GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

La ciberseguridad es parte de tu día a día

(Menores a partir de 14 años)

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017 TU AYUDA EN CIBERSEGURIDAD
CIBERCOOPERANTES incibe_

LICENCIA DE CONTENIDOS

ÍNDICE

1. CÓMO UTILIZAR ESTE GUION

Este guion se ha desarrollado para servir como referencia a los ponentes que utilicen la presentación “La Ciberseguridad es parte de tu día a día (escolares a partir de 14 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 normalización de la actividad autónoma en Internet y por tanto al fomento de la responsabilidad que supone, para protegerse a sí mismos frente a los riesgos. El objetivo es preparar sus conocimientos y habilidades para que la prevención sea la clave de su seguridad en Internet. También se les forma para saber cómo actuar en caso de problemas.

Debemos tener en cuenta que a partir de los 14 de años todos los menores tienen contacto habitual con Internet de una u otra forma. Además, tienen lugar cambios importantes en su rutina de conexión: menos límites a la hora de conectarse y experimentar, la llegada de su primer móvil, las redes sociales, etc. Siguen 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.

Es importante que en esta sesión tratemos a los menores como personas capaces de conocer e interiorizar información y conocimientos: no son niños o niñas, son jóvenes que tienen capacidad para entender a qué nos referimos con riesgos. El objetivo de esta sesión es hacerles más conscientes, recordarles información que posiblemente ya han oído anteriormente y además reforzarla con nuevas recomendaciones. Es por ello imprescindible hacer una valoración al inicio de la sesión, en la que tanteemos la experiencia general del grupo y poder adaptar así la explicación con esta premisa.

2. INTRODUCCIÓN

2.1.1. Diapositiva 1.

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

Brevemente nos presentamos e introducimos INCIBE y el teléfono de ayuda 017, el proyecto Cibercooperantes (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.

2.1.2. Diapositiva 2. ¿HACEMOS UN USO SALUDABLE DE INTERNET?

[A modo de introducción, tanteamos al grupo para valorar la experiencia que poseen en torno a Internet y la tecnología, para procurar adaptarnos a su nivel de conocimientos. Los menores a menudo no son conscientes de todas las actividades en las 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?, ¿videoconsolas con conexión a Internet?, ¿qué redes sociales utilizan?, ¿qué es lo que más les gusta hacer en Internet?, ¿cuándo y dónde se conectan?, ¿hablan con sus padres sobre sus actividades en línea?, ¿les supervisan de alguna forma?, ¿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.]

2.1.3. Diapositiva 3. NUESTRA RUTINA DE REDES SOCIALES

[Después de las preguntas anteriores, es posible que algunos menores manifiesten que no tienen o no les permiten en casa tener redes sociales, y debemos fomentar la normalización de esta situación: es una elección personal, debemos contar con la autorización familiar y la recomendación ante todo es estar preparado antes de crearse un perfil.]

(En la imagen aparecen los logotipos de WhatsApp, Snapchat, Pinterest, Facebook, Instagram, Skype, Tik Tok, Twitter y YouTube).

Preguntamos al grupo acerca de los logotipos que aparecen en pantalla, ¿los conocen? (seguramente sí, aunque aún no los utilicen todos, pero algunos sí serán habituales en su

tiempo de ocio). ¿Cuánto tiempo dedican a utilizar las redes sociales?, ¿por qué les interesan?, ¿qué ofrecen las redes sociales? Comunicación, sentimiento de comunidad, entretenimiento, etc. En definitiva, son una herramienta que permite la relación con otras personas. Primero hablamos en este punto de funciones positivas, beneficios que hacen de las redes sociales un medio útil y atractivo. Por último, planteamos al grupo la posibilidad de que también existan riesgos en el uso de estos servicios, ¿los conocen?

[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.]

2.1.4. Diapositiva 4. SABEMOS QUE EXISTEN RIESGOS

[La diapositiva contiene dos recortes de noticias reales algunos problemas derivados de un mal uso de Internet. Explicaremos los titulares y remarcaremos la idea de que los riesgos son una realidad, que cualquiera puede verse afectado.]

Comentamos las dos noticias de actualidad con el grupo: un delito derivado de la práctica del sexting y las consecuencias más graves del 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 jóvenes de su edad?

[A continuación explicaremos con más detalle algunos de estos riesgos.]

[Enlaces de interés: https://www.abc.es/espana/castilla-la-mancha/toledo/talavera/abci-detenido-difundir-fotos-intimas-amiga-sin-consentimiento-201812042137_noticia.html https://www.elmundo.es/cataluna/2018/09/01/5b8a57d222601daa0c8b45c2.html]

3. DESCRIPCIÓN DE RIESGOS Y CONSEJOS

3.1. CONTENIDOS POTENCIALMENTE PELIGROSOS

3.1.1. Diapositiva 5. CONTENIDOS POTENCIALMENTE PELIGROSOS

Internet ofrece un espacio inmenso en el que relacionarnos y obtener información de toda clase de temas, pero algunos de ellos son perjudiciales y pueden tener consecuencias graves.

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].

[Evitaremos alimentar en exceso su curiosidad por estos temas, dado que pueden llamar su atención de forma contraproducente, y que luego quieran buscar más información. Por ello nos centraremos en las consecuencias negativas y las estrategias de captación, no mencionando nombres de comunidades o hashtag concretos por ejemplo, y en ningún caso contenidos determinados, como vídeos o páginas web.]

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

3.1.2. Diapositiva 6. CONTACTO CON COMUNIDADES PELIGROSAS.

Hablamos de comunidades en las que, por ejemplo, se habla de hábitos poco saludables, o en las que se transmiten ideologías extremistas que fomentan el odio. En muchos casos, hay personas cuya función es captar usuarios que muestren cierto interés por estos temas en la Red, atacando sus inseguridades e inquietudes, para luego introducirles en una comunidad que será dañina y de las que no es tan fácil salir.

En estos casos, es imprescindible contar con la ayuda de un adulto y profesionales especializados, como la Línea de Ayuda en Ciberseguridad de INCIBE (017), el centro médico o el orientador escolar.

3.1.3. Diapositiva 7. LOS RETOS VIRALES Y SUS RIESGOS.

[La diapositiva contiene tres recortes de noticias reales sobre retos virales. Explicaremos los titulares y remarcaremos la idea de que en general, este tipo de retos son negativos a largo plazo e incluso peligrosos aunque parezcan divertidos en un principio.]

Comentamos las tres noticias de actualidad con el grupo: una en la que la plataforma Netflix se manifiesta en contra de un reto viral derivado de una de sus películas, otra sobre el reto de arrojarse agua hirviendo y otra que llama a la reflexión sobre el interés que suscitan estos retos. ¿Este tipo de noticias son habituales?, ¿por qué difundimos este tipo de retos si muchos llegan incluso a ser peligrosos para la salud?

Enlace de interés: https://www.20minutos.es/noticia/3528902/0/netflix-reto-viral-bird-box-challenge-sandra-bullock/
https://elpais.com/elpais/2017/09/15/hechos/1505477690_631109.html
https://www.elmundo.es/f5/comparte/2018/11/17/5bec53c546163fd52d8b460f.html]

3.2. PRIVACIDAD EN LÍNEA

3.2.1. Diapositiva 8. MI PRIVACIDAD EN LÍNEA.

[Explicaremos el concepto de privacidad, dado que para ellos este no es un riesgo tan evidente como otros. Para los adolescentes, la privacidad suele estar asociada a guardar en secreto frente a los adultos parte de su información más íntima, pero no dudan en compartirla con su grupo de iguales o incluso con desconocidos. 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. Por ejemplo, en la imagen vemos dos capturas de dos cuentas de Instagram de personas muy conocidas, que ya han compartido miles de imágenes personales. ¿Son demasiadas? ¿Qué información están aportando con estas publicaciones? El cuidado de la privacidad depende de qué información deciden mostrar y en qué cantidad, y qué datos prefieren guardarse para sí mismos.

¿Cuánta información sobre ellos existe en Internet? Deben ser conscientes de que 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 además otras personas publican datos sobre ellos, y algunos servicios de Internet también recogen información.

¿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]

3.2.2. Diapositiva 9. LA BÚSQUEDA DE RECONOCIMIENTO SOCIAL

Somos seres sociales, y esto implica que necesitamos sentirnos parte de un grupo, sentirnos queridos y apreciados. Muchas veces solo buscamos encajar, y a cualquiera nos seduce un comentario positivo, unos cuantos 'me gustas' o descubrir que tenemos un nuevo seguidor. Las empresas que han desarrollado las redes sociales son conocedoras de ello, y por eso nos lo ponen en bandeja.

[Podemos hacer referencia a la imagen en pantalla, en la que se ve a una chica sonriendo porque recibe 'me gustas' y comentarios, y tiene muchos seguidores. Recordaremos que las redes sociales, los juegos y otros servicios que utilizamos en Internet tienen como objetivo generar este tipo de sentimientos positivos, que nos hacen necesitar cada vez más y mantenernos enganchados.]

¿Quiere decir que las redes sociales son malas? No necesariamente, siempre que se usen con sentido común, y sobre todo con capacidad crítica. Hoy en día, este tipo de servicios de Internet nos presionan para que compartamos mucha información: debemos publicar fotos constantemente, decir qué hacemos en todo momento (para ello se crearon los 'estados' o las 'historias' de WhatsApp o Instagram por ejemplo), también si hacemos deporte, o si vamos a asistir a un evento. Sabemos que, si no lo hacemos, no conseguimos seguidores, ni 'me gustas', y qué cuanto más mostramos mejor. Pero es demasiada información si nos paramos a pensarlo.

3.2.3. Diapositiva 10. CREA UNA IDENTIDAD DIGITAL POSITIVA

Está en nuestras manos decidir qué hacemos público y qué no, y en eso consiste la gestión de la privacidad. Hay una parte de esa información que podemos guardar para nosotros, o para mostrarla fuera de Internet, a nuestra familia o amigos más cercanos. Porque el problema de Internet es que todo lo que se publica, se escapa a nuestro control, y en la mayoría de los casos, permanecerá durante años accesible a cualquiera que lo encuentre.

¿A qué nos referimos con identidad digital? Toda esa información que está en Internet ofrece una imagen a los demás de cómo somos, o de cómo nos ven: nuestro aspecto, nuestros gustos y aficiones, nuestra manera de ser, nuestros amigos... No siempre coincide con la realidad, ya sea porque nos mostramos en este medio de forma diferente, o porque nos perciben de forma diferente después de hacer una mala gestión de nuestra información.

(Por ejemplo, si durante el fin de semana publicamos una imagen de fiesta con los amigos, porque nos sentimos atrevidos o nos parece divertido, el lunes podemos descubrir que ofrece una imagen de nosotros equivocada, que no nos gusta o que ha generado reacciones que nos perjudican: rumores, burlas, etc. Pero esa imagen ya la han visto cientos de personas, o miles. Y no podemos dar marcha atrás.)

Por el contrario, si cuidan la información que publican, pueden ofrecer lo mejor de sí mismos, una imagen de la que se sientan orgullosos, aunque pase el tiempo.

3.2.4. Diapositiva 11. CONFIGURA TU PRIVACIDAD.

Es el momento de transmitirles la idea de que para utilizar Internet de forma responsable es necesario conocer cómo configurar su ciberseguridad, porque no es un juguete.

En cada red social o plataforma que utilicemos, por ejemplo, los videojuegos, debemos dedicar unos minutos a conocer qué opciones de privacidad ofrece y cómo queremos configurarlas. Si lo pensamos bien, tan solo serán unos minutos en comparación con las horas que dedicaremos a utilizarlas, y nos evitarán muchos problemas.

Lo recomendable en general es que mantengan los perfiles privados, de manera que nadie pueda conocer el contenido que publican sin que hayan autorizado y comprobado su perfil previamente. Y, aunque esto les aporte seguridad, no quita para que se obligatorio revisar de vez en cuando su lista de amigos, eliminando los que no consideren de confianza, y activando el registro de actividad si es posible. En cuanto alguien les moleste, no hay que dudar: se bloquea su perfil.

Por último, recordar que nunca deben mostrar datos personales como el nombre, la dirección, el teléfono o información sobre nuestra rutina diaria y nuestros horarios.

3.2.5. Diapositiva 12. ¿PRACTICAS SEXTING?

[Dado que es un tema delicado e íntimo, procuraremos no hacer preguntas a participantes concretos. Se trata de mantener un tono cercano pero serio, para que comprendan que en ningún caso es una práctica sin riesgos.]

Hacerse fotos o grabarse vídeos con cierta connotación sexual puede parecer divertido o tentador, pero lo cierto es que supone muchos riesgos. ¿Recuerdan la noticia que hemos comentado antes sobre un caso de sexting que terminó verdaderamente mal?, ¿creen que eso solo les ocurre a los demás? No, le puede pasar a cualquiera.

Porque por mucho cuidado que tengan, el simple hecho de almacenar ese tipo de imágenes en el móvil o en el ordenador es muy arriesgado. Pueden perderlo, que se lo roben, o que sea infectado por un virus informático, por ejemplo. Son situaciones que están ocurriendo a diario. ¿Han oído noticias sobre famosos que han pasado por algo así? Es bastante habitual hoy en día.

Si además de crear esa foto o vídeo, la envían, el riesgo se multiplica. Están poniendo en manos de otra persona su privacidad. Y, a pesar de que en ese momento confíen plenamente en la otra persona, las cosas pueden cambiar o no ser tan seguras como pensamos. ¿Les suena eso de “te la paso pero no se la enseñes a nadie”? La difusión en estos casos es imparable.

Y recordemos que, si antes corrían riesgo por guardar esas imágenes en su móvil, ahora el riesgo se multiplica de nuevo: son como mínimo dos móviles los que almacenan ese contenido y que pueden perderse o ser robados. El riesgo es muy alto.

Por ello, la recomendación es no realizar esta práctica, ni tampoco pedir a otras personas que la practiquen. Es una forma de respetar y respetarse, de cuidar nuestra intimidad: se trata de protegernos y proteger a nuestra pareja de las consecuencias. Además, hay que tener en mente que el simple hecho de tener imágenes íntimas de otros menores en el móvil puede considerarse un delito, más aún si se difunden. No es un juego.

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

3.3. RELACIONES SALUDABLES EN LÍNEA

3.3.1. Diapositiva 13. 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.

Y a pesar de que Internet ofrece un nuevo medio de comunicación con muchas ventajas, hay 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.

3.3.2. Diapositiva 14. CONVIVIR EN LA RED: NETIQUETA

¿Conocen el término netiqueta? Hace referencia a unas normas básicas de educación que debemos mantener también en Internet. Al igual que fuera de la Red, cuando tratamos con personas debemos cuidar nuestra forma de comunicarnos, nuestro lenguaje, ya que con mayor facilidad puede dar pie a malentendidos. En Internet, no podemos apoyarnos en nuestros gestos o expresiones, por lo que debemos intentar siempre que nuestras palabras transmitan realmente lo que queremos decir. Y de igual manera nos pondremos en la piel de los demás ante un malentendido: ¿realmente me están atacando, o estoy malinterpretando su mensaje? Mantener la calma y pedir una explicación es más sencillo que acabar enfrentados.

Cuando haya diferencias de opinión, hemos de respetarlas y aprender a argumentar y razonar, sin ofender a la otra persona. Lo fácil es insultar, lo que verdaderamente demuestra conocimiento es saber discutir.

Por último, todos sabemos que hay personas que se dedican a ofender y entorpecer la comunicación en las redes sociales. Contra ellos, la mejor herramienta es la indiferencia, no contestar y bloquear si se trata de nuestra propia cuenta.

3.3.3. Diapositiva 15. 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 una problemática muy normalizada 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.

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

3.3.4. Diapositiva 16. TÚ PUEDES PARARLO.

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

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. Así que sí es posible actuar y participar para que una persona deje de sufrirlo, y el acosador entienda que no tiene su apoyo.

¿Qué pueden hacer? 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, ¿les gustaría sentirse solos ante esta situación? Ante la excusa habitual de "si me pongo de su parte me acabarán atacando a mí", la respuesta es que si todos mostrásemos nuestro rechazo, los acosadores no se verían capaces de atacar. Y recordemos que cualquiera puede ser víctima de ciberacoso, y en ese caso, también necesitaremos apoyo.

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'.

3.3.5. Diapositiva 17. GROOMING: ¿QUÉ ES?

[Describimos el concepto de grooming y las claves para identificarlo.]

¿Sabéis que es el grooming? Es una realidad que hay personas que utilizan Internet como medio para acercarse a ellos con malas intenciones. Recordemos que cualquiera puede crear un perfil falso, cambiar su imagen, su edad y aparentar tener gustos parecidos a los nuestros. De esa forma, se ganan vuestra confianza, consiguen que acepten su solicitud de amistad y comienzan a conversar con ellos.

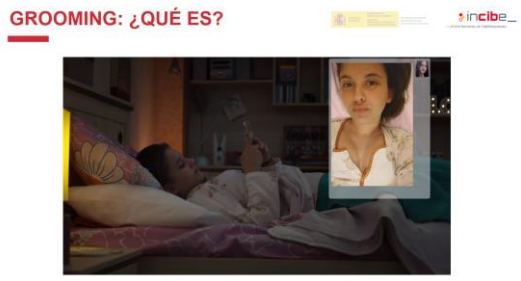
Cuando ya tengan una relación afianzada, les pedirán una imagen o un vídeo de connotación sexual, y habrán logrado su objetivo. A partir de ahí pueden chantajearles para conseguir más contenidos de este tipo, dinero o incluso que queden en persona, Todo con la amenaza de que si no lo hacen difundirán lo que ya está en su poder.

Estas personas utilizan todas las plataformas y redes sociales que ellos utilizan, porque saben que ahí encontrarán jóvenes y que es un lugar donde se puede establecer una comunicación.

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

3.3.6. Diapositiva 18. GROOMING: ¿QUÉ ES?

[Se incluye un vídeo que se puede visualizar con conexión a Internet. En este vídeo de Europol se muestra el proceso de acercamiento y contacto de un adulto con un menor a través de las redes sociales.



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.]

¿Os habíais planteado lo sencillo que puede ser que alguien se haga pasar por otra persona en Internet para engañar a un menor? ¿Creéis que los protagonistas del vídeo son muy ingenuos, o que le podría pasar a cualquiera? Pero entonces, ¿cómo evitarlo?

(Dejaremos que ellos mismos aporten sugerencias sobre cómo evitarlo)

La clave es no confiar en las amistades online, porque nunca sabemos qué se esconde detrás o cuales son las intenciones de esa persona. Y como comentamos anteriormente, evitar la práctica del sexting es fundamental, porque no sabemos qué uso se va a hacer al final de esa foto o de ese vídeo.

(Enlace al vídeo: https://www.youtube.com/watch?v=_whpii1co1g)

3.3.7. Diapositiva 19. HAZLE FRENTE: PROTÉGETE.

Prevenir este problema es posible:

- No ofrecer datos personales: cuanta menos información tengan de ti, menos probable es que les parezcas un menor vulnerable al que pueden chantajear.
- Nunca quedes en persona con alguien que has conocido en Internet: de hacerlo, hacerlo en compañía de sus padres. Si realmente están hablando con un delincuente no aceptará este tipo de respuestas.
- Si tienen dudas sobre la persona con la que están hablando: bloquear.

Si ya se han visto envueltos en un problema de grooming, o conocen a alguien en esta situación, es imprescindible contárselo a un adulto o a los cuerpos policiales.

3.4. USO EXCESIVO

3.4.1. Diapositiva 20. ¿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]

3.4.2. Diapositiva 21. 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?

Ellos mismos pueden darse cuenta de cuándo se están pasando: si están dejando de lado a sus amigos, si se pierden otras actividades por conectarse, si se notan irritables cuando no tienen el móvil o la consola, etc. 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. 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.

3.4.3. Diapositiva 22. NO DEJES DE LADO TODO LO DEMÁS.

[Se incluye un vídeo que se puede visualizar con conexión a Internet. En este corto la protagonista es la única que no tiene móvil, y por ello es consciente de todo el tiempo que dedican los demás a esta actividad y lo que se están perdiendo por hacer un uso excesivo.

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.]

¿Las escenas del vídeo son habituales o una exageración? ¿Merece la pena dedicar tanto tiempo a estar conectados, mientras nos estamos perdiendo otros acontecimientos o momentos de nuestra vida? ¿Qué podemos hacer para evitar hacer un uso excesivo del móvil y de Internet?

(Enlace al vídeo: https://www.youtube.com/watch?v=OINa46HeWg8)

3.5. CONFIGURACIONES SEGURAS

3.5.1. 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.

Por último, recordaremos la importancia de bloquear la pantalla para evitar que otras personas puedan acceder, ya sea en el móvil como en la tableta o el ordenador.

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

3.5.2. Diapositiva 24. VERIFICACIÓN EN DOS PASOS.

Esta función la ofrecen algunos servicios como Gmail, Facebook, Instagram… y resulta muy útil para proteger nuestra cuenta más allá de una simple contraseña. Su funcionamiento consiste en que, después de introducir su contraseña, enviarán a su móvil un mensaje, un código o una llamada de teléfono para comprobar que efectivamente están accediendo ellos. De esta forma, aunque alguien averiguara la contraseña, también necesitaría su móvil (y la clave del móvil) para poder acceder.

Puede parecer complicado, pero no lo es, activarlo es muy sencillo. Además, podemos configurarlo para que solo funcione en dispositivos ajenos, por lo que en nuestro día a día no sería necesario utilizarlo al usar el móvil o el ordenador de casa, por ejemplo.

3.5.3. Diapositiva 25. 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.

3.5.4. Diapositiva 26. EL WIFI GRATIS TE PUEDE SALIR CARO.

[Los menores utilizan habitualmente estas redes públicas en cafeterías o centros comerciales, sin percatarse de que puede suponer un riesgo.]

Es importante extremar la precaución al usar este tipo de redes 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).

4. REACCIÓN FRENTE A PROBLEMAS

4.1. SOLUCIONAR PROBLEMAS Y PEDIR AYUDA

4.1.1. Diapositiva 27. ¿CÓMO PROTEGERSE EN LA RED?

[En esta diapositiva se enumeran brevemente algunos de los riesgos a los que pueden enfrentarse los menores al navegar por Internet, y algunas recomendaciones sencillas de protección.]

¿Qué problemas nos podemos encontrar mientras navegamos por la Red? Algunos riesgos como virus, fraudes, phishing (páginas web que parecen ser auténticas pero que en realidad no lo son, y que pueden utilizarse para recabar información del usuario fácilmente, como datos de acceso, contraseñas, etc.) u otras estrategias de ingeniería social, entre otros.

Para protegernos, debemos tomar algunas medidas en nuestros dispositivos, son sencillas y seguro que las conocemos, pero ¿nos las tomamos en serio? Es necesario instalar un antivirus y mantenerlo actualizado, así como actualizar todas las aplicaciones que utilicemos y los sistemas de nuestro dispositivo. También debemos realizar copias de seguridad de nuestros datos periódicamente, procurar acceder a páginas web con certificado de seguridad (https) y descargar aplicaciones solo de desarrolladores oficiales.

[Enlaces de interés: https://www.osi.es]

4.1.2. Diapositiva 28. ¿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 identificar 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.

- 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 es 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.

4.1.3. Diapositiva 29. EN INCIBE OS AYUDAMOS.

Mostramos la información de INCIBE prestando especial atención a la Línea de Ayuda en Ciberseguridad de INCIBE a través de la cual 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 https://www.incibe.es/linea-de-ayuda-en-ciberseguridad.

Animamos a los participantes a visitar las diferentes webs de INCIBE en función del público (Ciudadanos, Menores o Empresas) y a seguirnos en redes sociales.

Además, explicamos que en la web pueden encontrar mucha información y actividades para trabajar cualquier tema de ciberseguridad, juegos y recursos pedagógicos.

(Se proponen como ejemplos:

Una serie de mensajes visuales sobre el cibercontrol “No le controles” https://www.is4k.es/convivencia-y-respeto-en-internet

Un cartel “Ciberacoso escolar: no comparto, no me gusta” https://www.is4k.es/ciberacoso

La iniciativa jóvenes https://www.is4k.es/jovenes).

Enlaces de interés:

Ciudadanos:

https://www.osi.es/es/campanas

https://www.osi.es/es/hackers

https://www.osi.es/es/juegos-mesa

https://www.osi.es/es/cuanto-sabes

Menores:

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

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

https://www.is4k.es/campanas

https://www.is4k.es/de-utilidad/test

5. CIERRE

5.1. 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 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.]

5.1.1. Diapositiva 30. ¿A QUÉ NOS REFERIMOS CON IDENTIDAD DIGITAL?

La respuesta 'a) Es un sinónimo de contraseña' no es correcta.

La respuesta 'b) Es la manera en que nos presentamos en Internet' no es correcta, ya que no solo nosotros influimos en la construcción de esta identidad, también lo hacen los demás cuando publican información o fotos sobre nosotros, por ejemplo.

La respuesta 'c) Es la información que hay sobre nosotros en la Red' es la opción correcta.

La respuesta 'd) Coincide con nuestra identidad real' no es correcta, ya que a pesar de lo que queramos transmitir, a veces los demás lo pueden percibir de manera diferente.

5.1.2. Diapositiva 31. ¿TENEMOS PODER PARA ACABAR CON EL CIBERACOSO?

La respuesta 'a) Sí, todos los que observamos la situación podemos ayudar a frenarla' es correcta, dado que podemos actuar de muchas maneras para no participar en el acoso.

La respuesta 'b) No, es imposible, siempre habrá acoso en Internet' no es correcta, ya que depende de nosotros hacer que los acosadores pierdan el interés en este tipo de prácticas.

La respuesta 'c) Sí, si no nos unimos a las burlas y humillaciones' no es correcta, ya que además de no apoyar al acosador es necesario comunicárselo a un adulto para que entre todos resolvamos el problema.

La respuesta 'd) No, algunos se lo tienen merecido' no es correcta, ya que nadie se merece un daño así.

5.1.3. Diapositiva 32. LA VERIFICACIÓN EN DOS PASOS…

La respuesta ‘a) Permite activar un teléfono nuevo’ no es correcta.

La respuesta ‘b) Te ayuda a proteger mejor tus cuentas de redes sociales y correo electrónico’ es correcta, ya que aporta un extra de seguridad a la contraseña.

La respuesta ‘c) Es un proceso muy complejo, no merece la pena’ no es correcta, configurar esta opción es muy sencillo.

La respuesta ‘d) Utiliza un mensaje de texto para autenticarte’ no es correcta, porque existen otros métodos de verificación como llamadas o códigos a través de una aplicación.

6. ANEXO

6.1. RECURSOS PARA AMPLIAR

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

- Grooming [10:34]
  [Ver diapositiva 18]
- Uso excesivo [2:10]
  [Ver diapositiva 22]

Otros:

- Rap Ciberacoso [2:45]
  [Emotiva canción del conocido rapero Arkano sobre su experiencia personal con el acoso escolar.
  ¿Creéis que es habitual una “ley del silencio” en torno al acoso?, ¿qué emociones os transmite Arkano al revivir aquellos momentos?, ¿qué dice sobre las personas que ven la situación y no hacen nada?]
- Cita a ciegas [3:01]
  [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 [1:05]
  [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 [3:10]
  [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?]