Guía de uso seguro y responsable de Internet para profesionales de servicios de protección a la infancia

is4k INTERNET SEGURA FORKiDS

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Observatorio Infancia

CÓMO CITAR ESTA GUÍA

Guía de uso seguro y responsable de Internet para profesionales de servicios de protección a la infancia. 2019. Observatorio de la Infancia e Instituto Nacional de Ciberseguridad (INCIBE).

LICENCIA DE CONTENIDOS

© Ministerio de Sanidad, Consumo y Bienestar Social
Secretaría General Técnica-Centro de Publicaciones
© Ministerio de Economía y Empresa
Instituto Nacional de Ciberseguridad (INCIBE)

NIPO papel: 731-19-070-3 (MSCBS)
102-19-114-9 (MEE)
NIPO en línea: 731-19-071-9 (MSCBS)
102-19-115-4 (MEE)
Depósito legal: M-30541-2019

Imprime: Solana e Hijos, Artes Gráficas, SAU
https://cpage.mpr.gob.es

0. Índice

1. Introducción

El contexto digital en el que se mueven las personas menores de edad en la actualidad incluye nuevos medios que es necesario conocer y comprender: las redes sociales, los dispositivos móviles e Internet. Para aquellos profesionales y educadores que participan en la vida de las personas menores de edad de un modo u otro, este aprendizaje ha adquirido gran importancia recientemente, al intervenir tanto en su trabajo diario, como en su relación con los propios niños, niñas y adolescentes (en adelante NNA). Las nuevas tecnologías, además de formar parte indiscutible de su vida, tienen unas características propias que las relacionan con determinados riesgos y problemáticas, que requieren unos procesos específicos de prevención y actuación.

Esta guía tiene por objeto dar soporte a los profesionales de servicios de protección a la infancia en la promoción del uso seguro y responsable de Internet por los menores de edad, mediante el asesoramiento en la prevención y actuación ante problemáticas reales y concretas, y la mejora en la adaptación de los principios básicos de ciberseguridad en las instituciones de protección de las personas menores de edad.

Conviene aclarar que las instituciones de protección reciben diferentes denominaciones en cada entidad o Comunidad Autónoma, y según su tipología, pueden establecer diferentes normativas respecto al uso que los NNA pueden hacer de los dispositivos tecnológicos e Internet.

A lo largo de esta guía, planteamos situaciones concretas en relación al uso que las personas menores de edad hacen de las Tecnologías de la Información y la Comunicación (TIC). Además, te proponemos actividades y dinámicas de los materiales didácticos de Internet Segura for Kids para poner en práctica los contenidos de cada bloque. Encontrarás consejos y recomendaciones para prevenirte ante los riesgos de Internet, y pautas para la gestión de la ciberseguridad como profesionales de servicios de protección a la infancia, incluyendo estrategias concretas de actuación en Centros de Acogimiento Residencial.

¿Quién hace esta guía y por qué?

Este recurso ha sido desarrollado por el centro Internet Segura for Kids (IS4K) del Instituto Nacional de Ciberseguridad (INCIBE) y el Observatorio de la Infancia, en el marco del Grupo de Trabajo del Observatorio de Infancia sobre «Elaboración de materiales de protección a la infancia en TICS para profesionales de servicios de protección a la infancia», con el objeto de facilitar los conocimientos y las herramientas necesarias para prevenir y reaccionar ante los problemas que surgen relacionados con la seguridad en Internet de la infancia y la adolescencia en los servicios de protección a la infancia.

El Grupo de Trabajo ha contado con la participación de:

MINISTERIO FISCAL

Juan Pedro Rodríguez del Val, Fiscal adscrito a la Fiscalía Coordinadora de Menores.

Luis Lafont Nicuesa, Fiscalía Coordinadora de Extranjería.

ADMINISTRACIÓN GENERAL DEL ESTADO

Daniel Moreno Gómez, Responsable del EMUME Central, Ministerio del Interior.

Salomé Corrochano de Castro, Coordinadora del Plan Director de la Unidad Central de Participación Ciudadana, Ministerio del Interior.

M. Elena Palacios Tejero, UFAM Central, Ministerio del Interior.

Verónica Casado Mateos, UFAM Central, Ministerio del Interior.

Eduardo Casas Herrero, Grupo I de Protección al Menor, Ministerio del Interior.

Pilar García Freire, INTEF, Ministerio de Educación y FP.

ADMINISTRACIÓN AUTONÓMICA

Lucas González, Junta de Extremadura.

Begoña Castellanos, Comunidad Autónoma de la Región de Murcia.

Teresa Gutiérrez Manjón, Xunta de Galicia.

Antonio José Molina Facio, Junta de Andalucía.

Gloria Villar Sáez, Comunidad Valenciana.

Cristina Blanco, Xunta de Galicia.

Elena Cubillo, Comunidad de Madrid.

Laura Lunar, Comunidad de Madrid.

OTROS PROFESIONALES

Mª Angustias Salmerón Ruiz, Pediatra del Hospital Universitario La Paz y el Hospital Ruber Internacional.

Jorge Flores Fernández, Pantallas Amigas.

Antonio Vargas, Google.

ONG

Ianire Molero Olmos, UNICEF.

Alejandra Pascual, FAPMI.

COORDINADORES DE LA GUÍA

Ana Belén Santos Pintor, Responsable de Área, INCIBE, Ministerio de Economía y Empresa.

Manuel Ransán Blanco, Coordinador en IS4K, INCIBE, Ministerio de Economía y Empresa.

Cristina Gutiérrez Borge, IS4K, INCIBE, Ministerio de Economía y Empresa.

José Luis Castellanos Delgado, Subdirector General de Infancia y Secretario del Observatorio de la Infancia, Ministerio de Sanidad, Consumo y Bienestar Social.

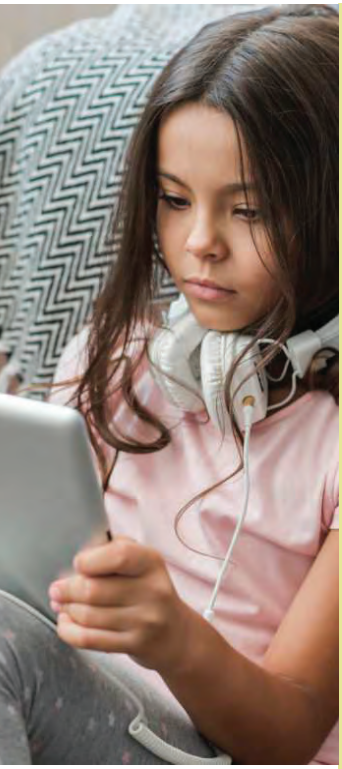
M. Asunción Pérez Uría, Jefa del Servicio del Observatorio de la Infancia y Cooperación, Subdirección General de Infancia, Ministerio de Sanidad, Consumo y Bienestar Social

1.1. El entorno en línea de las personas menores de edad

Para los padres y educadores, en ocasiones resulta complejo comprender por qué los NNA, en general, hacen un uso intensivo de Internet para divertirse y comunicarse con otras personas. A ellos no les suele parecer excesivo, no comparten las preocupaciones de muchos adultos a la hora de intentar controlar su uso, de limitar los tiempos o incluso prohibir algunos contenidos.

Al fin y al cabo ellos están creciendo viendo cómo las personas adultas de su entorno utilizan las nuevas tecnologías de manera cotidiana. Las personas menores de edad también se ven atraídas por el uso de la tecnología, y muchas veces son los adultos los que ponen en sus manos un móvil, una tableta o un ordenador sin reflexionar sobre las implicaciones y riesgos que traen consigo, sin poner normas ni límites, ni acompañarles para aprender a hacer un buen uso.

Pero debemos ser conscientes de que los NNA no saben por ellos mismos desenvolverse en el entorno digital al igual que no saben desenvolverse en la vida. Están aprendiendo a hacerlo. Lo que sí tienen por su curiosidad e impulsividad innata es una mayor capacidad para utilizarlos sin miedo al uso instrumental. Pero conviene resaltar que el uso instrumental de los dispositivos, servicios y aplicaciones digitales es extremadamente sencillo, están diseñados para que no sea necesario leer instrucciones y sean intuitivos. La supervisión, acompañamiento y comunicación para enseñarles cómo desenvolverse es labor del adulto, al igual que el establecimiento de normas de uso. Es decir, los NNA no saben usar las TIC de manera segura y responsable, aunque se desenvuelvan y hagan un uso instrumental perfecto de los dispositivos.



¿Por qué se conectan?

Para la infancia y la adolescencia, la Red es un entorno tan natural como cualquier otro, que complementa o mejora la variedad de espacios en los que pueden comunicarse o divertirse. Relacionarse con otras personas de su edad es uno de los objetivos principales, que en la actualidad puede combinarse con cualquier otra actividad. Por ejemplo, pueden ver un vídeo a través de Internet o competir en un juego en línea, y luego compartir su opinión o su experiencia en las redes sociales. De ese modo, conocerán otras personas que han visto el mismo contenido o que conocen el juego, con las que podrán interactuar. Estos espacios públicos les permiten relacionarse entre sus iguales teniendo cierta sensación de privacidad y autonomía, sin la supervisión de los adultos.

La Red es un entorno en el que encuentran también otras motivaciones, como una amplia oferta de ocio multimedia en continua evolución, información sobre cualquier temática que les interese o espacios de aprendizaje no formales, como blogs o canales de vídeo sobre música, deporte, aficiones, etc. La variedad de servicios que les ofrece Internet crece cada día, convirtiéndose en un medio atractivo y cotidiano para ellos.

La Red les ofrece unas características que les resultan más atractivas para determinadas actividades. Por una parte, tiene mucho que ver con la desinhibición que les ofrece Internet, sienten que en la Red pueden ser quienes quieran ser. Los menores de edad son más atrevidos en este entorno, movidos también por la impulsividad que les caracteriza, que se acentúa al tener un acceso continuo a través de su propio móvil, tableta u ordenador. Además, cada vez tienen menos obstáculos para conectarse a Internet, y se facilita su uso en todos los entornos sociales. Esto favorece las comunicaciones instantáneas, pudiendo localizar a cualquier persona al momento, y que la respuesta sea inmediata.

1.2. Los riesgos asociados a Internet para la infancia y la adolescencia

Estas características de Internet y de la tecnología actual ofrecen infinitas oportunidades en cuanto al acceso a información, contenidos y vías de comunicación. Pero a su vez, suponen un medio en el que surgen nuevos riesgos, que NNA y profesionales deben conocer. También es un entorno en el que los riesgos y conflictos tradicionales pueden volverse más complejos, de nuevo como consecuencia de dichas particularidades propias de la Red.

La presión social propia de esta etapa de desarrollo puede unirse a otras circunstancias que facilitan el contacto con las posibles amenazas de Internet, siendo más vulnerables aquellas personas menores de edad que se encuentren en situación de riesgo social. Una baja autoestima, un incorrecto desarrollo de las habilidades sociales o un entorno social inapropiado, pueden acentuar las posibilidades de caer en estos riesgos asociados al uso de la tecnología.

Para un NNA, las consecuencias de sus actos en Internet les pueden afectar de forma grave, tanto en su infancia y adolescencia, como en el futuro. El acompañamiento para adecuar el uso de la tecnología a su etapa de desarrollo, así como la sensibilización y formación son la clave para garantizar una prevención efectiva y una respuesta positiva ante los conflictos. Los adultos de referencia para la persona menor de edad, como un educador de confianza con el que pueda compartir sus preocupaciones, siempre serán el primer paso para gestionar los problemas y resolverlos de forma positiva.

Para ampliar la información

Portal de IS4K
(https://www.is4k.es)

2. Gestión de la información

Una de las principales utilidades de Internet es la búsqueda de información y contenidos. En este entorno las posibilidades son casi infinitas, y los NNA son muy conscientes de ello. Eso sí, como en cualquier otro contexto, las personas menores de edad deben aprender a gestionar toda esa información de forma adecuada y responsable, desconfiando de noticias falsas o contenidos poco rigurosos. Así, aprenderán a reconocer fuentes fiables de confianza para encontrar o contrastar la información.

2.1. ¿Qué es la alfabetización mediática e informacional?

> En la actualidad no hay duda de la importancia de la información en nuestra vida diaria. Por eso, es indispensable desarrollar habilidades para gestionarla adecuadamente, es decir, reconocer cuándo se necesita una información, cómo localizarla, evaluar su relevancia y fiabilidad, así como ser capaces de utilizarla efectivamente[1].

Además, ante la variedad de medios de comunicación disponibles, es necesario conocerlos para poder comprender adecuadamente la información que transmiten. Esto es lo que se conoce como alfabetización mediática e informacional.

Esta propuesta de alfabetización engloba a todos los medios de comunicación, tanto tradicionales como pueden ser bibliotecas o archivos, como medios tecnológicos (Google, YouTube, WhatsApp, etc.), y su objetivo es que todas las personas aprendan a buscar y gestionar la información que necesitan de forma adecuada. Para los NNA, los medios digitales siempre han estado accesibles, estableciéndose como un entorno de búsqueda de información y contenidos desde la primera infancia.

[1] "Presidential Committee on Information Literacy: Final Report". American Library Association (1989). Disponible en: http://www.ala.org/acrl/publications/whitepapers/presidential

Entran en contacto con una gran cantidad de información por estas vías, prioritariamente en redes sociales y mensajería instantánea, y tienen que aprender a diferenciar aquella que es válida y saludable, de los contenidos malintencionados, falsos o engañosos. Fomentando la alfabetización mediática e informacional, estaremos impulsando sociedades más capacitadas, formadas e independientes.

A pesar de que esta alfabetización es imprescindible, no es innata, esto requiere que sean los adultos los que les transmitan esas competencias: cómo identificar fuentes de información fiables, analizar los resultados que obtienen de sus búsquedas y desarrollar el pensamiento crítico necesario para administrar esa información.

2.2. Acceso a contenidos inapropiados o perjudiciales

Una persona menor de edad puede encontrar en la Red multitud de contenidos positivos y saludables, pero en ocasiones, también caerán en sus manos otros que resultan inadecuados teniendo en cuenta su madurez y su nivel de comprensión, o incluso peligrosos para su desarrollo.

Estos contenidos pueden aparecer en páginas web, videojuegos o vídeos, y también en entornos aparentemente más inofensivos, como redes sociales, buscadores de información o en la publicidad, o incluso se los pueden enviar directamente otras personas menores de edad de su grupo u otras personas a través de mensajería instantánea o redes sociales. No siempre son contenidos exclusivamente dirigidos a un público adulto, cualquier espacio en línea puede contener información accesible para una persona menor de edad, sea o no apropiada para él.

> Aquellos espacios de Internet limitados a personas menores de 18 años, a menudo incluyen únicamente una mera advertencia sobre la restricción, pudiendo acceder al contenido con un simple clic.

De este modo, un NNA puede acceder por ejemplo a contenidos de pornografía, pero también a otras temáticas sobre hábitos poco saludables, como pueden ser las dietas milagro o el consumo de drogas. Igualmente es posible encontrar vídeos o imágenes que fomenten la violencia, el discurso de odio, ideologías extremistas o incluso la autolesión. Estos pueden influir decisivamente en edades tempranas y en la adolescencia.

En general, todas las personas en la actualidad están afectadas por una sobrecarga informativa, debida a la inmensa cantidad de información que reciben por múltiples medios. A la infancia y la adolescencia, esto les afecta principalmente a la hora de tomar decisiones. Con un pensamiento crítico aún en desarrollo, les supone un obstáculo para diferenciar entre aquellos contenidos que son valiosos y positivos, de aquellos que son prescindibles o incluso nocivos para ellos.

Además, en Internet abundan aquellos contenidos que consideramos falsos o faltos de rigor, como noticias falsas, retos virales y leyendas urbanas, que para las personas menores de edad pueden resultar especialmente atractivos pero fácilmente engañosos, y que con frecuencia promueven actitudes y conductas peligrosas. Si desconocen cómo identificar una información verídica y fiable, su reacción ante estos contenidos tan llamativos e incluso sensacionalistas suele ser compartirlos con otros NNA, colaborando en su difusión.

Burbuja de filtros y cámaras de eco

El término burbuja de filtros se asocia al modo en que los algoritmos de muchas plataformas de Internet (buscadores, redes sociales) seleccionan el contenido que presentan al usuario, priorizando aquellos contenidos que consideran mejor encajan con sus intereses (por ejemplo, a partir del historial de navegación o la interacción con sus contactos).

Este filtrado automático puede resultar útil en ciertos momentos, aunque también implica que se ocultarán otros contenidos que en un principio le interesan menos al usuario, a pesar de que puedan ser relevantes para él. Por ejemplo, si es habitual que lea noticias con determinado sesgo, es probable que los algoritmos le presenten publicaciones que respalden sus opiniones y perspectivas para garantizar que disfrute con lo que está viendo.

Las burbujas de filtros pueden derivar en cámaras de eco. De forma que el usuario asuma que su visión es la mayoritaria y olvide que hay otras perspectivas. Objetivamente, una visión más completa e informada incluye diferentes puntos de vista que aportan más conocimiento y facilitan una mejor toma de decisiones.

La exposición a toda esta información tiene repercusiones en las personas menores de edad, que dependiendo de la tipología del contenido, van desde la desinformación o la manipulación, a daños a nivel psicológico, emocional o físico. Además, el acceso a determinados contenidos puede llegar a poner en contacto al NNA con desconocidos malintencionados, grupos violentos o extremistas, así como con sectas de carácter ideológico.

Para un NNA en situación de riesgo, es posible que su vulnerabilidad se vea incrementada con respecto a la de cualquier persona menor de edad con niveles de autoestima más bajos y un entorno social menos favorable en el que apoyarse. Las posibilidades de sufrir consecuencias asociadas de estos contenidos inapropiados es mayor, y la prevención es clave para evitarlo.

2.3. Recomendaciones para una apropiada gestión de la información

La prevención siempre debe ir por delante, y al hablar de contenidos, en la Red van a poder encontrarse con todo tipo de imágenes, vídeos o textos, que en algunos casos pueden no ser adecuados para su edad y madurez, que no entenderán o que les perturbarán. En definitiva, anticiparse a lo que van a ver en Internet. Para ello, las siguientes recomendaciones motivarán el desarrollo de habilidades útiles para hacer frente a este tipo de contenidos.

Fomentar el pensamiento crítico

Para enfrentarse al entorno digital con seguridad y de forma autónoma es necesario desarrollar su capacidad de crítica, ya que no estaremos siempre a su lado cuando se conecten a Internet. Así, la persona menor de edad podrá discernir entre los diferentes contenidos a su alcance e identificar cuáles son apropiados, cuándo una información es falsa o parece engañosa, o cuando se está intentando manipular sus ideas o valores.

El pensamiento crítico se enriquecerá gradualmente con cada nueva experiencia a la que se enfrente dentro o fuera de la Red, pero debe existir una base de entendimiento que le permita contrastar la información que encuentra, reconocer fuentes fiables y asumir en qué momento debe solicitar el apoyo de un adulto. Para ello es útil:

- Estar a su lado cuando se conecte a Internet, para poder reflexionar juntos acerca de los contenidos que aparezcan y que puedan considerarse potencialmente negativos. Por ejemplo, publicidad sobre dietas milagro o páginas de contenido sexual.
- Preguntar acerca de la clase de contenidos que visualiza a través de Internet, sin culpabilizar nunca al NNA. Tener curiosidad es normal y saludable, además muchas veces estos contenidos llegan a sus manos de forma no intencionada, como por ejemplo a través de los anuncios o las redes sociales.
- Ajustar el lenguaje a su madurez, explicarle la veracidad de esos contenidos, la motivación que hay detrás y por qué no son fiables o no es aconsejable que acceda a ellos.

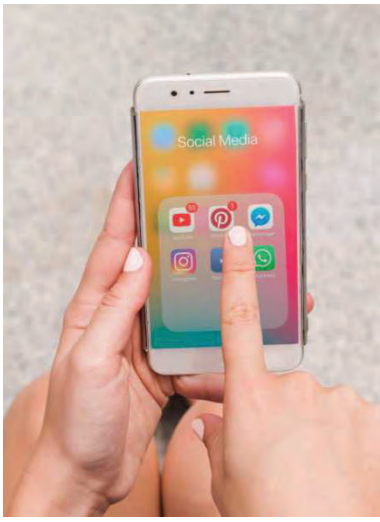
- Conversar con naturalidad sobre estos temas y fomentar la capacidad de crítica a la hora de analizar la información, su fiabilidad y la reputación de quien la emite. Por ejemplo, mientras ven un programa de televisión en el que utilizan un lenguaje agresivo, jugando a un videojuego que contiene escenas de violencia explícita o comentarios despectivos o extremistas.
- Elegir juntos contenidos educativos o de entretenimiento de calidad, que transmitan mensajes positivos y adaptados a la edad y la madurez del NNA.
- Compartir solo contenido positivo, útil, de calidad en la Red. En caso contrario, al difundir se contribuye a la desinformación o se genera alarma social.
- Ser su ejemplo a seguir, intentando utilizar también contenidos de calidad, evitando promover contenidos no adecuados, noticias falsas o bulos. Dar valor a los contenidos originales y su protección, como fuente de valor y promotora de una mejor Internet.

Conocer los mecanismos de denuncia

Como adultos, implicarse y denunciar los contenidos inadecuados o potencialmente peligrosos que se encuentran en la Red es fundamental para lograr un entorno más seguro.

> Cualquier contenido que sea engañoso, fraudulento o inadecuado se puede reportar y solicitar su eliminación.

Aun así, hay que ser conscientes de que la plataforma solamente tiene la obligación de aceptar esta solicitud si incumple la legislación vigente, su propia normativa o las políticas de uso. Cada servicio de Internet determina diferentes limitaciones para los contenidos, que establecen qué consideran inapropiado y qué no. Al tratarse de NNA, puede que algunos contenidos sean inadecuados para su edad, pero no para el público al que va destinado el contenido originariamente.

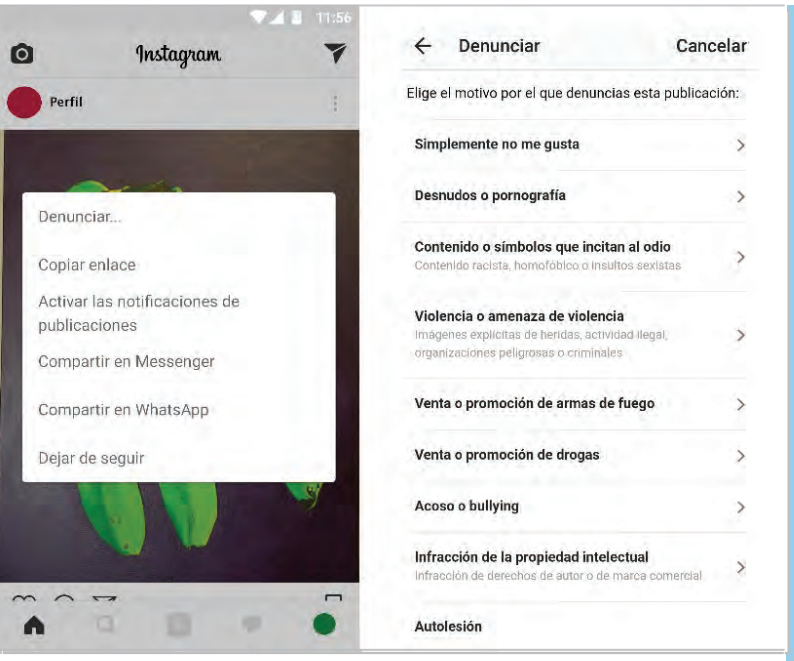


Por ejemplo, si se permite que una persona menor de edad utilice un juego online que está catalogado como violento y dirigido a mayores de 18 años, no parece razonable solicitar que eliminen algunos contenidos que parezcan excesivamente violentos para un niño. En consecuencia, es recomendable:

- Transmitir este hábito a los NNA, dado que son ellos los que más contenidos van a localizar, y muchas veces no tendrán la confianza necesaria para

compartirlos con un adulto. Deben ser capaces de denunciar y bloquear esta información de forma autónoma.

- Animar a las personas menores de edad a mostrar confianza a la hora de admitir que un contenido no les gusta o les perturba, sin dejarse llevar por la presión social o las modas.
- Valorar las denuncias de otros NNA, como conductas positivas, maduras y responsables, con las que mejora el entorno online y se evita que otros NNA encuentren contenidos inadecuados.



Cómo denunciar

Si se trata de una foto, vídeo o comentario inapropiado en una red social, normalmente dispondremos de algún botón u opción de menú (...) junto al contenido, donde tenemos la posibilidad de reportar o denunciar. A continuación, deberemos escoger entre los diferentes motivos de reporte.

Si se trata de un comentario en un videojuego, foro o cualquier otro servicio sin esta opción, podemos consultar la sección de ayuda o el centro de seguridad de la propia aplicación o página web, o contactar con el administrador para solicitar la revisión del mensaje o contenido.

Para gestores de centros: sistemas de filtrado de contenidos

Si disponemos de algún equipo para uso por parte de los NNA, es recomendable plantearse un sistema de filtrado para limitar su acceso a contenidos inapropiados para ellos. Existen diferentes alternativas al respecto, como puede ser implantar un filtrado de red, que actúe sobre todos los dispositivos conectados, o utilizar herramientas de control parental (que habitualmente incluyen opciones de filtrado) instaladas en cada equipo.

Además, se pueden utilizar aplicaciones específicas con un filtrado previo de la información, como *YouTube Kids*, buscadores infantiles, activar opciones de búsqueda segura como *SafeSearch* de Google, o las opciones de seguridad que ofrecen algunas plataformas o videoconsolas.

Estos sistemas ofrecen una limitación en cuanto a los contenidos a los que el NNA va a poder acceder, y son útiles siempre que se adapten a su edad, y vayan evolucionando a medida que crece. Aun así, hay que ser conscientes de que es posible que no se filtre correctamente la totalidad de los contenidos inapropiados, o que los NNA encuentren alguna forma de saltarse el sistema, por lo que deben utilizarse como complemento junto a otras pautas de prevención educativas. Paralelamente, también es fundamental supervisar de forma periódica los sitios web a los que acceden, conversando con los NNA, revisando el historial o con la ayuda de una herramienta de control parental.

2.4. Cómo actuar si... detectamos una tendencia o comportamiento potencialmente peligroso entre las personas menores de edad, derivado de un vídeo viral de Internet

Muchos de los contenidos que comparten las personas menores de edad entre sí son virales, es decir, contenidos elaborados por otras personas que se han difundido rápidamente mediante mensajería instantánea y redes sociales. Pueden ser vídeos, mensajes o imágenes que pretenden ser graciosos o impactantes. Es habitual que incluyan un reto que el receptor del contenido debe llevar a cabo, grabarlo y difundirlo.

Estos retos en ocasiones son inofensivos, pero a menudo suponen cierto riesgo, que es precisamente lo que les aporta cierta dificultad como reto, y una característica por la que las personas menores de edad se sienten atraídas en particular:

- Determinemos qué clase de contenido es, cómo se está difundiendo y en manos de cuántos NNA está para establecer el alcance del problema.
- Si son pocas las personas menores de edad afectadas, podemos mantener una charla en privado para explicarles por qué consideramos que es un contenido negativo y que las consecuencias pueden ser peligrosas. Evitaremos comentar el tema de forma genérica entre todos los NNA del centro, para evitar generar más curiosidad entre aquellos que aún no lo han visto.
- Si la mayoría de los NNA han visualizado el contenido, puede ser más práctico realizar una actividad en grupo, en la que tratemos el contenido del vídeo, desmitifiquemos el reto y expliquemos que el objetivo de este tipo de vídeos virales puede estar incluso relacionado con estafas, fraudes y virus informáticos.
- Les pediremos que eliminen ese contenido de forma permanente de sus dispositivos, haciéndoles ver la irresponsabilidad de difundir ese contenido entre otros NNA.

- Dado que es habitual que reciban este tipo de contenidos en el futuro, trabajar cotidianamente el pensamiento crítico les permitirá ignorarlos y razonar el peligro de difundirlos.
- Si la situación es grave puedes contactar con un servicio de ayuda especializado, como la **Línea de Ayuda en ciberseguridad de INCIBE (900 116 117)**.

Para trabajar con las personas menores de edad

Con la sesión 5.1 «Esto es un *fake*» de la Unidad 5, podemos trabajar pautas que les ayuden a contrastar la información que buscan o les envían por Internet, para determinar su veracidad e identificar posibles contenidos falsos.

Con la sesión 6.1 «¿Y tú qué ves en Internet?» trasladamos a los más pequeños las primeras pautas para visualizar contenidos en línea apropiados y positivos.

Cada sesión de trabajo de 50 minutos incluye notas para los docentes y plantillas para realizar la actividad.

Catálogo de Unidades Didácticas de IS4K

https://www.is4k.es/unidades-didacticas-20

Para ampliar la información

Sección «Necesitas saber: Contenido inapropiado» en la web de IS4K (https://www.is4k.es/necesitas-saber/contenido-inapropiado)

Artículo «*Fake news*: ayúdales a protegerse de las mentiras que circulan por Internet» del blog de IS4K (https://www.is4k.es/blog/fake-news-ayudales-protegerse-de-las-mentiras-que-circulan-por-internet)

Sección «Materiales didácticos» en la web de IS4K (https://www.is4k.es/de-utilidad/recursos/materiales-didacticos)

3. Seguridad de los dispositivos

Las personas menores de edad utilizan Internet de forma cotidiana y natural. En ocasiones, se conectarán con sus propios dispositivos como móviles o tabletas, pero también pueden utilizar equipos de uso compartido como los ordenadores del centro educativo o el móvil de un amigo/a. En cualquier caso, la seguridad en línea de la infancia y la adolescencia depende de su actitud y del nivel de protección y seguridad de los dispositivos que utilizan.

3.1. ¿Por qué proteger los dispositivos?

Al hablar de riesgos en Internet es sencillo mencionar temáticas de gran repercusión social y que conllevan graves consecuencias como el ciberacoso o el acoso sexual por parte de un adulto, entre otras. En la prevención de estos problemas resultan fundamentales las actitudes y comportamiento de los NNA, pero también se han de considerar las cuestiones relacionadas con la configuración de sus móviles, tabletas y ordenadores.

Por ejemplo se pueden dar situaciones como perder el móvil, o dejarse abierta la sesión de una red social en un equipo compartido, con lo que la persona que se lo encuentre podría acceder a sus fotos, contactos y el resto de información privada. Esto supone no solo una **pérdida de confidencialidad**, sino que también se podría utilizar esa información en su contra para **dañar su reputación**, hacer un chantaje, promover una campaña de ciberacoso... O incluso hacerse pasar por ellos para hacer daño a otras personas.

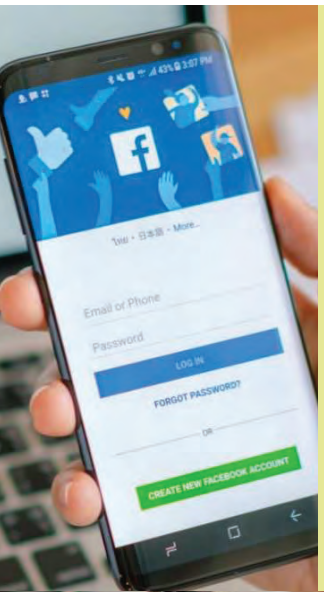
Si además ese dispositivo es el único en el que tienen guardada información importante, y lo extravían, se estropea o un *malware* (concepto más general que el de virus informático) lo secuestra, irremediablemente **perderían esa información**.

Se puede encontrar malware y virus informáticos en cualquier plataforma, también en los móviles.

En cualquier sistema o plataforma se pueden encontrar virus informáticos, ordenadores Windows, Linux y MacOS, tabletas y móviles Android e iOS, etc. Infectarse puede ser tan sencillo como hacer clic en un enlace para ver un supuesto vídeo impactante en una red social, o descargarse desde fuentes no oficiales una aplicación o el último videojuego popular para evitar pagar por él.

Con el mismo ejemplo, también se podría dar una **pérdida económica** (más allá del valor del propio dispositivo), por ejemplo si alguien utilizara sus datos para suscribir servicios de tarificación adicional, realizar compras dentro de una aplicación (como los *packs* de mejoras en un videojuego), etc.

En otras ocasiones los **problemas no son accidentales**, sino que alguien los provoca con intención de aprovecharse de los menores de edad: hacerse con datos bancarios, información personal para venderla en línea o chantajearles; o utilizar sus dispositivos para extender el ataque a más personas.



Las **técnicas de ingeniería social** son trucos o estrategias que tratan de engañar al usuario en Internet, en este caso a las personas menores de edad.

Para ello se simula ser una página web o un correo electrónico fiable (por ejemplo con el aspecto de su red social preferida), o bien se emplean mensajes atractivos que llaman su atención y curiosidad (por ejemplo "descubre quién ha visto tu perfil", "has ganado un premio").

Al hacer clic en los enlaces que indican o abrir los archivos adjuntos el dispositivo puede infectarse con un *malware* o virus, o bien ellos mismos pueden introducir sus datos personales y contraseñas, creyendo que la página o el mensaje era de confianza.

Para enfrentarse a estos riesgos es necesario tener un adecuado nivel de protección de los dispositivos y de la información que contienen, así como mantener una actitud crítica hacia los mensajes que les llegan.

3.2. Medidas de protección

A continuación se presentan algunas de las pautas preventivas básicas para proteger los dispositivos, su información y, en consecuencia, a las personas que los utilizan, que se pueden transmitir a los NNA:

- **Animarles a utilizar una buena contraseña**: crearlas combinando letras, números, símbolos, evitando patrones repetitivos y tratando que no sean fáciles de deducir por cualquiera que les conozca. Es fundamental que no las compartan con nadie, ni siquiera con su pareja o sus amistades más cercanas.
- **Proteger el acceso al dispositivo**: para ello se puede fijar una contraseña o un código PIN para el desbloqueo de la pantalla, un patrón de desbloqueo, o un método biométrico como los lectores de huella dactilar o reconocimiento facial.
- **El antivirus es un básico**: estas herramientas protegerán en gran medida a sus dispositivos, tanto ordenadores, tabletas o móviles, contra virus y malware. Suelen incluir otras funcionalidades útiles como el análisis de aplicaciones para reconocer su fiabilidad o la revisión de los contenidos almacenados.
- **Actualizaciones al día**: el sistema y las diversas aplicaciones instaladas en el dispositivo necesitan mantenerse actualizadas para que sus funciones de seguridad funcionen correctamente y se adapten a los cambios que continuamente se suceden en este ámbito.

Los menores de edad acostumbran a tener sus móviles repletos de aplicaciones, relacionadas con juegos, redes sociales y otras utilidades. A pesar de realizar un intenso uso instrumental de estas herramientas, no siempre lo hacen de la forma más adecuada. En ocasiones desconocen aspectos básicos para descargarlas con seguridad, cuando algunas aplicaciones pueden ser fraudulentas, utilizar sus datos personales de forma inadecuada o incluso infectar su dispositivo.

Por ello, antes de instalar una nueva aplicación, deben determinar que esta es auténtica, fiable y que los permisos que les solicitan para su utilización son coherentes:

- Procede de la tienda oficial.
- Informa de su propósito, política de privacidad, términos de uso, y contacto del desarrollador original.
- Tiene buenas valoraciones y un número significativo de descargas y comentarios.
- Solo pide permisos correspondientes a sus funcionalidades.

- **Configuraciones seguras**: los principales servicios o plataformas online que utilizan los menores de edad al conectarse disponen de múltiples opciones de seguridad que a menudo se desconocen, pero que en realidad son útiles y necesarias. Muchos servicios como Google por ejemplo, ofrecen la opción de verificación en dos pasos, con la que para acceder a la cuenta es necesario introducir la propia contraseña junto con un segundo código que envían a su móvil, o la búsqueda y bloqueo de un dispositivo si se extravía.

  Las redes sociales, como Instagram, YouTube o Facebook, permiten administrar los ajustes de configuración para aumentar la seguridad del usuario, aspecto indispensable tratándose de personas menores de edad. Por ejemplo, filtrar quién puede contactar directamente con su perfil, o cifrar los contenidos que se envían por mensajería, como ocurre en WhatsApp. Es importante hacerles conscientes de que su uso no empeorará su experiencia, los servicios seguirán siéndoles útiles y divertidos, pero estarán más protegidos.

- En cuanto a sus **hábitos de conexión**, es habitual que utilicen redes wifi públicas, pero deben entender que su uso requiere cierta precaución, principalmente evitar compartir información privada o íntima en este tipo de redes. Además, si van a navegar por Internet, es preferible indicar *https://*

antes de la dirección de la página web (en lugar de *http://*) para que la información intercambiada no sea visible para nadie más.

Si se conectan en algún equipo compartido, también han de cerrar la sesión antes de terminar, e impedir que el navegador recuerde sus usuarios y contraseñas para que nadie más pueda acceder a sus cuentas.

Para gestores de centros: Plan Director de Seguridad

Tanto las instituciones de protección a la infancia en general, como los Centros de Acogimiento Residencial de menores de edad en particular, presentan características comunes a cualquier otra organización. Disponen de personal y proveedores, manejan datos de sus usuarios, utilizan sistemas de gestión, se comunican con administraciones, etc. y para ello emplean medios informáticos e Internet.

Este hecho permite que se vean **expuestas a una serie de riesgos de ciberseguridad**, que en algunos casos podrían llegar a resultar críticos para su propia continuidad, o perjudicar gravemente a los menores de edad atendidos.

Por ejemplo, la difusión incontrolada de datos sensibles sobre un NNA o su familia, puede acarrear graves daños para su reputación en línea, con consecuencias indeseadas en su integración social y laboral, además de las lógicas responsabilidades a nivel legal.

Así pues, es recomendable avanzar hacia el desarrollo de un Plan Director de Seguridad, donde se analice la realidad del centro, se identifiquen posibles riesgos, la probabilidad de que ocurran y los efectos que podrían tener, para a continuación plantear posibles proyectos que **mejoren la prevención** de riesgos o permitan reaccionar y ser capaces de **recuperarse de un incidente**.

Este documento no ha de verse como un requisito burocrático, ni como un esfuerzo puntual en la organización, sino que la ha de acompañar en su evolución, contribuyendo a una mejora continua en su nivel de seguridad.

Para gestores de centros: Equipos destinados al uso por parte de los menores de edad

Si la institución posee equipos de uso compartido con conexión a Internet, ya sean ordenadores, tabletas o móviles, se debe dedicar tiempo a su correcta configuración, para que los menores de edad puedan utilizarlos con seguridad:

- **Planificar el espacio** donde se ubiquen los dispositivos, de manera que los educadores puedan controlar su utilización y estar al tanto de los tiempos de conexión, las páginas y plataformas a las que acceden.
  Si están colocados en un lugar transitado y público, es menos probable que hagan un uso inapropiado deliberadamente.
- Mantener bajo llave el acceso, tanto a los dispositivos como al router wifi, así como proteger su configuración con **contraseñas** robustas.
- Mantener el **equipo actualizado y** protegido **con un antivirus** es esencial para que las personas menores de edad puedan usarlo con seguridad.
- Establecer una cuenta de **usuario limitado** para los NNA (más acotada en cuanto a permisos, por ejemplo para instalar nuevas aplicaciones), reservando la cuenta de administrador para los educadores.
- Mantener las **cámaras tapadas** y solo permitir su utilización bajo la supervisión de un educador.
- Establecer unas **normas de uso** de estos espacios comunes y ser disciplinados en su cumplimiento.

  Es positivo que estén impresas y colocadas cerca del dispositivo, para que los NNA puedan verlas cada vez que se conecten.

  Incluso en ese mismo documento se puede recordar quién es el **adulto responsable en caso de duda o incidente**, de forma que sea accesible y genere confianza en el menor de edad.

3.3. Cómo actuar si... ha sido víctima de un fraude o virus

Cuando los NNA utilizan Internet sin precaución o seguridad, es posible que su dispositivo (ya sea un móvil, un ordenador o una tableta) pueda verse afectado por un virus y acabe siendo víctima de un fraude. Por ello, es fundamental seguir estos pasos:

- Analiza el dispositivo con un antivirus, e incluso haz un segundo análisis con un antivirus en línea como los disponibles en **www.osi.es**. Estas herramientas localizan y eliminan la mayoría de los virus siempre que estén actualizadas.

- Complementariamente, prueba a utilizar otras opciones como las herramientas de limpieza de temporales y cookies, así como las opciones para restaurar el sistema de tu dispositivo a un estado anterior haciendo uso de los puntos de restauración.
- Antes de cualquier restauración es recomendable hacer una copia de sus archivos, fotos, y otros contenidos para evitar pérdidas.
- Ayúdale a contactar con el servicio o empresa implicada, para reportar a través de las secciones de ayuda o los canales de contacto la situación de fraude.
- Apóyate en servicios especializados sobre un uso seguro en Internet, como la **Línea de Ayuda en ciberseguridad que ofrece INCIBE (900 116 117)**, para recibir orientación sobre cómo reparar la situación y reportar el fraude.
- Acude a la Oficina Municipal de Información al Consumidor, para tramitar una reclamación relativa al fraude en la compra a través de Internet. Localiza la OMIC más cercana a través de la página web del Centro de Información y Documentación de Consumo (CIDOC).
- Si, como consecuencia de la infección, se reciben intentos de chantaje en base a contenidos privados del NNA robados de su dispositivo, la primera premisa es: nunca se debe ceder ante un chantaje, menos aun cuando hay implicada una persona menor de edad.
- Si el problema persiste o se considera de gravedad se recomienda denunciarlo a los cuerpos policiales.

3.4. Cómo actuar si... ha perdido o le han robado el móvil

Se trata de una situación relativamente frecuente. Es muy sencillo dejarse el móvil olvidado encima de una mesa o en clase, y puede que otra persona sienta curiosidad por cotillear su contenido o quiera aprovecharse del dispositivo.

A la hora de reaccionar nuestro objetivo será doble, por un lado recuperar el móvil y por otro limitar o reducir los posibles daños causados al menor de edad.

- Lo primero es determinar si se trata de una pérdida o un robo, en qué momento aproximado ha sucedido, si ha sido dentro o fuera del centro, y en ese caso si hay implicado algún NNA del mismo centro.
- Si el móvil tenía configurada una opción "antirrobo", podemos consultar la web del fabricante para comprobar si disponemos de funcionalidades de búsqueda como «Encuentra mi dispositivo» en Android y «Busca mi iPhone» en iOS de Apple.
- Los servicios de búsqueda del dispositivo también permiten bloquear el terminal y borrar la información que contiene de forma remota, salvo la almacenada en la tarjeta SD.
- De la misma manera, se puede solicitar a la compañía de telefonía móvil el bloqueo de la tarjeta SIM y del móvil mediante su código IMEI para evitar que se puedan volver a utilizar. Se puede consultar el IMEI a través del menú "Ajustes" del dispositivo, marcando el código *#06# en el dispositivo o en el área web de clientes de la operadora.
- Si crees que el teléfono puede estar cerca, activa «reproducir sonido». Esta opción hará sonar el dispositivo a todo volumen durante 5 minutos para facilitar su localización (aunque esté en silencio o en vibración).
- Si a pesar de todo sigue sin aparecer, puede solicitarse ayuda al agente tutor del cuerpo policial correspondiente a esa zona.
- Si hay NNA del centro implicado, puede ser útil comentarlo en privado con ellos, o bien en el conjunto del grupo para reforzar la responsabilidad personal e invitar a devolverlo.
- Tratar de averiguar si alguien ha estado utilizando el teléfono, o su información (por ejemplo, si ha compartido algún mensaje en las redes sociales del propietario).
- En el caso de detectar actividad desde las cuentas de redes sociales, mensajería instantánea, correo electrónico del NNA, etc. se puede tratar de

entrar en las cuentas desde otro dispositivo para cambiar la configuración de "dispositivos vinculados", denegándole el acceso desde ese móvil (en aquellas redes sociales y servicios de mensajería que lo permiten). Además, sería interesante cambiar las contraseñas en estos servicios.

- Asimismo, puede ser útil avisar por otras vías a los contactos de la persona menor de edad para que sepan que alguien está suplantando su identidad y actuar en consecuencia.
- Los mensajes inapropiados se pueden denunciar/reportar a la plataforma correspondiente, indicando un uso fraudulento de la cuenta.
- Por último, es importante recordar que no estamos solos: siempre se puede acudir a un servicio especializado como la **Línea de Ayuda en ciberseguridad que ofrece INCIBE (900 116 117)**, desde la que nos pueden ayudar a denunciar ante Fuerzas y Cuerpos de Seguridad si consideramos que la situación está fuera de control.

Por último, comentar que después de gestionar una situación de este tipo, puede ser un buen momento para trabajar en grupo la manera de configurar adecuadamente sus dispositivos y de las aplicaciones que utilizan (por ejemplo protegiendo la pantalla de desbloqueo, configurando las opciones antirrobo, etc.).

Para trabajar con las personas menores de edad

La Unidad Didáctica 3 «Controla la Tecnología» está formada por:

La sesión 3.1 «Cierra con llave»: además de crear contraseñas seguras y fáciles, se asocian riesgos con herramientas y hábitos de seguridad.

La sesión 3.2 «¿Qué apps merecen la pena?» se incluye una dinámica debate para la reflexión crítica sobre las apps antes de instalarlas.

Cada sesión de trabajo de 50 minutos incluye notas para los docentes y plantillas para realizar la actividad.

Catálogo de Unidades Didácticas de IS4K

https://www.is4k.es/unidades-didacticas-20

Para ampliar la información

Serie de artículos «Coordinador TIC» del blog de IS4K (https://www.is4k.es/blog/oh-no-me-toca-ser-el-coordinador-tic-por-donde-empiezo-i)

Sección «Materiales didácticos» en la web de IS4K (https://www.is4k.es/de-utilidad/recursos/materiales-didacticos)

Portal de la Oficina de Seguridad del Internauta (www.osi.es)

Web de Protege tu empresa: Plan Director de Seguridad (https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad)

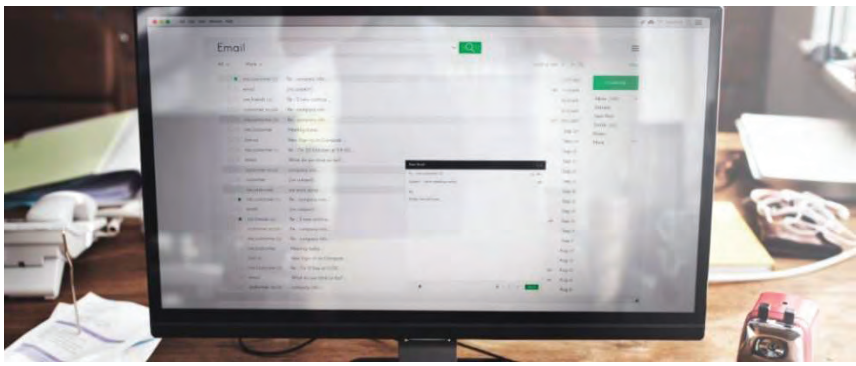
4. Protección de datos personales e identidad digital

Los datos personales que circulan por la red pueden ser utilizados con distintos fines, por lo que si no se gestionan adecuadamente pueden acarrear consecuencias no deseadas. Inevitablemente, hoy en día cualquier persona con independencia de su edad tiene cierta exposición en Internet. Esto se debe tanto a la información que se comparte, como la que aportan otras personas o incluso los datos que se recogen automáticamente en la red.

Así pues, como educadores se ha de ser consciente de la exposición personal en Internet para poder ayudar a los NNA a conocer esta realidad y gestionarla responsablemente.

4.1. ¿Qué son los datos personales y por qué interesa protegerlos?

Cualquier información concerniente a una persona, que permita identificarla o individualizarla fácilmente dentro de un colectivo, se considera un dato personal:



- Datos que identifican: nombre, fotografía, DNI, edad, etc.
- Datos que permiten tener contacto con su titular: correo electrónico, teléfono o dirección.
- Datos relativos a las características o actividades personales: fecha de nacimiento, características físicas o antropométricas, creencias, estado de salud, desempeño académico, etc.

Por ejemplo, el nombre y apellidos del menor de edad, de sus familiares, su dirección o su número de teléfono son datos de carácter personal. También son datos personales las imágenes en las que aparezca, o la profesión, los estudios o el lugar donde trabajan los padres.

Algunos datos personales son especialmente sensibles, por revelar circunstancias o información más íntima y personal, y requieren de una especial atención y protección: la religión, las creencias, el origen racial o étnico, la salud o la vida sexual, o los que se refieren a la comisión de infracciones penales o administrativas.

Los menores de edad se consideran además un colectivo especialmente vulnerable en cuanto a la protección de sus datos personales, más aún si se trata de NNA en situación de riesgo.

En el contexto de una institución de protección donde recae la responsabilidad integral del cuidado y protección de los NNA, es habitual el tratamiento de estos datos especialmente sensibles, por lo que se debe extremar la precaución y garantizar las medidas de seguridad oportunas que se establecen en la Ley Orgánica de Protección de Datos (LOPD) y el Reglamento General de Protección de Datos (RGPD). Estas tendrán por objeto evitar un uso inadecuado o malicioso de la información personal del menor de edad, que pueda perjudicarle ahora o en el futuro.

La Ley Orgánica de Protección de Datos (LOPD) tiene por objeto garantizar que toda persona tenga derecho a la protección de sus datos de carácter personal.

La filtración de datos como el estado de salud de una persona menor de edad o un informe psicológico, puede acarrear graves consecuencias en su entorno personal y social. En otros casos, la inadecuada gestión de sus datos de identificación o de contacto, puede conducir por ejemplo a su localización por parte de su familia de origen o su entorno anterior por vías no autorizadas.

4.2. Privacidad, identidad digital y reputación en línea

Los datos personales en la actualidad no solo se generan desde una perspectiva administrativa o de gestión, sino que cada persona produce multitud de información al conectarse a Internet y utilizar servicios virtuales como redes sociales, páginas web, compras online, videojuegos, etc. La infancia y la adolescencia, al hacer uso de estos servicios, también están compartiendo sus datos y su imagen, están creando su identidad digital.

Puede ocurrir que sean otras personas las que difundan su información personal de manera intencionada con el objetivo de dañar al NNA, o bien que ésta se difunda inconscientemente, por ejemplo con una mención inocente en un comentario, cuando la propia persona menor de edad o uno de sus contactos comparte una foto donde se incluya su ubicación o se muestre su casa o su centro educativo, o si un familiar o un amigo pierde un dispositivo donde tiene almacenados datos o imágenes del NNA. Toda esta información que acaba en Internet de una u otra forma, va configurando su imagen en línea, lo que influye decisivamente en la percepción que los demás tienen sobre él a través de Internet, es decir su reputación en línea.

¿Qué es la reputación en línea?

Todos los datos personales que se encuentran en Internet sobre una persona, hacen que los demás construyan una idea positiva o negativa sobre su personalidad, su aspecto, sus gustos y hábitos, que puede coincidir en menor o mayor medida con la realidad.

Para un niño o niña, más aún para un adolescente, esta percepción que los demás tienen de él es más importante en comparación con otras etapas, ya que su autoestima está aún en desarrollo, y siente la necesidad de definirse en sociedad. Además, la misma sociedad ejerce una presión sobre el NNA para cumplir con unas expectativas de exposición pública, lo que les empuja a compartir información privada o sensible. Es por ello que en ocasiones tienen dificultades para diferenciar qué tipo de información pueden hacer pública, y qué datos es mejor mantener en privado.

Internet posee ciertas características que dificultan la gestión adecuada de la privacidad, como puede ser la permanencia de la información. Lo que se publica en la Red perdura en el tiempo, es decir, siempre se puede volver a localizar con una simple búsqueda, e intentar eliminarlo puede llegar a ser imposible. Además, en Internet la capacidad de difusión de un contenido es vertiginosa, lo que se conoce como viralidad. A menudo estas dos cualidades provocan que la información se descontextualice, quedando su interpretación a merced de la percepción de quien la encuentra.

Internet no es sino un medio más complejo en el que proteger nuestra privacidad, que requiere un aprendizaje concreto para saber cómo gestionar esos datos personales de forma adecuada.

4.3. Recomendaciones para la creación de una identidad digital positiva

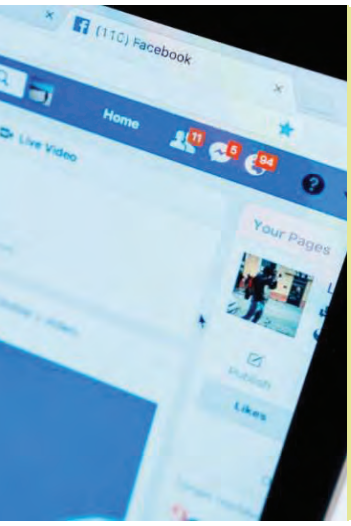
Siguiendo pequeñas pautas, las personas menores de edad pueden aprender a construir una identidad digital positiva, protegiendo la información más sensible y con ello impulsando su seguridad en la Red y fuera de ella.

Pensar antes de publicar:

- Si van a compartir información deben reflexionar previamente sobre quién la puede llegar a ver, cómo la podrá utilizar y qué posibles consecuencias puede tener esa publicación, tanto en ese momento como en el futuro.
- Cuidar su información es parte de su responsabilidad al utilizar Internet, y para ello deben mantener una actitud crítica y prudente, valorando cómo pueden repercutir sus publicaciones en la reputación propia y de los demás.

Imágenes y vídeos íntimos, sexting:

- No producir este tipo de contenidos: deben saber que el hecho de crear y almacenar imágenes o vídeos de carácter sexual ya supone un riesgo, alguien podría acceder a ellos si pierden o les roban el móvil por ejemplo, o si sufren un ataque por un virus informático.
- No compartirlos: los adolescentes tienen que conocer las consecuencias de esta práctica para ser más conscientes de los riesgos a los que se enfrentan si deciden difundir este tipo de contenidos.
- No promover esta práctica: solicitar a otros menores de edad imágenes o vídeos de este tipo, o compartir aquellos contenidos que lleguen a sus manos, les hace partícipes del problema. De nuevo, el respeto por los demás, así como el pensamiento crítico, juegan un papel clave.



Términos de uso / Políticas de privacidad

Cada servicio de Internet tiene sus propias normas al respecto de los datos personales que gestionan. Es importante prestar atención para conocer qué información recopilan, cuál es su propósito y cómo protegen esos datos. Además, incluyen los pasos a seguir para ejercer los derechos comúnmente denominados ARCO (acceso, rectificación, cancelación y oposición, ampliados con el Reglamento General de Protección de Datos con la limitación del tratamiento, la portabilidad de los datos y el no ser objeto de decisiones individualizadas automatizadas) que garantizan al usuario el control sobre sus propios datos.

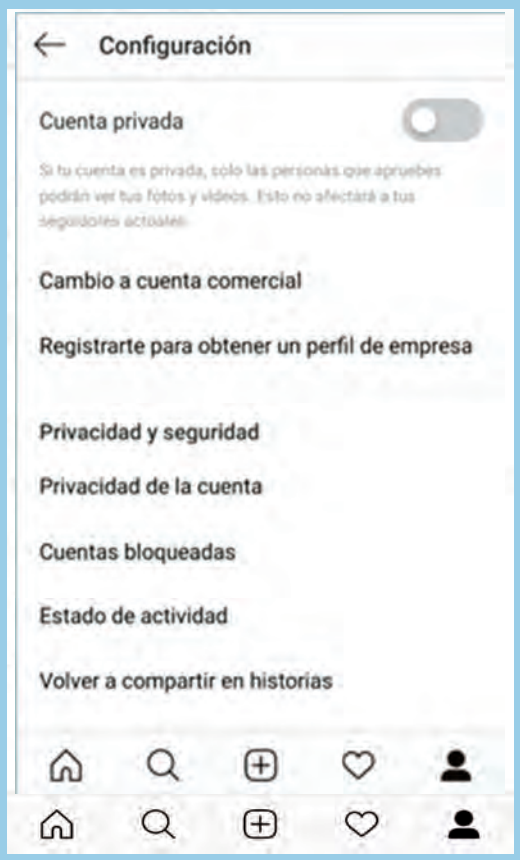
Configurar las opciones de privacidad:

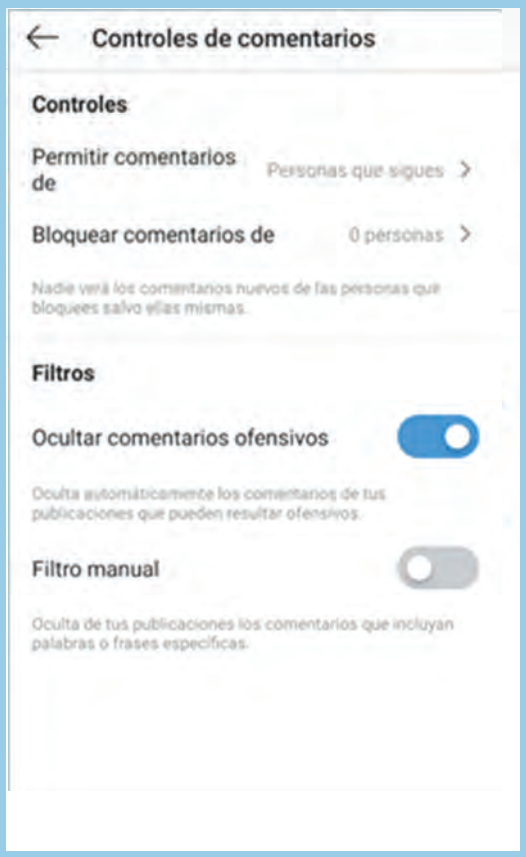
- Las personas menores de edad pueden administrar las opciones de privacidad de los móviles, navegadores, redes sociales y el resto de sus servicios en línea, decidiendo qué información quieren hacer pública o qué datos personales quieren ceder a terceros, entre otras preferencias.
- Las redes sociales como Instagram o Facebook, permiten escoger entre tener una cuenta privada o abierta al público. También en algunos casos limitan qué personas pueden acceder a las publicaciones, o dan la opción de filtrar las publicaciones en las que otras personas les hayan etiquetado.

Privacidad en Instagram

Algunos de los ajustes más destacados son:

- Cuenta privada, es decir, solo visible para los contactos.
- Estado de actividad, mostrando u ocultando el momento en el que se ha estado utilizando la red social por última vez.
- Volver a compartir en historias, si se permite o no que el contenido propio pueda ser compartido por otras personas en sus historias.
- Controles de comentarios, ajustando quién puede comentar los propios contenidos.





- Muchas aplicaciones permiten compartir la ubicación, lo que puede conllevar riesgos graves para los NNA. Además, la opción de geolocalizar las publicaciones, es decir, adjuntar automáticamente a cada foto o comentario la ubicación desde la que se ha hecho, se puede desactivar para mayor seguridad.

Ser selectivo aceptando ‘amigos’:

- Para los adolescentes, recibir solicitudes de amistad es algo habitual, y de hecho es uno de sus objetivos al abrirse un perfil en una red social. La mayoría de estas solicitudes serán de personas desconocidas o poco conocidas, para las que deben aprender a filtrar aquellas que no puedan reconocer.
- Fomentando el pensamiento crítico aprenderán a valorar los riesgos de mostrar sus fotos y hábitos de vida a personas que pueden tener malas intenciones.

En el momento en que los NNA deciden relacionarse a través de la Red con otras personas, deben ser conscientes de que esto conlleva una responsabilidad. El respeto, tanto hacia ellos mismos, como hacía las personas que están al otro lado de la pantalla debe ser la base sobre la que cimentar buenos hábitos, como por ejemplo no ceder a presiones para compartir información íntima, no reenviar información de otras personas sin permiso, no etiquetarles sin su consentimiento y no promover la difusión de información privada que pueda ser dañina u ofensiva para su propietario.

Para gestores de centros: protección de datos

La legislación en materia de protección de datos garantiza que todas las personas puedan decidir sobre qué organización tiene sus datos personales, conocer para qué los van a usar, y disponer de información sobre cómo modificarlos o borrarlos de sus ficheros de datos (derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad de los datos, oposición y a no ser objeto de decisiones individualizadas automatizadas).

Así pues las empresas o entidades están obligadas a informar al usuario de sus derechos, y a tratar sus datos con responsabilidad y seguridad.

Las instituciones de protección a la infancia también gestionan información personal, en su mayoría datos de carácter sensible sobre las personas menores de edad y sus familias, por lo que deben conocer cómo tratarlos y protegerlos.

En general, en relación a los centros de carácter educativo:

- **No es necesario el consentimiento firmado** para autorizar el tratamiento de los datos, ya que está justificado dado la finalidad del centro. No obstante, sí se debe informar de forma clara al menor de edad y a sus familias sobre por qué es necesario recogerlos y cuál va a ser su finalidad.

  En todo caso, es recomendable disponer del **consentimiento expreso** de los propios menores de edad (cuando tengan al menos 14 años) o de sus tutores legales (cuando no lleguen a esa edad).
- **En el caso de realizar otras actividades** que requieran el uso de datos personales, se debe pedir el consentimiento expreso.
- **El centro debe establecer un protocolo y unas directrices** concretas para que profesionales y educadores conozcan cómo tratar los datos personales, tanto digitalmente como en papel.

- **Es necesario determinar medidas técnicas que garanticen la seguridad de los datos**, como limitar el acceso a la plataforma o programa en el que se almacenen, mantener los equipos protegidos frente a ataques informáticos, evitar el traspaso de información personal a través de memorias USB, correos electrónicos, etc.
- **Si los datos se recogen en formatos físicos,** como papel o grabaciones, deben tomarse precauciones como conservar la documentación bajo llave o utilizar sistemas de vigilancia.
- Ante peticiones excepcionales de datos, o en casos que se salgan de los protocolos establecidos se debe ser especialmente cuidadosos, **priorizando el interés y el bienestar del menor de edad**, pues se trata de personas en situación de riesgo.

En todo caso, es preciso **estar al día** al respecto de los requerimientos legales sobre la protección de datos, y asumir que estos no son meros trámites burocráticos, sino **herramientas de ayuda** para la protección de la privacidad y la seguridad del centro y de las personas relacionadas con él, en especial los menores de edad atendidos.

4.4. Cómo actuar si... a un menor de edad le están suplantando la identidad en redes sociales

Crear un perfil fraudulento en una red social puede tener consecuencias graves para el NNA suplantado, por lo que es importante reaccionar ágilmente:

- Ayúdale a determinar de qué modo se están haciendo pasar por él: ¿han creado un perfil falso con su nombre y sus fotos?, ¿han comprometido sus cuentas reales de usuario y ya no puede acceder (secuestro de la cuenta)?
- Además, es útil guardar capturas de pantalla de la red social en la que están suplantando la identidad del menor de edad. Servirán de prueba a la hora de denunciar o reportar la situación.
- Revisar el resto de aplicaciones, redes sociales, juegos en línea u otras páginas que utilice, para comprobar si hay alguna más afectada y, en ese caso, igualmente tomar evidencias.
- Si el NNA sospecha de alguna persona, puede ser de utilidad mediar entre ambos para solucionar el conflicto más rápidamente.
- Podemos contactar con los administradores del servicio en línea para que sean ellos quienes eliminen el perfil falso, o le devuelvan el acceso al propietario real de la cuenta (si era el perfil auténtico).
- En el caso de que le estuvieran suplantando con su cuenta original, es necesario cambiar la contraseña, revisar otras plataformas en las que tuviera la misma contraseña, e incluso configurar las opciones de verificación en dos pasos para mejorar la seguridad del acceso.
- Si no podemos solucionarlo con estas medidas, si tenéis dudas, podéis solicitar asesoramiento gratuito a la **Línea de Ayuda en ciberseguridad de INCIBE (900 116 117)**.
- Si la situación escapa de nuestro control, podemos acudir al agente tutor del cuerpo policial correspondiente a nuestra zona para solicitar ayuda y denunciar la suplantación.

4.5. Cómo actuar si... circulan imágenes íntimas de un menor de edad por Internet

Lo ideal siempre, y más aún si se trata de *sexting*, es escuchar la versión del NNA con atención, sin culpabilizarle o juzgarle, y actuar con diligencia.

- La primera cuestión a determinar es quién tomó las imágenes: si fueron tomadas por él mismo, si otra persona le ha grabado con su consentimiento o si al contrario, ha sucedido de manera involuntaria o incluso forzosa.
- Es posible que conozcamos concretamente quiénes tienen en su poder esas imágenes, y podamos hablar con ellos directamente para explicarles la gravedad de la situación y solicitarles que las eliminen. No obstante, en estos casos es casi imposible tener la certeza de que no hayan difundido antes el contenido o lo conserven en el dispositivo.
- Tanto menores de edad, como adultos deben conocer que poseer o difundir imágenes de carácter sexual de un NNA es un delito y tiene consecuencias legales graves.
- Si las imágenes están circulando en alguna red social o página web, es útil guardar capturas de pantalla a modo de prueba, y solicitar a los administradores del servicio que eliminen el contenido.
- Si el contenido se encuentra alojado en plataformas digitales, utilizad los mecanismos de denuncia que facilitan para la retirada de contenidos. Desde IS4K os ayudaremos a agilizar el trámite.
- Si la difusión ha escapado a nuestro ámbito de actuación, o en los casos en que la toma de las imágenes ha sido forzosa, es necesario acudir a los cuerpos policiales o a la Fiscalía de Menores.

Para trabajar con las personas menores de edad

Con la sesión 2.1 «Protege tu historia» y 2.2 «Dejando una huella positiva» de la Unidad 2 «Tu información vale mucho», podemos trabajar pautas que fomenten el cuidado de la privacidad, así como la construcción de una identidad digital positiva.

Con la sesión 4.1 «Y así funciona Internet» dentro de la Unidad 4 «Mira más allá de tu pantalla», se plantean diversos modelos de negocio en la Red con sus implicaciones para la privacidad.

Con la sesión 5.2 «Contactos y redes sociales» de la Unidad 5 «Sabes elegir», se trata de reforzar el espíritu crítico frente a solicitudes de amistad, reconociendo la facilidad de creación de perfiles falsos.

Cada sesión de trabajo de 50 minutos incluye notas para los docentes y plantillas para realizar la actividad.

Catálogo de Unidades Didácticas de IS4K

https://www.is4k.es/unidades-didacticas-20

Para ampliar la información

Sección «Necesitas saber: Privacidad» en la web de IS4K
(https://www.is4k.es/necesitas-saber/privacidad)

Sección «Necesitas saber: *Sexting*» en la web de IS4K
(https://www.is4k.es/necesitas-saber/contenido-inapropiado)

Sección «Materiales didácticos» en la web de IS4K
(https://www.is4k.es/de-utilidad/recursos/materiales-didacticos)

Guía de Privacidad y Seguridad de OSI y AEPD
(https://www.osi.es/es/guia-de-privacidad-y-seguridad-en-internet)

Web de la Agencia Española de Protección de Datos
(www.aepd.es)

Web de PantallasAmigas sobre *sexting* seguro
(http://www.sextingseguro.com)

Web de PantallasAmigas contra la difusión no consentida de imágenes íntimas
(http://www.respetoimagenesintimas.com)

5. Bienestar de la infancia y la adolescencia en Internet

Las Tecnologías de la Información y la Comunicación forman parte de la vida cotidiana de niños, niñas y adolescentes (NNA). El uso que les dan influye en su desarrollo personal y puede repercutir positiva o negativamente en su salud y bienestar.

5.1. La salud y el uso de las TIC en la adolescencia

Al plantear la relación entre las tecnologías y la salud de niños y adolescentes, se puede hablar del uso intensivo que realizan de manera cotidiana y de los efectos negativos relacionados (por ejemplo, posturas, visión, dependencia, sedentarismo, obesidad, etc.).

Sin embargo, hoy en día sabemos que el concepto de salud es más complejo, entendiéndose como algo más que 'la ausencia de enfermedad', respondiendo al nivel de bienestar y de desarrollo de la persona. Desde este planteamiento, cada persona debe satisfacer ciertas necesidades básicas para lograr un estado de seguridad personal. Una vez cubiertas las condiciones mínimas que aseguren su supervivencia, como alimentarse, descansar o sentirse protegido, se establecen otras que proporcionan mejor calidad de vida a otros niveles: afecto, reconocimiento y autorrealización.

De este modo, el ser humano busca continuamente mejorar su bienestar en tres dimensiones. En primer lugar, de manera instintiva prioriza la salud física, evitando la enfermedad y optimizando el cuerpo para adaptarse al medio que le rodea. Después, a nivel psíquico, tomando consciencia de sus capacidades, afrontando la tensión o el conflicto de forma saludable. Por último, las personas como seres sociales, necesitan formar parte de un grupo, sentirse queridos, respetados y reconocidos positivamente por los demás. Estas tres dimensiones deben estar cubiertas para considerar que la

persona goza íntegramente de buena salud, y las tres pueden verse afectadas por el uso de las tecnologías de la información y la comunicación.

En la infancia, muchas de estas necesidades las solventan los adultos que están a cargo del menor de edad, y es en la adolescencia cuando la persona comienza a ser responsable de su propio bienestar.

En estas etapas, la persona madura de manera progresiva tanto física, psíquica, como socialmente. El objetivo es que el menor de edad llegue a ser autónomo, capaz de sobrevivir por sí mismo formando parte de una comunidad. En este periodo, la resolución de los distintos conflictos y problemas que van surgiendo en su relación con el entorno ayudan a los NNA a potenciar sus habilidades sociales, de comunicación y de reacción.

La aparición de las nuevas tecnologías, ha aportado muchos beneficios a este desarrollo, incrementando capacidades, experiencias, relaciones y aprendizajes. Internet es un nuevo entorno en el que los NNA crecen y maduran, donde se comunican con otras personas, donde se sienten reconocidos y realizados.

Los adolescentes no conciben su día a día sin el uso de los dispositivos conectados. Esto se debe a que para ellos, es un medio más para comunicarse y divertirse, les atrae su inmediatez, diversidad y facilidad de acceso. Además, ciertas características de los adolescentes favorecen esta buena relación con la tecnología, como por ejemplo la búsqueda de la autodefinición (mediante la posibilidad de acceder a una gran variedad de información de todas las temáticas, aficiones o tendencias) y la necesidad de reconocimiento social que pueden lograr a través de las redes sociales, o la demanda de independencia y autonomía que consiguen gracias a la sensación de anonimato que ofrece Internet.

Al igual que en otros entornos, también existen en Internet diferentes riesgos y problemáticas que, aunque no son exclusivos del entorno online, sí tienen particularidades específicas que es necesario conocer. Los adolescentes, debido al grado de desarrollo e inmadurez en el que se encuentran, no siempre tienen las habilidades necesarias para afrontar estos problemas.

Existen en Internet diferentes riesgos y problemáticas que tienen particularidades específicas que es necesario conocer.

Por ejemplo, la curiosidad natural de los NNA puede llevarles a entrar en contacto con contenidos o personas inadecuadas o peligrosas en la Red. También influyen en estas situaciones otras características propias de esta etapa, como un incremento de la presión social por encajar entre sus iguales, la dificultad para percibir las consecuencias de sus actos en el futuro o la impulsividad a la hora de responder o reaccionar de manera irreflexiva.

5.2. ¿Cuáles son los principales riesgos?

En Internet, como en cualquier otro contexto, existen situaciones de riesgo que pueden acarrear consecuencias graves. Es importante recalcar que no son problemáticas que se den de forma exclusiva en este entorno online, sino que pueden darse en un contexto no virtual, o en ambos simultáneamente. Internet solo añade cierta complejidad o características concretas a estos riesgos.

En multitud de ocasiones, las personas menores de edad son más vulnerables cuando existe un desequilibrio en su estado de bienestar, o lo que es lo mismo, cuando algunas de sus necesidades a nivel físico, psicológico o social no están cubiertas de manera apropiada.

Es habitual que en la etapa de la adolescencia, de alguna forma exista cierta inestabilidad, dado que son aspectos de la persona que aún están desarrollándose. En algunos casos, el contexto del NNA, sus experiencias en la infancia u otras condiciones específicas de salud física, mental o social, agravan ese desequilibrio.

Para cualquier NNA, una autoestima poco desarrollada, o un círculo afectivo insuficiente, pueden aumentar las posibilidades de una reacción inadecuada ante una situación de riesgo, como puede ser una petición de amistad por parte de un desconocido o una solicitud para compartir imágenes íntimas por mensajería instantánea.

Asimismo, también puede suceder que alguna de estas situaciones de riesgo se den mientras la persona menor de edad navega por la Red, perturbándolo o

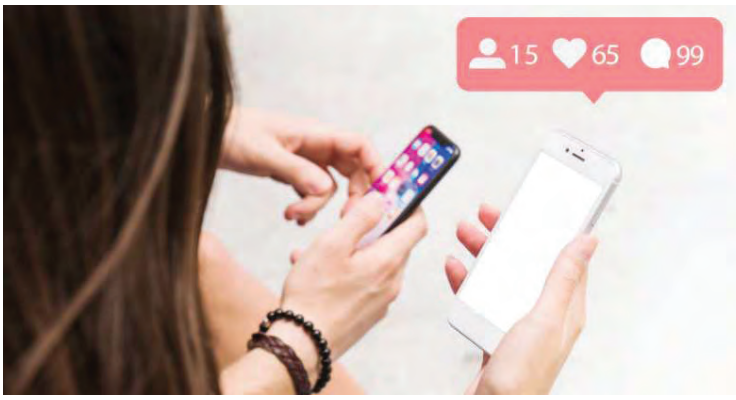
impactándolo de tal manera que su estado de bienestar o de salud, en cualquiera de sus dimensiones, se vean afectados.

Acceso a contenidos inapropiados y comunidades peligrosas:

Internet ofrece una variedad de contenidos extraordinaria, y por supuesto no todos son adecuados para NNA. Ya sea por tratarse de contenidos para los que se necesita cierta madurez o conocimiento (imágenes o vídeos de carácter sexual, violentos, etc.), información poco fiable o errónea (retos virales, noticias falsas...) o incluso contenidos dañinos que afectan tanto a personas menores de edad, como adultos (aquellos que fomentan el discurso de odio, el racismo o el machismo por ejemplo, u otros que promueven conductas perjudiciales como los hábitos alimentarios poco saludables, el consumo de drogas o los juegos de azar).

Además, determinados contenidos pueden facilitar el contacto del NNA con colectivos extremistas, violentos o racistas, llegando a ser captados por grupos políticos radicales, sectas de carácter ideológico o religioso, comunidades virtuales relacionadas con la anorexia y la bulimia, etc.

Conductas de riesgo:



Los NNA sienten una gran curiosidad, que les permite experimentar sin miedo a nivel instrumental, como sucede en sus primeros contactos con Internet. De este modo son capaces de hacer un uso intensivo de dispositivos tecnológicos y de Internet, aunque no siempre lo hagan de la forma más segura o adecuada, sobre todo en lo relativo a su privacidad. Por eso, algunas de sus prácticas a la hora de mostrarse en las redes sociales y otros servicios de Internet, pueden llegar a provocar consecuencias indeseadas o situaciones de indefensión.

La presión social que ejercen otras personas menores de edad, y la sociedad en su conjunto, no hace más que acentuar su necesidad de exponerse más, aunque suponga un riesgo del que no siempre son conscientes, ya sea por desconocimiento o inmadurez.

Así ocurre por ejemplo con la práctica del *sexting*, con la que se producen y se envían imágenes o vídeos de carácter sexual, que pueden acabar difundiéndose sin control, o utilizándose como material de chantaje. Otro ejemplo, lo encontramos en el acceso

a juegos de azar, actividad cada vez más habitual en los adolescentes, que son aún más vulnerables a la adicción en edades tan tempranas.

Uso excesivo:

La utilización continuada y desproporcionada de los dispositivos conectados, ya sea el móvil, el ordenador, la videoconsola o cualquier otro, puede generar dependencia. Es cierto que los adolescentes hacen un uso habitual de Internet, pero se considera excesivo cuando interfiere con sus actividades habituales, genera daños a su salud o a sus relaciones sociales y familiares. La falta de control, trastornos de conducta o de sueño, problemas de atención o cambios en su estado de ánimo, pueden ser indicadores de esta dependencia.

Situaciones de riesgo en las relaciones:

Internet es ante todo un medio de comunicación, y para las personas menores de edad es uno tan natural como cualquier otro, con la ventaja de ser inmediato y accesible. Por el contrario, al interactuar con otras personas en la Red, no siempre se comportan como lo harían en otros entornos no virtuales.

Las redes sociales, los foros o las comunidades en línea, ofrecen características específicas del entorno virtual. Principalmente, en Internet los NNA tienen más dificultad para sentir empatía hacía las personas que están al otro lado de la pantalla, viéndose más libres a la hora de expresarse de manera más cruda, fría y distante. En el mismo sentido, también se sienten más cómodos exponiendo sus sentimientos, su privacidad e incluso su cuerpo que al hacerlo fuera de la Red, debido a una falsa sensación de anonimato o seguridad. Estas particularidades favorecen algunas situaciones de riesgo a la hora de relacionarse:

- El **ciberacoso** (*ciberbullying*) es una forma más compleja de acoso entre iguales. A través de los medios tecnológicos, un menor de edad puede ser agredido verbalmente, ignorado entre sus compañeros y humillado mediante mensajes, imágenes o vídeos que otras personas publiquen en Internet.

  La diferencia está en que se trata de un acoso que no depende de horarios escolares, ni de espacios concretos como el aula o el patio de recreo. Además, las ofensas perduran al estar publicadas en la Red, se difunden

muy rápido y más personas tienen acceso a estos contenidos, intensificando el alcance del acoso.

Y es que Internet proporciona una falsa sensación de anonimato e impunidad, lo que unido a la distancia física y a la inmediatez de las comunicaciones facilita una mayor desinhibición, impulsividad y agresividad. Así también es más sencillo que se produzcan ataques indirectos, animando a los espectadores a dar "me gusta" o compartir un mensaje insultante con una mínima exposición personal.

- El *grooming* tiene lugar cuando una persona utiliza el engaño, el chantaje o la coacción a través de Internet para conseguir acercarse a NNA con fines sexuales. Los adolescentes suelen aceptar con facilidad solicitudes de amistad, incluso de personas desconocidas, que muchas veces no son quienes dicen ser. Por ejemplo, hay veces en que los acosadores son adultos que se acercan imitando sus gustos o aficiones, con imágenes de perfil atractivas para ellos con el fin de ganarse su confianza. Con el tiempo, pueden llegar a sugerirles realizar actividades sexuales en línea, enviarse imágenes o vídeos, y en los casos más graves, incluso pueden solicitarles verse fuera de Internet, en persona.

- La **violencia en la Red** es un efecto más de esa falsa sensación de anonimato, invencibilidad y de la falta de empatía, que facilitan que los NNA puedan actuar y comunicarse de una forma más agresiva o irrespetuosa que al hacerlo frente a personas cara a cara. Influyen también aspectos como la normalización de la violencia en otros medios (televisión, videojuegos, etc.), la impunidad que les proporciona Internet y en general la falta de consecuencias visibles ante sus acciones. En concreto, la violencia de género a través de los dispositivos conectados es cada vez más habitual entre las personas menores de edad, ejerciendo abusos mediante el uso de mensajes, aplicaciones o redes sociales. Las comunicaciones en Internet hoy en día se entienden como inmediatas, no se tolera el retraso a la hora de contestar, y esta característica puede utilizarse como un mecanismo de control.

Consecuencias

La realidad es que cualquier riesgo de las TIC puede terminar **afectando al bienestar del menor de edad en cualquiera de sus tres esferas: física, psíquica y social**. A la hora de determinar la gravedad de cada caso, han de considerarse desde factores personales del NNA, como factores familiares, escolares, sociales o socioeconómicos, entre otros.

En este sentido, son cada vez más los expertos que inciden en **efectos perjudiciales a largo plazo** relacionados con el uso desequilibrado de las TIC, como problemas de salud y la afectación de los procesos cognitivos, o en los agravantes ante riesgos como el *sexting* o el ciberacoso escolar, entre otros.

De forma resumida, las consecuencias del uso perjudicial de Internet – ya sea por mal uso, uso desproporcionado o por el impacto de uno de los riesgos anteriores – incluyen aquéllas **de índole físico y emocional** (dolencias, alteraciones del sueño o el apetito, ansiedad, estrés, apatía, autolesiones, etc.), **alteraciones en la conducta y en las relaciones sociales habituales** (incluyendo abandono de amistades, cambios en las actividades habituales de ocio y en la forma de usar los dispositivos, cambios bruscos de comportamiento, aislamiento, agresividad, etc.), así como **empeoramiento del normal desenvolvimiento** en entornos como el familiar o la escuela (incidentes y peleas, deterioro de resultados académicos, etc.).

Fuente:

- Common Sense Media (2008) *Media Child and Adolescent Health: A Systematic Review.*
- American Psychological Association (2018) *Cohort Effects in Children's Delay of Gratification.*
- The Lancet Child and Adolescents Health (2018) *Associations between 24 hour movement behaviours and global cognition in US children: a cross-sectional observational study.*

Vídeo: «Guía clínica sobre el ciberacoso»

Experta: María Angustias Salmerón, especialista en Medicina de la Adolescencia y problemas relacionados con salud y las TIC.

https://www.youtube.com/watch?v=myTahnQdWX0

5.3. Medidas de protección

La mayor parte de las pautas que se sugieren a continuación, no precisan de grandes conocimientos en informática o redes sociales, solo requieren de interés y experiencia a la hora de comunicarse y relacionarse de forma adecuada.

Utilización de contenidos positivos

- Mostrar a los NNA dónde pueden encontrar **contenidos de calidad**, adecuados a su edad y madurez. Seleccionar con ellos juegos, páginas web y redes sociales que sean positivos para su desarrollo, divertidos y actuales.

- Proporcionarles estrategias para comparar e **identificar fuentes de información fiables**, que les permitan satisfacer su curiosidad, resolver sus dudas y averiguar cuando un contenido es falso o erróneo.

Aplicar medidas de uso equilibrado, supervisión y control

- Establecer unas normas de uso de Internet y de los dispositivos conectados, que determinen por cuánto tiempo, en qué momentos y espacios se pueden usar, y con qué objetivo. Estas normas deberán adaptarse a cada NNA, por ejemplo, hasta los dos años de edad se recomienda que no haya uso, y desde ahí hasta los cinco años un máximo de dos horas diarias.

  En todo caso, se ha de evitar el uso en la cama, resaltando la necesidad de desconectarse al menos una hora antes de irse a dormir para prevenir la aparición de trastornos del sueño.

- Es interesante que las personas menores de edad tengan cierto grado de participación en la redacción de estos límites, para que puedan sentirse implicados y los acepten con más responsabilidad.

- La supervisión de horarios, contenidos visitados y contactos debe ser una tarea habitual y normalizada, de forma que los NNA sean más conscientes del uso que hacen de Internet, y se puedan identificar problemáticas derivadas de un empleo inadecuado de su tiempo de uso de dispositivos e Internet.

- Existen medidas tecnológicas que se pueden emplear para facilitar el control y la supervisión, como las herramientas de control parental, los sistemas de filtrado de contenidos o las opciones de administración de los dispositivos. Dichas herramientas no sustituyen en ningún caso la supervisión directa de un adulto, pero pueden ser un complemento que le ayude en dicha tarea.

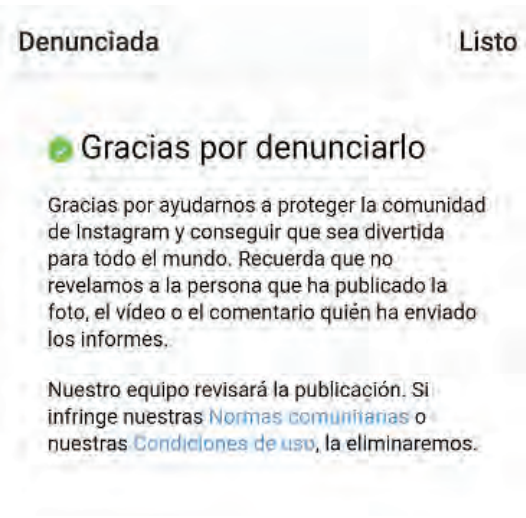
- Es necesario fomentar actividades alternativas de ocio saludable, ampliando las perspectivas de NNA.

Netiqueta para mejorar las relaciones en línea

En todos los espacios en los que existe comunicación, existe también un código de conducta, unas normas para relacionarse con respeto y evitar malentendidos. Internet no es una excepción, y es imprescindible conocer qué conductas son adecuadas y cuáles son socialmente conflictivas. Esto implica cuidar el lenguaje y el tono de las publicaciones y comentarios, respetar las normas de la comunidad (de la red social, del foro, del juego...) y aprender a discutir con otras personas sin despreciar u ofender sus opiniones.

Por ejemplo, entre las normas comunitarias de Instagram se promueve compartir imágenes y mensajes propios, originales, apropiados para todo tipo de personas y que resulten relevantes y positivos. Por ese motivo, en esta red social no se toleran imágenes de desnudez, ni mensajes violentos o amenazantes, etc., con lo que cualquiera puede denunciar ese tipo de contenidos para pedir su retirada.

Conocer los mecanismos de bloqueo y denuncia



- Ningún usuario debe tolerar que otra persona le moleste o le perturbe en Internet, y menos aun tratándose de personas menores de edad: siempre existen opciones para evitar este tipo de contactos.

- Las redes sociales, los foros y comunidades en línea ofrecen la posibilidad de bloquear a otro usuario: entrando en su perfil, dentro del menú de opciones, se debe seleccionar 'bloquear'. A menudo, es posible realizar esta misma acción desde cualquier publicación o comentario de ese usuario.

- Si no está claro, podemos acudir a la sección de ayuda del servicio o su centro de seguridad para que nos asesoren sobre cómo actuar, o tomen medidas. En este caso, es importante guardar pruebas (por ejemplo, con capturas de pantalla) de aquellos comentarios o mensajes ofensivos, para poder reportar la situación.

Para gestores de centros: gestión de la convivencia

Uno de los puntos críticos en el funcionamiento cotidiano del centro es la gestión de la convivencia entre todas las personas relacionadas con el mismo: las familias, el personal educativo, los servicios externos, etc., aunque lógicamente la principal preocupación esté centrada en las propias personas menores de edad que allí conviven.

En esta labor, no se puede dejar solos a los educadores. Es preciso disponer de unas pautas claras y compartidas, unas propuestas educativas que promuevan valores positivos para la convivencia, unos protocolos de actuación frente a problemáticas relevantes, además de una labor de coordinación continua entre las personas implicadas.

Todos estos aspectos se pueden concretar en un **plan de convivencia**, una herramienta similar a la empleada en los centros de educación primaria y secundaria (alineada con la propuesta de la administración educativa). Sin embargo, con un mero documento "administrativo" no se consigue nada. Los educadores han de consensuar su redacción y adaptarla a la realidad del centro, de los NNA atendidos y de la propia sociedad.

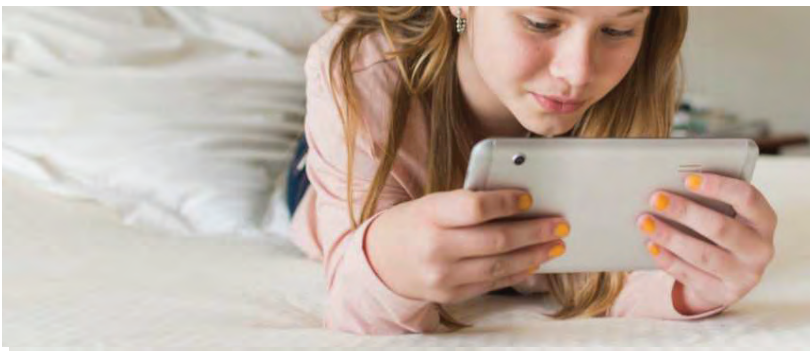
Además de mejorar la relación entre las personas menores de edad, se pretende complementar la normativa y reglamento interno del centro en conflictos de convivencia y afirmar la clara determinación del centro frente al acoso y cualquier otra forma de violencia.

Esto también implica adaptarse al contexto del uso de la tecnología por parte de los NNA, con fenómenos como el ciberacoso, la difusión de imágenes íntimas originadas en un envío voluntario (*sexting*), los chantajes o el *grooming*, entre otros.

También es posible plantear otras medidas complementarias como la adaptación del proyecto educativo del centro para reforzar el tratamiento transversal de la convivencia y las normas de uso de las tecnologías en todas sus actividades (a nivel escolar, extraescolar, en situaciones informales de aprendizaje, etc.). Incluso se pueden desarrollar programas formativos en uso seguro y responsable de Internet para el personal del centro y para los NNA.

5.4. Cómo actuar si...una persona menor de edad está haciendo un uso abusivo de Internet y del móvil

La aparición de un cambio de conducta, el abandono de amistades o aficiones, así como reacciones de ansiedad o irritabilidad al no poder conectarse, pueden considerarse señales de alerta. Ante cualquier signo de alerta, es necesario tomar medidas:



- Conversar con el NNA de forma abierta y respetuosa, para poder valorar el alcance del problema: preguntarle acerca de sus horarios de conexión, qué hace cuando se conecta, si le importaría cambiar su rutina de Internet por otra actividad puntual o si mantiene otras aficiones que no requieran el uso de la tecnología.
- Explicarle cuál es la preocupación y cómo puede ser consciente de un uso excesivo por sí mismo: que anote cuántas veces mira el móvil en una hora o en un día, que intente cambiar su rutina de conexión o que deje el móvil en la habitación mientras realiza otra actividad.
- Establecer unos límites de uso razonados con el NNA, de manera que no lo vea como algo impuesto y pueda ser responsable de sus acciones. Estas normas pueden incluir las consecuencias acordadas en el caso de que no se cumplan esos límites.
- Ofrecerle nuevas posibilidades de ocio que sean atractivas para él, así como otras formas de relacionarse con personas de su edad.
- Si no se logra controlar la situación, facilita que el NNA acuda a ayuda especializada (psicólogos, abogados y expertos en seguridad y educación). La **Línea de Ayuda en ciberseguridad de INCIBE (900 116 117)** puede ser un buen referente.
- Analiza por qué ha podido ocurrir y tomar medidas para prevenirlo a futuro en el centro. Realizar sesiones o dinámicas con los NNA para invitarles a reflexionar sobre el uso que hacen de las tecnologías y sobre cómo esto puede estar interfiriendo en cómo se sienten y actúan.

5.5. Cómo actuar si...identifico a una víctima o menor de edad implicado en una situación de ciberacoso

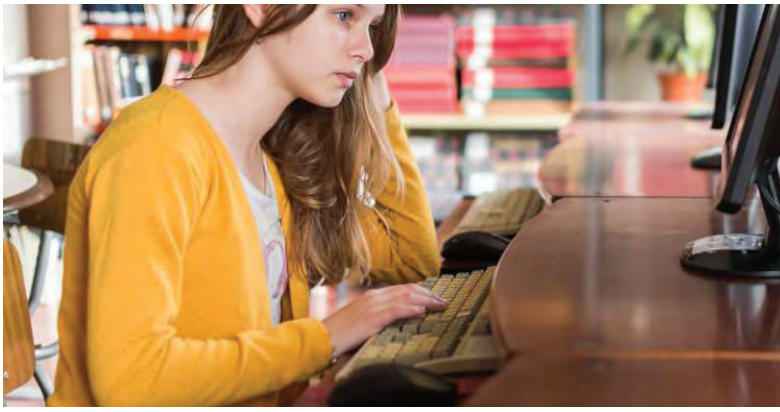
El ciberacoso es una de las principales situaciones de riesgo entre NNA. Identificar el problema en su inicio y cortarlo a tiempo reduce de forma significativa las consecuencias:

- Analiza el alcance de la situación en el centro (gravedad, nivel de difusión, alcance temporal, extensión al centro educativo, etc.) y determina qué otros profesionales deben conocer la situación. Cuida la confidencialidad en los procesos de comunicación.
- Complementariamente puede ser interesante hablar con el centro educativo para poner en su conocimiento el caso, recabar más información de contexto, y que puedan implicarse en su resolución a través de los planes y protocolos de convivencia, más aún si los acosadores acuden al mismo centro.
- Establece medidas para frenar el acoso y restaurar la convivencia. Dialogar, con ambas partes del conflicto si es posible, valorando una posible mediación para abordar el problema, reforzando la autoestima de la víctima y la empatía de los acosadores. Hacerles conscientes del daño que puede causar un simple comentario o una burla.
- Si se cuenta con su colaboración, solicitar a los acosadores que retiren todos los comentarios o contenidos ofensivos de las redes sociales, para evitar que sigan difundiéndose. Si se niegan a hacerlo, podemos denunciar o reportar dichas publicaciones en la red social para que las eliminen, así como bloquear a esos usuarios.
- Ayúdale revisar y configurar adecuadamente la privacidad y seguridad de los perfiles de redes sociales. El objetivo es impedir que potenciales acosadores puedan acceder y utilizar información nuestra de manera humillante o ilícita.
- Si tenéis dudas podéis solicitar asesoramiento gratuito a la **Línea de Ayuda en ciberseguridad de INCIBE (900 116 117)**, para conocer las primeras pautas de actuación, agilizar trámites y consultar a qué apoyos específicos acudir.
- El ciberacoso puede acarrear consecuencias psicológicas y sociales graves, que afectarán a su desarrollo, por lo que es aconsejable contar con apoyo especializado en el centro escolar o en el centro de salud.

- Siempre que la situación se agrave, debemos informar a los cuerpos policiales, al agente tutor correspondiente o a la Fiscalía de Menores.

5.6. Cómo actuar si...sospecho que el nuevo «amigo» de un menor de edad oculta intenciones sexuales (*grooming*)

Los NNA están acostumbrados a recibir solicitudes de amistad de personas desconocidas, si bien estas situaciones pueden suponer conflictos o incluso situaciones de riesgo con adultos, por lo que es importante actuar de inmediato y siempre teniendo en cuenta las políticas y normativas internas del centro.



- Mostrarse abierto a la escucha y el apoyo, sin juzgar. Hablar con el NNA para reunir información y datos sobre esa persona, así como recopilar capturas de pantalla de las conversaciones, mensajes o imágenes que haya podido recibir el menor de edad.
- Valorar la gravedad de la situación de acuerdo a la magnitud y el alcance de la información recopilada, teniendo en cuenta si el NNA ha llegado a enviar imágenes o vídeos, o si ha facilitado información personal. Nunca se debe ceder ante chantajes, ni ante otras alternativas que pueda ofrecer el acosador.
- Transmítele la importancia de evitar prácticas como el *sexting*, así como los riesgos de contactar o quedar con personas a las que no conocemos en persona.
- Establece un clima de confianza y trata de acordar con el NNA que, siempre que alguien proponga un encuentro, se lo comunique a un adulto de confianza.
- Rastrea las imágenes o vídeos del NNA que puedan estar circulando por la Red y que sean abusivas. Solicita la eliminación inmediata de los archivos a través de los mecanismos de denuncia de las plataformas digitales.
- Ayuda a la persona menor de edad a que bloquee o elimine al acosador en su lista de contactos. Revisa con él la protección de sus cuentas y dispositivos para evitar que siga manteniendo cualquier contacto o relación con el acosador.

- Indícale cómo tomar evidencias o pruebas electrónicas. Dado que la mera posesión de contenidos de abuso sexual infantil es un delito, el educador no debe acceder a este contenido, limitándose a facilitar los datos necesarios para comenzar la investigación (ej. dirección de la página web).
- En cualquier caso de *grooming* es necesario contactar con los Cuerpos de seguridad, para que puedan ofrecer asesoramiento sobre cómo actuar. También puede ser de utilidad consultar con agentes especializados como servicios de salud, equipo de orientación escolar, **Línea de Ayuda en ciberseguridad de INCIBE (900 116 117)**, etc. Aunque el menor de edad no haya llegado a intercambiar más que un par de mensajes, otros NNA pueden caer en el engaño.

5.7. Cómo actuar si...nos preocupa la preferencia de una persona menor de edad por foros en Internet con contenidos potencialmente problemáticos para su desarrollo

Los NNA sienten curiosidad por todo tipo de temas, e Internet les proporciona mucha información, no siempre adecuada para su edad. En algunas comunidades virtuales, los contenidos se centran en temáticas concretas que pueden ser perjudiciales para un menor de edad cuya personalidad, autoestima y valores aún están en desarrollo.

- Comunica la situación de riesgo detectada y contrasta la información que se pueda recabar tanto del NNA, como de otros compañeros y personal del centro.
- Interesarse por los motivos de la infancia y la adolescencia para indagar en temas inapropiados para su edad o en general dañinos para la sociedad. Escuchar con una actitud positiva porque el mismo hecho de que hable de ello con los adultos es un gran paso.

- Razonar acerca de los peligros y aspectos negativos de esas comunidades, desarrollando su capacidad de crítica.

- No hay que olvidar que a menudo son temáticas complejas para los que un NNA no está preparado, por lo que debemos facilitarle recursos para que pueda ver la situación con perspectiva y objetividad.
- En los casos en los que el NNA se haya adentrado activamente en estas comunidades puede ser necesario un apoyo profesional especializado, más aún si estos contenidos ya han tenido consecuencias a nivel de salud, problemas legales, cambios de conducta, etc.
- Aquellos contenidos cuya difusión sea ilegal o no cumpla las normas de la comunidad del foro o el espacio web en el que se encuentren, pueden ser reportados y denunciados para su eliminación por parte de los administradores del servicio, o ante los Cuerpos de seguridad. Servicios como la **Línea de Ayuda en ciberseguridad de INCIBE (900 116 117)** pueden ayudarte en esa tarea.

Para trabajar con las personas menores de edad

Con la sesión 1.1 «Con respeto en Internet» y 1.2 «No te quedes al margen» de la Unidad 1, podemos trabajar pautas para fomentar el respeto a los demás, las habilidades sociales, e incluso realizar dinámicas para analizar una situación de conflicto por un ciberacoso.

Mediante la sesión 4.2 «Mantén el equilibrio» de la Unidad 4, podemos promover la reflexión sobre el equilibrio en los tiempos y actividades diarias, y el espíritu crítico sobre los contenidos que consumimos.

Con la sesión 5.2 «Contactos y redes sociales» de la Unidad 5 «Sabes elegir», se trata de reforzar el espíritu crítico frente a solicitudes de amistad, reconociendo la facilidad de creación de perfiles falsos.

Con la sesión 6.2 «Juegas en línea» fomentamos el respeto y la reflexión en las conexiones en línea a la vez que prevenimos riesgos en los juegos con conexión.

Cada sesión de trabajo de 50 minutos incluye notas para los docentes y plantillas para realizar la actividad.

Catálogo de Unidades Didácticas de IS4K

https://www.is4k.es/unidades-didacticas-20

Para ampliar la información

Campaña de concienciación «Convivencia y respeto en Internet» en la web de IS4K
(https://www.is4k.es/convivencia-y-respeto-en-internet)

Sección «Necesitas saber: Ciberacoso escolar» en la web de IS4K
(https://www.is4k.es/necesitas-saber/ciberacoso-escolar)

Sección «Necesitas saber: Grooming» en la web de IS4K
(https://www.is4k.es/necesitas-saber/grooming)

Sección «Necesitas saber: Contenido inapropiado» en la web de IS4K
(https://www.is4k.es/necesitas-saber/contenido-inapropiado)

Sección «Necesitas saber: Comunidades peligrosas» en la web de IS4K
(https://www.is4k.es/comunidades-peligrosas)

Sección «Necesitas saber: Uso excesivo» en la web de IS4K
(https://www.is4k.es/uso-excesivo-de-las-tic)

Sección «Materiales didácticos» en la web de IS4K
(https://www.is4k.es/de-utilidad/recursos/materiales-didacticos)

Preguntas frecuentes de la Línea de Ayuda en ciberseguridad de INCIBE (900 116 117).
(https://www.is4k.es/preguntas-frecuentes)

6. El educador digital

[Contribución del Área de Programas de Atención a Familias de la Junta de Extremadura]

Es obligatorio partir, hoy en día, del axioma general en el cual todos nos convertimos en educadores y todas las personas a su vez nos pueden educar a nosotros. En el mundo tecnológico actual, no debemos perder la visión de influencias y corrientes mutuas que se producen.

Desde la óptica que nos ocupa, el educador digital debe añadir un "plus" que se puede localizar en el compromiso del mismo, en la responsabilidad que asume al colaborar y ayudar en sus procesos educativos, formativos y personales del niño, niña o adolescente (en adelante NNA), tratando de comprender sus especiales realidades y teniendo siempre presente sus singulares circunstancias.

Educar desde el punto de vista tecnológico se define también desde la vinculación, el afecto, el apego personal, del profesional con el NNA, ofreciéndole claves que le permitan adaptarse, distinguir, experimentar de manera más adecuada su presencia digital. No podemos olvidar que la intención máxima del educador ha de ser construir – independientemente de las tecnologías que utilice – un individuo preparado para abordar el mundo en el siglo XXI.

La competencia digital implica el buen uso, seguro, crítico y creativo de las Tecnologías de la Información y las Comunicaciones (TIC) para mejorar el desarrollo personal, el uso del tiempo libre y su adecuada inclusión en la sociedad.

Se hace necesario remarcar alguna serie de claves que al educador le permitan adaptarse, contribuir y permitir el desarrollo más adecuado de los menores de edad desde el mundo digital.

Existe una amplia serie de líneas y posibilidades para potenciar las competencias digitales por parte de los profesionales. Como es natural hemos de realizar una selección a modo de resumen que promuevan transformaciones y sobre todo posibles actitudes y aptitudes positivas hacia el entorno digital que faciliten cambios en el enfoque de trabajo.

Entre los aspectos básicos a implementar y desarrollar no podemos dejar de incidir en cuestiones como el desarrollo del pensamiento crítico, la capacidad de innovar, la colaboración activa e inclusión social, la curación de contenidos, etc.

> La conectividad es un asunto crucial y uno de los objetivos más importantes desde la responsabilidad de profesionales en contacto con la infancia. Debemos procurar su máximo desarrollo desde el punto de vista del acceso y la participación en las nuevas tecnologías.

También hemos de recordar la necesidad por parte de los educadores de situarse en línea con lo expresado en el *Marco Común de Referencia de la Competencia Digital Docente*[2], marco de referencia para el diagnóstico y la mejora de las competencias digitales del profesorado.

Áreas de la Competencia Digital Docente

Es necesario conocer e informarse sobre las 5 Áreas de la Competencia Digital Docente vigentes:

1. Información.
2. Comunicación.
3. Creación de contenidos.
4. Seguridad.
5. Resolución de problemas.

La competencia digital debe considerarse como un desafío transversal al trabajo realizado por todos los profesionales. Es interesante, dado su carácter de contacto y "pegamento" con las diferentes áreas de crecimiento personal de los menores de edad, tratar de incluir experiencias en este sentido comunes a las otras áreas de planes de trabajo.

Por último y no por ello menos importante, debemos tener en cuenta que los *Objetivos de Desarrollo Sostenible 2030*[3], en su meta 9, especifican la necesidad de

---

[2] Marco Común de Referencia de la Competencia Digital Docente de Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF) **http://aprende.intef.es/mccd**

[3] Objetivos de Desarrollo Sostenible de la Organización de Naciones Unidas (ONU) **https://www.un.org/sustainabledevelopment/es/**

construir un mundo igual para todos, promover una mayor igualdad y participación inclusiva y sostenible y fomentar la innovación. Es evidente que las TIC tienen un papel muy claro para que esta meta se pueda lograr. La conectividad es un asunto crucial y uno de los objetivos más importantes, por lo que desde la responsabilidad de profesionales en contacto con la infancia, debemos procurar su máximo desarrollo desde el punto de vista del acceso y la participación en las nuevas tecnologías.

Hemos de proporcionar a las personas el acceso y los cauces para aprovechar las ventajas del mundo digital como un activo para el crecimiento social y económico futuro.

6.1. Características necesarias para fomentar competencias digitales

El conjunto de características que como educadores debemos contemplar a la hora de fomentar las competencias digitales comprende las siguientes categorías:

- Acompañamiento responsable.
- Pensamiento crítico.
- Curación de contenidos.
- Fomento del trabajo en equipo.

Se desarrollan a continuación cada una de estas dimensiones.

Acompañamiento responsable

Desde el acompañamiento en responsabilidad, el educador digital ha de liderar grupos con enfoque pro-social y resiliente que fomenten en los NNA el desarrollo de la inteligencia emocional.

Hoy en día lo importante ya no está en la tecnología, sino en cómo nos adaptamos a los procesos que la tecnología provoca. Un ejemplo de ello es el *Big Data*, la recopilación de datos por parte de cualquier aparato que se conecte a Internet, y lo que ello significa desde el punto de vista de la privacidad del individuo. Éstas son cuestiones muy importantes y que el "educador digital" en su acompañamiento responsable debe reflexionar y valorar.

Los educadores, al igual que en las diferentes áreas en las que intervienen con los menores de edad, han de saber dar ejemplo con sus actuaciones, puesto que no podemos potenciar el uso adecuado de la Red, sin que nosotros mismos lo hagamos. Somos modelos de referencia activos y continuos, por lo que debemos enseñar a manejar los tiempos, los recursos y las "miradas" de las nuevas tecnologías responsablemente.

Por último, es importante fomentar la autoestima positiva en los individuos. El trabajo a través de la *netiqueta* puede ser un recurso adecuado para ello. Internet tiene sus propias reglas y protocolos de juego, debemos tratar de cumplirlas y adaptarnos para ser ciudadanos y ciudadanas respetuosos.

Pensamiento crítico

Se incluyen a continuación una serie de consejos para desarrollar y fomentar el pensamiento crítico y la mirada reflexiva en los niños, niñas y adolescentes.

- Tiempo y espacio para pensar. En la velocidad del día a día, es difícil encontrar un espacio en el que la mente se focalice solo en una cosa: pensar. Por ello, es recomendable establecer un momento del día para pensar de forma reflexiva, puesto que si estamos revisando constantemente los dispositivos, no podremos reflexionar sobre nuestros actos.
- Promover la curiosidad y las experiencias. Debemos animar a los más jóvenes a realizar nuevos descubrimientos, en su entorno más cercano o sobre ideas abstractas. Hay que proponer actividades que inciten a la curiosidad y al conocimiento, siempre adecuadas a su edad. Podremos así establecer puentes entre pensamientos y nuevos aprendizajes.
- Enseñar a dudar. Sin intención de generar desconfianza a los más jóvenes, es importante que cuestionemos la fiabilidad de las fuentes que consultan y la veracidad de la información que reciben, para que sean ellos mismos quienes aprendan a diferenciar entre lo que está fundamentado y lo que no, entre conocimientos completos e incompletos, y puedan así emitir juicios elaborados y propios.
- Acostumbrarnos a las preguntas. Es fundamental plantear interrogantes para fomentar el pensamiento crítico en los niños, niñas y adolescentes, como ¿qué opinas?, ¿cómo lo sabes?, ¿por qué? Es conveniente, además, compartir con los NNA nuestra forma de pensar, y nuestro punto de vista sobre los aspectos de las nuevas tecnologías. No hay mejor enseñanza que dar ejemplo.

- **Analizar, justificar, profundizar.** Debemos guiarles para profundizar en las razones y en el porqué de las cosas: explicar argumentos, comparar ideas de forma ordenada. Puesto que expresando pensamientos tomarán consciencia de la madurez y grado de elaboración de los mismos.
- **Procurar la autonomía**. Respetemos su espacio apoyándonos en lecturas, conversaciones, entornos y actividades que fomenten el desarrollo del pensamiento crítico de forma autónoma.
- **Ampliar miradas, manejar el "egocentrismo"**. Es igualmente interesante plantear a los NNA otras perspectivas y otros ángulos desde los que se pueda enfocar la realidad. Somos parte de un entorno social, político y cultural normalmente bien definido y nuestro punto de vista está siempre condicionado por ello. Por eso, intentar ponerse en el lugar de otros para comprender su punto de vista es una actividad formativa y creativa necesaria. Ante el deseo de notoriedad de los jóvenes en las redes sociales, es importante trabajar el ego personal, así como el deseo de *egosurfing*.

Video: «Egosurfing»

El *egosurfing* nos permite conocer la imagen que proyectamos en Internet. Esta imagen está formada por lo que hemos publicado nosotros mismos (por ejemplo, nuestros perfiles en redes sociales) y por lo que otros han publicado sobre nosotros. Es una buena práctica acostumbrarnos a practicarlo de vez en cuando, para saber qué se dice sobre nosotros, cómo y quién.

https://www.osi.es/es/actualidad/blog/2015/11/06/egosurfing-que-sabe-internet-de-nosotros

“Curación” de contenidos: más allá de la superficialidad.

Se entiende por “curación” de contenidos la búsqueda, selección y filtraje de información relevante, apoyándose en aplicaciones o programas que recopilen el contenido de mayor calidad o más adecuado a lo que pretendemos encontrar.

Ante la ingente cantidad de datos disponible en Internet, debemos buscar momentos de reflexión, filtraje de información y “curación” de contenidos para detectar y elegir lo más adecuado a lo que pretendamos trabajar.

Para ordenar y mejorar la localización de contenido adecuado para los NNA, el educador digital debe reflexionar al menos sobre los siguientes aspectos:

1. **Búsqueda.** Entendida como el adecuado conocimiento y uso de los distintos tipos de navegadores y su funcionamiento, tanto desde el punto de vista de recopilación de datos de los usuarios al utilizarlos, como en relación al tipo de resultados que ofrece, reconociendo las desviaciones de tráfico hacía páginas de publicidad o contenido engañoso.
2. **Selección.** Dado el ingente número de posibilidades que Internet ofrece ante una búsqueda de contenido de cualquier tema, el educador digital ha de entrenarse adecuadamente en la selección de los conceptos más próximos a lo que busca. Existen innumerables páginas y aplicaciones que ayudan a seleccionar lo que realmente se trata de identificar como útil.
    - Descubrir los temas fundamentales frente a los superfluos.
    - Clasificar y organizar el contenido que se localiza.
    - Decidir cómo puedo construir sobre el valor del contenido detectado.
    - Descubrir la mejor manera de compartirlo con los NNA.
3. **Filtrado.** Una vez que hemos seleccionado una serie de recursos, datos o definiciones de interés, debemos cribar y filtrar con carácter deductivo el material que nos interese trabajar o distribuir a los NNA. Seleccionando lo fundamental y las claves para transmitir como conocimiento o experiencia.
4. **Retroalimentación y reciclaje.** Los educadores digitales han de mantener una actitud de reciclaje constante, así como procurar localizar nuevos recursos o posibilidades en los medios digitales, empoderando a los NNA para que sean ellos los que realicen la enseñanza.

Fomento del trabajo en equipo

> "El talento gana partidos, pero el trabajo en equipo y la inteligencia ganan campeonatos".
>
> Michael Jordan

En el mundo actual, como educadores digitales debemos fomentar el trabajo en equipo y colaborativo, activo, democrático y participativo, donde el grupo supone la suma de las fuerzas individuales de cada persona.

El trabajo en equipo se puede definir por seis "Cs":

- Comunicación.
- Coordinación.
- Complementariedad.
- Confianza.
- Compromiso.
- Creatividad.

No olvidemos que el trabajo en equipo no es otra cosa que un conjunto de individuos realizando una tarea común para alcanzar resultados, con objetivos comunes, comprometidos con una relación de confianza y compromiso común.

Cuando conseguimos estos indicadores, el trabajo en equipo consigue crear un valor añadido a la actividad, generando beneficios como:

- Aumentar la motivación, implicando y motivando de mayor manera a los miembros del equipo.
- Reducir el estrés, al ser las responsabilidades compartidas.
- Reforzar la cohesión de capital humano, favoreciendo las relaciones interpersonales.
- Mejorar el clima, al aumentar los lazos personales y procurar un ambiente de trabajo más positivo.
- Potenciar la creatividad, al haber mayor capacidad de conexiones y retroalimentaciones.

Características de un equipo óptimo

Las 5 características que definen a un equipo que está trabajando de forma óptima son las siguientes:

- Estructura y claridad.
- Confianza.
- Propósito.
- Motivación.
- Seguridad psicológica.

6.2. Áreas de Competencia Digital Docente

Se describen a continuación las 5 áreas de la Competencia Digital Docente, con las principales características a tener en cuenta por el educador.

Información y Alfabetización informacional

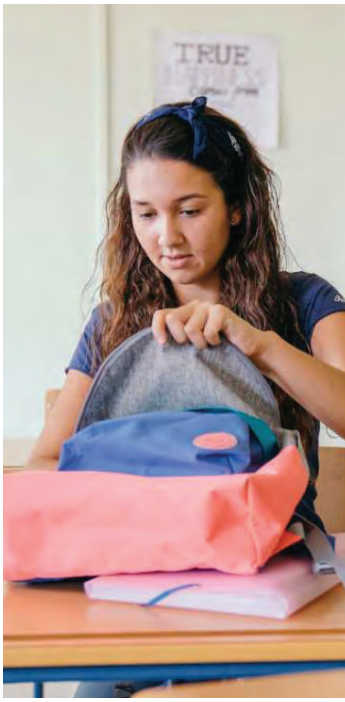
Se entiende como la capacidad de identificar, obtener, localizar, almacenar, organizar y analizar información digital, evaluando su finalidad y relevancia. Las competencias que se trabajan dentro de esta área son:

- Navegación, búsqueda y filtrado de información, datos y contenido digital: en esta dimensión la persona debe adquirir el conocimiento necesario para efectuar búsquedas efectivas y mostrar una actitud proactiva hacia la recensión de información.
- Evaluación de información, datos y contenido digital: el individuo adquiere el conocimiento de analizar la información que se obtiene, siendo capaz de manejar información dirigida al usuario y siendo crítico con la misma.
- Almacenamiento y recuperación de información, datos y contenido digital: en esta competencia se trabaja la importancia del almacenamiento y de la necesidad de realizar copias de seguridad.

Comunicación y colaboración

Es la capacidad de comunicarse en entornos digitales, compartir recursos por medios de herramientas en red, colaborar mediante instrumentos digitales, interaccionar y participar en comunidades y redes.

La *netiqueta* ayuda a estar acostumbrado al buen uso de las normas de conducta en interacciones en línea o virtuales, ser capaz de protegerse a sí mismo y a otros de posibles peligros en línea y desarrollar estrategias activas para la identificación de las conductas inadecuadas.



Creación de contenidos digitales

Es necesario conocer la elaboración de contenidos digitales, integración y relación de los mismos, derechos de autor y licencias y programación. El educador ha de tener una idea general de cómo funciona un software o ser capaz de aplicar configuraciones avanzadas a algunos programas.

Protección de información y datos personales, protección de la identidad digital, medidas de seguridad y uso responsable y seguro

Las competencias que se trabajan en el área de la protección de datos personales y de la identidad digital y de contenido digital, deben dirigirse a transmitir a los niños, niñas y adolescentes la importancia de proteger sus datos personales y su identidad digital.

Resolución de problemas

Es importante que el educador infiera la toma de decisiones más oportuna sobre las herramientas digitales necesarias desde el punto de vista creativo. Es importante dar posibles soluciones técnicas a los menores de edad por parte de los educadores.

Para finalizar, las áreas correspondientes a "Información y alfabetización informacional", "Comunicación y colaboración" y "Creación de contenidos digitales" abordan competencias específicas, mientras que las relativas a "Protección y seguridad" y "Resolución de problemas", se pueden considerar transversales a todas las áreas relacionadas con las nuevas tecnologías.

Para trabajar con las personas menores de edad

Con la sección de Materiales Didácticos de Internet Segura for Kids, se proponen recursos sobre diferentes temáticas con las que trabajar aspectos relativos a las competencias digitales que deben adquirir los niños, niñas y adolescentes.

Los materiales de trabajo incluyen unidades didácticas con sesiones de 50 minutos, presentaciones y actividades de larga duración, con información y orientaciones para realizar las distintas actividades.

Materiales Didácticos de IS4K

https://www.is4k.es/materiales-didacticos

Decálogo de uso seguro y responsable de Internet para la protección a la infancia

1. Fomentar el pensamiento crítico

Es necesario desarrollar su capacidad de crítica para discernir entre los contenidos a su alcance, identificar si son apropiados, o si se les está intentando manipular.

2. Proteger sus dispositivos y servicios

Tener un adecuado nivel de protección y configuración de los dispositivos y de la información que contienen es imprescindible para prevenir riesgos en Internet.

3. Crear una identidad digital positiva

Es fundamental que aprendan a proteger su información más sensible, construyendo una identidad digital positiva que refuerce su seguridad dentro y fuera de la Red.

4. La importancia de decir no

Es importante reforzar su confianza para decir no a las situaciones que les incomodan, o les puedan suponer un riesgo en el uso de

5. Uso equilibrado, supervisión y control

Desde la infancia es necesario ir promoviendo un uso equilibrado de Internet, con normas claras, medidas de supervisión y control, y fomentando contenidos positivos.

6. Aprender a actuar frente a un problema

Es fundamental conocer y utilizar los mecanismos de denuncia y bloqueo disponibles, y saber pedir ayuda. Los profesionales de servicios de protección a la

infancia han de disponer de pautas claras para afrontar las problemáticas relacionadas con Internet.

7. Gestionar la ciberseguridad

Los datos personales de NNA en muchos casos son especialmente sensibles. Se han de tratar y proteger adecuadamente para evitar daños a los menores de edad.

8. Mejorar la competencia digital

Debe existir el compromiso de colaborar y ayudar en los procesos educativos de los NNA, también en el medio digital, contribuyendo a su desarrollo e inclusión.

9. Recursos para menores de edad

La ciberseguridad es parte de su día a día. Para reforzarlo es útil trabajar de forma dinámica e interactiva con recursos atractivos como los Materiales Didácticos de IS4K.

10. Saber pedir ayuda

Ante un problema en línea, han de comunicarlo a un adulto de confianza. NNA y profesionales de servicios de protección a la infancia cuentan con apoyo gratuito y confidencial de la Línea de Ayuda en ciberseguridad de INCIBE (900 116 117).

900 116 117

Línea de ayuda EN CIBERSEGURIDAD

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta · protege tu empresa · is4k INTERNET SEGURA FORKiDS

Descarga la **Guía de uso seguro y responsable de Internet para profesionales de servicios de protección a la infancia** en: https://www.is4k.es/profesionales-infancia


DMR Consulting

is4k INTERNET SEGURA FORKiDS

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Observatorio Infancia

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA Y EMPRESA

GOBIERNO DE ESPAÑA
MINISTERIO DE SANIDAD, CONSUMO Y BIENESTAR SOCIAL