Política sobre un uso seguro y responsable del entorno digital y las redes sociales

ALDEAS
INFANTILES SOS

Política sobre un uso seguro y responsable del entorno digital y las redes sociales

1. Preámbulo

El contexto digital en el que se mueven los niños, niñas y adolescentes 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.

Por eso, este documento tiene el objetivo de desarrollar una política sobre un uso seguro y responsable del entorno digital y las redes sociales que contemple los factores de riesgo para los niños, niñas y adolescentes, y plantee una serie de recomendaciones para minimizarlos y favorecer un correcto uso, facilitando el trabajo preventivo de los educadores y de aquellos profesionales que acompañen de forma directa a los NNA.

Así mismo, este documento establece una serie de pautas para los empleados sobre el uso personal de sus redes sociales, poniendo el acento en aquellas acciones que quedan absolutamente prohibidas y resaltando otras que se pueden considerar inapropiadas. Estas pautas se exponen de forma clara y sencilla con el fin de facilitar su comprensión y su correcta aplicación.

Por último, el documento incluye un decálogo con una serie de recomendaciones para que todos y todas podamos proteger a la infancia y a la adolescencia de cualquier conducta negativa en el mundo online.

En definitiva, con esta guía, desde Aldeas Infantiles SOS España queremos sentar las bases sobre un uso seguro y responsable del entorno digital y de las redes sociales desde tres puntos de vista: el de la propia organización, el de los profesionales y el de los propios niños, niñas y adolescentes, con el objetivo de hacer de ellos verdaderos conocedores de la materia y de evitar cualquier comportamiento que pueda ponerles en riesgo.

2. Un entorno natural para la infancia y la adolescencia

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.

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.

3. Riesgos asociados a internet y recomendaciones para un uso seguro y responsable de niños, niñas y adolescentes

Las 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 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.

3.1 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.

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.

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. 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.

FACTORES DE RIESGO

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.

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.

RECOMENDACIONES

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. Por eso es fundamental anticiparse a lo que van a ver en internet y, 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.

PARA LOS EDUCADORES DE NUESTROS PROGRAMAS

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.

3.2 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.

FACTORES DE RIESGO

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.

En cualquier sistema o plataforma (también en los móviles) se pueden encontrar malware o 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.

RECOMENDACIONES

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.

- **Configuraciones seguras:** los principales servicios o plataformas online 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 necesario introducir la propia contraseña junto con un segundo código 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 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 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.

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; y solo pide permisos correspondientes a sus funcionalidades.

PARA LOS EDUCADORES DE NUESTROS PROGRAMAS

Nuestros programas disponen de equipos de uso compartido con conexión a internet, ya sean ordenadores, tabletas o móviles, por lo que 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 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. 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.

FACTORES DE RIESGO

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.

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 mayor o menor 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.

RECOMENDACIONES

Siguiendo unas 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.

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.

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 LOS EDUCADORES DE NUESTROS PROGRAMAS

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 organizaciones 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 nuestros programas:

- No es necesario el consentimiento firmado para autorizar el tratamiento de los datos, ya que está justificado dado la finalidad de los mismos. 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.

- 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.

3.4 BIENESTAR EN EL MUNDO ONLINE

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.

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. Por ejemplo, la curiosidad natural de los NNA 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.

FACTORES DE RIESGO

En internet o 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.

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 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.).

RECOMENDACIONES

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.

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 LOS EDUCADORES DE NUESTROS PROGRAMAS

Uno de los puntos críticos en el funcionamiento cotidiano de nuestros programas 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 los diferentes códigos y políticas de los que dispone la organización. Sin embargo, con un mero documento "administrativo" no se consigue nada. Los educadores han de conocer esos estándares y adaptarlos a la realidad de los programas.

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. Incluso se pueden desarrollar programas formativos en uso seguro y responsable de internet para el personal del centro y para los NNA

4. Uso institucional de las redes sociales

Aldeas Infantiles SOS cuenta con las siguientes pautas de estilo aplicables a las redes sociales (RRSS) con el fin de orientar, de forma sencilla y eficaz, la gestión, el mantenimiento y dinamización de las redes sociales corporativas de la organización, buscando una homogeneidad en los contenidos y estilo de estas. Unas pautas tanto para guiar a los encargados de la moderación de los canales sociales como para apoyarles en la generación de contenidos dentro de cada uno de los perfiles existentes.

Estas pautas nos permiten generar contenido de valor coherente, auténtico y continuo a través de todos los canales online de la organización y poner de manifiesto que las actividades que desarrollamos están basadas en nuestros cuatro valores: Compromiso, Confianza, Audacia y Responsabilidad.

Los canales de los que disponemos son los siguientes:

- Twitter: @AldeasEspaña
- FB: Aldeas Infantiles SOS de España
- Instagram: Aldeasinfantiles_es
- YouTube: Aldeas Infantiles SOS de España

Y estos son los principios que deben estar siempre presentes en todos los mensajes que publicamos (ya sean textos, imágenes o contenido audiovisual):

- El tratamiento que hacemos de la información se debe llevar a cabo de forma rigurosa, asegurando en todo momento que se preservan los derechos de la infancia. Por ejemplo, el derecho a la intimidad es vulnerado cuando se revela la identidad del niño o niña afectado o cuando se dan detalles sobre su lugar de residencia, centro educativo, círculo social o cualquier otra información que pueda desvelar su identidad.
- Salvaguardamos la imagen de los niños y las niñas de nuestros programas de protección y acogimiento familiar, y no incluimos ninguna imagen que permita su identificación.
- En todas nuestras publicaciones digitales intentamos publicar actividades de los niños y las niñas que rompan estigmas, en las que se vean empoderados y capaces.
- Siempre les mostramos con una imagen positiva, activa y de calidad, realizando actividades acordes a su edad.
- En los testimonios que ofrecemos de los niños, niñas y adolescentes, sus nombres son sustituidos por unos ficticios.
- Todas las imágenes/videos publicados de niños, niñas y adolescentes de otros países son descargados desde nuestra plataforma interna de imágenes (mediabox), que garantiza la protección de los derechos de imagen y de protección de datos de todos los niños y niñas.
- Favorecemos el derecho a la participación de los niños y las niñas, haciéndonos eco de sus mensajes y opiniones, para que tengan voz, y siempre velando por su privacidad.

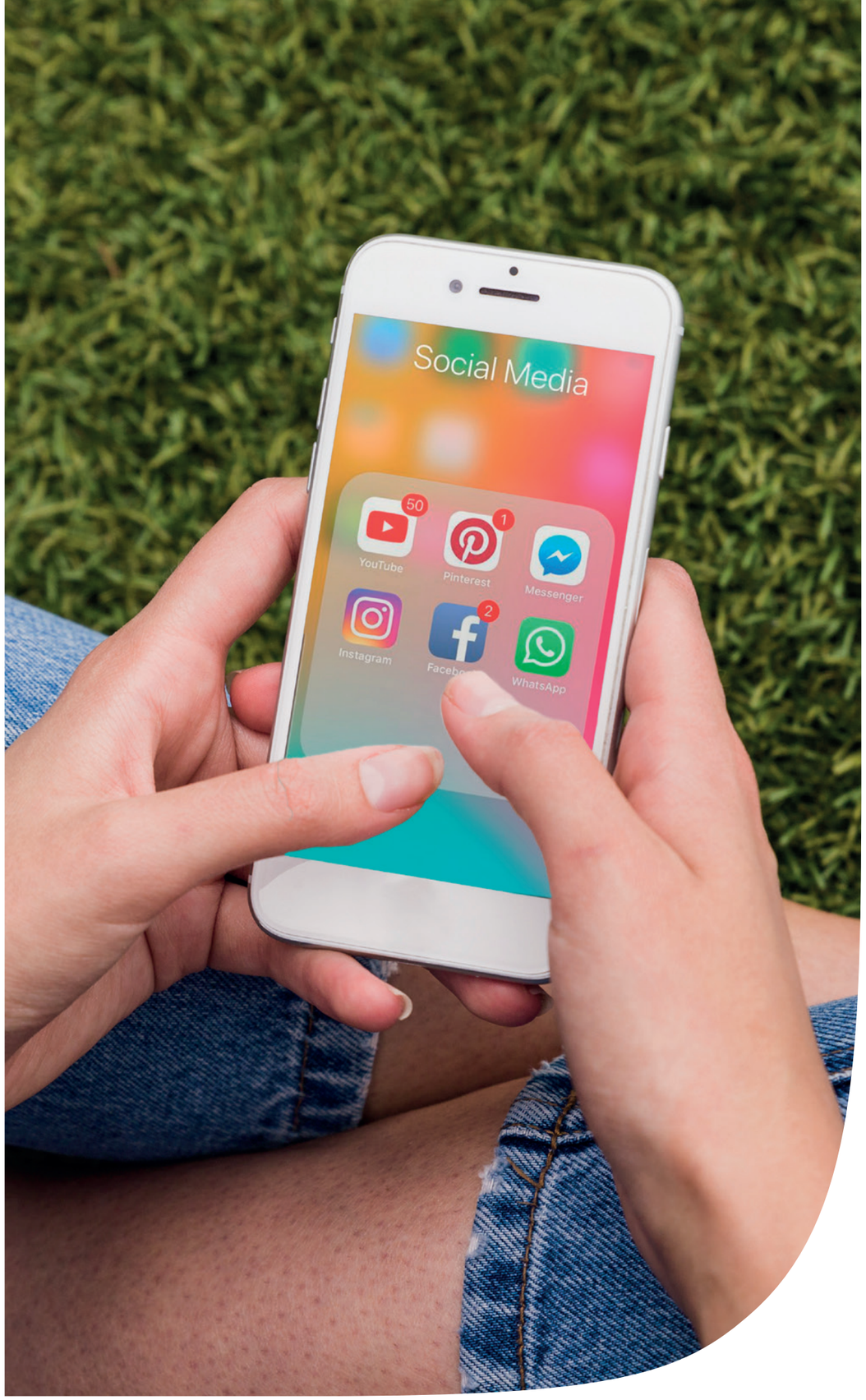
En relación a las comunicaciones de los distintos territorios y con el fin de velar por la coherencia de los mensajes, mantenemos una política interna en donde la coordinación se ejerce desde el departamento de Comunicación y Marketing. Es este departamento, por tanto, el encargado de marcar y definir aquellos contenidos aportados por territorios locales y/o departamentos externos que son válidos y óptimos para publicar en las redes sociales.

El proceso se desarrolla de la siguiente manera:

- El departamento de Comunicación y Marketing se reserva el derecho o la decisión final de publicación del contenido proporcionado por otras áreas o territorios de Aldeas Infantiles SOS.
- Igualmente se consultará previamente al departamento de Comunicación y Marketing sobre la publicación en redes de cualquier tipo de acuerdo con third parties para valorar su posible la publicación.
- El departamento de Comunicación y Marketing marcará los tiempos de publicación de todos los contenidos proporcionados por terceras partes.
- El departamento de Comunicación y Marketing elaborará y decidirá el plan de acción que marcará las redes mensualmente, priorizando siempre las acciones marcadas en el calendario editorial del departamento.
- Se dará difusión de una iniciativa empresarial siempre y cuando la comunidad general pueda participar activamente y podamos llegar a captar/fidelizar con ella.
- Las colaboraciones locales podrán tener (previa valoración) una campaña con segmentación de público objetivo.
- Se podrá compartir información de otros usuarios siempre y cuando sea útil y aporte información interesante.

El objetivo principal es posicionar de la manera más óptima a Aldeas Infantiles SOS en los canales sociales para dar a conocer su labor. Igualmente, las publicaciones cumplirán con otros objetivos:

- Demostrar a nuestros públicos que somos coherentes con nuestros valores de compromiso, confianza, audacia y responsabilidad.
- Aumentar el número de donaciones y socios para la organización.
- Participar en un diálogo activo con nuestros grupos de interés y realizar un seguimiento proactivo de sus cuentas.
- Compartir el trabajo “desde dentro”, ponerle cara a la organización y dar valor a los resultados obtenidos.
- Mostrar la labor que hacemos, demostrar nuestra experiencia y los resultados que logramos, tanto en el entorno local, nacional e internacional.
- Participar en conversaciones sobre el tercer sector siempre que sea posible, para alcanzar posibles usuarios dentro de este entorno, y que aún no nos conozcan, o identifiquen como un actor relevante en él.
- El tono de comunicación será siempre el mismo para todas las redes y publicaciones. Siguiendo siempre el calendario editorial marcado por el departamento de Comunicación y Marketing.



5. Pautas para los empleados sobre el uso personal de sus redes sociales

Los empleados podrán hacer uso de sus cuentas personales para difundir la labor de Aldeas Infantiles SOS siempre y cuando dejen claro en su perfil que se trata de cuentas personales y que en ningún caso hablan en nombre de la organización.

Está absolutamente prohibida la utilización del nombre y la imagen de la organización (logotipo, mensajes, campañas…) desde perfiles ajenos a los oficiales. También está prohibida la publicación de imágenes de los niños, niñas y adolescentes de nuestros programas sin previa autorización por parte de la organización y de los propios menores de edad.

Recomendaciones de uso de las redes sociales para trabajadores:

En Aldeas Infantiles SOS somos conscientes que, hoy en día, la comunicación de cualquier organización no puede plantearse sin tener en cuenta las redes sociales, siempre y cuando sean utilizadas correctamente para evitar los potenciales problemas derivados de su mal uso. En consecuencia, todos los trabajadores de Aldeas deben usar el sentido común en sus comunicaciones a través de las redes, teniendo presentes la confidencialidad y la lealtad a la compañía.

A efectos de esta política, entendemos por redes sociales todas las publicaciones y comentarios online en webs, portales, blogs, páginas y grupos en portales como LinkedIn, Twitter, Facebook, YouTube, Instagram, Flickr, Snapchat, etc.

Como empleado de Aldeas Infantiles NO se deben usar las redes sociales para:

- Difundir información corporativa (confidencial o no), es decir, publicar/compartir datos de la compañía en ningún formato (fotos, textos, vídeos, etc.), sin la autorización previa del departamento de Comunicación y Marketing de Aldeas Infantiles SOS.
- Difundir información (confidencial o no), es decir, publicar/compartir datos de ningún usuario que nos contacte en ningún formato (fotos, textos, vídeos, etc.), sin la autorización previa por escrito de dicho usuario.
- Participar en cualquier actividad o revelar información que desacredite o pueda perjudicar a la compañía.
- Atacar o abusar de usuarios de la red, clientes, proveedores, compañeros u otros trabajadores de Aldeas Infantiles SOS. Los empleados deben comunicarse siempre con educación y respeto, siendo profesionales.
- Publicar comentarios o enviar mensajes anónimos o con pseudónimos. Los empleados deben usar siempre su nombre real e identificarse como trabajadores de la compañía.
- Crear un grupo, página, blog, etc. que mencione a Aldeas Infantiles SOS, sin la aprobación previa del departamento de Comunicación y Marketing de la organización.
- Usar las redes sociales de forma que interfieran en el normal desarrollo de tu trabajo en la compañía.
- Mostrar comportamientos, actitudes y afinidades políticas o religiosas que puedan comprometer la imagen de la organización, que se declara públicamente “interconfesional e independiente de toda orientación política”.

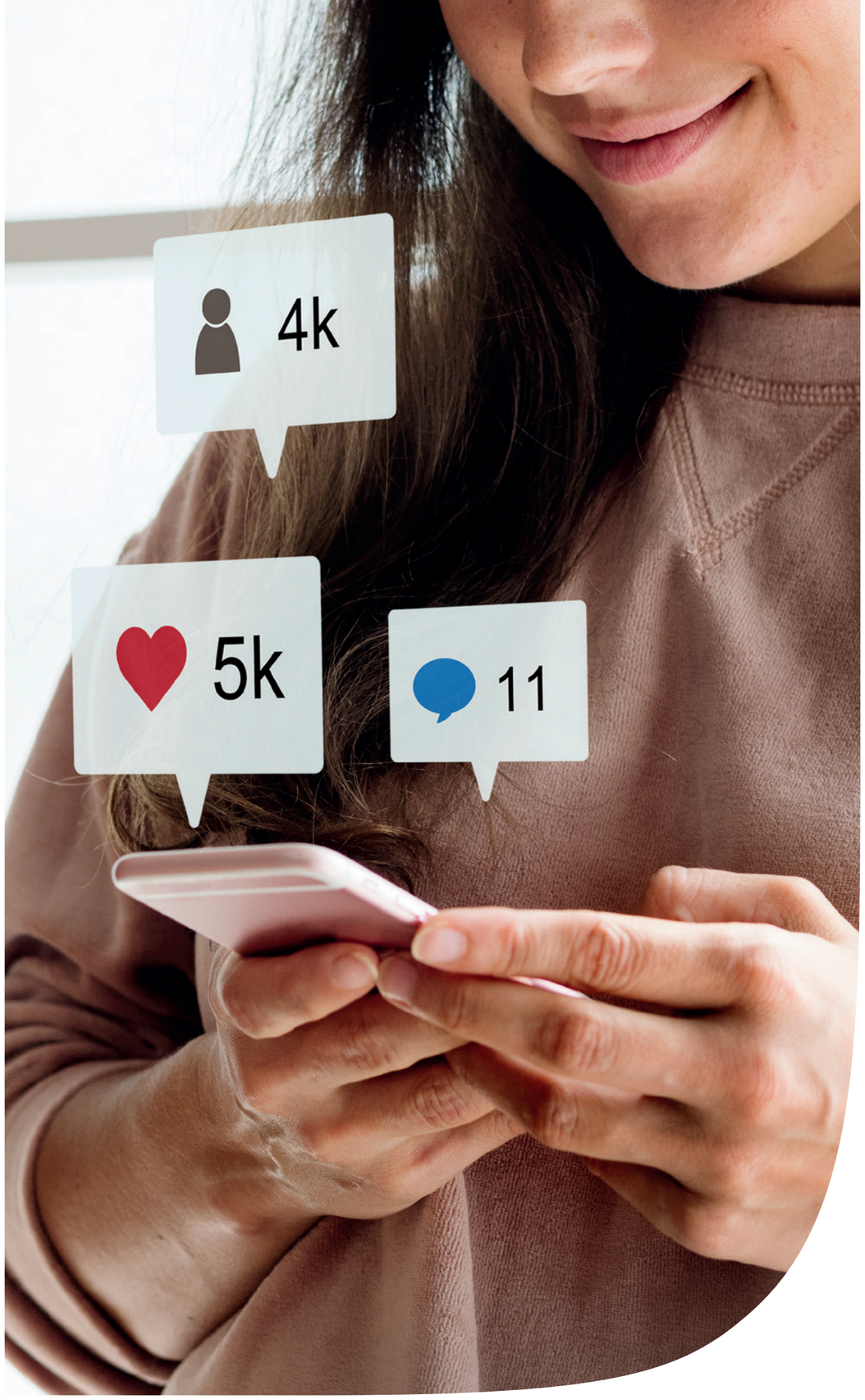
Cabe recordar que el Código de Conducta de Aldeas Infantiles SOS, en su apartado 7.5 relativo al "Uso de redes sociales", explica claramente cómo hacer un uso razonable de las mismas:

7.5. Uso de redes sociales

Las redes sociales nos ofrecen la posibilidad de estar conectados con familia, amigos y contactos profesionales, de compartir información y actualidad y establecer nuevos vínculos con personas y grupos con intereses afines. Las redes sociales suponen una excelente herramienta de comunicación pues informan sobre nuestra misión y actividades, posicionándonos sobre temas y acontecimientos de relevancia actual. Sin embargo, esta gran oportunidad conlleva una importante responsabilidad, ya que nuestras acciones individuales tienen repercusiones en la imagen corporativa de la Organización.

Por lo tanto, como empleado/voluntario/colaborador cumpliré unas normas básicas a la hora de participar en las redes:

- *Respetaré las normas de privacidad y protección de datos personales. Las leyes de protección de datos deben ser respetadas con el mismo rigor en las redes sociales que en las comunicaciones profesionales.*
- *Separaré el ámbito personal y profesional.*
- *Se debe evitar el uso de imágenes y logos referentes a la Organización en cuentas o publicaciones personales, ya que puede llevar a la confusión al interpretar mensajes personales como institucionales.*
- *Respetaré el papel de los portavoces y los procedimientos de comunicación externa y de atención a los donantes.*
- *Respetaré los criterios de comunicación interna y externa de la Organización.*



6. Decálogo de uso seguro y responsable de internet

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 las redes sociales y el entorno digital.

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.

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).

BIBLIOGRAFÍA

La presente publicación se ha nutrido de la ***Guía de uso seguro y responsable de Internet para profesionales de servicios de protección a la infancia***, publicada por el INCIBE y la Iniciativa Internet Segura for Kids, IS4K (https://www.incibe.es y https://www.is4k.es) y el Observatorio de la Infancia (https://www.observatoriodelainfancia.mscbs.gob.es).

aldeasinfantiles.es

@aldeasespana

Aldeas Infantiles SOS de España

www.youtube.com/user/AldeasInfantiles

aldeasinfantiles_es

ALDEAS
INFANTILES SOS