.ar/sites/default/files/cartilla-con-vos-web-2019.pdf

***Encriptación**: método de codificación de datos (mensajes, archivos, imágenes) en el que solo las y los usuarios autorizados pueden acceder a la información. Se utilizan algoritmos complejos para codificar y así obtener la información que se envía.*

SPYWARE: es un programa que se instala de modo encubierto y opera sin el conocimiento de la o el usuario. Este tipo de malware recauda información acerca de los sitios web que se utilizan, las direcciones URL que se visitan y los números de tarjetas de crédito que se usan para realizar diferentes actividades perjudiciales en el dispositivo, ofrecer ciertos productos a través de la publicidad o efectuar distintos tipos de fraudes.
ADWARE: son programas que exhiben publicidad a través de pantallas que se abren solas y que pueden robar información personal.
SCAREWARE: son correos electrónicos, mensajes o avisos que tienen la finalidad de engañar a las y los usuarios para que descarguen o instalen programas maliciosos.
KEYLOGGER: son programas que registran las pulsaciones de las teclas de los diferentes dispositivos y pueden guardar todo lo que escribe en un archivo de texto, incluyendo información comprometedora, como pueden ser las contraseñas.
ROOTKITS: son programas que permiten a personas no autorizadas ingresar a los diferentes dispositivos.
BOTNET: son programas que usan los equipos para atacar páginas de Internet o enviar **spam**.
También existe la minería de criptomoneda maliciosa denominada **cryptojacking**.

***Spam:** es un mensaje de correo que envía información no solicitada, la cual generalmente se encuentra vinculada a publicidad, datos falsos y propuestas engañosas. Aquellas personas que realizan esta práctica (spammers) buscan obtener direcciones de correo electrónicos válidas de aquellas usuarias y usuarios que suelen contestar este tipo de comunicaciones.*
*Para evitar el spam, **no** se debe contestar o reenviar los correos en cadena ni ingresar a un link propuesto por el correo electrónico de forma directa (es conveniente buscar el sitio desde el navegador).*
Se recomienda no publicar el email en webs públicas, utilizar la copia oculta para enviar un correo electrónico con distintas personas destinatarias, leer las políticas de privacidad de los sitios y utilizar filtro antispam.
https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/cert-ar/publicaciones/spam

Un dispositivo puede infectarse con un malware al[2]:

- Descargar cualquier software infectado e instalar una aplicación no oficial.
- Abrir archivos adjuntos de correos electrónicos de personas desconocidas.
- Insertar o conectar un USB, disco o unidad infectada.
- Navegar en sitios web sospechosos que solicitan suscribirse o descargar programas.
- No realizar actualizaciones.
- Descargar software, música o películas de sitios no oficiales.
- Aceptar términos y condiciones al descargar programas o aplicaciones sin leer.
- Ser adquirido en un negocio no oficial, ya que el malware puede estar preinstalado.

Existen señales de alarma para tener en cuenta que evidencian la presencia de un malware en los diferentes dispositivos.

En la PC, se debe prestar atención cuando: el equipo funciona lento, se reinicia o se bloquea sin motivo, el antivirus ha desaparecido, los archivos se encuentran bloqueados, surgen ventanas emergentes periódicamente, las descargas se ralentizan, los programa no funcionan, existen irregularidades con el correo electrónico y el navegador web no funciona.

El smartphone puede estar infectado cuando: el equipo se reinicia solo, la cámara del celular se enciende sola, el dispositivo se sobrecalienta, la batería tiene poca duración, el sistema operativo está muy lento, llegan mensajes de texto sospechosos, aumenta el uso del paquete de datos o surgen anuncios publicitarios indeseados.

Consejos para prevenir el malware:

- Instalar un antivirus original.
- Evitar conectarse a sitios web de dudosa procedencia.
- Conectarse a sitios seguros que tengan **HTTPS**.
- Descargar e instalar software de sitios oficiales.
- No abrir mails ni archivos adjuntos de correos de personas desconocidas.
- Activar las actualizaciones automáticas.
- Revisar los USB que se insertan en el equipo.
- Ante cualquier sospecha, puede restaurarse la configuración de fábrica.

[2] https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/como-saber-si-tengo-un-programa-espia-en-mi-celular

HTTPS (Protocolo Seguro de Transferencia de Hipertexto): *versión segura del protocolo de comunicación que permite las transferencias de información en Internet (HTTP).*

Ingeniería social

Se denomina ingeniería social a las diferentes técnicas de manipulación que usan las y los ciberdelincuentes para obtener información confidencial de las y los usuarios. El objetivo de este engaño consiste en apropiarse de datos personales, contraseñas o suplantar la identidad de la persona estafada[3].

Quienes practican la ingeniería social manipulan y engañan a las personas a través de llamadas telefónicas, visitas personales a domicilio, aplicaciones de mensajería instantánea, correos electrónicos y redes sociales.

Los principales métodos utilizados para la práctica de la ingeniería social son:

- Hacerse pasar por una o un familiar, una o un conocido, una o un compañero de trabajo.
- Ofrecer a la víctima premios o promociones únicas y limitadas a cambio de sus datos.
- Simular ser la o el técnico de la empresa o la persona responsable de sistemas.
- Invitar a completar formularios para ganar un premio o un producto.
- Ofrecer actualizaciones de navegadores o aplicaciones a través de páginas falsas.

Consejos para prevenir la ingeniería social:

- No entregar datos personales a personas extrañas por correos electrónicos, redes sociales o teléfono.
- Configurar la privacidad en las redes sociales para que no haya datos personales expuestos en forma pública.
- Informar y aprender sobre este tipo de amenazas.
- Usar una contraseña segura
- Configurar la autenticación de dos pasos para estar alerta de accesos indebidos a las cuentas.
- Prestar atención a cualquier persona que solicite información personal.

Una de las técnicas de Ingeniería Social más utilizada en la actualidad es el Phishing:

[3] https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-la-ingenieria-social-y-como-protegerte

***Phishing**[4]: la palabra phishing quiere decir “suplantación de identidad”. Es un método utilizado por las y los ciberdelincuentes para engañar a sus víctimas mediante el envío de correos electrónicos fraudulentos, que simulan provenir de fuentes legítimas y confiables, para lograr que revelen información personal importante, y, de esta manera, apropiarse de la identidad de esa persona.

Estos correos contienen información engañosa y enlaces que redirigen las respuestas brindadas hacia páginas de Internet falsas con formularios y preguntas para obtener datos personales. Generalmente solicitan:

- Rellenar formularios o hacer clic en un enlace para obtener alguna información o archivo clave.
- Hacer clic en un enlace que redirige a una página de registro falsa.
- Descargar un archivo adjunto importante.

Los datos que desean obtener las y los ciberdelincuentes son: contraseñas, números de tarjetas de crédito, información de los DNI, claves de CUIT o CUIL, datos de las y los usuarios y códigos PIN.

Cuando se obtienen estos datos, se realizan compras, reservas o extracciones de dinero en nombre de la persona estafada. Una forma de prevenir y verificar un ataque de phishing consiste en revisar en forma periódica los resúmenes bancarios y constatar que no se hayan realizado movimientos no autorizados en las diferentes cuentas.

Otra práctica de phishing se da cuando los ciberdelincuentes dejan colocados dispositivos informáticos (pendrives) con contenido malicioso en una computadora pública con la finalidad de obtener información de las personas que la utilizan.

Para establecer si los mensajes o correos son un intento de phishing, deben considerarse los siguientes detalles:

- Uso de remitentes similares a las y los de las páginas oficiales.
- Correos o mensajes de WhatsApp enviados por remitentes desconocidas o desconocicos.
- La página no presenta su certificado de seguridad.
- Redacción de los mensajes con errores gramaticales y ortográficos o con caracteres en otros idiomas.
- Presencia de enlaces y links dudosos.

[4] https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/phishing

- Direcciones URL erróneas, que presentan alguna modificación con respecto a la original.

Se debe tener en cuenta que ningún proveedor de servicios en línea pide a sus clientas o clientes información personal por medio del correo electrónico, debido a que la misma ya figura en sus bases de datos. Otro aspecto a considerar consiste en el tono del mensaje: generalmente las empresas se dirigen a sus clientas y clientes en tono cálido y personal y a través del nombre, que ya tienen registrado.

Se debe prestar atención a estos detalles y, en caso de duda, es recomendable chequear la información recibida a través de otros medios y no hacer clic sobre el enlace ni tampoco escribir manualmente la dirección en el navegador.

A continuación, se mencionan algunos consejos para prevenir el phishing:

- Comprobar si la dirección de Internet (URL) es igual a la de la empresa que escribe. En estos casos, puede realizarse una búsqueda online de la empresa y comparar las URL.
- Verificar el certificado de seguridad de la página de Internet. Es importante constatar que tenga el candado gris o verde y que sea una dirección https.
- Chequear la o el remitente del correo electrónico antes de abrirlo y verificar de esta manera que no sea falsa o falso.
- Comparar la o el remitente con los mensajes anteriores del banco o servicio que escribe el correo o mensaje.
- Ante cualquier duda, comunicarse con los servicios de atención al cliente antes de contestar cualquier comunicación por correo electrónico.
- No contestar formularios en línea enviados por personas desconocidas.
- No responder a ningún correo electrónico que solicite divulgar información personal.
- No enviar ni compartir contraseñas o códigos de seguridad por correo electrónico.
- Desconfiar de los archivos adjuntos que pueden causar la descarga del software spyware en el dispositivo.
- Actualizar el sistema operativo y el antivirus original.

Otras técnicas de Ingeniería Social son:

***Vishing:** a través de este método se obtiene información por medio de una llamada telefónica. El ciberdelincuente se hace pasar por un familiar, personal de una empresa, soporte técnico de la misma o empleada o empleado de una entidad bancaria para obtener datos financieros o información personal para efectuar el robo de identidad.

*__Concursos falsos:__ en esta acción, se engaña a las personas, a través de medios analógicos y digitales, al informarles que han ganado un premio (inexistente) con el objetivo de obtener datos financieros e información personal.

__*Farming:__ en esta práctica se realizan varias comunicaciones con las víctimas, mediante diferentes métodos, con la finalidad de recaudar la mayor cantidad de información posible. Una variante de este método es el robo de cuentas de correos electrónicos de usuarias o usuarios para cometer ilícitos entre los contactos de la víctima, enviar software malicioso u obtener información personal.

__*Estafas bancarias:__ desde hace algunos años, las entidades bancarias, por medio de distintas iniciativas, permiten realizar, a través de las web, diversas operaciones financieras, como abrir cuentas, realizar transferencias, consultar saldos, etc. Este cambio permitió resolver de manera simple determinados trámites, sin la necesidad de ir de manera presencial al banco, y optimizar así la experiencia de la y el usuario. Sin embargo, también se han abierto espacios para la acción de personas mal intencionadas que, con diferentes acciones, realizan estafas en el ámbito digital.

Este tipo de prácticas han aumentado en el último tiempo, por lo que a continuación se detallan algunos consejos para evitar estafas bancarias[5]:

- No se debe responder a un aviso sobre un supuesto error al realizar una transferencia bancaria. Ante cualquier duda, comunicarse telefónicamente con el banco.
- Nunca debe acudirse a un cajero automático, abrir la aplicación o acceder al home banking cuando se recibe una llamada supuestamente proveniente de la entidad bancaria. La o el cliente debe ser quien origina la llamada.
- No brindar ningún dato personal (nombre de usuario, claves, contraseñas, pin, Clave de la Seguridad Social, clave token, DNI original o fotocopia, foto, ni ningún tipo de dato) por teléfono, correo electrónico, red social, WhatsApp o mensaje de texto.
- No ingresar datos personales en sitios utilizando enlaces que llegan por correo electrónico, ya que podrían ser fraudulentos.
- Asegurarse siempre de estar en la página legítima antes de ingresar información de inicio de sesión.
- Utilizar contraseñas seguras y no compartir las claves.

[5] https://www.argentina.gob.ar/noticias/consejos-para-evitar-estafas-y-fraudes-bancarios

- No usar equipos públicos o de terceras personas para acceder a aplicaciones, redes sociales o cuentas personales.
- No usar redes de wifi públicas para acceder a sitios que requieran contraseñas.
- Mantener actualizado el navegador, el sistema operativo y las aplicaciones.
- Aprender a diferenciar un perfil verdadero de uno falso en redes sociales.
- Reportar y bloquear cualquier contacto sospechoso.

Es importante destacar que la entidad bancaria **nunca**:

- Iniciará una conversación por privado.
- Realizará contactos por WhatsApp.
- Solicitará claves ni contraseñas.
- Pedirá información personal que ya tiene registrada.

Es prioritario que la o el usuario, ante cualquier duda, tome la decisión de chequear y verificar la información. Resulta indispensable que siempre, frente a estas situaciones, se tome un minuto antes de actuar, ya que quienes realizan este tipo de estafas apelan a las emociones, los descuidos y las urgencias.

Compras en Internet[6]

Son aquellas que se realizan en sitios online de comercio electrónico o en páginas de Internet que venden productos.

Estos lugares digitales poseen muchas medidas para que las compras se encuentren protegidas, ya que utilizan “certificados de seguridad” que evitan que las transferencias de dinero sean vistas por otras personas y, de esta manera, se protegen los pagos entre los sitios y los bancos. Si la página usa estos protocolos seguros, en la barra de direcciones aparece un candado verde o gris y la sigla HTTPS.

Las medidas de seguridad a tener en cuenta para comprar por Internet son:

- No ingresar a un sitio que vende productos por Internet directamente desde un correo electrónico o desde un mensaje en aplicaciones de mensajería instantánea. Se debe escribir la URL en el navegador para asegurarse de que la página desde la cual se realizará la compra no es un sitio falso.

[6] https://www.argentina.gob.ar/justicia/convosenlaweb/como-me-protejo-cuando-compro-por-internet

- Verificar que sea un sitio seguro para efectuar la compra y no ingresar datos personales ni de tarjetas de crédito en páginas de procedencia dudosa.
- No guardar las tarjetas de crédito en sitios web.
- No compartir los números o fotografías de las tarjetas y códigos de seguridad por servicios de mensajería instantánea.
- Proteger las cuentas con una contraseña segura y activar la doble autenticación.
- No usar redes wifi públicas para realizar transacciones o compras por Internet.
- Recibir el comprobante de pago o la factura electrónica por mail.
- Leer las medidas de seguridad, las políticas de privacidad y los términos y condiciones.
- Conocer los derechos y obligaciones.

Herramientas

Ante estos riesgos presentes en la web, que han sido detallados anteriormente, resulta fundamental comentar que, como usuarias y usuarios, contamos con una serie de herramientas que nos protegen de las distintas acciones que buscan perjudicar nuestra vida personal y financiera en el mundo digital. Algunas de ellas son:

Contraseñas seguras

El uso de contraseñas constituye una de las herramientas más importantes con las que se cuenta para cuidar datos personales en el mundo digital. Las mismas deben ser seguras y poseer las siguientes características[7]:

- Ser mayores de 8 dígitos y poseer un patrón para que la o el usuario pueda recordarla.
- Se recomienda que sean alfanuméricas, con presencia de mayúsculas, minúsculas y signos.
- No utilizar la misma contraseña para todos los sitios.
- Modificarlas periódicamente.
- No compartirlas con nadie.
- Para evitar que otras personas tengan acceso a las claves, no se debe guardarlas en el navegador, ni tampoco pegarlas en un monitor o debajo del teclado. Se debe tener cuidado si se anotan las contraseñas en un cuaderno.
- Utilizar gestores de contraseñas de empresas de seguridad reconocidas.
- Evitar confeccionar las contraseñas con información personal.

Copias de respaldo o backups[8]

Es una de las maneras más accesibles para resguardar el acceso a la información en caso de pérdida, daño o robo de los dispositivos. Una de ellas consiste en realizar una copia de respaldo del smartphone a una PC de escritorio o notebook; otra radica en crear un **backup** en servicios denominados "nube", que presentan un espacio virtual de almacenaje en un servidor que funciona como un disco externo, como por ejemplo, Google Drive.

Backup: *copia de respaldo o seguridad. Realizar un backup es la acción de copiar archivos o datos de forma que estén disponibles en caso de que un fallo produzca la pérdida de los originales.*

Antivirus, antimalware y firewall

Son herramientas de protección que deben ser instaladas en los distintos dispositivos.

[7] https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/como-crear-una-contrase%C3%B1a-segura
[8] https://www.argentina.gob.ar/sites/default/files/cartilla-con-vos-web-2019.pdf

Antivirus: programa cuya finalidad es prevenir y curar los virus informáticos en una computadora, celular o tablet. Deben ser originales y tienen que estar actualizados en su última versión.

Antimalware: funciona como un complemento de seguridad, ya que no solo protege, sino que también elimina los malware.

Firewall: parte de un sistema o una red que se encuentra diseñada para bloquear el acceso no autorizado. Al mismo tiempo, permite comunicaciones autorizadas.

Actualización periódica de equipos y sistemas operativos[9]

Estas acciones permiten que los dispositivos funcionen correctamente, evitan que se infecten y mejoran su rendimiento.

Las actualizaciones instalan mejoras en el funcionamiento y en la seguridad del software; asimismo, posibilitan solucionar errores, resolver vulnerabilidades e incluir nuevas funciones.

Utilizar software original o libre

Se sugiere utilizar **software** oficial o antivirus originales para evitar programas maliciosos que puedan afectar al sistema operativo y al **hardware**, por lo tanto, no es recomendable descargar copias ilegales.

Hardware: *son las partes físicas tangibles de un sistema informático.*

Software: *es el conjunto de programas o aplicaciones, instrucciones y reglas informáticas que hacen posible el funcionamiento del equipo.*

Identificar sitios seguros en la web

En los sitios seguros, los datos que se ingresan son transmitidos al servidor de manera **encriptada** para evitar que la información sea manipulada. Al enviar información sensible, es importante verificar la configuración del sitio.

Encriptación: *es un proceso técnico por el cual la información se convierte en un código secreto que permite ocultar los datos que se envían, reciben o almacenan. Para ello, se usa*

[9] https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/por-que-es-importante-actualizar-el-sistema-operativo

un algoritmo que codifica los datos, para que luego la parte receptora descifre la información mediante una clave específica determinada.

Para identificar los sitios seguros, resulta necesario verificar que la dirección del lugar, en la barra de búsqueda, comience con la sigla HTTPS y revisar la presencia de un candado verde o gris. Si se hace clic en el candado, puede encontrarse a la información del certificado y la configuración de seguridad del espacio digital. Se recomienda mantener las direcciones habituales en favoritos, para acceder de manera más rápida y segura.

Consejos para el uso de las cookies

Las cookies son archivos que recolectan información sobre la experiencia de navegación de la o el usuario y la envían a las páginas de Internet que se visitan habitualmente. De esta manera, la carga de las páginas es más rápida y la publicidad que aparece cuando se navega se encuentra vinculada con los temas o lugares que la o el usuario ha estado consultando.

Más allá de que facilitan las búsquedas en la web, debe tenerse en cuenta que las cookies toman información de las acciones (páginas y archivos visitados) e identifican y almacenan el historial de la o el usuario en Internet. Por eso, es recomendable configurar la privacidad y seguridad del navegador con respecto a la política de cookies y borrarlas cada cierto tiempo.

Tener seguridad en el acceso al wifi

En la actualidad, es común conectarse como invitada o invitado en redes wifi públicas o abiertas, para así evitar el consumo de datos móviles. En este tipo de casos, se recomienda tomar ciertas precauciones, ya que cualquier persona puede conectarse a ellas, debido a que las restricciones de seguridad son escasas o nulas, y existe la posibilidad de que la presencia de un software malicioso pueda ingresar al dispositivo y ataque la transmisión de datos y la información guardada en el equipo.

Por lo tanto, debe evitarse ingresar a aplicaciones de bancos o servicios en las que se maneje información sensible. Del mismo modo, se recomienda no realizar registros o completar formularios con información importante. Ante cualquier inquietud, la presencia de antivirus y antimalware sirve como barrera de protección frente a cualquier amenaza presente.

Navegar en modo incógnito[10]

Es una modalidad en la cual el navegador no guarda ningún tipo de información sobre las páginas web visitadas y constituye una medida de seguridad que impide que los buscadores de Internet vean los sitios a los que se ingresa. A su vez, permite navegar sin que se guarde información sobre el historial de navegación, las cookies y los datos cargados en los formularios de los sitios web.

Si bien la actividad continúa siendo visible para los sitios web visitados y los proveedores de servicios de Internet, configura una medida de resguardo más, ya que los datos personales están más protegidos de aquellas personas que poseen acceso a dispositivos, celulares o computadoras de una o un usuario determinado, debido a que no podrán ingresar al historial de navegación.

Verificación en dos pasos

Este método permite agregar una nueva autentificación de identidad a una cuenta nueva u otra ya existente, de modo que, aunque alguien pueda averiguar la contraseña, no podrá acceder a la información. Se refuerza la identificación mediante un segundo código generado por una aplicación y enviado a la o el usuario, generalmente, a través de un correo electrónico o un mensaje de texto.

La mayoría de las plataformas presentan este método, el cual se activa mediante el menú de configuración. La verificación en dos pasos mejora el nivel de seguridad de una cuenta, independientemente del nivel de seguridad de la contraseña.

Control parental[11]

Son aplicaciones que las personas adultas pueden configurar en los dispositivos electrónicos con conexión a Internet para que los buscadores y plataformas solo ofrezcan contenidos adecuados a niñas, niños y adolescentes.

Las mismas restringen accesos a sitios en Internet, informan sitios visitados, localizan a las y los usuarios de los dispositivos en un mapa, activan medidas de seguridad y privacidad en los equipos para proteger datos, filtran contenido de aplicaciones o de páginas web y limitan el tiempo de uso de los dispositivos al programar diferentes funciones.

[10] https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/para-que-sirve-navegar-de-modo-incognito
[11] https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/controles-parentales

Pueden activarse en celulares, computadoras, televisores inteligentes, servicios de streaming, redes sociales, consolas de videojuegos y juegos en línea.

Para las niñas y los niños, constituye una herramienta recomendable, porque las y los protege de contenidos inadecuados. En el caso de las y los adolescentes, estas medidas pueden resultar menos efectivas, ya que existe mucha información en Internet sobre formas de evadir o deshabilitar las restricciones.

Por otra parte, con ellas y ellos también pueden llegar a ser contraproducentes, porque pueden resultarles invasivas y generar malestar, ya que se encuentran experimentando un período de transformaciones y definiciones identitarias, y construyendo una autonomía progresiva. Es fundamental reflexionar con las y los adolescentes y que se sientan respetadas y respetados en su privacidad.

Más allá de la importancia de esta herramienta, el método más efectivo es el diálogo y la información para generar confianza, explicándoles que su utilización es un gesto de cuidado. Es pertinente acordar formas de uso y acceso a los dispositivos y aprender a manejar las redes sociales y el acceso a Internet en forma responsable, desarrollando el uso seguro, reflexivo y creativo del mundo digital.

Precaución en el uso del pendrive o discos extraíbles

Es importante el cuidado del pendrive o disco extraíble, ya que estos, por sus características de comodidad y capacidad, se encuentran expuestos a daños físicos y extravíos. Estos riesgos se encuentran vinculados a la pérdida de información y a la posibilidad de que el dispositivo se infecte con software malicioso que lo dañe o perjudique el equipo en el cual se utilice. Por lo tanto, siempre deben ser revisados con un antivirus para evitar que esto suceda.

Seguridad en las redes y cuentas

Se debe tener precaución con la información que se brinda en las redes. Cuando se confirman los términos y condiciones de los servicios y aplicaciones, se está accediendo a ceder los derechos de toda la información que se publica. Con respecto a las cuentas, muchas aplicaciones piden el ingreso a través de redes o navegadores, como Google. Es necesario generar un equilibrio entre facilidad y seguridad, ya que, al aprobar la interacción entre un servicio y una cuenta, autorizamos el acceso a información sensible, como datos personales, búsquedas, imágenes y videos solicitados.

Por último, con respecto a las experiencias vividas en las diversas redes sociales y aplicaciones existentes, deben conocerse las maneras de configurar la seguridad y

privacidad de las mismas, ya sea desde el smartphone, tablet o notebook, y así comprender las opciones que ofrecen, para poder utilizarlas de forma más saludable y evitar pasar malos momentos con otras y otros usuarios en los distintos espacios digitales. A modo de ayuda, en el siguiente link se encuentran algunas indicaciones: https://www.educ.ar/recursos/157170/redes-sociales-configuraciones-de-seguridad

Normativa vinculada a ciberdelitos, protección de datos y derechos digitales[12]

Ley 11.723. Régimen Legal de la Propiedad Intelectual

http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/42755/texact.htm

Regula el derecho de propiedad de las obras científicas, literarias o artísticas y protege los derechos de sus autoras y autores.

Código Penal. Artículo 118. Delitos contra la integridad sexual

http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm

Describe los delitos contra la integridad sexual, como las agresiones sexuales que atentan contra la integridad, la privacidad y la identidad de las personas.

Ley 24.240. Defensa del Consumidor

http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/638/texact.htm

Protege las compras o contrataciones de servicios en Internet.

Ley 25.326. Protección de los Datos Personales

http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

Protege la información personal de cualquier tipo referida a personas físicas y manifiesta la confidencialidad del tratamiento de los datos personales, incluida la protección de la privacidad e intimidad en Internet.

Ley 25.506. Firma Digital

http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm

Reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica.

Ley 26.061. Protección Integral de los Derechos de las Niñas, Niños y Adolescentes

http://servicios.infoleg.gob.ar/infolegInternet/anexos/110000-114999/110778/norma.htm

[12] https://www.argentina.gob.ar/justicia/convosenlaweb/derechos-y-ciudadania-digital

Protege el derecho a la privacidad de niños, niñas y adolescentes.

Código Penal. Ley 26.388. Delitos informáticos

http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

Incorpora al Código Penal los delitos cometidos por medios informáticos. Permite legislar acerca de:

- Distribución y tenencia de material de abuso sexual infantil por cualquier medio.
- Interceptación de comunicaciones y sistemas informáticos.
- Publicación de correspondencia o comunicaciones electrónicas privadas.
- Acceso no autorizado a un sistema informático.
- Acceso a bancos de datos personales.

Ley 26.892. Promoción de la Convivencia y el Abordaje de la Conflictividad Social en las Instituciones Educativas

https://www.argentina.gob.ar/normativa/nacional/ley-26892-220645/texto

Regula la convivencia en las escuelas para reducir los conflictos en la comunidad educativa.

Código Penal. Ley 26.904. Ciberacoso

http://servicios.infoleg.gob.ar/infolegInternet/anexos/220000-224999/223586/norma.htm

Incorpora el ciberacoso o grooming como delito al Código Penal.

Ley 26.951. Creación del Registro Nacional "No Llame"

http://servicios.infoleg.gob.ar/infolegInternet/anexos/230000-234999/233066/texact.htm

Protege a las y los usuarios de los servicios de telefonía de los abusos en la publicidad, oferta, venta y regalo de bienes o servicios no solicitados.

Ley 27.078. Argentina Digital

https://www.enacom.gob.ar/multimedia/normativas/2014/Ley_27078-txt_actualizado.pdf

Declara de interés público el desarrollo de las TIC, las telecomunicaciones y sus recursos asociados, con el objetivo de garantizar el acceso de toda la ciudadanía a los servicios de la información y las comunicaciones en condiciones sociales y geográficas equitativas y con los más altos parámetros.

Ley 27.275. Derecho de Acceso a la Información Pública

http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/265949/texact.htm

Garantiza el acceso para conocer y utilizar la información que producen o poseen los tres poderes del Estado.

Ley 27.483. Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal

https://www.argentina.gob.ar/normativa/nacional/ley-27483-318245/texto

Garantiza a cualquier persona el respeto de sus derechos y libertades, en especial, con relación al tratamiento automatizado de sus datos personales.

Ley 27.555. Régimen Legal del Contrato de Teletrabajo

http://servicios.infoleg.gob.ar/infolegInternet/anexos/340000-344999/341093/norma.htm

Regula los derechos y obligaciones de las partes en la relación laboral que se desarrolla a distancia.

Ley 27.590. "Mica Ortega"

http://servicios.infoleg.gob.ar/infolegInternet/anexos/345000-349999/345231/norma.htm

Crea el Programa Nacional de Prevención y Concientización del Grooming o Ciberacoso contra Niñas, Niños y Adolescentes

Resolución ENACOM 8507/16. Reglamento para la Nominatividad y Validación de Identidad de los Usuarios Titulares de los Servicios de Comunicaciones Móviles

https://www.enacom.gob.ar/multimedia/normativas/2016/res8507.pdf

Establece que todas las compañías de telefonía celular deben registrar y validar la identidad de las y los dueños de todas las líneas de telefonía móvil activas.

Denuncias

Ante un ciberdelito:

- No se debe borrar ni destruir la información relacionada con el hecho, debido a que la integridad de la información resulta vital para poder iniciar las causas penales.

Realizar la denuncia. En el link que se presenta a continuación, se describen alternativas en todo el país para solicitar asesoramiento de equipos especializados o presentar una denuncia: https://www.argentina.gob.ar/justicia/convosenlaweb/denuncia