



INSTITUTO NACIONAL DE CIBERSEGURIDAD

¡Aprendemos sobre Ciberseguridad!

(Menores de 9 a 13 años)

Guion presentación

Guion para charlas sobre ciberseguridad para menores

Este guion se ha desarrollado para servir como referencia a los ponentes que utilicen la presentación “¡Aprendemos sobre Ciberseguridad! (menores de 9 a 13 años)”.

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 que captan la atención de los menores, de modo que la persona que imparte la presentación debe ampliar las explicaciones adecuándose al grupo.

Esta sesión se enfoca a la iniciación de la actividad autónoma en Internet. El objetivo es prepararles para los primeros contactos con otras personas a través de la Red, así como presentarles los posibles riesgos que pueden encontrarse, ofreciéndoles recursos para afrontarlos.

Debemos tener en cuenta que este rango de edades contempla varios momentos clave en el contacto con Internet y la tecnología conectada: menos límites a la hora de conectarse y experimentar, la posibilidad de acceder a su primera tableta o incluso a su primer móvil, sus primeras redes sociales, etc. A su vez, están teniendo lugar cambios importantes en su desarrollo psicológico y emocional, que pueden influir en sus objetivos a la hora de conectarse: ya no solo les interesan los juegos en línea o el entretenimiento audiovisual, también las comunicaciones y relaciones sociales que pueden crear en Internet.

La complejidad radica en que no todos los menores se inician al mismo tiempo, e incluso en muchos casos ni siquiera tienen acceso a un dispositivo propio o a las redes sociales hasta más adelante. Por lo tanto, es imprescindible hacer una valoración al inicio de la sesión, en la que tanteemos la experiencia general del grupo y poder adaptar así la explicación.

1. Introducción

Diapositiva 1.



[Antes de iniciar la sesión, preparamos la presentación para mostrarla a pantalla completa con esta primera diapositiva]

Brevemente nos presentamos e introducimos el proyecto Internet Segura For Kids (trata de promover la colaboración de personas particulares en la divulgación de la ciberseguridad a través de charlas de sensibilización) y los objetivos de la sesión: mostrar cómo utilizar Internet de forma segura en su día a día, conocer algunos de los riesgos que pueden encontrarse y cómo afrontarlos.

Diapositiva 2. ¿CÓMO USAMOS INTERNET?



[A modo de introducción, tanteamos al grupo para valorar la experiencia que poseen en torno a Internet y la tecnología. Procuraremos adaptarnos a su nivel de conocimientos, evitando generar necesidades que aún no tienen, como tener móvil o redes sociales.

- Si ya tienen cierta experiencia o disponen de sus propios dispositivos y redes sociales,

podremos utilizar un vocabulario más amplio y plantearles situaciones más complejas.

- En caso contrario, procuraremos adaptarnos a su nivel de conocimientos, evitando generar necesidades que aún no tienen: si aún no tienen móvil o redes sociales es porque no los necesitan ni están preparados para ellos, pero deben conocer esta información para cuando llegue el momento.

Los menores a menudo no son conscientes de todas las actividades que en su día a día utilizan Internet, y por tanto cuánto tiempo pasan 'conectados'. En esta diapositiva aparecen varias actividades relacionadas.]

¿Tienen tableta o móvil propio?, ¿utilizan los dispositivos de sus padres?, ¿qué es lo que más les gusta hacer en Internet?, ¿tienen redes sociales?, ¿y videoconsolas que puedan conectarse?, ¿les resultan familiares las imágenes que aparecen en pantalla?

[Dejaremos que sean ellos mismos los que se animen a comentar qué ven, qué utilizan, con qué frecuencia, etc. De esta manera podremos hacernos una idea de su experiencia con Internet y cuáles son sus intereses.]

Diapositiva 3. ¿NOS COMUNICAMOS POR INTERNET?



Preguntamos al grupo acerca de los logotipos que aparecen en pantalla, ¿los conocen? (seguramente sí, aunque aún no los utilicen, otros serán habituales en su tiempo de ocio). ¿Por qué les interesan?, ¿qué ofrecen estos servicios, apps o juegos? Nos centramos en dos de los objetivos fundamentales: diversión y comunicación. El entretenimiento suele ser obvio, pero pocas veces se paran a pensar en

que las redes sociales o los videojuegos son una herramienta que permite la relación con otras personas. En cualquier caso, hablamos en este punto de funciones positivas, beneficios que hacen de Internet un medio útil y atractivo.

(En la imagen aparecen los logotipos de Nintendo Switch, Instagram, Play Station, Facebook, Snapchat, Nintendo DS, WhatsApp, Fortnite, Tik Tok).

[En esta sesión nos centraremos en los videojuegos y las redes sociales, por ser las actividades que más les llaman la atención a esta edad.]

2. Descripción de riesgos y consejos

Diapositiva 4. ¿EXISTEN RIESGOS?



Planteamos al grupo la posibilidad de que existan consecuencias negativas del uso de Internet.

[Dejamos que sean ellos mismos los que expongan sus ideas al respecto, de modo que podamos valorar su experiencia y conocimientos para adaptar las explicaciones posteriores.]

Diapositiva 5. ¿EXISTEN RIESGOS?



[La diapositiva contiene dos recortes de noticias reales sobre los riesgos de Internet. Dependiendo de su edad puede que no comprendan los titulares, que deberemos explicar, de manera que comprendan que sí hay riesgos y que son una realidad.]

Comentamos dos noticias de actualidad con el grupo: el uso excesivo de videojuegos y el ciberacoso a través de Internet. ¿Escuchan a menudo noticias como estas?, ¿son conscientes de que a diario podemos encontrarnos con casos similares que afectan a niños y niñas de su edad?

[Se trata de acercarlos a la realidad de los riesgos de Internet, sin necesidad de generar miedos o exponerles situaciones excesivamente complejas para su madurez y comprensión. A continuación, explicaremos con más detalle algunos de estos riesgos.]

[Enlaces de interés:

https://elpais.com/elpais/2018/06/11/mamas_papas/1528706334_714292.html

https://www.abc.es/tecnologia/abci-adolescentes-entre-11-y-14-anos-representan-mayor-tasa-ciberacoso-201707261422_noticia.html]

CONTENIDOS INADECUADOS

Diapositiva 6. NO TODO EN INTERNET NOS SIENTA BIEN



Explicamos el concepto de ‘contenido’: imágenes, vídeos, juegos o textos que podemos encontrar en Internet. Los contenidos pretenden transmitir información, ideas o emociones sobre diferentes temas. Existen multitud de contenidos en la Red, de hecho, es una de las principales ventajas de este medio: no está limitado por el espacio y su capacidad para albergar todo tipo de contenidos no deja

de crecer. Pero ¿todos los contenidos que existen en Internet son adecuados para ellos?

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

Diapositiva 7. ¿QUÉ ES UN CONTENIDO INADECUADO?



- Contenidos para otras edades
- Contenidos que no entendemos
- Contenidos negativos
- Contenidos falsos

¿QUÉ ES UN CONTENIDO INADECUADO? 

No todos los contenidos de Internet son adecuados para todos los públicos. Algunos están creados para públicos de otras edades, y es necesario tener cierto nivel de madurez y conocimientos para afrontarlos bien, o simplemente pueden ser demasiado complejos para su nivel de comprensión.

[Podemos utilizar ejemplos genéricos para ilustrar estos conceptos, sin nombrar contenidos concretos que puedan atraer su curiosidad. Por ejemplo, pueden encontrarse un vídeo sobre medicina, que por el vocabulario que utilizan no pueden entender, o una fotografía de algo extremadamente violento que les puede impactar. Se muestran imágenes de apología violenta radical, sexo y el reto viral 'In my feelings challenge', en el que los protagonistas debían bajarse de un coche en marcha y bailar, provocando accidentes graves en algunos casos].

Otros se consideran negativos para cualquier edad, como ocurre con los contenidos que fomentan la violencia o los hábitos poco saludables, o falsos si contienen información que no es cierta. En todos estos casos hablamos de contenidos inadecuados.

¿Dónde se encuentran estos contenidos? No es necesario que busquen estos contenidos de manera directa, pueden aparecer mientras visualizan otros, por ejemplo, en un videojuego o en plataformas como YouTube, también pueden enviárselos otras personas por mensajes o a través de redes sociales, e incluso que aparezcan como publicidad mientras visitan una página web.

Diapositiva 8. CÓMO ACTUAR ANTE ESTOS CONTENIDOS



- Pausar la reproducción
- No difundirlo
- Contárselo a un adulto
- Reportar

CÓMO ACTUAR ANTE ESTOS CONTENIDOS 

[Aunque parezca sencillo, ante una situación compleja como esta un menor puede no saber cómo actuar o sentirse bloqueado para pedir ayuda. Estos momentos pueden acompañarse de cuadros de ansiedad, estrés, miedos, deficientes habilidades sociales, etc. Incluso es posible que se sientan culpables si han buscado esos contenidos por curiosidad o los han reproducido siendo conscientes de que no se les

permitía hacerlo. Por ello, es útil recordarles que siempre pueden pedir ayuda si siguen estos pasos.]

Si se encuentran ante uno de estos contenidos, es importante que sepan cómo actuar. Aunque en un principio puedan parecer divertidos o llamen su curiosidad, pueden llegar a afectarles de diversas formas: miedos, ideas erróneas o confusas, etc.

De modo que:

- Lo primero es detener la visualización del contenido en cuanto sean conscientes de que no es apropiado para ellos.
- No reenviarlo y cortar la difusión para que no pueda afectar a otros menores.
- Hablar con un adulto de confianza, como sus padres, mostrarle cómo han llegado hasta el contenido, y preguntarle sus dudas al respecto.
- Denunciar y reportar el contenido para que otros menores no puedan tener acceso a él, o sea eliminado si corresponde. Ya sea una página web o una red social, siempre existe un medio para contactar con los administradores del servicio e informar de estas situaciones.

Es algo que nos puede pasar a todos, no hay que tener vergüenza o miedo de hablar de ello. Los adultos no se van a enfadar porque les cuenten algo así, todo lo contrario, les ayudarán y les explicarán aquello que no han entendido o les ha disgustado.

PRIVACIDAD

Diapositiva 9. CUIDA TU PRIVACIDAD



[Explicaremos el concepto de privacidad, que para los menores puede resultar complejo o confuso. Para ellos este no es un riesgo tan evidente como otros, dado que en estas edades no siempre son conscientes de las consecuencias de una mala gestión de la privacidad.]

¿A qué nos referimos con privacidad? En Internet todos compartimos mucha información sobre nosotros mismos: escribimos comentarios y opiniones, publicamos fotos y vídeos, mostramos quienes son nuestros

amigos y familiares, etc. El cuidado de la privacidad depende de qué información deciden mostrar y en qué cantidad, y qué datos prefieren guardarse para sí mismos.

No solo comparten información en las redes sociales, también al enviar mensajes a sus contactos de WhatsApp por ejemplo, o al comunicarse con otros jugadores en un videojuego.

¿Pero por qué se considera un riesgo? El problema radica en que, una vez que comparten su información privada, pasa a ser pública y es un paso que no tiene marcha atrás. Más adelante pueden arrepentirse de haber compartido esos datos o esas imágenes, y estos pueden acabar en manos de personas desconocidas que pueden utilizarlos para hacerles daño.

Enlace de interés: <https://www.is4k.es/necesitas-saber/privacidad>
<https://www.is4k.es/necesitas-saber/grooming>
<https://www.is4k.es/necesitas-saber/comunidades-peligrosas>]

Diapositiva 10. ¿POR QUÉ COMPARTIMOS LA VIDA PRIVADA?



En la actualidad, solo con ver el perfil de una persona en cualquier red social podemos conocer mucho sobre ella: sus gustos, aficiones, sus amistades, su aspecto físico, sus sentimientos, dónde vive, dónde estudia o trabaja, etc. Los motivos para compartir toda esta información y hacerla pública son diversos, pero principalmente tienen que ver con la necesidad de establecer relaciones sociales y

comunicarse con otras personas. También existe cierta presión social: parece que es obligatorio utilizar redes sociales y compartir mucha información para mantener las amistades y ganar popularidad.

[Animaremos a los participantes a reflexionar sobre la presión social que empiezan a sentir por unirse a las redes sociales y compartir todo lo que hacen en su día a día. También les plantearemos la posibilidad de que no es necesario publicar información privada para ganarse el reconocimiento social].

Diapositiva 11. MIS PRIMERAS REDES SOCIALES



[En estas edades suele aparecer el interés por las redes sociales: observan a las personas de su alrededor y ven cómo todos las utilizan para comunicarse y conocerse, y es normal que surja la curiosidad.]

Es importante que comprendan que es necesario cierto nivel de madurez y responsabilidad para utilizarlas, y que siempre deben contar con la aprobación y el apoyo de sus padres para crearse un perfil. Podemos recordar que, de hecho, la mayoría de las redes sociales no pueden utilizarse legalmente hasta tener 14 o 16 años.

Cuando llegue ese momento, estará en sus manos la gestión de su privacidad, y deben recordar que por seguridad no deben mostrar determinada información. El primer perfil siempre debe crearse en compañía de un adulto, con lo que reforzaremos la idea de que el acompañamiento de sus padres en su andadura por Internet y las redes sociales es algo natural, y que poco a poco irán consiguiendo más autonomía, con el tiempo y el aprendizaje.

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

Diapositiva 12. PIENSA ANTES DE COMPARTIR



[Los menores deben interiorizar que Internet no es el lugar donde compartir información privada, porque puede caer en manos de desconocidos o personas con malas intenciones. Dado que para ellos puede resultar confuso y complejo diferenciar qué es privado y qué no, podemos marcar unos límites claros con los siguientes datos que en ningún caso deben compartir.]

Da igual con quién hablemos en Internet, hay algunos datos que nunca debemos revelar, como su nombre real, su teléfono o su dirección, o en qué colegio estudian. Tampoco

deben concretar los horarios de sus clases o sus actividades extraescolares, o compartir los datos de otras personas (familia, amigos, compañeros, etc.).

Es mejor usar un nick o alias en la Red, que servirá para identificarnos sin necesidad de que todos sepan cómo se llaman en realidad.

El mensaje clave para cuidar su privacidad es que reflexionen siempre antes de compartir información personal, porque una vez publicado o compartido no podrán recuperarlo: ¿puede suponer un riesgo compartir esta foto o este dato?, ¿qué pasaría si se hace pública y la ve todo el mundo?, ¿podrían utilizar esta información para hacerles daño?, ¿hay más personas implicadas cuya privacidad deben respetar?

[Remarcaremos la importancia de que sus padres sean conscientes de quiénes son sus amigos en Internet antes de mantener conversaciones con esas personas.]

Diapositiva 13. A VECES NO ELEGIMOS LO QUE PUBLICAMOS



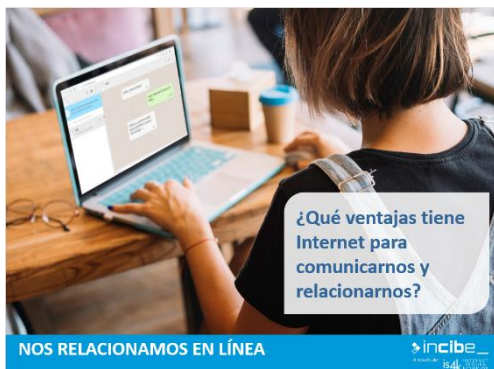
Para cerrar el tema de la privacidad, les haremos conscientes de que no solo ellos comparten información sobre sí mismos, también otras personas pueden publicar datos personales sobre ellos o hacer pública información que consideran privada. Por ejemplo, pueden difundir una imagen que ellos han enviado de forma privada a una persona, o pueden acceder a una de sus cuentas de redes

sociales o a su teléfono móvil, y difundir información privada para hacerles daño.

Por ello, es importante que extremen la precaución, más aún si se trata de un equipo compartido (por ejemplo, en el centro educativo). Deben mantener su dispositivo siempre bloqueado, cerrar sesión al terminar de utilizar sus cuentas de redes sociales o de juegos en línea, y en general, evitar en la medida de lo posible compartir o almacenar información sensible (imágenes íntimas, datos personales privados, etc.).

RELACIONES SALUDABLES EN LÍNEA

Diapositiva 14. NOS RELACIONAMOS EN LÍNEA



Animaremos al grupo a reflexionar acerca de la posibilidad de comunicación que nos ofrece Internet: ¿por dónde nos comunicamos en Internet? No solo a través de mensajería instantánea o redes sociales, también en los videojuegos, los foros y comunidades, las páginas web que permiten comentarios, etc. Es un nuevo medio por el que creamos relaciones sociales.

Diapositiva 15. HABILIDADES PARA COMUNICARNOS BIEN

Al otro lado de la pantalla hay una persona, por eso:

- Respeto: trata como te gusta que te traten a ti
- Empatía: ponte en su lugar
- Asertividad: da tu opinión sin herir a los demás
- Pensamiento crítico: reflexiona sobre lo que ves



HABILIDADES PARA COMUNICARNOS BIEN 

Internet y las nuevas tecnologías ofrecen un nuevo medio de comunicación con muchas ventajas, pero una contraprestación importante: pueden perder de vista que al otro lado de la pantalla hay una persona que tiene sentimientos y que se ve afectada por nuestros mensajes y actitudes.

Por ello debemos fomentar una comunicación basada en el respeto y la responsabilidad, a la vez que recordamos habilidades sociales imprescindibles como son la empatía, la asertividad o el pensamiento crítico. En este punto podemos realizar alguna dinámica en grupo para trabajar estas habilidades, como las que encontramos en 'Educa y aprende' (<https://educayaprende.com/juego-educativo-para-desarrollar-la-asertividad/>) o en 'Escuela en la nube' (<https://www.escuelaenlanube.com/asertividad-infantil/>).

VIOLENCIA EN LÍNEA

Diapositiva 16. DECIMOS NO A LA VIOLENCIA



La falta de empatía y asertividad en Internet, así como la falsa idea de que en la Red pueden comportarse de forma diferente ya que su actividad es ‘anónima’, favorece la difusión de la violencia en línea. Dado que toda la sociedad participa en esta conducta de comunicación (en la televisión, los videojuegos, la música, etc.), es habitual que los menores normalicen la comunicación agresiva a través de Internet, los

mensajes humillantes, insultantes, etc. de forma que no perciben el daño que puede causar en la persona que los recibe.

Diapositiva 17. DECIMOS NO A LA VIOLENCIA



[Plantearemos preguntas al grupo que fomenten la reflexión al respecto de la violencia en línea.]

¿Sus mensajes son demasiado agresivos? o ¿son excesivamente críticos con los demás? Podemos poner de ejemplo cualquier vídeo de YouTube o una imagen de Instagram protagonizados por personas de su edad, donde

es fácil encontrar comentarios negativos o humillantes. Por ejemplo, mensajes como ‘vaya basura de vídeo’, ‘qué pintas lleva esta chica’ o ‘odio este canal’. También encontramos ejemplos similares en los juegos en línea, donde los jugadores a menudo insultan a su adversario o fomentan la violencia. Cerraremos este tema valorando con una lluvia de ideas los aspectos positivos de crear un buen ambiente de comunicación en la Red.

CIBERACOSO

Diapositiva 18. DECIMOS NO AL CIBERACOSO



[Recordaremos el concepto de ciberacoso y sus características.]

El ciberacoso se manifiesta como un daño intencional y repetido a través de Internet y los diferentes medios en los que este se utiliza. Es un problema muy normalizado en la actualidad, tanto que en muchos casos ni siquiera se considera acoso desde el punto de vista de los

menores e incluso de los adultos. Pero el ciberacoso no es una broma.

¿Por qué lo hacemos? Las motivaciones para mantener este tipo de prácticas tan dañinas son diversas, desde la presión de los compañeros y la búsqueda de popularidad, hasta deseos de venganza o por falta de autoestima. Debemos recalcar al grupo que en ningún caso está justificado herir de esta forma a un compañero.

Frenar el ciberacoso sí es posible, y está en manos de todos ellos. El ciberacoso se alimenta del reconocimiento de los demás. Es decir, si un acosador no siente el apoyo del grupo, por lo general pierde el interés por seguir haciendo daño.

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

Diapositiva 19. TÚ PUEDES PARARLO



[Fomentaremos el papel de los observadores a la hora de frenar una situación de ciberacoso en su entorno.]

Existen muchas formas de actuar frente al ciberacoso, empezando por no difundir y frenar la cadena de divulgación del mismo. Cada 'me gusta' o cada vez que se comparte un mensaje humillante cuenta, del mismo modo que si

participan en grupos creados para ofender y burlarse de una persona.

El apoyo a la víctima puede marcar la diferencia, y es importante hacerles conscientes de que cualquiera puede acabar siendo víctima de ciberacoso, por lo que deben ponerse en su lugar: ¿les gustaría sentirse solos ante esta situación?

Pasar de ser meros observadores pasivos, a actuar y ayudar a la víctima es más sencillo de lo que parece: pedir ayuda a un adulto de confianza, no apoyar al acosador y ponerse del lado de la víctima.

A modo de cierre de este tema, recordamos la importancia de crear un ambiente positivo en Internet: sacar una sonrisa a un compañero, sí se merece un ‘me gusta’.

Diapositiva 20. TÚ PUEDES PARARLO



TÚ PUEDES PARARLO



[Se incluye un vídeo que se puede visualizar con conexión a Internet. En este corto se ofrece una visión sencilla de todo lo que es posible hacer por los demás con muy poco esfuerzo. El hecho de no mirar hacia otro lado y ayudar a los demás puede cambiar los acontecimientos.

Dependiendo la edad 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.]

¿Alguna vez miramos hacia otro lado cuando vemos que alguien tiene problemas? En el vídeo hemos visto todo lo que se puede conseguir simplemente ‘sacando las manos de los bolsillos’, y aportando lo mejor de nosotros mismos a los demás. En el ciberacoso, cualquier muestra de apoyo o ayuda puede hacer que el problema se minimice o incluso terminemos con esa situación.

(Enlace al vídeo: https://www.youtube.com/watch?v=VbkJDZr_Ue8)

USO EXCESIVO

Diapositiva 21. ¿CUÁNTO TIEMPO PASAS CONECTADO?



[Los menores no siempre son conscientes de la cantidad de tiempo que invierten entre pantallas. Móviles, tabletas, ordenadores, consolas y televisiones pueden absorber demasiado tiempo de su rutina, llegando incluso a ser excesivo y provocar cambios de humor, pérdida de aficiones, problemas de salud, etc.]

Animaremos al grupo a reflexionar sobre esta cuestión, dejando que sean ellos los que compartan la frecuencia con la que se conectan: ¿cuánto tiempo pasan conectados?, ¿se conectan a diario o solo algunas veces por semana? Es importante que piensen en todas las actividades que realizan en Internet: juegos en línea, redes sociales, mensajería, visualización de vídeos, etc. ¿Es demasiado tiempo?, ¿cuánto tiempo dedicamos a otras cosas que nos gustan, como un deporte o un hobby?

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

Diapositiva 22. NO DEJES DE LADO TODO LO DEMÁS



[Los menores que pasan demasiado tiempo conectados están dedicando menos tiempo a otras actividades, como la vida familiar, los estudios, las amistades, los deportes o las aficiones.]

Internet puede ofrecernos muchas cosas, pero la clave para utilizarlo bien es repartir el tiempo y hacer un uso equilibrado.

¿Les suenan estas escenas? Comidas familiares en las que alguien no puede dejar de mirar el móvil, reuniones de amigos en las que cada uno está más pendiente de su móvil que de disfrutar de la compañía de los demás, aficiones que dejan de lado por conectarse o jugar en línea, o momentos divertidos que tienen que ser fotografiados para ser perfectos. ¿Cómo se sienten cuando intentan hablar con sus padres y no les prestan atención por estar con el móvil?

[Seguramente muchas de estas situaciones aún no sean tan habituales a su edad, pero son conscientes de que otros menores o adultos sí lo hacen a su alrededor. Por ello, se trata de hacerles ver que estas actitudes no son atractivas, sino que son un problema, y es necesario dar más valor a las actividades alternativas y la búsqueda de un equilibrio.]

Nunca deben perderse otras actividades por conectarse, porque si se organizan bien pueden tener tiempo para todo. Estudiar, hacer deporte y descansar siempre debe estar por delante de un videojuego o un vídeo. ¿Qué tal si negociamos unas normas entre toda la familia? En IS4K podemos imprimir un pacto para ello (<https://www.is4k.es/de-utilidad/recursos/pacto-para-compartir-los-dispositivos-familiares-con-seguridad>). Y lo más importante: las personas primero. Pasar tiempo en familia, y apagar el móvil o la tableta cuando les hablan es una norma de educación, pero también es cuestión de sentido común. Nada de lo que puedan encontrar en Internet es más importante que la gente que les rodea.

CONFIGURACIONES SEGURAS

Diapositiva 23. CONFIGURA TU SEGURIDAD



[A pesar de utilizar habitualmente móviles, tabletas y ordenadores, no siempre conocen pautas básicas de seguridad para hacer un buen uso de los mismos. A modo de introducción en la ciberseguridad técnica, explicaremos cómo hacer una correcta gestión de acceso.]

¿Alguna vez han creado una contraseña para un juego o una aplicación? Cada vez es más habitual tener que crear un usuario para poder utilizar servicios de Internet, y aunque parezca tedioso, es importante hacerlo bien. Una buena contraseña debe contener letras minúsculas y mayúsculas, números y si es posible algún símbolo especial, como por ejemplo guiones o arrobas. De esta forma, será más complicado que otras personas puedan averiguarla.

Pero, ante todo, la clave es no compartirla, una contraseña debe ser secreta. Solo sus padres deben conocerla para poder acceder en caso necesario.

[Para trabajar la creación de contraseñas podemos realizar una práctica en el ordenador con el juego de Google 'Tower of treasure']

https://beinternetawesome.withgoogle.com/en_us/interland/landing/tower-of-treasure]

También recordaremos la importancia de bloquear la pantalla para evitar que otras personas puedan acceder, y la necesidad de extremar la precaución al utilizar redes WiFi públicas. Cualquiera podría ver qué páginas web visitan o qué hacen en ellas cuando usan esas redes, de modo que no deben emplearlas para entrar en sus redes sociales (con usuario y contraseña) o realizar compras, por ejemplo.

Lo mismo sucede con las apps que no cifran la información que se envía y recibe (para comprobarlo se puede buscar información en el centro de seguridad o la ayuda de la app).

[Enlace de interés: <https://www.is4k.es/necesitas-saber/uso-configuracion-segura>]

Diapositiva 24. APPS CON SENTIDO COMÚN



[Los menores utilizan habitualmente aplicaciones y suelen realizar numerosas descargas, a menudo sin contar con unas medidas mínimas de seguridad. Detallaremos los aspectos en los que deben fijarse al realizar descargas en los mercados de aplicaciones, que siempre deben ser los oficiales.]

¿Cuántas aplicaciones tienen para jugar o ver vídeos?, ¿todas ellas son seguras? Hay muchas aplicaciones disponibles en Internet, pero algunas de ellas no son fiables o son engañosas. ¿Alguna vez han descargado por error una app que parecía divertida y resultó ser algo completamente diferente? Esto se puede evitar fijándonos en la información que está disponible antes de descargarla, contando siempre con la ayuda y la autorización de un adulto. De este modo, nos fijaremos en el número de descargas, quién es el creador de la aplicación, qué permisos necesita, qué opinan otros usuarios, etc. El sentido común es nuestra mejor herramienta de seguridad.

Diapositiva 25. APPS CON SENTIDO COMÚN



[Se incluye un vídeo que se puede visualizar con conexión a Internet. En este vídeo se muestra con claridad qué ocurre cuando descargan determinadas aplicaciones en sus móviles, que resultan ser engañosas o cuyos permisos son excesivos.

Dependiendo de la edad 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.]

Cuando descargáis aplicaciones y juegos, ¿os fijáis en los permisos y otras características? ¿Os imaginabais que podría tener este tipo de consecuencias? No es complicado verificar si una aplicación es segura o adecuada, tan solo nos llevará unos minutos y nos puede ahorrar muchos problemas.

(Enlace al vídeo: https://www.youtube.com/watch?v=UXeR3iLG_ro)

Diapositiva 26. FRAUDES EN LÍNEA



[No es necesario entrar en detalles técnicos, solo dar algunas pautas para identificar contenidos fraudulentos y recalcar la pauta de actuación a seguir: comunicárselo a un adulto.]

Explicaremos de forma sencilla qué tipo de fraudes pueden encontrarse mientras navegan por Internet, poniendo ejemplos adaptados a su edad (Apps engañosas, mensajes de descuento fraudulentos, publicidad falsa en juegos en línea, etc.). Para evitar caer en estos engaños, es importante:

- Evitar los mensajes de descuentos, premios o sorteos.
- Descargar de forma segura apps y juegos en mercados oficiales y revisando su información.
- Evitar los juegos en línea con compras integradas (como por ejemplo para comprar ampliaciones u objetos virtuales), o en su caso extremar la precaución al utilizarlos.

- No difundir mensajes virales que pueden contener un fraude o un virus.

Ante la duda, preguntar siempre a un adulto de confianza si no sabemos si un contenido es seguro.

[Enlace de interés: <https://www.osi.es>]

3. Reacción frente a problemas

CÓMO PEDIR AYUDA

Diapositiva 27. ¿Y SI SURGE UN PROBLEMA?



[Es esencial que los menores tengan la certeza de que siempre existe una solución para cualquier problema que surja en Internet. Aunque resulte evidente, ante una situación compleja un menor puede no saber cómo actuar o pedir ayuda.]

Es cierto que no se puede volver atrás, y puede que haya consecuencias, pero se puede salir adelante de cualquier situación siempre que contemos con el apoyo de un adulto de confianza y profesionales especializados. Por ello, les recordaremos que pedir ayuda es sencillo si siguen estos pasos:

- **Protégete:** la prevención es su mejor herramienta de protección. Después de todo lo que han aprendido en la sesión, pueden defenderse de los riesgos y seguir aprendiendo a utilizar Internet con seguridad.
- **Reacciona:** cuando surja un problema, no sirve de nada cerrar los ojos y hacer como que no ha pasado, o esperar que se solucione con el tiempo. Deben hacerle frente y asumir que es necesario actuar.
- **Cuéntalo:** siempre deben contar con el apoyo de una persona adulta de confianza, les ayudarán a buscar una solución y se sentirán acompañados durante todo el proceso. Afrontar un problema en soledad no es buena idea. En cualquier caso, siempre está a su disposición la Línea de Ayuda en Ciberseguridad de INCIBE (teléfono 017).
- **Actúa:** Con la ayuda de un adulto, encontrarán la manera de solucionar paso a paso el problema. En un principio puede parecer que es una situación imposible de

arreglar, pero poco a poco verán que se puede salir adelante y afrontar las consecuencias. Es útil en este momento tomar capturas de pantalla y guardar pruebas que puedan ser de utilidad.

- Aprende: No caer en el mismo error dos veces: reflexionar sobre los errores o las precauciones que no tomaron y ponerle remedio. Protegerse en la Red y actuar con seguridad está en sus manos.

Diapositiva 28. EN IS4K OS AYUDAMOS



Mostramos la información de Internet Segura for Kids y animamos a los participantes a interactuar dentro de la web con ayuda de sus padres, para aprender divirtiéndose con juegos en línea como CyberScouts o Hackers Vs. CyberCrok, o actividades como las CyberTasks (actividades de sensibilización, concienciación y formación en materia de ciberseguridad para ser desarrolladas en los centros educativos).

También comentamos que existen otros recursos que pueden ser de su interés, como el cómic de los Vengadores contra el ciberacoso, los Árboles de decisiones o los Pactos para acordar unas normas en familia.

Prestamos especial atención a la Línea de Ayuda en Ciberseguridad de INCIBE. Cualquier menor o adulto puede contactar de manera gratuita y confidencial cuando tengan una duda o un problema en Internet, llamando al número de teléfono 017 o enviando un mensaje a través de la página web www.is4k.es. Además, en la web pueden encontrar mucha información y actividades para trabajar estos temas, en el colegio o en familia.

[Remarcaremos la característica de que es gratuita y confidencial, para que los menores entiendan que siempre pueden utilizar este recurso si no saben cómo actuar o tienen miedo de contárselo a otras personas.]

Enlaces de interés:

<https://www.is4k.es/de-utilidad/cybertasks-kids>

<https://www.is4k.es/de-utilidad/cyberscouts>

<https://www.is4k.es/de-utilidad/recursos/juego-hackers-vs-cybercrok>

<https://www.is4k.es/de-utilidad/recursos/comic-los-vengadores-acoso-nunca-mas>

<https://www.is4k.es/de-utilidad/recursos/arboles-de-decisiones-para-trabajar-la-seguridad-en-internet>

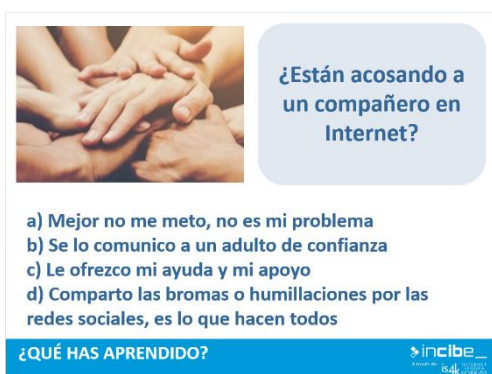
<https://www.is4k.es/de-utilidad/recursos/pactos-familiares-para-el-buen-uso-de-dispositivos>
<https://www.is4k.es/ayuda>]

4. Cierre

REPASO Y CONCLUSIÓN

[A continuación se incluyen tres preguntas para responder entre todos, que servirán de repaso y cierre de la sesión. Solo hay una única respuesta correcta, pero la clave de este ejercicio está en explicar por qué unas respuestas son válidas y otras no, animando a los menores a que sean ellos los que razonen estas cuestiones.]

Diapositiva 29. ¿ESTÁN ACOSANDO A UN COMPAÑERO EN INTERNET?



¿Están acosando a un compañero en Internet?

- a) Mejor no me meto, no es mi problema
- b) Se lo comunico a un adulto de confianza
- c) Le ofrezco mi ayuda y mi apoyo
- d) Comparto las bromas o humillaciones por las redes sociales, es lo que hacen todos

¿QUÉ HAS APRENDIDO?

La respuesta 'a) Mejor no me meto, no es mi problema' no es correcta, ya que la víctima necesita su apoyo y deben ponerse en su lugar. Ellos podrían ser los siguientes en tener este problema.

La respuesta 'b) Se lo comunico a un adulto de confianza' es correcta, ya que deben tener conocimiento de lo que está pasando, sabrán

cómo actuar y con su apoyo es más fácil terminar con el problema.

La respuesta 'c) Le ofrezco mi ayuda y mi apoyo' no es correcta. Es cierto que refuerza la idea de que la víctima no está sola, y el acosador a menudo perderá el interés si todo el grupo se pone del lado de la persona que está siendo acosada. Pero también deben contárselo a un adulto para que juntos puedan terminar con el problema.

La respuesta 'd) Comparto las bromas o humillaciones por las redes sociales, es lo que hacen todos' no es correcta, deben evitar participar en la difusión de estas publicaciones para terminar con el problema, hablando con un adulto y ofreciendo su apoyo a la víctima.

Diapositiva 30. ¿EXISTE LA VIOLENCIA EN LA RED?



¿Existe la violencia en la Red?

- a) Sí, pero no hace daño porque es virtual
- b) No, solo son bromas, no es real
- c) Sí, en forma de mensajes de odio, comentarios humillantes o difusión de la violencia
- d) No, todos los mensajes son positivos en Internet

¿QUÉ HAS APRENDIDO? 


La respuesta ‘a) Sí, pero no hace daño porque es virtual’ no es correcta, ya que cualquier mensaje ofensivo o negativo afecta a otras personas que están al otro lado de la pantalla. Un insulto duele igual tanto si se hace cara a cara, como a través de Internet.

La respuesta ‘b) No, solo son bromas, no es real’ no es correcta, cualquier forma de violencia en Internet tiene consecuencias en la vida ‘real’. Internet es solo un medio de comunicación más, forma parte de nuestra realidad.

La respuesta ‘c) Sí, en forma de mensajes de odio, comentarios humillantes o difusión de la violencia’ es la opción correcta.


La respuesta ‘d) No, todos los mensajes son positivos en Internet’ no es correcta, deben ser conscientes de que cada vez hay más violencia en Internet y cambiar esto está en manos de todos.

Diapositiva 31. ¿QUÉ PUEDO HACER ANTE UN PROBLEMA EN INTERNET?



¿Qué puedo hacer ante un problema en Internet?

- a) Pedir ayuda a mis amigos, mejor que no se enteren mis padres
- b) Contactar con un Centro de Ayuda especializado
- c) Nada, con el tiempo se solucionará...
- d) Contárselo a cualquier adulto, es lo mejor

¿QUÉ HAS APRENDIDO? 

La respuesta ‘a) Pedir ayuda a mis amigos, mejor que no se enteren mis padres’ no es correcta, porque les ayudará contar con su apoyo y no sentirse solos, pero igualmente deben contárselo también a un adulto de confianza.

La respuesta ‘b) Contactar con un Centro de Ayuda especializado’ es la opción correcta, ya que cuentan con profesionales que saben cómo solucionar todo tipo de problemas, y pueden ofrecer además su apoyo, como hacemos desde la Línea de Ayuda en Ciberseguridad de INCIBE.

La respuesta ‘c) Nada, con el tiempo se solucionará...’ no es correcta, ya que hacer como que no ha pasado nada solo retrasará la solución del problema, y puede que incluso lo empeore. Hay que afrontarlo, pedir ayuda y actuar.

La respuesta ‘d) Contárselo a cualquier adulto, es lo mejor’ no es correcta, ya que cuando tengan un problema deben contárselo a un adulto de confianza, no a cualquier persona.

Por ejemplo, a sus padres, sus hermanos mayores, orientadores o tutores de su centro educativo, etc.

DESPEDIDA

Diapositiva 32.



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 en el aula a lo largo de la sesión:

- Amabilidad [2:28] https://www.youtube.com/watch?v=VbkJDZr_Ue8
[Ver diapositiva 20]
- Permisos en apps [2:36] https://www.youtube.com/watch?v=UXeR3iLG_ro
[Ver diapositiva 25]

Otros:

- Ciberacoso [1:20] <https://www.youtube.com/watch?v=asTti6y39xl>
[Varios niños/as “cabeza cuadrado” se burlan por el móvil e Internet de una compañera “cabeza triángulo”. Ella pide ayuda en casa, hablan con algunos compañeros/as, con su profesora, y todos le apoyan.]

¿Cuándo y dónde se meten con la chica?, ¿cuál es el paso clave para que todo se resuelva?, ¿con qué mensajes nos encontramos todos/as más a gusto, con unos de burla y ofensivos o con otros en tono positivo?]

- Piensa antes de publicar (inglés) [2:49]

<https://www.youtube.com/watch?v=QiTJCyxWZoM>

[El famoso gato Garfield pide ayuda a una experta en ciberseguridad cuando ve que su amigo Nermal está compartiendo demasiada información en las redes sociales, incluyendo información personal como su dirección, edad, etc.

¿Nermal se para a pensar antes de compartir una foto o un mensaje en línea?, ¿qué mensajes publica que podrían ser peligrosos para él?, ¿cómo gestiona la situación Garfield?, ¿a quién más podría pedir ayuda?]

- Videojuegos gratuitos [2:35] <https://www.youtube.com/watch?v=8q3EJnZKsx4>

[En este vídeo Pilar se descarga un juego gratuito, pero para poder avanzar y superar niveles tiene que hacer pequeños pagos, que acaban siendo excesivos.

¿Alguna vez os habéis encontrado con un juego o una app que os ofrezca hacer pequeñas compras de objetos virtuales, mejoras, etc. mientras la utilizáis?, ¿por qué Pilar realiza esos pequeños pagos?, ¿no habría sido mejor que consultara primero a sus padres?]