COMUNICACIONES

SECRETARÍA DE COMUNICACIONES Y TRANSPORTES

GUÍA DE CIBERSEGURIDAD PARA EL USO DE REDES Y DISPOSITIVOS DE TELECOMUNICACIONES EN APOYO A LA EDUCACIÓN

AGOSTO DE 2020

COMUNICACIONES
SECRETARÍA DE COMUNICACIONES Y TRANSPORTES

Guía de Ciberseguridad para el uso seguro de redes y dispositivos de telecomunicaciones en apoyo a la Educación

AMENAZAS MÁS COMUNES

- Códigos maliciosos o ***malware*** (virus, gusanos, troyanos, etc.).
- Amenazas relacionadas con la ingeniería social.
  - ***Phishing***, método de ataque a través del correo electrónico.
  - ***Smishing***, método de ataque a través de mensajes de SMS.
  - ***Vishing***, estafa mediante llamada telefónica.
- Contacto con depredadores en línea.
  - ***Online Grooming****, acoso o abuso sexual en línea que implica la interacción de un adulto con niñas, niños y adolescentes (NNA).*
  - ***Ciberacoso****, incluye enviar, publicar o compartir contenido negativo o dañino sobre otra persona a través de cualquier dispositivo o medio digital.*
  - ***Sexting****, Envío de contenidos (fotografías y/o videos) que contienen imágenes que muestran o describen actividades sexuales.*
- Acceso a ***contenido potencialmente dañino o ilegal.***
  - Exposición a información falsa, contenido que atente contra la integridad de NNA y jóvenes o bien que incite a la violencia, al suicidio u otras conductas de riesgo.

QUÉ SÍ HACER: RECOMENDACIONES PARA NNA Y JÓVENES

- Respetar la privacidad de los demás.
- Usar un alias/nombre alternativo como nombre de usuario al interactuar con otros en línea.
- Informar a padres, tutores, docentes o adultos de confianza sobre cualquier contenido dañino, amenaza o situación negativa.
- Aplicar la configuración de privacidad a las cuentas de redes sociales.
- Conectarse sólo con personas conocidas.
- Reportar en sitios web o redes sociales cualquier situación abusiva, ofensiva, amenazante o comportamientos inapropiados.

QUÉ NO HACER: RECOMENDACIONES PARA NNA Y JÓVENES

- NO compartir información personal.
- NO publicar en redes actividades cotidianas.
- NO enviar fotos a personas desconocidas, especialmente si éstas son con poca o nula ropa, o compartirlas en redes sociales.
- NO abrir correos electrónicos ni archivos adjuntos de remitentes desconocidos.
- NO compartir contraseñas con terceros por ningún medio.
- NO guardar nombres de usuario y contraseñas en el navegador.
- NO instalar códigos maliciosos en las computadoras o dispositivos de otras personas.
- NO intimidar, acosar, amenazar a otras personas, hacer burlas o comentarios con connotaciones negativas.
- NO organizar encuentros con desconocidos ni acceder a hacerlo si algún extraño lo solicita.

RECOMENDACIONES PARA PADRES, TUTORES Y DOCENTES

- Tener el conocimiento y la sensibilidad de los riesgos y amenazas que existen en línea.
- Empoderar a NNA y jóvenes con herramientas y conocimiento para hacer uso de las comunicaciones y tecnologías de la información.
- Mantener un diálogo constante y abierto con NNA y jóvenes para promover una cultura de ciberseguridad y para que se sientan cómodos buscando ayuda.
- Verificar y discutir con regularidad el uso que NNA y jóvenes dan a la tecnología, los sitios que visitan, identificar qué tipo de actividades realizan en línea, así como el contenido que comparten.
- Fomentar el pensamiento crítico para analizar el tipo de información a la que NNA y jóvenes tienen acceso.
- Configurar los controles parentales para la navegación en Internet y el acceso a contenidos.
- Establecer reglas para administrar el tiempo frente a la pantalla y promover un equilibrio entre el tiempo en línea y otras actividades.

CONTENIDO

Introducción 4
Amenazas más comunes a la Ciberseguridad 6
Contacto con depredadores en línea 7
Online Grooming 7
Cyberbullying o ciberacoso 7
Sexting 8
Acceso a contenido potencialmente dañino o ilegal 9
Recomendaciones de Ciberseguridad 9
Recomendaciones generales 9
Recomendaciones de ciberseguridad para el uso seguro de las redes y dispositivos de telecomunicaciones en apoyo a la educación 10
Sistema Operativo 10
Antivirus 10
Seguridad de la red Wi-Fi 11
Contraseñas 12
Ataques con técnicas de ingeniería social 13
Navegación segura 13
Uso seguro de las herramientas de la nube 14
Teleconferencias para impartir clases en línea 15
Uso de Redes sociales para impartir o complementar clases en línea 16
Red Privada Virtual 16
Recomendaciones dirigidas a padres, tutores y docentes para la ciberseguridad de NNA y jóvenes 17
Recomendaciones de Ciberseguridad para NNA y jóvenes en línea 19
¿Qué sí hacer? 19
¿Qué no hacer? 19
Recursos 20
Conclusión 21

INTRODUCCIÓN

La emergencia sanitaria generada por el virus SARS-CoV2 y la enfermedad que éste provoca **(COVID-19), ha obligado a diversos países al cierre generalizado de escuelas y al uso de soluciones de telecomunicaciones y radiodifusión para continuar con los esfuerzos educativos**. Lo anterior, como parte de las medidas de distanciamiento social para mantener la salud y bienestar de la comunidad educativa: estudiantes, padres de familia, tutores, docentes y demás personal de las instituciones educativas.

De acuerdo con la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), a nivel global al menos 1 mil 370 millones de alumnos -más de tres de cada cuatro niños y jóvenes en el mundo o cerca del 80% de la población estudiantil- y 60.2 millones de docentes fueron afectados por el cierre de escuelas y universidades para contener el contagio del COVID-19[1]. Por su parte, el Foro Económico Mundial reportó una cifra similar, al indicar que más de 1 mil 200 millones de niños en 186 países resultaron afectados por el cierre de escuelas debido a la pandemia[2].

La Unión Internacional de Telecomunicaciones (UIT) señala que **el uso de Internet ha aumentado un 50% en algunas partes del mundo tras la propagación del COVID-19[3], lo que habla de la importancia de este servicio durante la respuesta a la pandemia**.

Ante este panorama, y con el objetivo de mitigar el efecto de la interrupción de clases presenciales, muchos **países han implementado soluciones en línea**, las cuales se han convertido en **herramientas esenciales para dar continuidad a la enseñanza** en beneficio de sus alumnos.

Lo anterior, ha sido posible **a través de una amplia variedad de servicios, aplicaciones, plataformas y entornos virtuales que brindan enormes oportunidades para el aprendizaje, a la vez que promueven la socialización y desarrollo de Niñas, Niños y Adolescentes (NNA), así como de jóvenes estudiantes**.

Factores como la **mayor dependencia de las comunicaciones y tecnologías de la información, el uso de múltiples soluciones digitales en el ámbito educativo, el mayor tiempo en línea**, entre otros, incrementan la exposición de NNA, jóvenes estudiantes y docentes a amenazas y riesgos en línea.

En este contexto, **expertos en ciberseguridad advierten un entorno propicio para que prosperen los cibercriminales**[4] y que, tanto los miembros de la comunidad educativa como las instituciones académicas, se encuentren mayormente expuestos a múltiples amenazas de ciberseguridad.

¿POR QUÉ?

- En muchas ocasiones, tanto adultos (padres, tutores o docentes) como NNA y jóvenes no cuentan con la suficiente **sensibilización sobre los riesgos** a los que se enfrentan al utilizar de manera cotidiana las comunicaciones y tecnologías de la información.

- NNA y jóvenes están dedicando **gran parte de su tiempo al uso de redes y dispositivos** de telecomunicaciones, en muchos casos **sin la debida vigilancia parental**, lo cual puede ser aprovechado por los piratas informáticos.

---

[1] Portal de noticias de la Organización de las Naciones Unidas (ONU). "Más de 156 millones de estudiantes están fuera de la escuela en América Latina debido al coronavirus", 20 de marzo de 2020. https://news.un.org/es/story/2020/03/1471822

[2] Foro Económico Mundial. "La pandemia de COVID-19 ha cambiado la educación para siempre. Así es cómo" https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning/

[3] Unión Internacional de Telecomunicaciones (UIT). https://www.itu.int/en/ITU-D/Cybersecurity/Documents/COP/COVID19%20and%20Its%20Implications%20for%20Protecting%20Children%20Online.pdf

[4] Unión Internacional de Telecomunicaciones (UIT). COVID 19: Strategies to Reduce Cyber Risk While Working from Home (OPINION). https://news.itu.int/covid-19-strategies-to-reduce-cyber-risk-while-working-from-home-opinion/

- Es importante considerar las situaciones en las que los **padres, tutores o docentes no se encuentran familiarizados con el uso de nuevas tecnologías o bien, con las herramientas y/o recursos** que existen para **prevenir riesgos y enfrentar amenazas de ciberseguridad**.

- Es relevante hacer referencia a la **compartición de dispositivos** (computadoras, tabletas, celulares, etc.) **para la educación en línea, el teletrabajo y el esparcimiento**. Este hecho no sólo sucede entre los miembros del hogar. En muchas instituciones educativas, los alumnos o docentes se encuentran **utilizando dispositivos propiedad de las escuelas para poder estudiar o trabajar** (en el caso de los docentes y demás personal de las instituciones educativas) remotamente.

- Los miembros de la comunidad educativa realizan sus actividades desde casa, utilizando **redes Wi-Fi poco seguras y dispositivos propios** que, comúnmente, no están alineados o configurados con controles o políticas de seguridad adecuados, lo cual los vuelve excepcionalmente vulnerables a ataques cibernéticos.

- Los **piratas informáticos** son **extremadamente creativos al idear formas de aprovecharse de los usuarios y de la tecnología** para acceder a contraseñas, redes y datos, a menudo, sirviéndose de herramientas de ingeniería social y de temas y tendencias populares para hacerlos caer en comportamientos inseguros en línea.

- En ese sentido, los **piratas informáticos están aprovechando el miedo y la confusión por la emergencia sanitaria por COVID-19** para difundir virus informáticos y/o llevar a cabo fraudes en línea[5]. La comunidad educativa no está exenta.

- De acuerdo con el **Índice de Civilidad Digital** de Microsoft (ICD) 2020[6], de 2016 a la fecha, se identifica una creciente ola de incivilidad en línea. En este periodo, el ICD a nivel global aumentó cuatro puntos para llegar a 70 por ciento. Esto se traduce en una **muy alta incivilidad percibida entre los usuarios que, cotidianamente, ingresan a la red y mantienen una activa interacción en las redes** sociales, así como la generación de otras tendencias negativas como dolor emocional y psicológico, resultado de la exposición a riesgos. En el caso de los adolescentes, los riesgos más comunes identificados fueron el contacto no deseado por gente extraña, sexting no deseado y ciberacoso[7].

Todo lo anterior, ha creado una **enorme superficie de exposición a ataques cibernéticos dirigidos a NNA, jóvenes, padres de familia, tutores, docentes, la red, la computadora portátil, el teléfono inteligente, la tableta**, etc. con la intención de cometer delitos informáticos.

Dichos factores plantean **importantes retos relacionados con la ciberseguridad de la comunidad educativa, en su conjunto, y la necesidad de un mayor involucramiento y acompañamiento** social e institucional para lograr comunidades escolares seguras y resilientes.

---

[5] Foro Económico Mundial (WEF, por sus siglas en inglés). ¿Por qué la ciberseguridad es más importante que nunca durante la pandemia de coronavirus?https://es.weforum.org/agenda/2020/03/por-que-la-ciberseguridad-es-mas-importante-que-nunca-durante-la-pandemia-de-coronavirus/

[6] El concepto de Civilidad Digital se refiere a promover entre los usuarios interacciones en línea más seguras, saludables y respetuosas. El índice de Civilidad Digital es una iniciativa que mide e identifica los riesgos de las personas en Internet y sus consecuencias.

[7] Microsoft. Centro de noticias para Latinoamérica. "En el Día del Internet Seguro, Microsoft revela que la Civilidad Digital mundial alcanza su nivel más bajo en 4 años" 11 de febrero de 2020.
https://news.microsoft.com/es-xl/en-el-dia-del-internet-seguro-microsoft-revela-que-la-civilidad-digital-mundial-alcanza-su-nivel-mas-bajo-en-4-anos/#:~:text=El%20%C3%8Dndice%20de%20Civilidad%20Digital%20(ICD)%20de%20Microsoft%2C%20una,alcanzado%20un%20porcentaje%20de%2070.

Por lo anterior, resulta necesario que la comunidad educativa cuente con la **suficiente sensibilización sobre los riesgos y amenazas** que enfrenta derivado del uso de redes y dispositivos de telecomunicaciones, así como sobre la **importancia de implementar medidas** para evitar y contener daños por la ocurrencia de incidentes de ciberseguridad.

Por estas razones, la Secretaría de Comunicaciones y Transportes (SCT) pone a disposición de NNA, jóvenes estudiantes, padres de familia, tutores, docentes y demás personal de las instituciones educativas, la **Guía de Ciberseguridad para el uso seguro de redes y dispositivos de telecomunicaciones en apoyo a la Educación**. En ella se **describen los riesgos y amenazas más comunes de ciberseguridad en el ámbito escolar y se proporcionan recomendaciones sencillas y prácticas para ayudar en la prevención de incidentes de ciberseguridad**. Todo ello, con el fin de promover experiencias positivas en línea, que favorezcan el aprendizaje, la creatividad y el desarrollo seguro de las actividades en línea de la comunidad educativa.

La ciberseguridad se trata de proteger los dispositivos que todos usamos y los servicios a los que accedemos en línea, tanto en casa y escuela como en el trabajo. A través de ella se busca evitar el acceso no autorizado a la información personal que almacenamos en estos dispositivos y en línea.

(Centro Nacional de Ciberseguridad del Reino Unido)
https://www.ncsc.gov.uk/files/NCSC_NEN%20cards_PRINT-2.pdf

AMENAZAS MÁS COMUNES A LA CIBERSEGURIDAD

Una de **las principales amenazas a la ciberseguridad de la comunidad educativa y que afecta directamente a los dispositivos tecnológicos** es el **malware**, también conocido como **código malicioso**. Éste se define como cualquier programa informático que se coloca de forma oculta en un dispositivo, con la intención de comprometer la confidencialidad, integridad o disponibilidad de los datos, las aplicaciones o el sistema operativo.

Los **tipos más comunes de amenazas de malware** incluyen virus, gusanos, troyanos, rootkits[8] y spyware[9]. Las amenazas de malware pueden infectar cualquier dispositivo por medio del correo electrónico, los sitios web que se visitan, las descargas y el uso compartido de archivos, el software punto a punto y la mensajería instantánea[10].

[8] Karspersky. ¿Qué es un Rootkit?: Es un tipo de malware diseñado para infectar una PC, el cual permite instalar diferentes herramientas que dan acceso remoto al ordenador. Este malware se oculta en la máquina, dentro del sistema operativo y sortea obstáculos como aplicaciones antimalware o algunos productos de seguridad. El rootkit contiene diferentes herramientas maliciosas como un módulo para robar los números de tarjeta o cuentas bancarias, un bot para ataques y otras funciones que pueden desactivar el software de seguridad. https://www.kaspersky.es/blog/que-es-un-rootkit/594/.

[9] Avast. Spyware: detección, prevención y eliminación. El Spyware es un tipo de malware que puede rastrear y registrar la actividad en equipos y dispositivos móviles. Hay cepas con comportamientos específicos; en general, los ciberladrones usan el spyware para recabar datos e información personal. https://www.avast.com/es-es/c-spyware

[10] Scarfone y Souppaya. "User's Guide to Securing External Devices for Telework and Remote Access Recommendations of the National Institute of Standards and Technology" 2016. National Institute of Standards and Technology (NIST). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-114.pdf

Además, **existen amenazas relacionadas con la ingeniería social como el Phishing, Smishing y Vishing**[11], por medio de las cuales los atacantes intentan engañar a las personas para que revelen información confidencial o realicen ciertas acciones, como descargar y ejecutar archivos que parecen ser benignos, pero que en realidad son maliciosos:

- El ***Phishing*** es un método de ataque a través del correo electrónico enviado por un delincuente pretendiendo ser otra persona, compañía o sitio de confianza, para robar la contraseña o información sensible. Este tipo de amenazas también pueden buscar tomar el control del dispositivo o computadora.

- El ***Smishing*** ocurre cuando se recibe un mensaje de texto corto (SMS) al teléfono celular, por medio del cual se solicita al usuario llamar a un número de teléfono o ir a un sitio web.

- El ***Vishing*** es la estafa que se produce mediante una llamada telefónica que busca engañar, suplantando la identidad de una persona o entidad para solicitar información privada o realizar alguna acción en contra de la víctima.

Además, existen otro tipo de riesgos y amenazas de ciberseguridad que están asociados al uso de las redes y dispositivos de telecomunicaciones por parte de NNA y jóvenes, los cuales se describen a continuación:

Contacto con depredadores en línea

En la medida en que NNA y jóvenes estudiantes pasan más tiempo utilizando redes y dispositivos de telecomunicaciones, **incrementan su exposición a entrar en contacto con depredadores en línea**, quienes realizan actividades ilícitas como pueden ser delitos de explotación y abuso sexual, así como trata de personas.

Online Grooming[12]

El *online grooming* se refiere al **acoso o abuso sexual en línea e implica la interacción de un adulto con NNA o jóvenes para ganarse su confianza e involucrarlos en alguna actividad sexual**. Esta práctica tiene diferentes niveles de interacción y peligro: desde hablar de sexo e intercambiar material íntimo, hasta mantener un encuentro sexual.

En el caso del online grooming el abusador envía, a través de un medio tecnológico, material sexual a NNA o jóvenes. En algunos casos, haciéndose pasar por un menor y adaptando su lenguaje al de la víctima.

Es esencial tener en cuenta que, especialmente, en el online grooming el engaño es lento y no hay consentimiento de la víctima, por lo que **nunca podrá ser culpa de ella**.

Cyberbullying o ciberacoso

El ***cyberbullying*** **o ciberacoso** tiene lugar a través de dispositivos digitales como teléfonos celulares, computadoras y tabletas. Esta conducta puede ocurrir a través de cualquier plataforma o servicio en donde se pueda compartir contenido.

---

[11] Santander. Cómo detectar el phishing. https://www.santander.com/es/stories/como-detectar-el-phishing
[12] Save the Children España. "Grooming: Qué es, cómo detectarlo y prevenirlo". https://www.savethechildren.es/actualidad/grooming-que-es-como-detectarlo-y-prevenirlo

El *cyberbullying* o ciberacoso incluye enviar, publicar o compartir contenido negativo, dañino, falso o malo sobre otra persona; por ejemplo, información personal o privada que cause vergüenza o humillación. Algunas conductas de ciberacoso cruzan la línea hacia comportamientos ilegales o criminales. Los lugares más comunes donde se produce el ciberacoso son[13]:

- Redes sociales.
- Mensajería de texto y aplicaciones de mensajería en dispositivos móviles o tabletas, como mensajes cortos (SMS).
- Mensajería instantánea, mensajería directa a través de Internet.
- Teleconferencias, foros en línea y salas de chat.
- Correo electrónico.
- Comunidades de juegos en línea.

El ciberacoso es una preocupación muy importante entre la comunidad educativa, pues tiene efectos negativos de gran alcance. El cambio de las aulas a los medios electrónicos pone a los alumnos mucho más en contacto con la tecnología y podría incrementar su exposición al ciberacoso[14].

NNA y jóvenes estudiantes, incluyendo aquéllos con discapacidades y quienes son percibidos como diferentes, pueden sufrir un mayor riesgo de acoso y discriminación en línea. Por lo anterior, es de suma relevancia aprender a detectar el ciberacoso a tiempo y cómo actuar con quien lo ejerce sobre otros.

Sexting[15]

El *sexting* no es un problema de seguridad por sí mismo, sino una práctica de riesgo, sobre todo cuando implica a menores de edad. Consiste en el envío de contenidos de tipo sexual (principalmente fotografías y/o videos que contienen imágenes con poca o nula ropa, o que muestran o describen actividades sexuales). Estos contenidos son producidos, generalmente, por el propio remitente, para ser enviados a otras personas por medio de teléfonos móviles u otros dispositivos tecnológicos como tabletas o computadoras.

El riesgo de practicar sexting radica en que, una vez que se envían estos contenidos, pueden ser utilizados de forma dañina por los demás.

Es posible que el envío de este tipo de contenidos sea involuntario, ya que otra persona puede utilizar el dispositivo en el que están almacenados (como en el caso de robo o pérdida del teléfono celular o uso sin permiso) y compartir el material comprometedor. También puede ocurrir que una persona sea grabada por otra sin su consentimiento.

Es importante sensibilizar a NNA y jóvenes sobre los riesgos de practicar el *sexting*. Debido a esto, la prevención debe centrarse en la reducción de riesgos y el desarrollo de la capacidad de crítica, para que actúen de forma responsable y eviten exposiciones a riesgos de extorsión, acoso y humillación, a sabiendas de que los materiales compartidos una vez en línea, estarán siempre en línea.

[13] Sitio Stop Bullying del Gobierno de Estados Unidos. https://www.stopbullying.gov/cyberbullying/what-is-it
[14] Fondo de las Naciones Unidas para la Infancia (UNICEF)."COVID-19 and its implications for protecting children online". Abril, 2020. https://www.unicef.org/sites/default/files/2020-04/COVID-19-and-Its-Implications-for-Protecting-Children-Online.pdf
[15] Instituto Nacional de Ciberseguridad de España (INCIBE). Portales Incibe. https://www.is4k.es/necesitas-saber/sexting

Acceso a contenido potencialmente dañino o ilegal

El aumento de la actividad en línea puede exponer a NNA y jóvenes a contenido potencialmente dañino como noticias falsas, retos que atenten contra su propia integridad, contenido violento, misógino, misándrico, xenófobo o que incite a la violencia, al suicidio, la autolesión o a desórdenes como la bulimia, anorexia u otras conductas dañinas.

También, NNA y jóvenes pueden estar expuestos a una mayor cantidad de mercadotecnia en línea que promueva alimentos poco saludables, estereotipos de género o resulte inapropiada para la edad.

En el contexto de la emergencia sanitaria, NNA y jóvenes pueden estar expuestos a información errónea que podría generar miedo y ansiedad adicionales.

RECOMENDACIONES DE CIBERSEGURIDAD

En la actualidad, existen muchas herramientas y recursos útiles y sencillos para minimizar los riesgos y amenazas de ciberseguridad derivados del uso de redes y dispositivos de telecomunicaciones, así como de múltiples soluciones digitales en el ámbito educativo.

Recomendaciones generales

- No dejar a la vista de otras personas información relevante, como aquélla sensible o claves de acceso.

- Mantener siempre la computadora, tableta, teléfono celular o cualquier otro dispositivo, en un lugar seguro y con contraseña, a fin de restringir el acceso a éstos por parte de personas no autorizadas.

- Al alejarse de los dispositivos, es importante bloquear la sesión.

- Mantener cubierta la cámara web cuando no se esté utilizando, para limitar el acceso que pudieran llegar a tener a ésta aplicaciones o programas no autorizados.

- Deshabilitar la auto ejecución de memorias USB para evitar que, por ese medio, se ejecuten programas maliciosos.

- Si la institución educativa facilita los dispositivos (computadora, tableta, etc.) para el desarrollo de las actividades de educación en línea, es indispensable realizar un uso exclusivamente educativo de los medios proporcionados. No se recomienda, en ninguna circunstancia, manipularlos, modificar su configuración, o prestarlos a otras personas.

- Realizar copias de seguridad periódicas de la información que se almacena en los dispositivos para garantizar el acceso a la información almacenada, ya sea personal o vinculada a las actividades de educación en línea. Así, en caso de que ocurra cualquier incidente de seguridad (robo, pérdida del dispositivo, o avería, etc.) se podrá mantener el acceso a la misma.

- **Proteger con contraseña (encriptar) los dispositivos** donde se almacene información (memorias USB o discos externos) para proteger la información de posibles accesos malintencionados y garantizar así su confidencialidad e integridad.

Recomendaciones de ciberseguridad para el uso seguro de las redes y dispositivos de telecomunicaciones en apoyo a la educación

En caso de que NNA, jóvenes, padres, tutores, docentes y demás personal de las instituciones educativas utilicen dispositivos personales para las actividades de educación en línea, aunque éstos no cuenten con políticas de seguridad rigurosas, pueden reducir sus vulnerabilidades poniendo en práctica las siguientes recomendaciones:

Sistema Operativo

- **Mantener actualizados los sistemas operativos y las aplicaciones** de los dispositivos, incluidas las computadoras personales (PC), los teléfonos inteligentes y las tabletas. Estas actualizaciones normalmente incluyen cambios importantes que mejoran el rendimiento y la seguridad de los equipos; muchos de estos programas, incluso, se actualizan de manera automática.

- Se recomienda **activar funcionalidades de protección, como el cortafuegos (*firewall*), incorporadas en los sistemas operativos más comunes**. Un cortafuegos es la primera línea de defensa ante un ataque a una red desde Internet y permite proteger el equipo de programas maliciosos o de atacantes que intenten conectarse al equipo de forma remota[16]. Además, permite establecer reglas para indicar qué conexiones de red se deben aceptar y cuáles no. Al mismo tiempo, admite el intercambio normal de datos entre la computadora y servicios verificados de Internet.

Antivirus

Los antivirus son programas que ayudan a proteger los dispositivos contra la mayoría de los virus, gusanos, troyanos y otros tipos de *malware* que pueden infectar a los dispositivos. Por ello se recomienda:

- Instalar y mantener actualizados los **antivirus, prefiriendo aquéllos** que incorporan funcionalidades de protección contra malware y cortafuegos (firewall), también conocidos como **"suites de seguridad"**.

- **Evitar tener dos antivirus en un mismo dispositivo. Tener dos antivirus activos no significa mayor protección**; de hecho, puede ocasionar diferentes problemas en el sistema. Un antivirus que esté trabajando se convertirá en un "software malicioso" a los ojos del otro, el cual intentará bloquearlo y eliminarlo, y se corre el riesgo de afectar el desempeño del sistema por el consumo extra de recursos[17].

---

[16] Soporte de Microsoft. Activar o desactivar el Firewall de Microsoft Defender. https://support.microsoft.com/es-es/help/4028544/windows-10-turn-microsoft-defender-firewall-on-or-off
[17] Oficina de Seguridad del Internauta del Instituto Nacional de Ciberseguridad de España (OSI-INCIBE). ¿Sabías que utilizar tus dispositivos personales para trabajar puede ser peligroso?

- **Todas las instalaciones y actualizaciones de programas y aplicaciones deben hacerse desde el sitio web oficial del fabricante**[18] **o desde las tiendas oficiales de apps** -verificando la identidad del autor de la aplicación-, evitando descargar e instalar aquéllas de dudosa procedencia.

Seguridad de la red Wi-Fi

Una parte importante de la educación en línea es la **aplicación de medidas de seguridad de las redes en el hogar**. Es cada vez más común que los usuarios cuenten en casa con un ruteador inalámbrico (Wi-Fi) para conectar sus dispositivos a Internet sin necesidad de cables.

Para evitar que usuarios no autorizados se conecten de forma inalámbrica al ruteador y tengan la posibilidad de acceder a la conexión, e incluso al resto de los dispositivos conectados y a la información que se transmite, **es importante asegurar que la red Wi-Fi cuente con contraseña que el usuario debe introducir al conectar por primera vez un dispositivo**.

Los ruteadores ofrecen varios tipos de contraseñas y cifrados (que codifican los datos del usuario, usando un valor o clave secreta y los hace incomprensibles para terceros), como los siguientes:

- **Las redes sin cifrado, o abiertas**, son aquéllas que no tienen ninguna contraseña o cifrado y permiten a cualquier usuario conectarse. Una red con estas características **no es recomendable**.

- El **cifrado *Wired Equivalent Privacy*** (WEP, por sus siglas en inglés) es considerado, hoy en día, un **sistema poco seguro y no se aconseja su utilización** ya que, con las herramientas y conocimientos adecuados, se puede llegar a conseguir la clave de acceso a la red Wi-Fi en pocos minutos.

- El **cifrado *Wi-Fi Protected Access*** (WPA, por sus siglas en inglés), específicamente en su versión 2 (WPA2) o más actualizada, **es considerado seguro y se recomienda comprobar que esté habilitado** como parte de las medidas de seguridad de la red.

  Para comprobarlo, es necesario entrar desde la computadora a las propiedades de la red, para ver el tipo de seguridad de la conexión. **Se recomienda tener habilitada alguna de las variantes de WPA2**, al menos[19]. Puedes solicitar apoyo a tu proveedor de servicio de Internet para más orientación.

- Se recomienda **cambiar las contraseñas predeterminadas en el ruteador por unas de elección del usuario, utilizando una contraseña robusta para la red Wi-Fi**. Asimismo, se sugiere que incluya mayúsculas, minúsculas, números y símbolos. Cuanto mayor sea la longitud de la contraseña, más difícil será que un atacante pueda descubrirla[20].

- Es importante **evitar compartir la clave de la red Wi-Fi con otras personas**, pues quien tenga acceso a tu red inalámbrica podría tener acceso a todos los dispositivos conectados a ella.

---

https://www.osi.es/es/actualidad/blog/2019/05/15/sabias-que-utilizar-tus-dispositivos-personales-para-trabajar-puede-ser

[18] Ídem.

[19] Santander. Redes más seguras en casa. https://www.santander.com/es/stories/redes-mas-seguras-en-casa

[20] Oficina de Seguridad del Internauta del Instituto Nacional de Ciberseguridad de España (OSI-INCIBE). Tu router, tu castillo. Medidas básicas para su protección. https://www.osi.es/es/actualidad/blog/2016/11/03/tu-router-tu-castillo-medidas-basicas-para-su-proteccion

- Se recomienda **evitar la conexión a redes Wi-Fi públicas abiertas** (o hotspots Wi-Fi) **para compartir contenido sensible**. Estas redes no son recomendables para el intercambio de información delicada ya que permiten que cualquier dispositivo se conecte al ruteador sin ningún tipo de seguridad, por lo que cualquier usuario podría capturar la información se transmita a través de dicha conexión.

Contraseñas

Las **contraseñas protegen la información que contienen los dispositivos y cuentas de los usuarios**. No obstante, ante la cantidad de claves y combinaciones que cotidianamente se deben utilizar, la mayoría de las personas opta por contraseñas fáciles de recordar por la comodidad que esto implica, o bien, por la falta de conocimiento de lo fácil que puede ser para un ciberdelincuente obtenerlas.

Para asegurar la efectividad de las contraseñas y evitar el robo de éstas, es recomendable poner en práctica las siguientes acciones[21]:

- **Al generar las contraseñas de los dispositivos y cuentas** se deben utilizar claves largas y únicas para cada caso, **evitando utilizar la misma contraseña** para diferentes dispositivos o cuentas.

- Se deben **evitar las combinaciones sencillas** como fechas de nacimiento, secuencias consecutivas, repeticiones de un mismo dígito o palabras simples como "password" o "contraseña".

- La mayor **longitud de la contraseña**, así como la **incorporación de mayúsculas, minúsculas, números y caracteres especiales**, contribuyen a que ésta sea más segura y difícil de vulnerar.

- Se debe **evitar escribir contraseñas en papeles o tener archivos con esa información** que sean fácilmente accesibles para otros.

- **Habilitar el doble factor de autenticación o verificación en dos pasos**. Esta medida es una capa adicional de seguridad disponible para cada vez más servicios en la que, además de la contraseña, durante el inicio de sesión se solicita información sobre otro medio al que sólo el usuario autorizado tiene acceso (por ejemplo, verificación para entrar al correo electrónico mediante la recepción de un código vía SMS, llamada o mensaje de WhatsApp).

- Es importante **no facilitar a nadie, aunque así lo solicite, por ningún medio, contraseñas y/o códigos** para el inicio de sesión.

- Es recomendable **cambiar con frecuencia las contraseñas** a efecto de evitar accesos no autorizados.

[21] Oficina de Seguridad del Internauta del Instituto Nacional de Ciberseguridad de España (OSI-INCIBE). Campañas/ Contraseñas Seguras. https://www.osi.es/es/campanas/contrasenas-seguras

Ataques con técnicas de ingeniería social

Los ataques de ingeniería social **buscan engañar a los usuarios para obtener nombres de usuario y contraseñas, así como otra información** sensible.

La capacidad de **identificar un ataque de ingeniería social minimiza, en gran medida, el riesgo de ser víctimas de los ciberdelincuentes** y ver comprometida información personal. Por ello, se recomienda[22]:

- **Estar alertas ante comunicaciones**, como llamadas, correos electrónicos, mensajes cortos (SMS), enlaces de teleconferencias e invitaciones de calendario **de remitentes desconocidos**.

- **Antes de abrir cualquier enlace, archivo anexo, mensaje de texto o llamada** de un remitente desconocido, **hay que preguntarse** lo siguiente:

    - **¿Espero esa información?** Si el mensaje proviene de un remitente desconocido (persona u organización), **analizar bien antes de responder o hacer clic y/o descargar** cualquier archivo adjunto.
    - **¿Reconozco al remitente? Comprobar si la dirección está bien escrita** (verificar que no haga falta ninguna letra, por ejemplo) y si el dominio (la terminación del correo electrónico) **es de confianza y corresponde a quien envía el mensaje**.
    - **¿Solicitan que haga algo?** Los correos electrónicos fraudulentos (*phishing*) o los mensajes de texto de este tipo (*smishing*) **suelen pedir que se realice alguna acción** como: **hacer clic** en un hipervínculo, **descargar** algún archivo, responder al mensaje proporcionando información personal, etc. Con frecuencia, **buscan generar una sensación de urgencia y provocar una reacción inmediata e irracional. Es necesario analizar con calma** antes de proporcionar cualquier información que pudiera resultar comprometedora.
    - Se debe **desconfiar, particularmente, de los mensajes que parecerían genéricos** (como "Estimados:", "A quien corresponda:", etc.).
    - **Algunos correos electrónicos de *phishing*** son más sofisticados que otros, por lo que resulta muy útil saber **identificar las pistas más obvias**, que incluyen: imágenes de **logotipos de baja calidad, errores ortográficos o gramaticales, se dirigen al usuario como "querido amigo"** en lugar de por su nombre o se refieren a un mensaje anterior inexistente, etc.
    - En el caso de **comunicaciones referentes a instituciones bancarias y financieras**, se recomienda **NUNCA dar clic en los enlaces contenidos en un correo o SMS y NO proporcionar información de acceso a tus cuentas**. Si tienes alguna duda, debes contactar directamente a tu institución financiera (utilizando el número telefónico que vienen atrás de tu tarjeta, por ejemplo) para más orientación.

Navegación segura

A efecto de promover la navegación segura en Internet, se sugiere adoptar las siguientes recomendaciones:

- **Ingresar sólo a sitios web confiables**, escribiendo uno mismo la dirección de la página a la que se quiere acceder y evitando utilizar ligas proporcionadas por terceros.

[22] Santander. Cómo detectar el phishing. https://www.santander.com/es/stories/como-detectar-el-phishing

- **Conocer y aplicar las funcionalidades de "navegación privada" o "navegación segura"**, que impiden el almacenamiento del historial en el navegador, así como imágenes, nombres de usuario y contraseñas.

- Cuando se realicen transacciones o intercambio de información sensible, **asegurarse de que la dirección de la página web comience con "https"** (no "http"), lo que contribuye a mantener segura la información transmitida.

- **Desactivar la compartición de tu ubicación geográfica**, a menos que sea estrictamente necesario.

- **Evitar el ingreso de información personal en formularios dudosos**. Si te encuentras ante un formulario que solicita información delicada (por ejemplo, nombre de usuario y contraseña), es recomendable verificar la legitimidad del sitio antes de responder.

- Al terminar de navegar en Internet, es **importante cerrar la sesión, sobre todo si se utiliza un equipo compartido**, para evitar que otras personas tengan acceso a cuentas e información privada.

Uso seguro de las herramientas de la nube

La nube permite almacenar y administrar datos, así como ejecutar aplicaciones en línea, entre muchas otras funciones. Con relación al almacenamiento, **la nube permite acceder a archivos y datos desde cualquier dispositivo conectado a Internet**; es decir, **la información está disponible en cualquier lugar en el que te encuentres y siempre que la necesites**[23].

Para hacer uso de los servicios de la nube de manera segura y evitar el robo o mala utilización de la información almacenada, es conveniente tener en mente las siguientes recomendaciones[24]:

- Tener conocimiento de las **condiciones de uso y las políticas de privacidad** antes de utilizar cualquier servicio en la nube.

- Utilizar servicios de almacenamiento que cuenten con **cifrado "https" y certificado de seguridad**. Esto lo puedes verificar en la barra de direcciones de tu navegador de Internet.

- **No subir a la nube información sensible con acceso público o abierto**. Se recomienda utilizar herramientas de cifrado, como es el uso de **carpetas con contraseña y acceso restringido**.

- **Verificar periódicamente los archivos y carpetas que tenemos compartidos** desde nuestra cuenta, a fin de **deshabilitar los enlaces y acceso a terceros que ya no sean necesarios**.

- **Utilizar contraseñas robustas para acceder al servicio** y, preferentemente, activar el doble factor de autenticación o verificación en dos pasos.

[23] Microsoft Azure. ¿Qué es la nube? https://azure.microsoft.com/es-es/overview/what-is-the-cloud/
[24] Oficina de Seguridad del Internauta del Instituto Nacional de Ciberseguridad de España (OSI-INCIBE). Tu información en la nube. https://www.osi.es/es/tu-informacion-en-la-nube

- Realizar periódicamente un **respaldo de la información almacenada** en la nube en otro tipo de dispositivo, por ejemplo, en un disco duro externo debidamente protegido por contraseña. De esa manera, se mantiene el acceso a la información en caso de cualquier contratiempo, como una conexión limitada a Internet.

- **Cerrar la sesión de la nube al concluir las actividades** que se estén realizando.

Teleconferencias para impartir clases en línea

La demanda de servicios de teleconferencias para la impartición de clases en línea, o bien, para sesiones de estudio, especialmente a partir de la emergencia sanitaria generada por COVID-19, **se ha incrementado considerablemente**. Las teleconferencias se han convertido en una herramienta indispensable para desarrollar las actividades de educación en línea, dar continuidad a asuntos laborales, la vida cotidiana y la comunicación con familiares y amigos.

Lo novedoso de estos servicios para muchos usuarios y la aparición de algunas vulnerabilidades en ciertas plataformas, supone para los ciberdelincuentes la **oportunidad para el acceso no autorizado** a información, robo de credenciales y acceso a los distintos recursos del dispositivo (como micrófono, cámara, etc.)[25].

Por lo anterior, es necesario **promover la adecuada protección de los usuarios** para evitar incidentes al usar estos servicios[26], tomando en consideración las siguientes recomendaciones:

- **Informarse sobre las políticas de privacidad y las medidas de seguridad que implementa el servicio** que se desea utilizar.

- **Descargar e instalar la aplicación correspondiente desde la página web oficial del desarrollador o desde las tiendas oficiales** de apps.

- **Mantener actualizada la aplicación que se utilice**, pues es a través de este proceso que se puede asegurar que las vulnerabilidades detectadas y corregidas por el desarrollador se están implementando.

- Al organizar una teleconferencia se recomienda tener en cuenta:

    - En el caso de reuniones privadas, **compartir el enlace** directamente con los participantes, **haciendo uso de las funciones de compartición de las propias aplicaciones**, y evitando el uso de redes sociales o canales de comunicación abiertos que podrían promover accesos no deseados.
    - **Proteger la conferencia con una contraseña robusta**, para restringir el acceso a ésta a personas no autorizadas.
    - Poner a los asistentes en **sala de espera**, si la plataforma permite dicha funcionalidad. Previa verificación, se podrá aceptar su ingreso, de ser el caso.

[25] Jaimovich Desirée. (02 de abril de 2020). Zoom: alertan por graves fallas de seguridad en la popular aplicación de videollamadas. Infobae. https://www.infobae.com/america/tecno/2020/04/02/zoom-alertan-por-graves-fallas-de-seguridad-en-la-popular-aplicacion-de-videollamadas/
[26] Instituto Nacional de Ciberseguridad de España (INCIBE). Aplica estos consejos y protege tus videollamadas. https://www.incibe.es/protege-tu-empresa/blog/aplica-estos-consejos-y-protege-tus-videollamadas

- Los participantes en teleconferencias deben:
    - **Evitar compartir su escritorio de forma predeterminada**, ya que esto podría provocar fugas de información.
    - **Cuidar el encendido del micrófono y la cámara de video** para evitar situaciones incómodas o embarazosas.
    - **Si la teleconferencia es grabada, el organizador debe comunicarlo** a los participantes.
    - **No usar los chats de la plataforma** para enviar **mensajes de índole personal**.
    - **No compartir información personal** mediante la plataforma, principalmente información de identificación personal.

Uso de Redes sociales para impartir o complementar clases en línea[27]

- **Mantener un perfil u orientación académica** que vaya acorde al ambiente educativo.
- Publicar información relativa a las actividades educativas y **evitar compartir información confidencial** o de tipo personal con colegas o estudiantes.
- Utilizar **contraseñas seguras y nunca compartirlas**.
- Prestar mucha **atención a las noticias, mensajes o cualquier otra información que se reciba a través de las redes sociales, para evitar ser víctimas** de fraudes en línea, acoso o ser engañado para descargar e instalar malware.
- Ser cuidadoso en la forma de responder, a efecto de **transmitir mensajes de manera clara y directa**.
- **Respetar la opinión de los demás y aceptar los diferentes puntos de vista** del resto de los usuarios.

Red Privada Virtual

Una **Red Privada Virtual** (**VPN**, por su acrónimo en inglés) es un **servicio mediante el cual se establece una conexión segura a través de Internet**, entre los usuarios de Internet y los servicios o páginas web a los que éstos acceden[28].

Si imaginamos el Internet como un río en el que fluye el agua (datos e información), la VPN es un tubo, sumergido en el río, que impide ver todo lo que pasa dentro de él, debido a que la conexión entre los dispositivos y el servidor VPN siempre está cifrada (protegida). De esa manera, **si alguien interceptara tus comunicaciones, sería incapaz de interpretar la información transmitida**.

Para añadir una capa extra de seguridad a tus comunicaciones, **las VPN pueden contratarse como servicio, si tu institución educativa no te lo proporciona (no se recomienda utilizar servicios de VPN gratuitos**, pues éstos podrían tener el efecto contrario al deseado de proteger la información).

---

[27] Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES). "Ciberseguridad para la educación en línea: Recomendaciones". https://recursosdigitales.anuies.mx/ciberseguridad-para-la-educacion-en-linea2/recomendaciones/

[28] Oficina de Seguridad del Internauta del Instituto Nacional de Ciberseguridad de España (OSI-INCIBE). Te explicamos qué es una VPN y para qué se usa. https://www.osi.es/es/actualidad/blog/2016/11/08/te-explicamos-que-es-una-vpn-y-para-que-se-usa

RECOMENDACIONES DIRIGIDAS A PADRES, TUTORES O DOCENTES PARA LA CIBERSEGURIDAD DE NNA Y JÓVENES[29]

Mantener la ciberseguridad de la comunidad educativa requiere de la **participación activa de los padres, tutores, docentes y autoridades escolares** para que puedan ayudar a NNA y jóvenes a hacer un **uso de las redes y dispositivos de telecomunicaciones de manera segura, responsable y positiva**:

- **Empoderar a NNA y jóvenes en línea**.

  Padres, tutores, docentes y autoridades escolares deben reconocer la necesidad de que **NNA y jóvenes cuenten con todas las herramientas y el conocimiento para hacer uso de las comunicaciones y tecnologías de la información** y manejar su vida "online" de manera segura y responsable.

  La información orientada a NNA y jóvenes (mensajes y consejos) **para un mejor desempeño en el mundo digital debe dirigirse por las vías y en las formas en las que mejor puedan comprenderla y asimilarla**. En este sentido, es necesario poner a su disposición recursos para que accedan a ayuda y apoyo especializado.

  NNA y jóvenes deben ser **motivados para hacer uso de su voz** *"online"* y dotarles de herramientas para apoyar a otros NNA en situación de riesgo.

- **Tener el conocimiento y la sensibilidad de los riesgos y amenazas que existen en línea**.

  Es necesario que **padres, tutores y docentes conozcan sobre las amenazas y riesgos** a los que se enfrentan NNA y jóvenes **al utilizar dispositivos, plataformas, aplicaciones y, en general, las comunicaciones y tecnologías de la información. Es importante conocer las acciones para prevenir** y enfrentar dichos riesgos, así como controlar los daños en caso de incidentes de ciberseguridad que afecten su integridad y bienestar físico y emocional.

  Es muy relevante **conversar con NNA y jóvenes sobre los temas de acoso y el peligro que representa compartir** información, así como entablar cualquier comunicación **con extraños**.

- **Mantener un diálogo constante y abierto con NNA y jóvenes para promover una cultura de ciberseguridad**.

  Crear **una red de apoyo para que NNA y jóvenes se sientan cómodos buscando ayuda**: el diálogo abierto y la discusión son cruciales. La forma en que los adultos reaccionan tiene una influencia crítica en la disposición de los niños a revelar si están molestos, preocupados por algo que han visto o que les ha sucedido en línea. **Diversas investigaciones han demostrado que muchos jóvenes son reacios a hablar con un adulto sobre una experiencia negativa en línea por temor a las regaños y castigos o represalias**[30]. Es relevante mantenerse atento a cualquier signo de angustia.

---

[29] UNICEF. "COVID-19 and its implications for protecting children online", Abril, 2020. https://www.unicef.org/sites/default/files/2020-04/COVID-19-and-Its-Implications-for-Protecting-Children-Online.pdf

[13] UIT. "Protección de la Infancia en Línea: Guía para padres, tutores y educadores" https://www.itu.int/en/cop/Documents/guidelines-educ-s.pdf

[30] UNICEF. "COVID-19 and its implications for protecting children online" Abril, 2020. https://www.unicef.org/sites/default/files/2020-04/COVID-19-and-Its-Implications-for-Protecting-Children-Online.pdf

- Discutir con NNA y jóvenes el uso que le dan a aplicaciones, juegos y plataformas que utilizan frecuentemente, teniendo en cuenta aspectos que ayuden a garantizar su seguridad y privacidad. En este sentido, es importante realizar en conjunto la identificación de aplicaciones que podrían no ser apropiadas.

- Verificar con regularidad, por parte de padres, tutores y docentes, el uso que NNA y jóvenes dan a la tecnología a su disposición, estar familiarizados con los sitios que visitan regularmente, identificar qué tipo de actividades realizan en línea, el contenido que comparten, cómo están utilizando teléfonos celulares, tabletas, computadoras, así como qué nuevas herramientas y aplicaciones podrían estar usando.

- Fomentar el pensamiento crítico para analizar el tipo de información a la que NNA y jóvenes tienen acceso.

  El análisis y la discusión con NNA y jóvenes de ciertos contenidos en línea ayudará a éstos a formar un criterio para la identificación de contenido regular, publicidad engañosa y contenido dañino que promueva la violencia, la discriminación y conductas de riesgo, o bien la comprensión y manejo de noticias falsas o de dudosa procedencia.

- Configurar los controles parentales para la navegación en Internet y el acceso a contenidos.

  Los principales navegadores incluyen un modo de control parental. Además, algunos proveedores de servicio de Internet y operadores móviles proporcionan herramientas de control parental adicionales que bloquean o restringen el acceso a ciertos tipos de contenido.

- Establecer reglas para el uso y exposición a las comunicaciones y tecnologías de la información.

  Es muy relevante que padres, tutores y, de ser el caso, docentes establezcan reglas para administrar el tiempo frente a la pantalla de NNA y jóvenes, así como los límites para las actividades en línea, siempre que sea posible. En complemento, es fundamental promover un equilibrio entre el tiempo en línea y otras actividades.

- Mantener la seguridad de los dispositivos.

  Asegurarse de que se encuentren actualizados los sistemas operativos y las aplicaciones de los dispositivos que utilizan NNA y jóvenes. Asimismo, asegurarse de que en estos dispositivos se encuentran instalados y actualizados programas antivirus.

- Si la institución educativa cuenta con lineamientos de ciberseguridad, es esencial que los padres, tutores y docentes tengan conocimiento de su contenido y aseguren que NNA y jóvenes han leído y entendido éstos, para su cumplimiento en las actividades de educación desde casa.

- Fomentar la resiliencia de NNA y jóvenes en línea.

  Fortalecer las capacidades de NNA y jóvenes para superar los desafíos que se presentan en el mundo digital, los cuales pueden generar angustia, ansiedad, enojo, tristeza, aislamiento, etc. Lo anterior, a través de la puesta en práctica de algunas de las siguientes estrategias:

- Identificar y reconocer el desafío o la situación adversa.
- Dialogar con la persona involucrada e intentar resolver el problema de manera amigable.
- Pedir apoyo o consejo a un adulto de confianza sobre el tema.
- Realizar actividades alternas que ayuden a mejorar el ánimo ante una situación estresante, incómoda.
- Dar un espacio y alejarse de la situación.
- Reconocer que todos los usuarios de Internet comenten errores.

Recomendaciones de Ciberseguridad para NNA y jóvenes en línea

¿Qué sí hacer?

- Respetar la privacidad de los demás.
- Identificar e informar a padres, tutores o docentes sobre contenido potencialmente dañino o ilegal en las redes sociales o plataformas que utilizan.
- Usar un alias/nombre alternativo como nombre de usuario si necesitan interactuar con otros en línea.
- Informar a padres, tutores, docentes o adultos de confianza sobre cualquier amenaza o situación negativa.
- Aplicar la configuración de privacidad a las cuentas de redes sociales, de modo que las publicaciones sólo sean visibles para amigos cercanos y conocidos.
- Conectarse sólo con personas conocidas.
- Mantener una reputación digital: Pensar dos veces antes de publicar algo embarazoso, dañino, inapropiado o de fuentes dudosas.
- Reportar en sitios web o redes sociales cualquier situación abusiva, ofensiva, amenazante o comportamientos inapropiados.
- Informar inmediatamente al administrador de los servicios si se sospecha que alguna cuenta (por ejemplo, de correo electrónico o redes sociales) ha sido hackeada. Si todavía se tiene acceso a la misma, lo mejor es cambiar la contraseña al instante.
- Antes de reportar o durante el proceso, enterar de lo acontecido a padres, tutores, docentes o adultos de confianza.
- Compartir número de teléfono sólo con familiares y amigos cercanos.

¿Qué no hacer?

- NO compartir información personal (nombre completo, fecha de nacimiento, número de teléfono, etc.) de uno mismo o de sus familiares si no es necesario.
- NO publicar en redes todas las actividades cotidianas.
- NO enviar fotos a personas desconocidas, especialmente si éstas son con poca o nula ropa, o compartirlas en redes sociales.
- NO abrir correos electrónicos ni archivos adjuntos de remitentes desconocidos.
- NO responder a mensajes de desconocidos ni visitar páginas web que soliciten información personal.
- NO ingresar contraseñas en presencia de otras personas
- NO compartir contraseñas con terceros por ningún medio (papel, mensaje de texto, *inbox* o correo electrónico).
- NO guardar nombres de usuario y contraseñas en el navegador.
- NO utilizar ni difundir en medios electrónicos información de otras personas.

- NO acceder ni usar archivos de otras personas sin su consentimiento.
- NO copiar ni utilizar software que tenga derechos de autor sin las autorizaciones correspondientes.
- NO descargar contenido no autorizado o ilegal.
- NO intimidar, acosar, amenazar a otras personas, hacer burlas o comentarios con connotación racista, xenófoba, misógina, misándrica, o que promuevan la violencia o conductas de riesgo. No se debe utilizar lenguaje ofensivo, despectivo o con tintes de odio.
- NO iniciar sesión como otra persona para ingresar a su perfil de redes sociales o leer sus correos electrónicos u otra información privada.
- NO instalar códigos maliciosos en las computadoras o dispositivos de otras personas.
- NO organizar encuentros con desconocidos ni acceder a hacerlo si algún extraño lo solicita. Se debe informar inmediatamente de la situación a un adulto, amigo o persona de confianza.

RECURSOS

A continuación, se ponen a disposición algunos **recursos de interés**, que pudieran resultar de utilidad para la comunidad educativa que participa en el desarrollo de actividades educativas en línea:

SCT:

- Guía de Ciberseguridad para el uso seguro de las redes y dispositivos de telecomunicaciones en apoyo al teletrabajo de la SCT
- Simulador de Ciberseguridad de la SCT
- Guía para las familias sobre el uso de las tecnologías de telecomunicaciones y radiodifusión
- Cursos en línea y certificaciones a través de los Centros de Inclusión Digital de la SCT, en colaboración con Coursera

SEP:

- Plataforma @prende 2.0 de la Secretaría de Educación Pública (SEP)/Canal de ciberseguridad

Microsoft:

- Informar sobre contenido terrorista
- Notificar pornografía sin consentimiento
- Informar sobre contenido con lenguaje inflamatorio
- Notificar abuso en OneDrive
- Notificar un problema a Bing
- Reto de Civilidad Digital (original en inglés)
- Índice de Civilidad Digital
- Recursos de seguridad en línea (original en inglés)

INCIBE – España:

- Recurso pedagógico para mejorar contraseñas
- Plataformas de videoconferencia y aspectos de seguridad que te interesa conocer
- Material didáctico del portal Internet Segura for Kids (IS4K)
- Consejos para la utilización segura de dispositivos personales
- Material didáctico e informativo de la Oficina de Seguridad del Internauta

Material didáctico e informativo específico para los docentes y centros educativos:

- Consejos de teletrabajo para docentes
- Uso de aplicaciones de gestión educativa que debemos saber
- Buen uso del correo electrónico en el entorno educativo
- Ciberseguridad en el centro educativo

Material didáctico e informativo para la familia:

- Ciberseguridad para familias (con menores en edad escolar)

Instituciones académicas:

- Recomendaciones al elegir una suite de seguridad de la Coordinación de Seguridad de la Información de la UNAM (UNAM CERT)
- Recursos digitales de la ANUIES relacionados con la educación en línea

Unión Internacional de Telecomunicaciones:

- Protección de la Infancia en Línea: Directrices para los niños
- Guía de ciberseguridad para los países en desarrollo
- Protección de la Infancia en Línea: Guía para padres, tutores y educadores

Otros organismos internacionales:

- Derechos de la infancia en la era digital de la Comisión Económica para América Latina y el Caribe (CEPAL)
- Los seguidores que tú no ves de UNICEF
- Cinco formas de moverte seguro en línea de UNICEF Colombia

Google:

- Centro de Seguridad
- Material didáctico Sé genial en Internet

Facebook:

- Centro de Seguridad

Otros:

- Plan de aprendizaje en Ciberseguridad de Open P-TECH

CONCLUSIÓN

La educación en línea representa una oportunidad para desarrollar las tareas educativas de forma innovadora y motivadora, abre nuevas posibilidades y, a la vez, nuevas vulnerabilidades de las que debemos estar conscientes y alertas para responder de manera adecuada.

El acceso a Internet está cada día más presente en la vida de las personas y, en ese sentido, el uso seguro de las telecomunicaciones en apoyo a la educación cobra especial relevancia como un quehacer que es relevante para toda la comunidad educativa que utiliza estos servicios.

Es importante continuar el desarrollo de instrumentos que, como esta guía, contribuyan a seguir avanzando en el impulso del uso seguro de las telecomunicaciones en apoyo a la educación, en beneficio de todas y todos los mexicanos.