INSTITUTO NACIONAL DE CIBERSEGURIDAD

Ciberseguridad para familias

(con menores en edad escolar)

Guion presentación

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

INSTITUTO NACIONAL DE CIBERSEGURIDAD

INTERNET SEGURA FORKiDS

Guion para charlas sobre ciberseguridad para familias

Este guion se ha desarrollado para servir como referencia a los ponentes que utilicen la presentación "Ciberseguridad para familias (con menores en edad escolar)".

Los [textos entre corchetes] corresponden a notas aclaratorias sobre la organización, adaptación y desarrollo de la sesión.

Los textos normales corresponden a los mensajes clave e ideas a transmitir a las personas participantes.

Los (textos entre paréntesis) corresponden a aclaraciones o explicaciones ampliadas en cuestiones que pueden ser relevantes, por ejemplo, para responder a una pregunta.

La presentación incluye mensajes breves y directos, acompañados de imágenes decorativas/aclaratorias para captar la atención de padres y madres, de modo que la persona que imparte la presentación amplíe las explicaciones adecuándose al grupo.

Esta sesión se enfoca tanto al conocimiento de los diferentes riesgos de la tecnología e Internet, como al apoyo de las familias para que puedan desempeñar una mediación parental activa y eficaz, dado que esta es su mejor herramienta para apoyar a sus hijos/as en un uso seguro y responsable de Internet.

En cuanto a los riesgos no se trata de escandalizar a las familias, sino escuchar sus inquietudes en materia de ciberseguridad y menores, partir de sus conocimientos y experiencias, para complementarlas y mejorar su perspectiva en este ámbito. El objetivo es que puedan ser más eficaces a la hora de detectar tempranamente o resolver un incidente en línea.

Asimismo, es fundamental rebatir la extendida idea de que "eso a mi hijo/a no le va a pasar" (baste reflexionar brevemente sobre algunos datos: según el estudio Net Children Go Mobile[1], un 18% de los menores se habían sentido molestos por algo sucedido en Internet, un 32% había sufrido bullying, un 31% había recibido mensajes sexuales de algún tipo, un 21% había contactado en línea con personas desconocidas, un 32% había visto contenidos inapropiados y potencialmente dañinos, etc.).

Se puede decir que nuestro objetivo es implicar a las familias en la educación digital de sus hijos/as. Sin embargo, la forma de concretar esta labor puede variar notablemente según la edad y el grado de madurez de cada menor. Desde un acompañamiento continuo, en un entorno acotado, para progresivamente ir ganando autonomía,

[1] Garmendia, M. Jiménez, E., Casado, M.A. y Mascheroni, G. (2016). Net Children Go Mobile: Riesgos y oportunidades en internet y el uso de dispositivos móviles entre menores españoles (2010-2015). Madrid: Red.es/Universidad del País Vasco/Euskal Herriko Unibertsitatea (https://netchildrengomobile.eu/ncgm/wp-content/uploads/2013/07/Net-Children-Go-Mobile-Spain.pdf).

demostrando responsabilidad, hasta desenvolverse libremente en Internet, con una supervisión basada en el diálogo y la confianza.

Por este motivo puede ser buena idea comenzar la presentación preguntando a las familias por las edades de sus hijos/as, de modo que nos sirva de orientación para adaptar nuestra exposición.

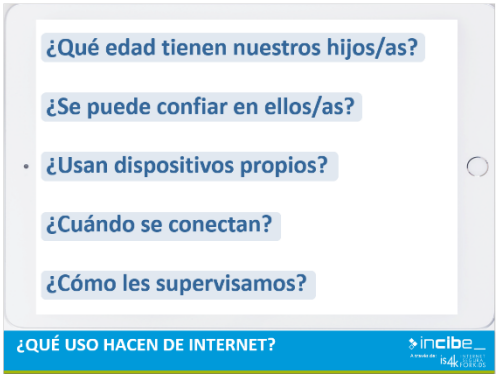
1. Introducción

Diapositiva 1.

[Antes de iniciar la sesión, tratamos de mostrar la presentación a pantalla completa con esta primera diapositiva.]

Vamos a comenzar esta sesión sobre ciberseguridad y uso seguro y responsable de Internet dirigida a familias con menores en edad escolar.

Diapositiva 2. ¿QUÉ USO HACEN DE INTERNET?



Para empezar, vamos a comprobar si sabemos ¿qué uso hacen nuestros hijos/as de Internet?

[Puede ser buena idea hacer algunas preguntas a las personas participantes para contextualizar la presentación, especialmente si hay rangos de edades similares.]

¿Cuáles son las edades de sus hijos/as? ¿Se puede confiar en ellos/as (son responsables y maduros)? ¿Qué dispositivos utilizan (son suyos propios o de la casa)? ¿Cuándo y desde dónde se conectan? ¿Hablan con ellos/as de lo que hacen en Internet? ¿Cómo les supervisan?

[Les animaremos a responder a estas preguntas, dejando abierta la posibilidad de que vayan comentando de forma natural sobre sus intereses y hábitos en línea.]

Diapositiva 3. ¿QUÉ USO HACEN DE INTERNET?

[Completando la introducción, tanteamos al grupo en cuanto a su experiencia en torno a Internet y la tecnología.]

Algunos menores utilizarán una tableta común de la familia o nos pedirán nuestro móvil, mientras que otros ya tendrán su propio dispositivo. Pero en todo caso, para ellos/as se trata de divertirse y pasar un buen rato con Internet, ya sea escuchando música, viendo vídeos, películas y series, jugando en línea, charlando con sus amigos/as, aunque también lo utilizan para conocer gente, ligar o encontrar pareja.

¿Reconocemos (los iconos) las apps (aplicaciones) de este teléfono?

[No se trata de describir una a una, sino ver si a los padres y madres les suenan, las conocen o no, ya que son una pequeña selección de apps representativas de los principales usos de los menores]

(En la primera fila tenemos contenido de música, vídeo, películas y series (aunque también encontramos programas educativos y tutoriales): “YouTube Kids” y “Netflix”.

En la segunda fila están dos juegos: “Salón de uñas Hello Kitty” y “Fortnite”.

A continuación, dos redes sociales: “Instagram” y “Snapchat”.

En la última fila la red social “Tik tok” (antigua musical.ly), y la app para ligar “Tinder”.)

Diapositiva 4. ¿CONOCEMOS A SUS AMIGOS/AS?

Igual que nos preocupamos por conocer a sus amigos/as en persona, también hemos de estar al tanto de sus contactos en línea:

Sabemos cuántos amigos/as tienen en persona, les conocemos, pero… ¿sabemos cuántos contactos tienen en sus cuentas de redes sociales o juegos en línea?, ¿les conocemos a todos/as?

Como veremos más adelante, es importante ser conscientes que no nos podemos fiar de alguien con quien solo nos relacionamos por Internet, no es un amigo/a "de carne y hueso".

Diapositiva 5. RIESGOS QUE SE PUEDEN PREVENIR

[Se muestra un par de noticias de ejemplo, con el propósito de preguntar a las personas asistentes y ver su nivel de concienciación y alarma ante los riesgos en línea:

Los adolescentes entre 11 y 14 años son los más acosados por internet en España (ABC Tecnología) https://www.abc.es/tecnologia/abci-adolescentes-entre-11-y-14-anos-representan-mayor-tasa-ciberacoso-201707261422_noticia.html

Una niña de 9 años, en rehabilitación por su adicción al videojuego 'Fornite' (El País Mamás y Papás) https://elpais.com/elpais/2018/06/11/mamas_papas/1528706334_714292.html

Las imágenes correspondientes tienen enlace a la noticia completa, por si se considera relevante profundizar en la exposición.]

Diapositiva 6. RIESGOS QUE SE PUEDEN PREVENIR

[Detenido un acosador de 69 años en Valladolid por intentar concertar citas sexuales con menores (El Mundo) https://www.elmundo.es/espana/2017/11/14/5a0b189922601dfa0f8b45ab.html

El 'sexting' se expande entre los adolescentes (La Vanguardia) https://www.lavanguardia.com/vida/20180317/441574135083/sexting-adolescentes-sexts.html

Las imágenes correspondientes tienen enlace a la noticia completa, por si se considera relevante profundizar en la exposición.]

Vemos algunas noticias sobre menores y sus problemas con Internet. ¿Son algo extraordinario en los medios de comunicación, o tenemos la sensación de que este tipo de noticias aparecen con cierta frecuencia?

¿Qué riesgos o problemas en línea son los que más aparecen en las noticias?, ¿y los que más afectan a los menores en su día a día?

[Pueden surgir como temáticas el ciberacoso o ciberbullying, acoso sexual/grooming, uso excesivo, captación hacia comunidades peligrosas (hábitos poco saludables, sectas, grupos violentos, etc.), la difusión no deseada de información privada (por ejemplo, imágenes originadas en un sexting), el cibercontrol, noticias falsas, fraudes, virus…]

A continuación, entramos más en detalle en algunos de los riesgos más relevantes para los menores.

2. Descripción de riesgos y consejos

CONTENIDOS INAPROPIADOS

Diapositiva 7. ACCESO A CONTENIDOS INAPROPIADOS

No todo lo que vemos en Internet es apropiado para todas las personas, ya sea por su sensibilidad o grado de madurez.

En el caso de los menores conviene que consuman únicamente contenidos dirigidos específicamente para ellos/as, que se adecúen a su edad y madurez. Adelantarnos a su desarrollo con contenidos dirigidos a otras edades puede tener consecuencias, desde simplemente no entender el contenido, hasta asumir como ciertas creencias erróneas, sentirse perturbado/a o angustiado/a. Un mensaje que puede ser útil reforzar en los menores es el de la paciencia, valorando que cada cosa tiene su momento.

No se trata solo de prohibir o limitar los contenidos, ya que esto incrementaría su curiosidad, y podría tener el efecto contrario al deseado. Hemos de explicar y razonar los motivos, además de ofrecer contenidos alternativos que resulten adecuados para ellos/as, e incluso sean positivos para su desarrollo.

Por último, recordemos que en muchas ocasiones los menores no buscan contenidos inapropiados en Internet, sino que otras personas les envían material dañino (peligroso para la salud, promoción de la violencia, etc.) a través de mensajería instantánea o redes sociales. Es fundamental cortar su difusión, evitando darles me gusta, compartirlos o reenviarlos.

[Enlace de interés: https://www.is4k.es/necesitas-saber/contenido-inapropiado]

PRIVACIDAD, IDENTIDAD DIGITAL Y REPUTACIÓN EN LÍNEA

Diapositiva 8. PENSAR ANTES DE COMPARTIR

Cuando hablamos de redes sociales, de la web 2.0 o de las páginas en Internet en las que podemos opinar y colaborar, hay una premisa que es fundamental: PENSAR ANTES DE COMPARTIR. Una vez enviado algo puede ser imposible borrarlo, no sabemos hasta dónde se puede difundir, ni qué pueden llegar a hacer con ello ni nuestros contactos, ni otras personas que ni siquiera conocemos.

Así pues, los menores no deben compartir ninguna información que pueda ponerles en riesgo, ni a ellos/as ni a otras personas, como datos personales, nombre real, teléfono, dirección, lugares a los que se acude (centro educativo, extraescolares, rutinas), etc.

[Enlace de interés: https://www.is4k.es/necesitas-saber/privacidad]

Diapositiva 9. SI SE COMPARTE, NO SE PUEDE CONTROLAR

Como decíamos, una vez enviado (compartido) un mensaje o una foto, ya no depende de nosotros mismos. Las personas que lo hayan recibido pueden a su vez guardarlo y compartirlo con otras personas, quienes pueden a su vez repetir esta dinámica. Así pues, ese mensaje o esa foto le puede acabar llegando a muchas personas con las que no se contaba.

Por este motivo, es especialmente relevante fomentar en los menores el valor de su intimidad. Un desarrollo saludable de su sociabilidad implica también el respeto a un espacio privado de intimidad. No tienen por qué compartir toda su vida, las cuestiones más privadas, personales o sensibles con nadie.

A la hora de compartir un contenido (ya sea propio o algo que hayan visto o recibido), han de reflexionar primero sobre si alguien podría utilizarlo en su contra (por ejemplo, ese comentario sarcástico se puede malinterpretar, y otras personas que no me conocen pueden pensar equivocada y negativamente sobre mí).

En cuanto al uso de Internet entre menores en pareja o que están explorando una relación afectiva, aplica la misma norma de sentido común que fuera de la red: el amor implica respeto. Respeto por uno/a mismo/a, para quererse, valorarse y ser libre de elegir lo que quiere hacer en cada momento. Y también respeto por la otra persona, para ponerse en su piel, comprenderla y no presionarle ni chantajearle para que haga algo que no se desea.

Así pues, los menores deben ser conscientes del riesgo que implican situaciones típicas, como cuando se piden y/o envían imágenes íntimas (sexting). Aunque inicialmente confíen en la otra persona, se pueden distanciar, se las puede enseñar o enviar a otras personas, alguien le puede coger el móvil en un despiste, etc. Está claro que son un tipo de contenidos sensibles que pueden traer repercusiones negativas para los menores, por lo que lo mejor es que no los creen, ni los compartan.

[Enlace de interés: https://www.is4k.es/necesitas-saber/sexting]

Diapositiva 10. CUIDAR SU IMAGEN PÚBLICA

Lo que se comparte en Internet puede permanecer durante mucho tiempo, y puede llegar a cualquier persona. Por eso deben cuidar su imagen pública, de forma que lo que comparten no les limite o dificulte su desarrollo personal y profesional en el presente o en el futuro (por ejemplo, compartir unas fotos inapropiadas en redes sociales, puede luego influir negativamente en un proceso de selección de personal).

Paralelamente, es conveniente limitar el alcance de sus publicaciones en redes sociales configurando sus opciones de privacidad (por ejemplo: estableciendo su cuenta como privada, evitando la publicación automática de imágenes en las que se les etiqueta, evitando el acceso a su información desde los buscadores, etc.).

RELACIONES SALUDABLES EN LÍNEA (CIBERACOSO, GROOMING, COMUNIDADES PELIGROSAS)

Diapositiva 11. UN CONTACTO EN LÍNEA NO ES UN AMIGO/A

En Internet es muy fácil parecer alguien que no se es. Se pueden elegir las fotos en las que nos mostramos, retocarlas, e incluso utilizar otras que no sean las nuestras. Podemos decir que somos de una ciudad, o de otra, que nos gustan unas cosas u otras, sin que se pueda comprobar. Así pues, es muy fácil hacerse pasar por otra persona.

Cuando charlamos o jugamos en línea con alguien, realmente no sabemos quién es la persona que está efectivamente al otro lado de la pantalla, si es o no como nos dice ser. Cuando ya llevamos un tiempo en contacto, podemos tener una falsa sensación de familiaridad e incluso confianza. Si no conocemos previamente a la otra persona, esta podría estar engañándonos [como por ejemplo veremos a continuación].

[Enlaces de interés: https://www.is4k.es/necesitas-saber/grooming

https://www.is4k.es/necesitas-saber/comunidades-peligrosas]

Diapositiva 12. DESCONOCIDOS CON MALAS INTENCIONES

Por supuesto que no todas las personas con las que nos cruzamos por Internet tienen malas intenciones, pero es una realidad que en Internet hay pederastas que tratan de ganarse la confianza de un menor para chantajearle sexualmente, personas que tratan de obtener material comprometido para extorsionarles económicamente, o que tratan de captar a menores para comunidades peligrosas (por ejemplo, hábitos alimenticios poco saludables, prácticas de riesgo para la salud, grupos sectarios, violentos, etc.).

En la diapositiva vemos una secuencia de imágenes extraídas del vídeo de Europol para su campaña Di no (Say No) al acoso sexual y la extorsión de los menores en línea.

En estas imágenes podemos ver de forma resumida la secuencia de pasos con los que se van ganando la confianza de un menor:

- Solicitud de amistad: es alguien desconocido, pero con un perfil atractivo para el menor. Incluso puede tener amigos/as en común (quienes tampoco le conocen).
- Confianza: chateando a lo largo del tiempo parece alguien cercano, con afinidad y que valora y quiere al menor.
- Material comprometido: puede ir subiendo de tono la conversación, llevándola a temática sexual y pidiendo alguna foto o conectar la webcam.
- Chantaje: en cuanto tiene en su poder algún tipo de material comprometido, inicia un chantaje en busca de más material, dinero o encuentros personales.

[Si se tiene tiempo disponible, puede ser útil visualizar el vídeo, que está enlazado desde la diapositiva, Campaña Di No (Europol) https://www.youtube.com/watch?v=_whpii1co1g (10:34 minutos), en lugar de explicar las imágenes. En ese caso, resaltar que en el vídeo se entremezclan dos historias, la de un grupo organizado para extorsionar económicamente, y la de un pederasta que se gana la confianza de los menores para chantajearles sexualmente (grooming)

Otros vídeos interesantes en esta temática podrían ser:

Grooming ¿Sabes con quién quedan tus hijos a través de Internet? (Orange España) https://www.youtube.com/watch?v=OetekyrQj-k

Love Story (Movistar) https://www.youtube.com/watch?v=o3zbPAT0DuQ

Campaña prevención Grooming (PDI Chile) https://www.youtube.com/watch?v=c1dEKmA8vVw]

Diapositiva 13. SE PUEDE PARAR EL CIBERACOSO

Uno de los problemas que más sensibilidad despierta hoy en día entre la ciudadanía es el ciberacoso a menores. Se trata de un daño repetido e intencional contra un menor utilizando las tecnologías. Aunque en ocasiones se trate como algo menor, bromas sin importancia, no es así, ya que puede tener serias consecuencias. Todos, familias, menores y profesorado hemos de implicarnos para parar el ciberacoso.

En casa hemos de reforzar el papel activo de nuestros hijos. Quienes presencian el ciberacoso tienen más poder del que creen para pararlo. Lo primero es evitar dar me gusta o compartir mensajes humillantes. Apoyar a las víctimas (aunque sea en privado) para que se sientan acompañadas. Y es fundamental pedir ayuda a una persona adulta de confianza (padres, profesores).

La mejor clave que podemos transmitir a los menores es que en Internet compartan solo mensajes positivos, y sean respetuosos con todo el mundo.

[Enlaces de interés: https://www.is4k.es/necesitas-saber/ciberacoso-escolar]

USO EXCESIVO DE INTERNET

Diapositiva 14. DETECTAR Y EVITAR UN USO EXCESIVO

Una de las preocupaciones habituales en las familias es el uso excesivo de la tecnología por parte de los menores. El mejor camino para afrontar esta problemática es la prevención. Para ello se han de fijar en el hogar unas normas de uso de móviles, tabletas, ordenadores, videoconsolas… Si se consensuan entre padres e hijos, será más probable que se vayan cumpliendo.

Además, es útil promover entre los menores otras alternativas a las tecnologías, como por ejemplo el deporte, la naturaleza, dedicar tiempo a las amistades, la lectura, etc.

Aun así, es posible caer en una situación de uso excesivo. Para darnos cuenta podemos fijarnos en algunas señales de alerta como, por ejemplo, cuando el deseo de utilizar el móvil o jugar a la videoconsola provoca una alteración en sus relaciones con la familia, las amistades (más aislamiento), el abandono de sus responsabilidades escolares o domésticas (cambios en rutinas), se muestra más irritable, etc. En caso de dudas, conviene pedir ayuda en su pediatra, departamento de orientación del centro educativo y la Línea de Ayuda de Ciberseguridad de INCIBE 017.

[Enlace de interés: https://www.is4k.es/necesitas-saber/uso-excesivo-de-las-tic]

3. Medidas a aplicar en el ámbito familiar

TRABAJAR LA CIBERSEGURIDAD DESDE EL ÁMBITO FAMILIAR

Diapositiva 15. LA CLAVE: LA MEDIACIÓN PARENTAL

[Entramos en un nuevo bloque de la presentación, centrándonos ahora en cómo trabajar la ciberseguridad en el ámbito familiar.]

Para empezar, destacamos la principal clave para ello: la mediación parental. Podemos definirla como la implicación de las familias en la supervisión, acompañamiento y orientación de los menores para un uso seguro y responsable de Internet.

Esta implicación ha de partir del convencimiento personal, de nuestra responsabilidad hacia nuestros hijos/as. No se trata de convertirnos en expertos en las tecnologías, sino de estar al tanto del entorno en el que se desenvuelven, conocer sus actividades y amistades en línea, ponerse al día sobre los riesgos de Internet y cómo tratarlos.

Es fundamental saber escucharles para reconocer sus necesidades y preocupaciones, y así poder ayudarles a afrontar dificultades y problemas. Tanto el sentido común, como nuestra experiencia vital serán nuestros mejores aliados (al fin y al cabo, que alguien les insulte en línea, no deja de ser un insulto).

Enlace de interés: https://www.is4k.es/necesitas-saber/mediacion-parental https://www.is4k.es/de-utilidad/recursos/guia-de-mediacion-parental]

Diapositiva 16. IMPRESCINDIBLE: EL ACOMPAÑAMIENTO.

[Se incluye un vídeo que se puede visualizar con conexión a Internet. En este vídeo de IS4K se ofrecen algunas recomendaciones para que las familias aprendan a implicarse y acompañar a sus hijos/as en el proceso de aprender a usar Internet de forma segura.

Dependiendo de los participantes o el tiempo disponible se pueden visualizar otros vídeos

incluidos en el anexo de este guion. De igual forma, es posible saltar esta diapositiva si no resulta conveniente su reproducción.]

Tenemos claro que queremos implicarnos en esta parte tan importante de su formación, pero ¿por dónde empezar? Puede que nos veamos desbordados por esta tarea, pero en el fondo los mensajes que debemos transmitir a los menores son los mismos que los de la 'vida real'. Tan solo hay que adaptarse al nuevo medio de relación y comunicación que supone Internet.

(Enlace al vídeo: https://www.youtube.com/watch?v=fuchWXz4m10)

Diapositiva 17. LA MEJOR SUPERVISIÓN: EL DIÁLOGO

Lógicamente no es lo mismo un niño/a pequeño/a que un adolescente, por lo que deberemos adaptar nuestro acompañamiento y supervisión al momento y grado de madurez en que se encuentren nuestros hijos/as. En todo caso, la mejor herramienta a nuestro alcance para supervisar su actividad, prevenir problemas y detectarlos lo antes posible es el diálogo. Es suficiente con que los minutos que dedicamos a hablar distendidamente con ellos/as sobre su día en el cole, instituto, etc., les preguntemos también sobre lo que han estado haciendo en la red, su último juego, con quién han estado chateando, etc.

De manera complementaria (nunca sustituyendo al diálogo personal), es posible apoyarse en una herramienta de control parental. De este modo se puede limitar el acceso a la red (permitir a unas horas, pero no a otras, a unos sitios web sí, pero a otros no, prohibir búsquedas que incluyan ciertas palabras clave, etc.), supervisar su actividad en línea (obtener informes periódicos y alertas puntuales con el tiempo de uso, las aplicaciones utilizadas, el historial de navegación…), controlar tiempos de uso (bloquear el dispositivo o una aplicación pasado un cierto límite de tiempo), etc.

Diapositiva 18. IMPRESCINDIBLE: EL ACOMPAÑAMIENTO

Es imprescindible acompañar a nuestros hijos/as en el uso de Internet a fin de poder aprender juntos a disfrutarlo de manera segura. Se trata de un aprendizaje para ambas partes, pues ellos/as verán en nosotros una guía o modelo a seguir (por ejemplo, cómo reaccionamos ante un problema, de qué resultados de búsqueda nos fiamos más, cómo gestionamos la publicidad, etc.), pero nosotros también comprenderemos mejor el entorno en el que se mueven (qué aplicaciones y actividades están de moda, con quiénes se relacionan, cómo se exponen en la red, etc.).

Lógicamente nuestro acompañamiento tendrá que adaptarse paulatinamente a sus necesidades y grado de madurez y autonomía. Con los/as más pequeños deberemos estar a su lado cada vez que se conecten, para poco a poco ir ayudándoles a crecer en responsabilidad, ganar en autonomía, e ir acompañándoles de forma más ocasional (por ejemplo, navegando juntos de vez en cuando, pidiéndoles que nos enseñen a utilizar una nueva app, juego, etc.).

Diapositiva 19. IMPRESCINDIBLE: EL ACOMPAÑAMIENTO.

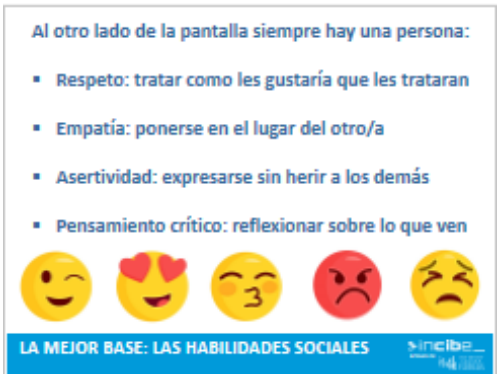
[Se incluye un vídeo que se puede visualizar con conexión a Internet. En el vídeo se representa una escena en la que un menor, mientras juega en Internet, se ve interrumpido por contenidos publicitarios que no sabe cómo manejar. Con un adulto a su lado, aprenderá cómo prevenir riesgos.

Dependiendo de los participantes o el tiempo disponible se pueden visualizar otros vídeos incluidos en el anexo de este guion. De igual forma, es posible saltar esta diapositiva si no resulta conveniente su reproducción.]

Aprender a usar Internet de forma segura es un proceso que requiere tiempo y ayuda por parte de un adulto. Así aprenderán cómo enfrentarse a los riesgos, cómo identificarlos y cómo reaccionar.

(Enlace al vídeo: https://www.youtube.com/watch?v=d5kW4pI_VQw)

Diapositiva 20. LA MEJOR BASE: LAS HABILIDADES SOCIALES



En todo momento hemos de recordar y recordarles que al otro lado de la pantalla siempre hay una persona (en un juego en línea, una conversación en redes sociales, un equipo de desarrolladores de una app…), de modo que les ayudemos a tener unas adecuadas habilidades sociales, clave para relacionarse y prevenir problemas en línea:

- Respeto: por ellos/as mismos/as, y por los demás. No permitiendo que nadie les trate mal, y tratando a los demás como les gustaría que les trataran (dejándoles hablar, aceptando sus diferencias, etc.).
- Empatía: siendo capaces de ponerse en el lugar del otro/a, comprender sus sentimientos, sensibilidades y motivaciones (ampliando nuestras perspectivas, evitando críticas hirientes, etc.).
- Asertividad: defender las opiniones e intereses propios de forma firme y activa, pero al mismo tiempo respetuosa con los demás (con una comunicación en positivo, sin herir a los demás, llegando a acuerdos, etc.).
- Pensamiento crítico: de cara a reflexionar sobre todo aquello que ven y viven (distinguiendo informaciones falsas, bulos y fraudes, interpretando la comunicación de otras personas, detectando mensajes malintencionados o peticiones de riesgo, etc.).

Diapositiva 21. RECURSOS DE UTILIDAD

Como decíamos antes, no se trata de convertirse en informáticos, ni tecnólogos, sino ponernos al día con las implicaciones de las nuevas aplicaciones tecnológicas que continuamente van surgiendo, para la seguridad en línea de nuestros hijos/as.

Para ello nos puede resultar de utilidad seguir a Internet Segura for Kids, www.is4k.es. En esta web encontraremos:

- El contacto con la “Línea de Ayuda” en Ciberseguridad de INCIBE 017, además de la posibilidad de utilizar la “línea de reporte” de contenidos de abuso sexual de menores u otros contenidos peligrosos para ellos/as.
- “Programas” y “campañas” de sensibilización como el Programa de Cibercooperantes [en el que se enmarca esta sesión] y las Jornadas Escolares (que permiten llevar talleres prácticos a los centros escolares).
- La información que “necesitas saber”, temas de actualidad en el “blog”.
- Multitud de recursos “de utilidad” para prevenir problemas, aprender sobre ciberseguridad y promover un uso más seguro y responsable de Internet (guía para familias de mediación parental, juegos, herramientas de control parental, materiales didácticos, etc.).

[Para terminar animaremos a las personas participantes a seguir en redes sociales a IS4K:

En Facebook: @is4k.es

En Twitter @is4k]

Diapositiva 22. MODELOS DE PACTOS Y ACUERDOS

Como decíamos, en casa es fundamental tener unas normas claras respecto al uso de la tecnología. Para que sean más eficaces lo ideal es que las consensuemos llegando a un acuerdo con nuestros hijos/as, y nos comprometamos también a cumplirlas. Si nosotros no cumplimos lo que les pedimos, seguramente ellos/as tampoco lo harán (por ejemplo, si andamos con el móvil mientras comemos o cenamos en familia, es difícil que interioricen la importancia de tener momentos “libres de tecnología” para centrarse en las personas que más les importan, y están a su lado). En el catálogo de recursos “de utilidad” de Internet Segura for Kids podemos encontrar distintos modelos de pactos sobre el uso compartido de los dispositivos familiares, móviles, tabletas, ordenadores, videoconsolas.

[Enlaces de interés: https://www.is4k.es/de-utilidad/recursos/pactos-familiares-para-el-buen-uso-de-dispositivos]

CONFIGURACIONES DE SEGURIDAD

Diapositiva 23. ASEGURANDO LOS DISPOSITIVOS FAMILIARES

Tratamos ahora de ver algunas medidas sencillas que podemos poner en marcha para ayudar a proteger los dispositivos y servicios en línea que utilizan nuestros hijos/as.

En primer lugar, destacar la importancia de que todos nuestros ordenadores y portátiles cuenten con un antivirus, esté actualizado, y realicemos análisis de vez en cuando.

De la misma manera, es fundamental tener el sistema operativo y las aplicaciones actualizadas en todos los dispositivos (ordenadores, móviles, tabletas, videoconsolas, televisiones inteligentes, etc.). Las actualizaciones permiten, entre otras, corregir fallos de seguridad, que son una de las principales vías de ataque a cualquier sistema. Si no se actualiza, cualquier malware (concepto más amplio de virus informático) podría ponernos en riesgo (por ejemplo, como sucedió en el famoso caso WannaCry https://www.incibe.es/protege-tu-empresa/avisos-seguridad/importante-oleada-ransomware-afecta-multitud-equipos).

Siempre que sea posible, es preferible emplear cuentas de usuario limitado en lugar de administrador, a fin de limitar el riesgo si sufrimos una infección o cometemos un error.

[Enlaces de interés: https://www.is4k.es/necesitas-saber/uso-configuracion-segura

https://www.osi.es]

Diapositiva 24. OPCIONES DE BÚSQUEDA SEGURA

[En la diapositiva hay enlaces a las páginas, aplicaciones y configuraciones correspondientes, por si se considera relevante ampliar información.]

Aunque no sea una solución perfecta, puede resultar útil limitar el acceso a contenidos inapropiados a través de los buscadores. Para ello podemos emplear aplicaciones específicamente dirigidas a menores (por ejemplo, cuando son más pequeños), como los buscadores KidRex (https://www.alarms.org/kidrex), Bunis (http://bunis.org), o la aplicación de vídeos de YouTube Kids (https://www.youtube.com/yt/kids/).

En los buscadores más utilizados también se puede establecer una configuración de búsqueda segura: Google (https://support.google.com/websearch/answer/510), Bing (https://help.bing.microsoft.com/#apex/18/es/10003/0).

Diapositiva 25. HERRAMIENTAS DE CONTROL PARENTAL

Como ya hemos comentado, las herramientas de control parental pueden ser un complemento útil para la supervisión de las actividades en línea de los menores, aunque no pueden sustituir la presencia física e implicación de los padres en este proceso.

Hay herramientas con multitud de funciones (control de tiempo, filtrado de contenidos, bloqueo de aplicaciones, seguimiento de actividad, alertas y notificaciones, geolocalización, etc.), y están disponibles para diferentes plataformas (Windows, Android, iOS, etc.). Para ayudarnos a localizar la más apropiada en nuestro caso, disponemos del catálogo de herramientas de control parental de Internet Segura for Kids (https://www.is4k.es/de-utilidad/herramientas). [También está disponible un enlace desde la imagen del cuadro de búsqueda de herramientas de control parental en la parte derecha de la diapositiva.]

Diapositiva 26. CONTRASEÑAS MÁS SEGURAS

Las contraseñas siguen siendo indispensables para garantizar la seguridad en el acceso a dispositivos y servicios en línea. Incluso cuando se utilizan otros métodos como el reconocimiento facial o la lectura de la huella dactilar, sigue siendo necesaria una contraseña como mecanismo secundario de acceso.

A pesar de la importancia que tienen, se utilizan muchas contraseñas que no son suficientemente seguras. Deben ser largas, contener letras minúsculas y mayúsculas, números y si es posible algún símbolo (por ejemplo, guiones, paréntesis, arrobas). Han de ser fáciles de recordar, y difíciles de adivinar, incluso por alguien que nos conozca bien (por ejemplo, se pueden juntar dos palabras significativas para cada uno, cambiar algunas letras a mayúsculas, otras a números, añadir algún símbolo, como sucede en el ejemplo en pantalla: "Let's play!" → "LeT$pL@y!4").

Pero, ante todo, la clave es no compartirla, una contraseña debe ser secreta, solo para nosotros. En el caso de los menores, únicamente deben conocerlas ellos/as y sus padres.

[La imagen inferior corresponde al juego de Google 'Tower of treasure', al cual está enlazado: https://beinternetawesome.withgoogle.com/en_us/interland/landing/tower-of-treasure Se puede utilizar como actividad práctica, si disponen de dispositivos, para trabajar la creación de contraseñas.]

Por último, siempre que sea posible, se debe emplear un mecanismo de doble autenticación (verificación en dos pasos), como por ejemplo generando una clave de un solo uso (y que caduca en pocos segundos) en una app en el teléfono móvil (como en la imagen superior derecha), o recibiéndola como mensaje SMS. Así, para iniciar sesión nos pedirán la contraseña y esta clave. Aunque alguien fuera capaz de vernos teclear la contraseña, tendría que hacerse también con nuestro teléfono para entrar en nuestra cuenta.

[En el caso de disponer de tiempo disponible, se puede hacer una pequeña demostración, o una práctica con las personas asistentes, para ver cómo activar la autenticación en dos pasos en servicios de uso común, como los correos electrónicos de Google https://www.google.com/landing/2step/?hl=es y Microsoft https://support.microsoft.com/es-es/help/4028586/microsoft-account-turning-two-step-verification-on-or-off, o las redes sociales de Facebook https://es-

es.facebook.com/help/148233965247823?helpref=faq_content e Instagram https://es-es.facebook.com/help/instagram/566810106808145?helpref=related.]

Diapositiva 27. BLOQUEO DE PANTALLA SEGURO

En sus dispositivos, los menores han de tener una adecuada protección, lo que pasa sin duda por evitar que cualquiera pueda desbloquear su teléfono y ver sus mensajes, fotos, e incluso hacerse pasar por ellos/as. Para ello se ha de configurar una pantalla de desbloqueo protegida con reconocimiento facial o huella digital, con una contraseña, un pin o al menos con un patrón de desbloqueo.

En todo caso, para que sea efectivo, se ha de desbloquear el teléfono con discreción, evitando miradas indiscretas que podrían memorizar el pin o el patrón.

Diapositiva 28. DESCARGAS DE CONFIANZA

Otro de los puntos clave para la protección de los menores es la utilización únicamente de apps de confianza en sus tabletas y móviles. Una app pirateada, o descargada de un mercado (tienda de aplicaciones) no oficial podría infectar el dispositivo, espiar los datos del menor, ofrecer publicidad engañosa, etc.

Dentro de las tiendas oficiales de aplicaciones (App Store y Google Play) también hay que revisar la información disponible de cada app, ya que puede haber algunas más o menos recomendables.

Para ello hemos de fijarnos en la clasificación por edades de la app (código PEGI en Google Play, y clasificación equivalente en App Store) y en la reputación de la app (¿el desarrollador es el oficial?, ¿cuántas descargas tiene?, ¿cuál es su valoración media?, ¿cuántos comentarios tiene?).

Además, es fundamental revisar la información sobre permisos para garantizar que son coherentes y se ajustan a las funciones de la app (en caso contrario pueden, por ejemplo,

enviar mensajes publicitarios no deseados a sus contactos, espiar sus acciones en línea para dirigirle publicidad personalizada, etc.).

[En la diapositiva se incluye enlace a la ficha de la app WhatsApp en la tienda de aplicaciones oficial de Android: Google Play.]

4. Reacción frente a problemas

CÓMO PEDIR AYUDA

Diapositiva 29. PREPARADOS PARA TODO

[Entramos en la última parte de la presentación, en la que abordamos la reacción frente a problemas y situaciones conflictivas.]

Es importante que seamos conscientes que tarde o temprano, nuestros hijos/as van a tener que enfrentarse a situaciones conflictivas en Internet (es inevitable, al igual que sucede cuando salen a la calle). Por eso se trata de prevenir, reduciendo las posibilidades de sufrir un problema (como hemos estado comentando hasta ahora), pero también de estar preparados para gestionarlo cuando surja.

La mejor forma de prepararse es potenciando su desarrollo personal y habilidades sociales: con una autoestima positiva, sentido de la responsabilidad, y una adecuada comunicación con los demás.

Por nuestra parte, es importante que hagamos un esfuerzo por cuidar y mantener una relación de confianza con ellos/as, con un diálogo cercano, fluido y cotidiano, de modo que si tienen alguna cuestión que les genera dudas o inquietud nos lo comenten.

Diapositiva 30. CUANDO SURJAN LOS PROBLEMAS

Lógicamente cuando surjan los problemas tienen que tener la tranquilidad de saber que pueden contar con nosotros, que no vamos a reaccionar exageradamente, ni culpabilizarles, sino que vamos a escucharles, confiar en ellos/as y buscar una solución.

Si nos sentimos perdidos, o simplemente tenemos alguna duda, siempre vamos a poder contar con Internet Segura for Kids (www.is4k.es) y la Línea de Ayuda en Ciberseguridad de INCIBE en el teléfono 017 (servicio gratuito y confidencial).

5. Cierre

REPASO Y CONCLUSIÓN

[A continuación se incluyen tres preguntas para responder entre todos, que servirán de repaso y cierre de la sesión. Lo más importante no es acertar o no, sino reflexionar sobre nuestra situación personal y familiar, por qué unas respuestas son más o menos adecuadas.]

Diapositiva31. ¿ES UN PROBLEMA TENER TANTOS AMIGOS 'EN LÍNEA'?

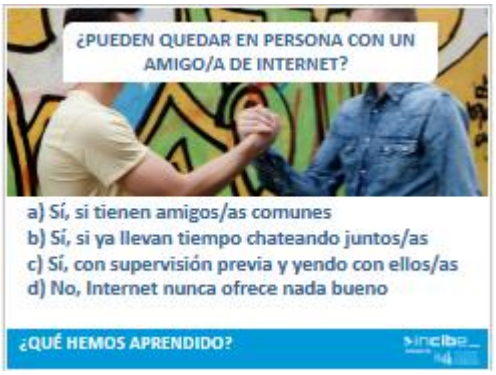
La respuesta 'a) No, cuanto más socialicen mejor' no es correcta.

La respuesta 'b) Sí, porque muchos de ellos son desconocidos' es la opción correcta.

La respuesta 'c) No, esas amistades no son reales así que no pueden hacerles daño' no es correcta. Para los menores no existen barreras entre la vida 'virtual' y la 'real'.

La respuesta 'd) Sí, pierden mucho tiempo enviándose mensajes' no es correcta. Con la mayor parte de esas 'amistades' apenas tienen contacto, pero si pueden ver las imágenes o mensajes que publican, y pueden contactar con ellos.

Diapositiva 32. ¿PUEDEN QUEDAR EN PERSONA CON UN AMIGO/A DE INTERNET?



La respuesta 'a) Sí, si tienen amigos/as comunes' no es correcta, ya que tener amigos/as en común en Internet les puede dar sensación de confianza, pero no es ninguna garantía.

La respuesta 'b) Sí, si ya llevan tiempo chateando juntos/as' no es correcta. También les puede dar sensación de confianza, pero sin garantías.

La respuesta 'c) Sí, con supervisión previa y yendo con ellos/as' es correcta si hemos estado acompañando y supervisando a nuestro hijo/a, tiene un adecuado grado de madurez y responsabilidad, su amigo/a en línea nos resulta fiable, y por supuesto le acompañamos nosotros en persona, quedando en un lugar público y concurrido.

La respuesta 'd) No, Internet nunca ofrece nada bueno' no es correcta, ya que sí es posible que hagan amistades a través de Internet que les aporten experiencias positivas, igual que en cualquier otro medio.

Diapositiva 33. ¿CÓMO DEBE SER NUESTRA SUPERVISIÓN?

La respuesta 'a) No hace falta, saben más que nosotros de la red' no es correcta. Puede que sepan de aquello que usan en Internet, pero aún están creciendo, madurando y aprendiendo de la vida, en lo que nosotros podemos apoyarles con nuestra experiencia.

La respuesta 'b) Es suficiente con poner un control parental' no es correcta, un control parental puede resultar de ayuda para gestionar la supervisión, pero no puede sustituir nunca la presencia de los padres.

La respuesta 'c) Adecuada a su madurez, y basada en el diálogo' es la opción correcta, dado que reconoce la necesidad de una supervisión, sitúa su pilar fundamental en el diálogo con los hijos/as, y se adapta en cada momento a su grado de desarrollo y madurez.

La respuesta ‘d) Revisar todos sus mensajes antes de enviarlos’ no es correcta, ya que supone una intervención excesiva que perjudica el desarrollo de la autonomía, responsabilidad y autorregulación del menor. En cualquier caso, sería una medida de protección insuficiente.

DESPEDIDA

Diapositiva 34.

Para terminar, dejamos la información de contacto de IS4K e INCIBE:
Las webs www.is4k.es y www.incibe.es
El correo electrónico contacto@is4k.es

Redes sociales:

- Facebook: Internet Segura for Kids
- Twitter: @is4k y @incibe

Suscripción a boletines: https://www.is4k.es/newsletter/subscriptions

Y recordamos que, si necesitan más información o tienen cualquier duda, pueden contactar con **Internet Segura for Kids** en **www.is4k.es** y llamando gratuita y confidencialmente al teléfono **017**.

Muchas gracias por su atención.

ANEXO

A continuación, se nombran algunos enlaces de interés con vídeos cortos que se pueden reproducir a lo largo de la sesión:

- Grooming (Europol) [10:34] https://www.youtube.com/watch?v=_whpii1co1g [ver diapositiva 12]
- Implicarse [1:55] https://www.youtube.com/watch?v=fuchWXz4m10 [ver diapositiva 16]
- Acompañamiento [1:51] https://www.youtube.com/watch?v=d5kW4pI_VQw [ver diapositiva 19]

Otros:

- Cita a ciegas [3:01] https://www.youtube.com/watch?v=THb8FdsUx38
  [Vídeo en el que tres chicas chatean con varios desconocidos enmascarados en la misma sala. Según avanza la conversación van descartando candidatos hasta que solo queda uno. Descubren su identidad y se llevan la sorpresa de que no es como esperaban.
  ¿El tipo de conversaciones que están llevando es realista?, ¿es fácil o difícil engañar dando las respuestas que espera la otra persona?, ¿cuál es el consejo que nos dan ante estas situaciones?]
- Grooming (Orange) [1:05] https://www.youtube.com/watch?v=OetekyrQj-k
  [Una adolescente parece estar confesando a su padre una cita con un amigo online, pero se descubre que en realidad es un pederasta que le obliga a usar esa coartada para sus encuentros, manteniendo el secreto.
  ¿Os parece una situación posible o exagerada?, ¿qué quiere conseguir al obligar que la chica le cuente eso a sus padres?, ¿cómo se siente ella al salir del coche?, ¿qué debería hacer en realidad?]
- Grooming (Movistar) [3:12] https://www.youtube.com/watch?v=o3zbPAT0DuQ
  [El vídeo muestra la forma en que van ganando confianza un chico y una chica que se han conocido por Internet, hasta que quedan en persona y se descubre que ninguno de los dos era quien decía ser.
  ¿Sus conversaciones son realistas?, ¿con qué detalles van ganando confianza uno en el otro?, ¿las fotos que se intercambian son reales?, ¿qué podría haber pasado si uno de ellos hubiera sido un adolescente de verdad?]
- Grooming (PDI Chile) [2:19]
  https://www.youtube.com/watch?v=c1dEKmA8vVw
  [Vídeo que muestra como una chica ha ido confiando en un chico al que conoció en línea, cómo quedan en persona y finalmente resulta ser un pederasta.
  ¿Qué hay de cierto y de falso en sus conversaciones?, ¿por qué no le cuenta nada a su madre?, ¿es una situación realista?]
- Consejos para sus primeros pasos en las redes sociales [2:04]
  https://www.youtube.com/watch?v=zCcAhZia8pA
  [Vídeo de IS4K con algunos consejos para familias a la hora de afrontar el momento de que los menores tengan su primer perfil en redes sociales.
  ¿Entendemos el interés, e incluso necesidad, de los menores para tener redes sociales?, ¿tienen madurez para ello?, ¿es necesario que nos impliquemos en el proceso?]
- Un móvil no es un juguete [1:58]
  https://www.youtube.com/watch?v=e4VET8PPJp4
  [Vídeo de IS4K con consejos para afrontar la decisión de comprar o no un móvil a un menor.

¿Un móvil es un juguete?, ¿valoramos su necesidad, capacidades y responsabilidad?, ¿conocemos los riesgos?]

- Comunicarse bien en Internet [2:46] https://www.youtube.com/watch?v=vahkiJAh2No
  [Vídeo de IS4K sobre la importancia de comunicarse adecuadamente en Internet. ¿Siempre somos conscientes de que detrás de la pantalla hay una persona?, ¿alguna vez hemos tenido un malentendido, o hemos prejuzgado a alguien por un mensaje en línea?, ¿cuál es la clave para una buena comunicación?]