Unidad de Contenido

Control Parental

Proyecto: B-SAFE
Número: 2018-1CZ01-KA204-048148
Nombre del autor: UDIMA
Último procesamiento de datos: 24.9.2020

Funded by the
Erasmus+ Programme
of the European Union

Co-funded by the
Erasmus+ Programme
of the European Union

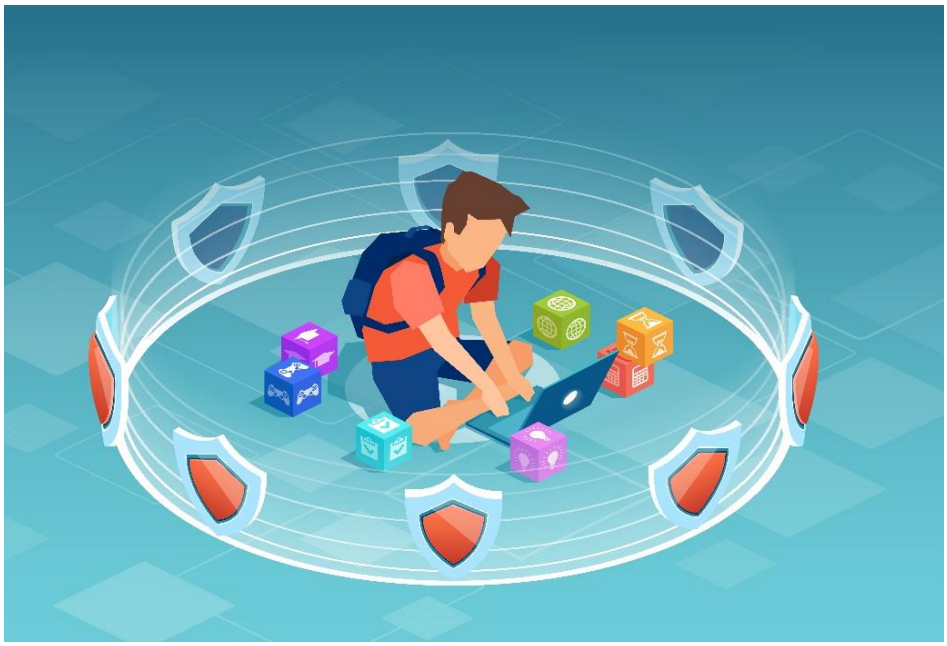
Control Parental

Introducción

Ejercer el control parental para garantizar la seguridad de los menores a su cargo ha sido siempre una de las funciones de los padres y tutores. Hoy en día se espera que esta función sea llevada a cabo por ellos y se vuelve aún más importante.

Pueden enfrentarse a numerosos peligros como el sexting, el grooming, el ciberacoso, la adicción a internet y la divulgación no deseada de información. Estos peligros consisten en exponerse o ser expuesto a contenido sexual, ser acosado por un adulto, ser intimidado, convertirse en adicto a Internet, o tener sus datos expuestos.

Todos ellos pueden acarrear consecuencias negativas para la víctima en lo que respecta a su salud emocional y física. Prestando atención a estos peligros y a sus primeras consecuencias es posible establecer algunos consejos y detectar el problema.



Importancia práctica– ¿Para qué necesitas estos conocimientos y habilidades?

Después de aprender esta unidad de contenido, conocerás la importancia del control parental a la hora de proteger a los niños y adolescentes de situaciones peligrosas en las que podrían verse involucrados al utilizar diferentes dispositivos tecnológicos.

1. Construye conocimiento – ¿Cuáles son los principios del control parental y por qué es necesario?

Hoy en día, dado el gran avance de las nuevas tecnologías, los niños, adolescentes y jóvenes tienen cada vez más contacto con ellas. De hecho, en numerosas ocasiones, se encargan de enseñar a los adultos que les rodean a utilizar ordenadores, tabletas o teléfonos móviles.

No es posible separar a los menores de estas tecnologías, o al menos, no es fácil. El uso de Internet se ha convertido en algo necesario en los trabajos e incluso en nuestra vida cotidiana. La necesidad de enseñarles a utilizar los dispositivos tecnológicos se ha convertido en un hecho y, por lo tanto, también se ha visto la necesidad de integrarlos en el sistema educativo. En realidad, son un pilar fundamental en su educación y muy útiles a la hora de buscar información y realizar tareas escolares.

Muchos centros ya han incluido plataformas a través de las cuales ofrecen recursos en línea a sus alumnos, les envían tareas e incluso les piden que entreguen dichas tareas a través de la plataforma. En este punto en el que mantenerlos alejados de las tecnologías de la información es tan difícil e incluso contraproducente, parece apropiado considerar cómo protegerlos.

Los peligros que pueden afectar a los niños, adolescentes y jóvenes en Internet son múltiples, empezando por el ciberacoso o el sexting, que pueden ocurrir con personas que conocen y están a su alrededor (de su escuela o de su vecindario, por ejemplo), e incluso continuando con las amenazas externas, que son las que provienen de extraños. Las personas desconocidas tienen la posibilidad de recopilar información sobre menores y contactar con ellos, no siempre con las mejores intenciones.

Además, herramientas tecnológicas como los teléfonos móviles u ordenadores portátiles dan acceso a los menores a una gran cantidad de contenido web que puede ser completamente inapropiado, como el contenido violento, la pornografía o contenido radical. Uno de los aspectos que más preocupan a los padres y que puede llevar a los menores a cualquiera de las amenazas mencionadas son las redes sociales. Las redes sociales permiten el acceso de menores que entran por debajo de la edad estipulada para su uso, porque pueden mentir fácilmente y marcar la edad deseada sin que se haga ninguna verificación.

Antes de la aparición de las nuevas tecnologías, todo el proceso de experimentación, establecimiento de nuevas relaciones, etc. por el que pasan los menores, ocurría ante los ojos de todos. Era más visible. Por eso el ejercicio del control parental era mucho más sencillo y no había tantas complicaciones para alejar los peligros. Es también por eso que, hoy en día, la definición de control parental adquiere nuevos matices y nuevos medios, pero sigue manteniendo su esencia. El control parental se define, por lo tanto, como:

Definición
Control parental

… la forma en que los padres supervisan e intervienen, si es necesario, para garantizar que las experiencias y los procesos de socialización y crecimiento personal de sus hijos se produzcan adecuadamente y sin riesgos para ellos.

Los riesgos a los que se enfrentan los menores no han cambiado en esencia, sino la manera y los medios a través de los cuales pueden verse amenazados. Las nuevas formas de riesgo conducen a nuevas formas y métodos de control parental para garantizar la seguridad de los menores.

Ejemplo
Por ejemplo, los niños pueden sufrir intimidación en forma de insultos, rechazo, amenazas, ridiculización o difusión de bromas, ya sea cara a cara o a través de Internet, llegando más rápido y más lejos.

Un sistema de control parental es una herramienta que permite a los padres controlar y/o limitar el contenido al que sus hijos pueden acceder a Internet desde sus dispositivos, ya sean ordenadores, móviles o tabletas. Existen muchas herramientas parentales diferentes y pueden ser utilizadas en los dispositivos de los menores para detener algunas acciones, páginas o contenidos o para controlarlos desde el mismo dispositivo o incluso desde el dispositivo de los adultos.

Ejemplo
Si los padres están preocupados por la seguridad de sus hijos, deben considerar qué dispositivos utiliza el niño y la edad de este. Existen aplicaciones y programas para controlar el uso de Internet, pero no todos están disponibles en todos los dispositivos. La edad del niño también guiará a los padres a elegir una herramienta u otra, ya que pueden esperar cosas diferentes según sus necesidades. Para los pequeños, puede ser una herramienta adecuada en el mismo dispositivo para detener el contenido que no está hecho para los niños, mientras que para los adolescentes puede ser necesario controlar la hora en el mismo dispositivo o lo que ven desde los dispositivos de los padres. Las herramientas de control parental están disponibles en todos los dispositivos, pero si se desea algo más específico, se pueden encontrar otras herramientas en las tiendas en línea o en las tiendas de aplicaciones o herramientas ofrecidas por las compañías de seguros y de seguridad y los proveedores de Internet.

En general, los sistemas de control parental con los que contamos hoy en día se utilizan para garantizar la seguridad de los menores en la red, evitando así posibles amenazas y malas experiencias. Más específicamente, los sistemas de control parental son herramientas que han sido diseñadas para bloquear y filtrar el acceso a diferentes puntos de Internet y para vigilar su uso. Estas herramientas ofrecen cada vez más funcionalidades y pueden ser personalizadas y adaptadas a las necesidades de los padres. Estas funcionalidades pueden dividirse en las siguientes secciones:

- Monitoreo: para realizar un seguimiento de la actividad en línea. Permite al usuario analizar dónde entra el niño, generando avisos si entra en sitios web no recomendados.

- Controlar el contacto con otras personas: esta funcionalidad permite al usuario evitar el contacto de su hijo con extraños, que según el INCIBE (Instituto Nacional de Ciberseguridad), ocurre en el 40% de los menores.

- Limitar el tiempo de uso: permite controlar tanto el tiempo máximo de acceso del niño como el tiempo en el que tiene permiso para mantener el dispositivo encendido.

- Controlar el acceso a sitios inapropiados: permite al usuario controlar o bloquear el acceso a sitios web cuyos contenidos son sensibles para edades tempranas o que comprometen sus datos.

- Restringir las aplicaciones: esta funcionalidad impide el uso o la descarga de ciertas aplicaciones.

- Evitar las compras en línea: es posible desactivar la compra, intencionada o no, de aplicaciones u otros artículos en línea.

- Geolocalización: permite conocer la ubicación exacta del niño.

- Segundo factor de autenticación: además de la contraseña para desbloquear el dispositivo, se requiere un código que se envía a los padres para desbloquear el dispositivo. De esta manera, son los padres los que dan acceso a los menores en todo momento.

- Bloqueo de llamadas.

Todas estas formas de control parental se utilizan para garantizar la seguridad de los menores, protegiéndolos de extraños y de contenidos o páginas inapropiadas. También ayudan a proteger a los niños y adolescentes del uso indebido de Internet por parte de ellos mismos o de otros, ya sea de forma intencionada o no. Esta protección puede llevarse a cabo mediante la vigilancia del uso de Internet por parte de los niños o mediante el bloqueo y el control de diferentes funciones.

En el caso de los pequeños, las herramientas de control parental que suelen elegirse son las que limitan e impiden el acceso a determinados contenidos inapropiados para su edad o limitan el tiempo de uso de las diferentes aplicaciones y dispositivos. Estas herramientas utilizan diferentes técnicas para lograrlo. La mayoría de ellas utilizan listas en las que se filtran los sitios que no deben ser vistos (listas negras) o permiten el acceso sólo a los contenidos que están en las listas blancas, listas de contenidos adecuados para los pequeños. También es posible bloquear el acceso a contenidos con determinadas palabras clave (pornografía, drogas, compras, etc.), lo que puede dar lugar a que se bloqueen páginas adecuadas para los menores debido a falsos positivos. Además, este tipo de herramientas de control parental permiten también bloquear el acceso a aplicaciones específicas, permitir su uso sólo sin acceso a Internet, desactivar la función de chat o controlar el tiempo y el horario en que se les da acceso.

Por otro lado, y pensando en los adolescentes, también se han creado herramientas de control parental que permiten el uso de dispositivos electrónicos y la vigilancia de la actividad. Se llega a un punto en el que los niños necesitan utilizar sus dispositivos con mayor libertad, mientras que su conocimiento de estas herramientas aumenta y sienten curiosidad por saber más y contactar con otras personas. A partir de estas herramientas de control parental que permiten a los padres monitorear la actividad, es posible conocer los servicios a los que acceden los adolescentes, lo que hacen, las personas con las que contactan y dónde se conectan. Esto último es posible gracias al GPS y a las técnicas de localización que incluyen todos los dispositivos móviles.

Este control parental se puede ejercer desde diferentes puntos:

- Routers y servidores DNS (Domain Name System): el router es el acceso digital de una casa y a través de él se pueden gestionar las restricciones de navegación de todos los dispositivos que se conectan a él. Desde el router es posible controlar y filtrar los contenidos a los que tienen acceso y a los que ya han accedido todos estos dispositivos conectados, marcar los límites de tiempo de conexión y aplicar filtros en las páginas web. También puede ser filtrado por los servidores DNS.

Análisis

Es una buena opción para controlar todos los dispositivos de la casa, pero puede no ser la mejor opción si se quieren establecer restricciones específicas para cada dispositivo. Además, no es posible controlar los dispositivos cuando no se encuentran conectados al servidor.

- El dispositivo en sí: todos los dispositivos que tenemos en casa (ordenadores, tabletas, teléfonos móviles e incluso juguetes) incluyen paquetes de control parental y permiten bloquear el acceso a contenidos que no son adecuados y controlar la actividad en línea.

Análisis

Al encontrarse incluido en el dispositivo, no necesitamos buscar otros sistemas de control parental y evitamos pagar por este servicio. Además, nos permite aplicar el control en cada dispositivo individualmente. Sin embargo, no suele ser posible personalizar y adaptar el servicio a nuestras necesidades.

- Software: Además de los programas de control informático que protegen contra diversos peligros que podemos encontrar en Internet, como virus y malware, también es posible bloquear sitios web, marcar límites de tiempo o controlar la actividad en línea, recibir resúmenes o información sobre chats.

Análisis

Puede ser menos intuitivo que otras herramientas, pero es posible controlar tanto el contenido visitado en Internet como el uso del propio dispositivo.

- El navegador de Internet: a través del navegador, es posible establecer filtros y evitar que se abran ciertos sitios web e incluso se pueden seleccionar los dominios que se desee bloquear.

Análisis

Es muy útil bloquear las direcciones que contienen ciertas palabras, páginas específicas o todas aquellas páginas que pertenecen a ciertas categorías. Aunque esta herramienta es muy útil para controlar el uso de Internet, no sirve para controlar el dispositivo en sí.

- APPs: Son aptas para cualquier dispositivo móvil, a través del cual los menores suelen conectarse. Con estas aplicaciones es posible controlar los sitios que visitan, el tiempo que pasan, evitar la descarga de otras aplicaciones, evitar el contacto con extraños e impedir la divulgación de sus datos.

Análisis

Se trata de potentes herramientas a elegir de entre el gran número existente y que son fáciles de instalar y usar. El único problema es que estas aplicaciones suelen estar disponibles para teléfonos móviles y a veces para tabletas, pero no siempre para otros dispositivos como ordenadores o portátiles.

El nivel de supervisión que ofrecen estas aplicaciones, especialmente este último grupo de herramientas, es muy alto, lo que puede llevar a ser percibidas como intrusivas. Además, así como los menores tienen derecho a ser protegidos contra todas las formas de abuso que se puedan encontrar en la red, también tienen derecho a la privacidad. Por consiguiente, es aconsejable no hacer un uso

abusivo de esos instrumentos de control parental, evaluar su utilización y tratar de establecer relaciones de confianza con los niños que promuevan el diálogo.

1. Aplica conocimiento

Ejercicio de OPCIÓN SIMPLE

Asociado al objetivo específico OE_ControlParental_01_01: sabrás qué amenazas tecnológicas afectan a los menores

Situación: ¿Qué amenazas tecnológicas impactan a los menores?
Tarea: Elige la opción correcta entre las que se presentan. Solamente una respuesta es correcta.

- Solo el ciberacoso
- Existen múltiples daños que pueden afectar a niños, adolescentes y jóvenes en internet (ciberacoso, sexting…)
- No hay ningún peligro tecnológico que amenace a los menores

Ejercicio de OPCIÓN SIMPLE

Asociado al objetivo específico OE _ControlParental_01_02: podrás definir el "control parental"

Situación: ¿Cuál es la definición del término "control parental"
Tarea: Elija las opciones correctas siguiendo el principio de opción múltiple: solo una respuesta es verdadera.

- "Control Parental" es la forma en que los padres supervisan e intervienen, si es necesario, para garantizar que las experiencias y los procesos de socialización y crecimiento personal de sus hijos se produzcan adecuadamente y sin riesgos para ellos.
- "Control Parental" es una herramienta que permite a los padres controlar y/o limitar los contenidos a los que sus hijos pueden acceder a Internet desde sus dispositivos, sean estos ordenadores, móviles o tabletas.
- "Control Parental" es una amenaza tecnológica que puede afectar a los menores.

Ejercicio de OPCIÓN SIMPLE

Asociado al objetivo específico OE _ControlParental_01_03: puedes explicar para qué sirve el control parental.

Situación: ¿Para qué sirve el control parental?
Tarea: Elija las opciones correctas siguiendo el principio de opción múltiple: solo una respuesta es verdadera.

- Para controlar y/o limitar el contenido al que los niños pueden acceder a Internet desde sus dispositivos, sean estos ordenadores, móviles o tabletas.
- Para dar a los niños la oportunidad de navegar por Internet como deseen.
- Para controlar las cuentas de medios sociales de los niños

Ejercicio de OPCIÓN SIMPLE

Asociado al objetivo específico OE _ControlParental_01_04: sabes cómo funciona el control parental tecnológico.

Situación: ¿Cómo funciona el control parental tecnológico?
Tarea: Elija las opciones correctas siguiendo el principio de opción múltiple: solo una respuesta es verdadera.

- El control parental tecnológico evita que el niño acceda a Internet apagando el router.
- El control parental tecnológico evita que los menores utilicen dispositivos electrónicos en casa mediante el uso de contraseñas online.
- El control parental tecnológico se puede ejercer desde diferentes puntos: servidores externos y DNS, el propio dispositivo, software, navegador de Internet o APPs.

2. Construye conocimiento – ¿Qué es el sexting?

El sexting consiste en el envío de imágenes o vídeos sexuales, realizados por el propio remitente, principalmente a través del teléfono móvil, o por otros dispositivos tecnológicos. El término es un anglicismo que proviene de unir la palabra sexo, y el texting, el envío de mensajes. Sus inicios fueron en los países anglosajones en 2005, que se han ido extendiendo gradualmente al resto del mundo.

Para diferenciar el sexting del grooming es importante señalar que, en el primer caso, las imágenes o vídeos son realizados por el mismo remitente voluntariamente o por otra persona, pero quien los protagoniza da su consentimiento., Cuando los menores realizan sexting con el acosador, por engaño o coacción, no sería sexting como tal, ya que aunque en algunos casos es voluntario están siendo engañados. El sexting distingue entre dos actors: los que realizan el acto de filmación, sexting active; o los que reciben las imágenes, sexting pasivo.

Algunos jóvenes lo hacen como un regalo a sus parejas, como un elemento de coqueteo o para llamar la atención. El riesgo que contiene esta práctica es que el receptor puede enviar las imágenes o utilizarlas para coaccionar para obtener más imágenes, u otros objetivos. También es posible una distribución no percibida por descuido o error.

Definición
Sexting

… consiste en enviar (emisor) imágenes o vídeos de contenido sexual por teléfono móvil a sus parejas (receptor). La persona que protagoniza estos videos o imágenes es quien las envía y lo hace voluntariamente.

El sexting activo es cuando la persona toma fotos o videos con poses sugestivas o sexuales y los envía a otra persona.El sexting pasivo es cuando la gente recibe fotos tomadas por otras personas.
¿Por qué el sexting es una amenaza potencial para los niños y jóvenes? Se trata de un grave peligro en Internet porque, después de enviar estas imágenes, el remitente pierde todo el control sobre ellas. De esta manera, este contenido puede llegar a muchas más personas por diversas razones:

- El destinatario envía ese contenido a propósito a otras personas, que lo reenvían sin cesar hasta llegar a un público muy amplio.
- El protagonista de las imágenes las envía por error a una persona equivocada, que las envía a otras personas.
- Alguien roba el móvil, la tableta o el ordenador de uno de los propietarios de las imágenes, que las publica en Internet.
- Alguien entra en el móvil o el ordenador de uno de los propietarios de las imágenes, enviándolas así a más personas, publicándolas en Internet o reenviándolas a su protagonista para iniciar una fase de chantaje o extorsión.

Esas imágenes pueden terminar en múltiples lugares:

- En los dispositivos móviles de los conocidos del protagonista, como, por ejemplo, sus propios padres.
- En las redes sociales, donde se tiene acceso público a ellas.
- Páginas de contenido sexual y/o pornográfico.
- En manos de los *groomers*, que ven en ellas a su presa perfecta para poder cumplir con sus peticiones (ver grooming).

Las consecuencias para la víctima son:

- Humillación y linchamiento social para el protagonista de las imágenes.
- El menor se enfrenta al insulto público, afectando en primer lugar a su autoestima, en una edad en la que su personalidad se está formando y depende en gran medida de la imagen que los demás perciban, ya que la opinión de los demás es importante.
- También hay sentimientos de indefensión, principalmente cuando el caso se le cuenta a los padres, o a los educadores, o de culpa por haberse puesto en esa situación.
- Estos sentimientos pueden conducir a una profunda tristeza, ansiedad, depresión, disminución o aumento del apetito, o incluso, en los casos más extremos, a intentos de suicidio.

Importante
El descubrimiento de la distribución de las imágenes lleva a la pérdida de confianza en terceros: problemas para relacionarse en el entorno escolar, contribuyendo a un aislamiento autoimpuesto para evitar miradas, comentarios insultantes, etc.

La prevención del sexting puede llevarse a cabo por los padres, madres o tutores, y también por los propios menores. En el caso de los padres o tutores:

- Deben enseñar a los menores que lo que comparten en Internet tiene sus consecuencias, y que, aunque lo compartan en privado con una persona muy cercana, esto puede llevar a muchos problemas más adelante.

- Enseñarles a respetar su cuerpo y su intimidad. Y que nadie puede obligarlws a hacer algo que no quieran.
- Localizar el ordenador o hacer uso de los dispositivos móviles tanto como sea posible en los lugares compartidos con la familia.

Los menores deben evitar enviar cualquier tipo de fotos, pero se sabe que, a medida que crecen, comienzan a usar estas funciones también. Incluso en esta transición hacia la madurez, es importante tomar algunas medidas:

- No intercambies fotografías íntimas, y mucho menos con extraños.
- No publiques imágenes comprometidas en las redes sociales o en Internet- Estas fotos son muy difíciles de borrar después y pueden llegar a muchas personas.
- Si envías una imagen, trata de enviarla sin posibilidad de ser identificado, sin mostrar tu cara, tatuajes o marcas que puedan identificarte fácilmente.
- No envíes imágenes con coordenadas de geolocalización, ya que algunos móviles o dispositivos tienen la opción de marcar en la imagen la posición donde se tomó la foto. Esto puede ser un peligro añadido en caso de difusión de la foto o de robo del dispositivo, ya que terceras personas pueden saber dónde fue tomada y localizar al menor.
- Si tomas una foto y no quieres que vea la luz, la mejor opción es borrarla del dispositivo.

2. Aplica conocimiento

Ejercicio OPCIÓN SIMPLE

Asociado al objetivo específico OE _ControlParental_02_01: puedes definir el término “sexting”

Situación: El sexting consiste en…
Tarea: Elija las opciones correctas siguiendo el principio de opción múltiple: solo una respuesta es verdadera.

- Enviar mensajes sexuales amenazantes a un niño o adolescente.
- Enviar imágenes o videos sexuales producidos por el propio remitente.
- Enviar contenidos sexuales, como imágenes o videos producidos por el acosador.

Explicación: El sexting no implica amenazas. Además, el contenido no es enviado por ningún acosador ni creado bajo la amenaza de un tercero. Por eso las opciones 1ª y 3ª no son correctas.

Ejercicio OPCIÓN SIMPLE

Asociado al objetivo específico OE _ControlParental_02_02: conoces la diferencia entre el sexting activo y pasivo.

Situación: El sexting activo es cuando…

Tarea: Elija las opciones correctas siguiendo el principio de opción múltiple: solo una respuesta es verdadera.

- La persona toma fotos o videos con poses sugestivas o sexuales y los envía a otra persona.
- El acosador le pide a la otra persona que envíe imágenes con poses sugestivas o sexuales.
- El acosador amenaza a la otra persona para que envíe imágenes con poses sexuales o de sufrimiento.

Ejercicio OPCIÓN SIMPLE

Asociado al objetivo específico OE _ControlParental_02_03 conoces los riesgos asociados a la práctica y difusión del sexting.

Situación: Después de enviar las imágenes, el emisor pierde el control sobre ellas porque…

Tarea: Elija las opciones correctas siguiendo el principio de opción múltiple: solo una respuesta es verdadera.

- Hay muchas consecuencias para la víctima
- El acosador gana poder
- El contenido puede llegarle a mucha más gente

Explicación: Las tres afirmaciones son ciertas, pero solo la tercera es la causa directa del efecto de perder el control sobre las imágenes.

Ejercicio OPCIÓN SIMPLE

Asociado al objetivo específico OE _ControlParental_02_03 puedes explicar tres estrategias para prevenir el sexting

Situación: Para prevenir el sexting:

Tarea: Elija las opciones correctas siguiendo el principio de opción múltiple: solo una respuesta es verdadera.

- Padres y educadores deben enseñar a los menores que todo lo que se comparte en Internet tiene consecuencias.
- Padres y educadores deben comprobar lo que los menores hacen en Internet.
- Sus iguales deben enseñarles respeto por su cuerpo.

Explicación: Por un lado, es necesario que los menores aprendan a valerse por sí mismos, para que no deban ser vigilados eternamente (especialmente los adolescentes, cuya privacidad debe respetarse). Por otro lado, pueden aprender de sus compañeros, pero sus iguales no se encargan de transmitir este conocimiento para decir que los iguales “deben enseñarles” nada. Por eso la única respuesta correcta es la primera.

Co-funded by the
Erasmus+ Programme
of the European Union

3. Construye conocimiento knowledge – ¿Qué es el grooming?

El grooming se define como el acoso cibernético llevado a cabo deliberadamente por un adulto para establecer una relación y un control emocional sobre un menor con el fin de preparar el terreno para el abuso sexual.

En algunos casos, se realiza entre menores, pero normalmente con una diferencia de edad, donde el mayor suele ser el acosador.

El objetivo de la captación de menores es ganar la confianza del menor, obtener imágenes o vídeos de contenido sexual, e incluso conocerse en persona. Estos actos pueden constituir delitos de corrupción, prostitución y abuso sexual de menores.

Este tipo de ciberacoso está estrechamente relacionado con la pedofilia, ya que muchos también se aprovechan de las imágenes que han obtenido para extorsionar, al menos, difundiendo las imágenes si no aceptan las condiciones impuestas por el agresor.

Definición
Grooming … el adulto intenta ganarse la confianza del menor, generalmente con fines sexuales. Esto sucede en Internet, pero a veces el acosador trata de establecer contacto en persona.

: Normalmente, los“groomers” – acosadores – llevan a cabo las siguientes fases:

- Gancho: El acosador hace preguntas a la víctima para conocerla, como su edad y ubicación geográfica. Posteriormente, intenta conocer sus gustos y preocupaciones, para adaptarse a ellos, tener aspectos en común y ganarse su confianza. Aquí, el acosador no presiona con preguntas que puedan asustar o alejar al niño, sino que trata de fortalecer los lazos de amistad con ellos.

- Lealtad: Después de hacerse amigo de la víctima y de ser amable, interesante y con muchas afinidades, el acosador se asegura de que su nuevo amigo quiera seguir hablando con él. Para lograrlo, suele hablar de temas de interés mutuo: deportes, música, escuela, etc., y luego continúa con los asuntos familiares, con quién vive, cómo es su familia, lo que hacen sus padres, etc.

- Seducción: Con toda la información y la confianza construidas hasta el momento, el acosador se dedica a seducir, incluyendo temas sexuales en las charlas, e intentando intercambiar imágenes con la víctima.

Al halagarlas y generar en ellas un sentimiento de deuda, el acosador conseguirá que cumplan la mayoría de sus peticiones.

- Acoso: En este punto el acosador ya tiene una idea cercana de lo que puede obtener del niño: tiene su información privada y familiar, conoce sus gustos, miedos y tiene fotos de él o ella. El objetivo ahora se hace más claro: establecer una relación sexual, aunque inicialmente sea virtual. Es posible que en esta etapa el acosador se muestre tal y como es, utilizando el chantaje, las amenazas y la manipulación para lograr sus objetivos.

En algunas ocasiones, las primeras etapas pueden comenzar cara a cara con una persona conocida previamente por el niño, que posteriormente continúa con el abuso sexual.

En algunos casos, puede haber dos fases más:

- Búsqueda: En una primera fase, gracias a toda la información que los menores ponen en las redes sociales no supervisadas, en los chats, las redes sociales y los foros, el acosador busca a sus víctimas teniendo en cuenta factores como; la vulnerabilidad, la necesidad emocional, la baja autoestima, la soledad y la poca atención de los padres.

- Aislamiento: En una fase intermedia entre el enganche y la seducción, el agresor aprovecha la confianza que ha ganado con el niño y el conocimiento adquirido para tratar de aislarlos de sus amigos y familiares, con el fin de controlar mejor al niño, convertirse en la persona más cercana e impedir que se pongan en contacto con alguien para contarle lo que les está pasando.

Los cambios o síntomas que sufre la víctima pueden dividirse en cuatro grupos diferentes:

Cambios en los hábitos en relación con diferentes áreas:

- en el uso de dispositivos o Internet.

- en la asistencia a clase. Por ejemplo, la ausencia mal justificada.

- abandono o ausencia en las actividades habituales.

- altibajos en los tiempos de estudio y en el rendimiento escolar.

- variaciones en las actividades de ocio.

- modificación de los hábitos alimenticios.

- disminución de la capacidad de concentración y mantenimiento.

- ocultación especial al comunicarse a través de Internet o del teléfono móvil.

Cambios de humor:

- cambio de humor.

- momentos de tristeza, apatía o indiferencia.

- actitudes inusuales de relajación y tensión, incluso reaccionando agresivamente.

- explosiones momentáneas de agresividad.

Cambios en sus relaciones:

- cambios de grupo extraños y repentinos, ausencia de amigos y relaciones sociales.

- no defenderse o reaccionar exageradamente a las supuestas bromas u observaciones públicas. Pueden ser comentarios aparentemente inofensivos, pero para la víctima pueden tener otro significado.

- miedo u oposición a salir de casa.

- reservas excesivas en la comunicación.

- cambios en sus grupos de amigos, a veces cambios radicales.

- variaciones en la relación con los adultos, en términos de su frecuencia y su dependencia.

- la variabilidad de los grupos e ídolos o modelos a seguir e imitar.

cambios y síntomas físicos y psicosomáticos, tales como:

◦ modificaciones en su lenguaje corporal en presencia de ciertas personas, evitando el contacto o encerrándose en sí mismos.

◦ en el ámbito escolar, el miedo al recreo y a los lugares visibles.

◦ manifestaciones frecuentes de enfermedades o dolencias.

◦ frecuentes lesiones físicas sin explicación razonable, pérdida o deterioro de las prendas de vestir.

◦ mareos frecuentes con síntomas poco communes.

◦ dolores de cabeza o de estómago que causan la pérdida de actividades o de asistencia a la escuela.

Las recomendaciones para prevenir el grooming son:

En el núcleo familiar es importante promover una comunicación intrafamiliar fluida, facilitando así la posibilidad de hablar con los niños sobre Internet, las redes sociales y los posibles peligros relacionados con ellas, por lo que es esencial advertirles sobre los datos que no deben proporcionar a través de estos canales.

También es aconsejable educar al menor en el uso seguro de Internet, sus herramientas, servicios y sobre las redes sociales, con el consejo previo de no proporcionar datos, ni de aceptar extraños. Se trata de formarles ofreciéndoles los conocimientos y herramientas necesarias para que sean cada vez más autónomos en el uso de las redes. Las medidas de supervisión y control deben adaptarse a la edad del niño, niña o joven que se desea supervisar.

Los centros educativos pueden elaborar acciones concretas contra el acoso sexual, contando entre el personal docente con expertos que canalicen y faciliten la información y el funcionamiento técnico de los mecanismos y dispositivos.

También pueden adoptar metodologías que faciliten la inserción y enfocar dentro de los contenidos los problemas de grooming, así como lanzar medidas dirigidas a la prevención.

En el caso de los menores, deben evitar proporcionar imágenes e información comprometedoras a nadie, así como hacerlas accesibles a terceros. Deben rechazar los mensajes sexuales o pornográficos y, en todo caso, pedir ayuda en situaciones nuevas o delicadas, especialmente si implican inseguridad o angustia emocional.

3. Aplica conocimiento

Ejercicio OPCIÓN SIMPLE

Asociado al objetivo específico OE _ControlParental_03_01: puedes dar la definición del término "grooming".

Situación: el Grooming se define como:

Tarea: Elija las opciones correctas siguiendo el principio de opción múltiple: solo una respuesta es verdadera.

- Ciberacoso llevado a cabo deliberadamente por un adulto.
- Ciberacoso llevado a cabo deliberadamente por un igual.
- Ciberacoso llevado a cabo deliberadamente por un compañero de clase en internet.

Ejercicio OPCIÓN SIMPLE

OE _ControlParental_03_02: conoces las fases y características del grooming.

Situación: el Grooming sigue diferentes fases. En la fase "gancho"...

Tarea: Elija las opciones correctas siguiendo el principio de opción múltiple: solo una respuesta es verdadera.

- El acosador se asegura de que su nuevo amigo quiera seguir hablando con él
- El acosador hace preguntas a la víctima para conocerla.
- El acosador busca a sus víctimas y su información en Internet.

Ejercicio OPCIÓN SIMPLE

Asociado al objetivo específico: OE _ControlParental_03_03: puedes identificar los síntomas en una víctima de grooming.

Situación: Los cambios que sufre la víctima se pueden agrupar en cuatro diferentes:

Tarea: Elija las opciones correctas siguiendo el principio de opción múltiple: solo una respuesta es verdadera.

- Hábitos, estado de ánimo, aficiones y salud.
- Hábitos, estado de ánimo, relaciones y salud.
- Hábitos, estado de ánimo, relaciones y psicosomáticos.

Ejercicio de OPCIÓN SIMPLE

Asociado al objetivo específico: OE _ControlParental_03_04: puedes explicar tres estrategias de prevención del grooming.

Situación: Para evitar que los menores sufran de grooming, es aconsejable…:

Tarea: **Elija las opciones correctas siguiendo el principio de opción múltiple: solo una respuesta es verdadera.**

- Controlar lo que ven, no dejes que lo hagan solos y localiza los dispositivos en un área común.
- Tener comunicación, enséñales a usar diferentes herramientas, dispositivos y redes sociales.
- **Dejarles usar Internet sólo cuando sean lo suficientemente autónomos.**

4. Construye conocimiento – ¿Qué es el cyberbullying?

Definición
Cyberbullying o ciberacoso El cyberbullying o acoso cibernético es cualquier tipo de intimidación que tiene lugar a través de dispositivos digitales: ordenadores portátiles, tabletas o teléfonos inteligentes.

El acosador perjudica al acosado en Internet, dañando su reputación online al difundir mensajes a través de medios sociales como Facebook, Instagram Twitter, etc., publicando en blogs o enviando información por correo electrónico, SMS, aplicaciones para smartphones como WhatsApp o WeChat.

Uno de los primeros pasos del ciberacoso suele ser un acosador que insulta o amenaza a la víctima diciendo que va a filtrar información que dañará su reputación. La información enviada por el acosador sobre el acosado puede ser cierta, pero en este caso se filtrará a propósito debido a que es negativa o perjudicial para los intereses del acosado. También puede ser directamente falsa. Si es así, se convierte en desinformación.

Ejemplo
Por ejemplo, una chica recibe un mensaje a través de WhatsApp con un enlace a un sitio web que incluye algunas fotos de ella desnuda. Un acosador le pide que haga sus deberes o le enviará este enlace a sus amigos y familiares.

Algunas de las tácticas habituales de ciberacoso que el acosador le hará a la víctima son:

- insultar u ofender a otros a través de Internet
- pedir a las víctimas que se hagan daño a sí mismas o que se suiciden
- amenazar
- crear un sitio web o un blog que incluya información embarazosa sobre la víctima
- hackear perfiles de medios sociales, a menudo llamados "sockpuppet"
- filtrar datos privados de la víctima
- compartir fotos de desnudos
- celos e intimidación
- el acoso basado en la religión, la raza o la orientación sexual

En general, el acosador cibernético, también conocido como stalker será alguien cercano a la víctima: un compañero de clase o de actividades culturales o deportivas, y la mayoría de las veces habrá un grupo de acosadores y no sólo un individuo. Este tipo de comportamiento es muy dañino para la víctima debido a las siguientes características:

- Persistencia: Vivimos en un mundo conectado 24/7, donde la comunicación nunca se detiene.
- Permanencia: La mayor parte de la información publicada en Internet permanece en la red y es pública. Además, una vez que el ciberacoso ha comenzado, los acosadores no suelen parar, sino que aumentan sus ataques.
- Esconderse: Las víctimas no quieren hablar de las agresiones debido al miedo, por lo que es difícil que los padres, los profesores y otras autoridades se den cuenta.

Normalmente, cuando los menores sufren el ciberacoso, se repliegan en sí mismos y esto afecta no sólo a sus vidas en Internet, sino también a su forma de vivir en el mundo real.

Las víctimas del ciberacoso no quieren seguir yendo a los lugares donde les están sucediendo estas experiencias traumáticas. A menudo abandonan las actividades que antes les gustaban, incluso empiezan a faltar a clase fingiendo sentirse enfermos, lo que pone en peligro sus resultados académicos, y a veces incluso enferman de verdad debido a trastornos de la alimentación o depresiones.

Aumentarán o disminuirán el uso de los dispositivos y se volverán más protectores de su privacidad, no dejando que nadie en casa vea lo que están haciendo en los medios sociales en particular o en Internet en general. A veces incluso cierran sus perfiles y crean otros nuevos.

Con el fin de prevenir el ciberacoso, hay algunas estrategias que podemos ejecutar:

- Los padres y los profesores deben hablar con los niños sobre el ciberacoso, reforzando y recompensando el buen comportamiento hacia los demás y no sólo centrándose en el acosador, sino también en los espectadores.
- Los adultos deben establecer reglas claras sobre qué contenidos deben ser vistos y compartidos y sobre la cantidad de tiempo que pasan en los medios sociales. Además, deben establecer las expectativas sobre un correcto comportamiento digital.
- En la escuela, los profesores pueden crear un "buzón de acoso" anónimo, que los estudiantes puedan utilizar para contar que están experimentando este problema y para activar los protocolos de ciberacoso.
- Los padres y los profesores deben estar siempre atentos a cualquier cambio de humor de los niños, por mínimo que sea.

4. Aplica conocimiento

Ejercicio RESPUESTA SIMPLE

Asociado al objetivo específico: OE _ControlParental_04_01: puedes definir el término ciberacoso.

Situación: ¿Cuál de las siguientes respuestas es correcta en relación al ciberacoso?
Tarea: **Elija las opciones correctas siguiendo el principio de opción múltiple: solo una respuesta es verdadera.**

- Insultar o amenazar a otros tanto físicamente como a través de Internet.
- Acosar a otros en los medios sociales, sitios web, aplicaciones o usando cualquier otro canal digital.
- Colocar cualquier comportamiento negativo en Internet.

Ejercicio RESPUESTA SIMPLE

Asociado al objetivo específico: OE _ControlParental_04_02: puedes definir los roles y características involucrados en el ciberacoso.

Situación: ¿Cuál es la definición de cibervíctima?
Tarea: **Elija las opciones correctas siguiendo el principio de opción múltiple: solo una respuesta es verdadera.**

- El que insulta, amenaza o filtra cualquier información perjudicial o mezquina sobre otra persona.
- La persona que sufre los procesos y a menudo se cierra en sí misma.
- El término "cibervíctima" es incorrecto.

Ejercicio RESPUESTA SIMPLE

Asociado al objetivo específico: OE _ControlParental_04_03conoces las consecuencias del ciberacoso para el acosador y el acosado.

Situación: ¿Cuál de los siguientes no es un indicador de estar sufriendo ciberacoso?

Tarea: **Elija las opciones correctas siguiendo el principio de opción múltiple: solo una respuesta es verdadera.**

- Prefiere centrarse en el estudio y suele mejorar sus notas.
- Las víctimas suelen cerrar sus perfiles en los medios sociales y abrir otros nuevos.
- Las personas que sufren de ciberacoso cambian el estado de ánimo y se retraen en sí mismos.

Ejercicio RESPUESTA SIMPLE

Asociado al objetivo específico: OE _ControlParental_04_04: puedes explicar tres estrategias de prevención del ciberacoso.

Situación: ¿Cómo podrías prevenir el ciberacoso?
Tarea: **Elija las opciones correctas siguiendo el principio de opción múltiple: solo una respuesta es verdadera.**

- **Llamando a la policía tan pronto como tengamos la más mínima sospecha.**
- **Evitando el uso de aparatos electrónicos en casa.**
- **Estableciendo reglas claras sobre lo que se debe y no se debe hacer cuando se usa Internet.**

5. Construye **conocimiento knowledge – ¿Qué es la adicción a internet?**

La curiosidad, la ausencia de un conocimiento bien fundamentado, el tiempo libre y un lugar llamado Internet donde se pueden encontrar todas las respuestas a cualquier pregunta que se pueda tener o contactar con cualquier persona que se desee, son un caldo de cultivo para pasar la mayor parte del tiempo en ese lugar. Los menores tienen esas características en común.
Internet ha ampliado el mundo de los adolescentes y los niños, permitiéndoles socializar y expresarse, aumentando sus recursos para el estudio, introduciendo una forma de interacción y aprendizaje más basada en la relación entre pares. Esos son los lados brillantes de Internet, pero también tiene un lado oscuro, que no podemos ignorar.

Hay dos tipos de adicciones: Puedes hacerte adicto a una sustancia, pero también puedes hacerte adicto a un proceso. Este tipo de adicción se suele categorizar como "nuevas adicciones", "adicciones no

químicas" o "adicciones de comportamiento". A veces, cuando pasas mucho tiempo haciendo algo, puedes desarrollar una adicción a este proceso. Cuando se es adicto a pasar el tiempo en Internet, eso tiene un nombre: adicción a internet o netolismo.

Definición

Adicción a internet o netolismo

El netolismo es un trastorno de adicción a Internet, también conocido como uso compulsivo de Internet. No consiste en pasar mucho tiempo en Internet, sino en dejar que esto interfiera con la vida diaria debido a la dependencia de su uso.

Este desorden ha aumentado profusamente debido al hecho de vivir en una sociedad permanentemente conectada. Cualquier cosa que puedas necesitar, puedes encontrarla en Internet: si no encuentras la talla adecuada de una camisa en una tienda, puedes comprarla en Internet; si no quieres cocinar, puedes pedir comida para que te la entreguen allí; si no tienes un hermano con quien jugar a la vídeoconsola, puedes jugar con un extraño en línea; si necesitas estudiar, puedes acceder a todos los libros, artículos y otros recursos a través de Internet.

En estos escenarios, es muy difícil poder distinguir si un menor está experimentando algún tipo de trastorno de adicción a Internet. No obstante, hay algunas formas de descubrir este tipo de trastorno. Para ello, como padres, podríamos hacernos algunas preguntas:

5. ¿Es el menor incapaz de dejar de usar los medios sociales cuando se le pide que lo haga?
6. ¿Está el menor comprando compulsivamente por Internet?
7. ¿Juega excesivamente a los videojuegos online?
8. ¿Está apostando en Internet?
9. ¿Pasa todo el día frente a la computadora?
10. ¿Tiene problemas con las relaciones sociales fuera de Internet?
11. ¿Está experimentando algún problema por no hacer sus tareas o sus notas están bajando?

Si la respuesta a cualquiera de estas preguntas es afirmativa, debemos examinar a fondo el comportamiento del menor, ya que podría estar experimentando un trastorno de adicción a Internet o netolismo.

Sin embargo, sólo será una pista. Como dijimos antes, vivimos en un mundo conectado las 24 horas y las barreras entre el uso normal de la red y el uso abusivo de la misma son leves. Por lo tanto, hay que comprobar si este tipo de comportamiento tiene algún impacto negativo en la vida del menor. Si el menor no es capaz de priorizar sus deberes y tareas por encima de estar conectado, está claro que tiene un problema.

Ejemplo

Es la hora de la cena y llamas a tu hijo para que acuda a la mesa, pero no viene. Lo llamas tres veces, pero tiene el smartphone en la mano, y no está dispuesto a dejar lo que está haciendo. Incluso en la mesa, continúa revisando las historias de su perfil de Instagram. Coges su smartphone y lo guardas en el bolsillo y está literalmente sufriendo porque no puede seguir con lo que estaba haciendo.

Otra forma de averiguar si el menor sufre este trastorno es analizar la cantidad de tiempo que pasa utilizando los dispositivos digitales, la frecuencia y las manifestaciones emocionales por no estar conectado. Si el menor parece estar deprimido, ansioso o agitado cuando no está conectado, o si experimenta frecuentes cambios de humor, la razón podría ser la adicción a internet.

El trastorno de la adicción a Internet también puede tener manifestaciones físicas, como mala nutrición, dolor de cuello, insomnio, sequedad de ojos o mala higiene. Con el fin de prevenir la adicción a internet, es preciso adoptar algunas medidas útiles:

- Limitar el tiempo de uso de los dispositivos digitales. No sólo por un número fijo de horas, sino también controlando el tiempo del día para utilizarlos. Por ejemplo, nunca utilizar el ordenador después de la cena.
- Organizar charlas en la escuela sobre la correcta utilización de Internet.
- Priorizar los momentos familiares sobre las TIC
- Los niños siempre deben usar Internet bajo la supervisión de un adulto
- Se deben instalar herramientas de control parental (véase el capítulo 1) para evitar la entrada de niños y adolescentes en sitios web de juegos de azar o pornográficos.

5. Aplica conocimiento

Ejercicio OPCIÓN SIMPLE

Asociado al objetivo específico: OE _ControlParental_05_01: puedes dar la definición de la adicción a internet.

Situación: ¿Cuál es definición correcta de adicción a internet?
Tarea: Elija las opciones correctas siguiendo el principio de opción múltiple: solo una respuesta es verdadera.

- Desorden que consiste en pasar mucho tiempo en Internet.
- Adicción que no permite a la víctima vivir una vida normal debido a la dependencia del uso de Internet.
- Un acosador acosa a la víctima amenazándola con filtrar fotos de desnudos en un sitio web.

Ejercicio OPCIÓN SIMPLE

Asociado al objetivo específico: OE _ControlParental_05_02: puedes identificar laas señales de alarma sobre el abuso en la utilización de internet.

Situación: ¿Cuál de las siguientes afirmaciones no es una señal de alarma sobre un uso abusivo de internet?
Tarea: Elija las opciones correctas siguiendo el principio de opción múltiple: solo una respuesta es verdadera.

- El menor no quiere estar en línea porque tiene miedo de un matón.
- El menor juega excesivamente a los videojuegos online.
- El menor tiene problemas al tener relaciones sociales fuera de Internet.

Ejercicio OPCIÓN SIMPLE

Asociado al objetivo específico: OE _ControlParental_05_04: conoces tres estrategias de prevención de la adicción a internet.

Situación: ¿Cuál sería la mejor estrategia para prevenir el uso abusivo de internet?

Tarea: Elija las opciones correctas siguiendo el principio de opción múltiple: solo una respuesta es verdadera.

- **limitar los momentos de uso de Internet durante los días.**
- dar a los niños la oportunidad de navegar por Internet como deseen.
- controlar las cuentas de medios sociales de los niños

6. Construye conocimiento – ¿Qué es la revelación de información?

Hoy en día casi toda nuestra vida descansa en Internet. Si somos hackeados el hacker encontrará nuestras contraseñas de la tarjeta de crédito, tendrá acceso a nuestros perfiles de medios sociales, nuestras cuentas de correo electrónico o a nuestro historial de navegación.

Debido a esta sobreexposición, debemos cuidar nuestros datos y evitar su divulgación. Sin embargo, aunque nos comprometamos a un uso responsable de Internet, debemos asegurarnos de que los menores estén tan comprometidos como nosotros, porque utilizan los dispositivos de la familia y también los suyos propios.

Una amplia gama de delitos implica la eliminación de datos, o la fuga de datos y los adolescentes y niños son uno de los colectivos más propensos a compartir sus datos, debido a dos razones principales:

- Los nativos digitales pasan más tiempo conectados.
- No tienen la sensación de peligro cuando navegan.

Se pueden utilizar varias técnicas para filtrar secretamente datos de un dispositivo digital. A veces los perpetradores ocultan sus intenciones mostrándose como algo diferente a lo que son. Por ejemplo, en los anuncios, pidiendo información para visualizar el contenido o pidiendo las contraseñas para disfrutar de un servicio online. Pero, más a menudo los menores comparten sus datos porque no son conscientes del peligro, por lo que resulta vital contra con una forma más responsable de actuar en Internet.

Definición

Revelación de información

Revelar significa exponer, sin querer, información privada que no debe ser filtrada a otras personas. Puede ocurrir por medio de la piratería informática o porque la fuente no se dé cuenta de la importancia de mantener los datos privados en privado.

Podemos decir que hay divulgación cuando alguien da su información personal o la coloca en una posición en la que puede ser descubierta por personas que podrían utilizarla de manera perjudicial, arriesgando su privacidad o seguridad.

Este problema se ha incrementado profusamente debido a la mejora y sofisticación de la piratería informática: el malware, el spyware son sólo algunos de los problemas conocidos. Pero, como dijimos antes, uno de los principales problemas es que la gente esté dispuesta a compartir tanta información sobre ellos mismos. Constituye un problema creciente debido a las aplicaciones de los teléfonos inteligentes, que nos piden acceso a información como ubicación, contactos, etc. para poder disfrutar de sus servicios. Este es un cambio de paradigma que Internet ha traído consigo. En la televisión te muestran contenidos a cambio de tu atención. En Internet te darán acceso a aplicaciones y servicios a cambio de tus datos.

Esto no constituiría un problema en sí mismo si los datos revelados no fueran sensibles. Pero, ¿sabe un niño si la información expuesta es sensible y potencialmente riesgosa o no? Incluso los adultos a veces pueden no notar esta diferencia. Para descubrir si los menores están filtrando información, los padres deben hacerles algunas preguntas:

- ¿A qué sitios ingresan?
- ¿Qué aplicaciones se descargan?
- ¿Alguien les ha pedido que compartan algún dato personal para disfrutar de un servicio, como la dirección de correo electrónico o el número de tarjeta de crédito?

Ejemplo

Paul quiere descargar una aplicación en su smartphone para hablar con sus amigos. Aunque la aplicación es gratuita, se le pide que rellene un formulario que incluye la tarjeta de crédito y el código de verificación de la tarjeta.

Si las aplicaciones o servicios en línea te piden que compartas alguna información para el funcionamiento adecuado de la misma que no van a utilizar, o si alguien te pide de manera inusual información privada, como la dirección de tu casa, es probable pensar que hay un riesgo de revelar información sensible.

A veces la fuga de datos se produce mediante el uso de un virus troyano. Si tienes alguna sospecha de un software, no deberías descargarlo nunca. Puedes sospechar de programas que te permitan ver películas o programas en streaming de forma gratuita, así como sitios web y aplicaciones de juegos. La mejor manera de actuar es descargar cada servicio después de que lo hayan comprobado tus padres.

Para evitar que este tipo de información se revele, hay algunas estrategias que, como padre, se pueden implementar:

- Decirle al menor que no dé ningún dato personal sin permiso
- Si tu hijo utiliza el mismo dispositivo que tú: No guardes nunca las contraseñas o los códigos de identificación en el navegador.

- Instalar programas de control parental como Qustodio, Secure Kids o Parental Click
- Habla con los menores para que no publiquen ninguna foto que permita a los extraños saber la dirección exacta de donde viven o de la escuela donde estudia.

La mejor táctica de prevención es hablar frecuentemente con los menores sobre los riesgos de revelar información y sobre la importancia de un uso responsable de Internet.

6. Apply knowledge

Ejercicio de RESPUESTA SIMPLE

Asociado al objetivo específico: OE _ControlParental_06_01: puedes dar la definición de la revelación de informacion.

Situación: ¿Qué respuesta es correcta para definir de revelación de información?.
Tarea: Elija las opciones correctas siguiendo el principio de opción múltiple: solo una respuesta es verdadera.

- Adicción a los dispositivos digitales.
- Fuga de información sensible.
- Lanzamiento de información falsa en Internet.

Ejercicio de RESPUESTA SIMPLE

Asociado al objetivo específico: OE _ControlParental_06_02: puedes identificar cuando un niño está revelando informacion.

Situación: ¿Cuál de las siguientes no es una alarma de revelación de información?
Tarea: Elija las opciones correctas siguiendo el principio de opción múltiple: solo una respuesta es verdadera.

- **El menor pide permiso para descargar una aplicación para el smartphone.**
- El menor debe enviar el número de la tarjeta de crédito.
- El menor pone algunas fotos en la entrada de la casa.

Explicación: Cuando el menor no es bueno en las relaciones fuera de Internet o juega excesivamente a los videojuegos online, podríamos pensar que está haciendo un uso abusivo de Internet. Aquí se pregunta cuál NO es una señal de alarma sobre el uso abusivo de Internet. Si el menor no quiere estar en línea no está enganchado a Internet.

Ejercicio de RESPUESTA SIMPLE

Asociado al objetivo específico: OE _ControlParental_06_03: puedes explicar tres estrategias para evitar el filtrado de informacion.

Situación: ¿Cuál sería la mejor estrategia para prevenir la fuga de información?

Co-funded by the
Erasmus+ Programme
of the European Union

Tarea: Elija las opciones correctas siguiendo el principio de opción múltiple: solo una respuesta es verdadera.

1. **no guardar las contraseñas y los códigos PIN en el navegador.**
2. que los menores puedan descargar cualquier aplicación que quieran.
3. difundir las fotos personales en los medios sociales.

Co-funded by the
Erasmus+ Programme
of the European Union

Fuentes

Garaigordobil, M. (2019). Prevención del cyberbullying: variables personales y familiares predictoras de ciberagresión. Retrieved from: https://dialnet.unirioja.es/servlet/articulo?codigo=7041022

Garcia Ganchon, J. O. Seguridad y riesgos: Ciberbullying, grooming y sexting. Retrieved from: http://openaccess.uoc.edu/webapps/o2/handle/10609/72526

Stuttgen, K., McCague, A., Bollinger, J., Dvoskin, R., & Mathews, D. (2020). Whether, when, and how to communicate genetic risk to minors:'I wanted more information but I think they were scared I couldn't handle it'. Journal of Genetic Counseling. Retrieved from: https://onlinelibrary.wiley.com/doi/abs/10.1002/jgc4.1314

Villanueva-Blasco, V. J., & Serrano-Bernal, S. (2019). Patrón de uso de internet y control parental de redes sociales como predictor de sexting en adolescentes: una perspectiva de género. Revista de Psicología y Educación, 14(1), 16-26. Retrieved from:https://www.almendron.com/tribuna/wp-content/uploads/2020/05/patron-de-uso-de-internet.pdf

1. Save knowledge

Summary

Esta unidad se centra en la importancia del control parental para proteger a los niños y adolescentes de situaciones peligrosas utilizando Internet o dispositivos tecnológicos.

Dado que estamos en un mundo cambiante donde la tecnología evoluciona día a día, los peligros a los que siempre se han enfrentado los menores pueden surgir por nuevas vías. Estos riesgos también pueden extenderse y ampliarse fácilmente a través de Internet.

Para llevar a cabo la tarea de mantener seguros a los menores mientras interactúan y amplían su círculo, es necesario conocer los riesgos y las formas de evitarlos. Para ello, es importante establecer las formas en las que los peligros podrían llegar a los más pequeños (redes sociales, juegos, plataformas de vídeo, etc) y las herramientas disponibles para detenerlos o detectarlos.

Habiendo expuesto las diferentes formas en que los peligros pueden llegar a los niños y adolescentes y las herramientas y funciones para mantenerlos bajo control, se hace necesario precisar estos riesgos y sus consecuencias. Algunos de los peligros a los que se enfrentan los menores son el sexting, el grooming, el ciberacoso, el neolismo y la divulgación de información. Estos peligros deben entenderse para afrontarlos o incluso para detectarlos.

Algunas de estas consecuencias pueden afectar directamente a la salud emocional e incluso física de los menores. Si prestamos atención, hay efectos visibles que pueden llevarnos a la raíz del problema, para tomar medidas.

Sin embargo, la mejor opción, cuando sea posible, sería prevenir situaciones como sexting, grooming, cyberbullying, adicción a internet y divulgación de información, en lugar de lidiar con ellos. Para ello se expondrán formas de ejercer el control parental en Internet y dispositivos tecnológicos y algunas

herramientas. También será posible encontrar algunos consejos para mantener a los menores alejados de cada uno de los peligros mencionados anteriormente.

Las respuestas correctas están marcadas en negrita

Situación: ¿Qué amenazas tecnológicas impactan a los menores?
Tarea: Elige la opción correcta entre las que se presentan. Solamente una respuesta es correcta.

- Solo el ciberacoso
- **Existen múltiples daños que pueden afectar a niños, adolescentes y jóvenes en internet (ciberacoso, sexting…)**
- No hay ningún peligro tecnológico que amenace a los menores

Situación: ¿Cuál es la definición del término "control parental"
Tarea: Elige la opción correcta entre las que se presentan. Solamente una respuesta es correcta.

- **La forma en que los padres supervisan e intervienen, si es necesario, para garantizar que las experiencias y los procesos de socialización y crecimiento personal de sus hijos se produzcan adecuadamente y sin riesgos para ellos.**
- Una herramienta que permite a los padres controlar y/o limitar los contenidos a los que sus hijos pueden acceder a Internet desde sus dispositivos, sean estos ordenadores, móviles o tabletas.
- Una amenaza tecnológica que puede afectar a los menores.

Situación: ¿Para qué sirve el control parental?
Tarea: Elige la opción correcta entre las que se presentan. Solamente una respuesta es correcta.

- **Para controlar y/o limitar el contenido al que los niños pueden acceder a Internet desde sus dispositivos, sean estos ordenadores, móviles o tabletas.**
- Para dar a los niños la oportunidad de navegar por Internet como deseen.
- Para controlar las cuentas de medios sociales de los niños

Situación: ¿Cómo funciona el control parental tecnológico?
Tarea: Elige la opción correcta entre las que se presentan. Solamente una respuesta es correcta.

-
- El control parental tecnológico evita que el niño acceda a Internet apagando el router.
- El control parental tecnológico evita que los menores utilicen dispositivos electrónicos en casa mediante el uso de contraseñas online.
- **El control parental tecnológico se puede ejercer desde diferentes puntos: servidores externos y DNS, el propio dispositivo, software, navegador de Internet o APPs.**

Situación: El sexting consiste en…
Tarea: Elige la opción correcta entre las que se presentan. Solamente una respuesta es correcta.

- Enviar mensajes sexuales amenazantes a un niño o adolescente.
- **Enviar imágenes o videos sexuales producidos por el propio remitente.**
- Enviar contenidos sexuales, como imágenes o videos producidos por el acosador.

Situación: El sexting activo es cuando…

Tarea: Elige la opción correcta entre las que se presentan. Solamente una respuesta es correcta

- La persona toma fotos o videos con poses sugestivas o sexuales y los envía a otra persona.
- El acosador le pide a la otra persona que envíe imágenes con poses sugestivas o sexuales.
- El acosador amenaza a la otra persona para que envíe imágenes con poses sexuales o de sufrimiento.

Situación: Después de enviar las imágenes, el emisor pierde el control sobre ellas porque…

Tarea: Elige la opción correcta entre las que se presentan. Solamente una respuesta es correcta

- Hay muchas consecuencias para la víctima
- El acosador gana poder
- El contenido puede llegarle a mucha más gente

Situación: Para prevenir el sexting:

Tarea: Elige la opción correcta entre las que se presentan. Solamente una respuesta es correcta

- Padres y educadores deben enseñar a los menores que todo lo que se comparte en Internet tiene consecuencias.
- Padres y educadores deben comprobar lo que los menores hacen en Internet.
- Sus iguales deben enseñarles respeto por su cuerpo.

Situación: el Grooming se define como:

Tarea: Elige la opción correcta entre las que se presentan. Solamente una respuesta es correcta.

- Ciberacoso llevado a cabo deliberadamente por un adulto.
- Ciberacoso llevado a cabo deliberadamente por un igual.
- Ciberacoso llevado a cabo deliberadamente por un compañero de clase en internet.

Situación: el Grooming sigue diferentes fases. En la fase “gancho”...

Tarea: Elige la opción correcta entre las que se presentan. Solamente una respuesta es correcta.

- El acosador se asegura de que su nuevo amigo quiera seguir hablando con él
- El acosador hace preguntas a la víctima para conocerla.
- El acosador busca a sus víctimas y su información en Internet.

Situación: Los cambios que muestra la víctima se pueden agrupar en cuatro diferentes:

Tarea: Elige la opción correcta entre las que se presentan. Solamente una respuesta es correcta.

- Hábitos, estado de ánimo, aficiones y salud.
- Hábitos, estado de ánimo, relaciones y salud.
- Hábitos, estado de ánimo, relaciones y psicosomáticos.

Situación: Para evitar que los menores sufran de grooming, es aconsejable…:

Tarea: Elige la opción correcta entre las que se presentan. Solamente una respuesta es correcta.

- Controlar lo que ven, no dejes que lo hagan solos y localiza los dispositivos en un área común.
- **Tener comunicación, enséñales a usar diferentes herramientas, dispositivos y redes sociales.**
- Dejarles usar Internet solo cuando sean lo suficientemente autónomos.

Situación: ¿Cuál de las siguientes respuestas es correcta en relación al ciberacoso?
Tarea: Selecciona la opción correcta entre las que se presentan. Solamente una es correcta.

- Insultar o amenazar a otros tanto físicamente como a través de Internet.
- **Acosar a otros en los medios sociales, sitios web, aplicaciones o usando cualquier otro canal digital.**
- Soportar cualquier comportamiento negativo en Internet.

Situación: ¿Cuál es la definición de cibervíctima?
Tarea: Selecciona la opción correcta entre las que se presentan. Solamente una es correcta.

- El que insulta, amenaza o filtra cualquier información perjudicial o mezquina sobre otra persona.
- **La persona que sufre los procesos y a menudo se cierra en sí misma.**
- El término "cibervíctima" es incorrecto.

Situación: ¿Cuál de los siguientes no es un indicador de estar sufriendo ciberacoso?
Tarea: Selecciona la opción correcta entre las que se presentan. Solamente una es correcta.

- **Prefiere centrarse en el estudio y suele mejorar sus notas.**
- Las víctimas suelen cerrar sus perfiles en los medios sociales y abrir otros nuevos.
- Las personas que sufren de ciberacoso cambian el estado de ánimo y se retraen en sí mismos.

Situación: ¿Cómo podrías prevenir el ciberacoso?
Tarea: Selecciona la opción correcta entre las que se presentan. Solamente una es correcta.

- Llamando a la policía tan pronto como tengamos la más mínima sospecha.
- Evitando el uso de aparatos electrónicos en casa.
- Estableciendo reglas claras sobre lo que se debe y no se debe hacer cuando se usa Internet.

Situación: ¿Cuál es la respuesta más adecuada en relación a la adicción a internet?
Tarea: Elige la respuesta correcta entre las que se presentan. Solamente una respuesta es la correcta.

- Desorden que consiste en pasar mucho tiempo en Internet.
- **Adicción que no permite a la víctima vivir una vida normal debido a la dependencia del uso de Internet.**
- Un acosador acosa a la víctima amenazándola con filtrar fotos de desnudos en un sitio web.

Situación: ¿Cuál de las siguientes no es una señal de alarma sobre un uso abusivo de internet?
Tarea: Elige la respuesta correcta entre las que se presentan. Solamente una respuesta es la correcta.

- **El menor no quiere estar en línea porque tiene miedo de un matón.**
- El menor juega excesivamente a los videojuegos online.

- El menor tiene problemas al tener relaciones sociales fuera de Internet.

Situación: ¿Cuál sería la mejor estrategia para prevenir el uso abusivo de internet?
Tarea: Elige la respuesta correcta entre las que se presentan. Solamente una respuesta es la correcta.

- Limitar los momentos de uso de Internet durante los días.
- Dar a los niños la oportunidad de navegar por Internet como deseen.
- Controlar las cuentas de medio sociales de los niños.