Programa de Jornadas Escolares

Promoción del uso seguro y responsable de Internet entre los menores

---

Uso seguro y responsable de las TIC

Charla sensibilización alumnado. Guía de preparación

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

Cofinanciado por la Unión Europea
Mecanismo «Conectar Europa»

Licencia de contenidos

CONTENIDO

1. Introducción

El contenido de esta guía servirá como orientación al profesorado a la hora de desarrollar en el aula una charla de sensibilización sobre **Uso seguro y responsable de las TIC,** apoyándose en la presentación **Uso seguro y responsable de las TIC. Charla de sensibilización dirigida al alumnado**. La guía y la presentación anexa a ella tratarán de responder al objetivo general de identificar los principales riesgos asociados al uso de las TIC, abordando estrategias y pautas de conducta que nos ayuden a prevenirlos y/o saber actuar ante ellos.

Para ello, plantearemos algunos de los principales riesgos asociados al uso de las TIC como son el acceso a contenidos inapropiados, los bulos y mentiras en la red, los virus y fraudes electrónicos. También trataremos el ciberacoso escolar así como los conceptos de privacidad e identidad digital. Finalmente, además de proporcionar las principales recomendaciones para prevenir este tipo de riesgos hablaremos sobre el concepto de Netiqueta y las principales pautas de buen comportamiento para comunicarse en la red con el objeto de construir entre todos un espacio cada vez más agradable y seguro.

El docente encargado de la sesión con el alumnado desarrollará una estrategia metodológica de reflexión-participación, invitando y animando a éste en la reflexión y el debate. Al mismo tiempo promoverá el análisis crítico de los contenidos que se tratan en ella, impulsando la participación y animando así a la exposición de los puntos de vista, reflexiones y sobre todo al planteamiento de las dudas de los participantes.

1.1. Objetivos didácticos

- Identificar los principales riesgos relacionados con el uso de las TIC.
- Identificar pautas para prevenirlos y saber actuar ante ellos.
- Reconocer la importancia de adquirir buenos hábitos en nuestra relación con las TIC.

1.2. Metodología

Durante la charla de sensibilización sobre **Uso seguro y responsable de las TIC**, dirigida al alumnado, el docente realizará la exposición de contenido, combinando el método **expositivo**[1] y el **interrogativo**[2]. Actuará también como facilitador de una sesión participativa, con objeto de animar a compartir información, ideas, inquietudes, dudas, etc. Buscará en todo momento promover un entorno que favorezca la motivación del alumnado.

Promoverá la construcción del conocimiento a partir de la permanente reflexión del alumnado siempre orientada por aquél, asesorando y facilitando recursos e información y procurando poner ejemplos vinculados a la realidad objetiva del perfil del alumnado destinatario. También utilizará un

[1] **METODOLOGÍA EXPOSITIVA:** centrada en la transmisión de información, posibilita la transmisión de conocimientos ya estructurados, facilitando demostraciones de tipo verbal y la transmisión de información y conocimiento, de manera rápida y generalizada.

[2] **METODOLOGÍA INTERROGATIVA**: centrada en el proceso de aplicación del contenido a trabajar, basada en el proceso de comunicación que se establece entre docente y grupo, a través de ***la pregunta***. Esta se convierte en elemento dinamizador, que desencadena el proceso de enseñanza aprendizaje.

lenguaje acorde con el nivel de conocimientos previstos en el alumnado destinatario para facilitar la comprensión de los contenidos expuestos.

2. Fundamentos teóricos sobre Uso seguro y responsable de las TIC

TRANSPARENCIA 3: Acceso a contenido inapropiado

Entre los muchos contenidos que encontramos en Internet, no es difícil "toparse" con páginas que nos enlazan a **contenido no adecuado** (y en ocasiones ilícito).

Pueden ir desde el acceso a contenidos violentos o pornográficos, a contenidos falsos o carentes de rigor (bulos, mensajes en cadena o vídeos virales), juegos de apuestas o fraudes que se distribuyen libremente a través de Internet.

Este tipo de contenido puede provocar, sobre todo en el caso de menores, sentimientos de confusión, tristeza o miedo, emociones que es importante detectar y canalizar, enseñando a los menores a solicitar la ayuda y opinión de las personas adultas de referencia en cada caso (familia, profesorado).

Durante la presentación de este concepto, el formador resumirá brevemente **qué entendemos por contenido inapropiado:** aquel que percibido por el menor de edad, pueda ser dañino o molesto para él/ella, representado a través de imágenes, vídeos o textos que manifiestan valores negativos y moralmente reprobables.

TRANSPARENCIA 4: Riesgos de acceso a contenidos inapropiados

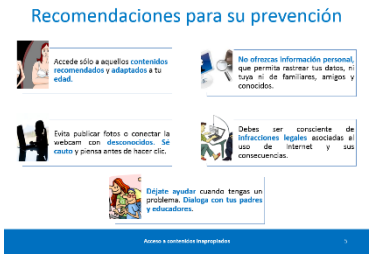
Vamos a ver algunos riesgos a los que se exponen los menores si acceden a contenidos inapropiados:

- **Acceso a información, conductas y consejos no adecuados a su edad**: algunos ejemplos de contenidos inapropiados pueden ser aquellos que muestran y/o fomentan racismo, violencia, terrorismo, el uso de armas, la pertenencia a sectas, pornografía y abusos infantiles, tráfico y/o consumo de drogas, apuestas ilegales, páginas que fomentan hábitos y conductas que dañan la salud, física y psicológica: como las páginas *ProAna* (a favor de la anorexia y sus hábitos y conductas) y *proMía* (que promueven la bulimia, como estilo de vida.
- **Amistades poco recomendables**: cualquier persona en la red puede en principio mentir y engañar haciéndose pasar por otra persona. Puede mentir sobre su edad, su género, puede subir una foto de otra persona diciendo que es suya, puede incluso crear un perfil en alguna red con todos estos engaños. Este perfil falso puede resultar muy atractivo para algunas personas, pero lo que tenemos que tener bien claro es que puede resultar muy peligroso. Si alguien crea un perfil falso en la red y miente sobre su aspecto, sus aficiones etc. es muy probable que no tenga buenas intenciones, como por ejemplo captación de menores para formar parte de comunidades peligrosas como las comentadas anteriormente sobre

anorexia, bulimia u otras que incitan al odio y la violencia vinculadas por ejemplo, a extremismos ideológicos.

- **Víctima de ciberacoso y ciberbullying**.
- **Víctimas de potenciales engaños y estafas** (anuncios publicitarios)
- Contenidos fraudulentos para engañar a los usuarios y obtener así, un acceso no autorizado a su dispositivo y robar información personal de la víctima. Vamos a ver más adelante en la presentación algunos de estos ejemplos.

TRANSPARENCIA 5: Recomendaciones para su prevención



- Selecciona los blogs, foros, páginas etc. a los que vas a acceder, evitando aquellos de carácter violento, pornográfico o discriminatorio. Es fundamental que accedas sólo a aquellos contenidos recomendados y adaptados a tu edad.
- No ofrezcas información personal, para evitar que alguien pueda rastrear tus datos. De igual forma no ofrezcas información personal de familiares, amigos y conocidos.
- Evita publicar fotos o conectar la webcam con desconocidos. Aun estando chateando con amigos, debes ser cauto y pensar qué es lo que vas a enviar. Piensa cómo se sentirían otras personas que pudieran acceder a lo que estás dispuesto a enviar.
- Debes ser consciente de la existencia de infracciones legales asociadas al uso de Internet así como de sus consecuencias, como por ejemplo delitos contra la propiedad intelectual, amenazas o coacciones, intimidación sexual, estafas o robos informáticos.

Déjate ayudar cuando tengas un problema con las TIC, o te resulte violento o incómodo algún contenido. Dialoga con tus padres y educadores acerca de esos episodios.

TRANSPARENCIA 6: Verificación de la información

De manera dicional, explicaremos al alumnado la importancia de verificar la información que localizamos en Internet porque no todo lo que se publica es cierto.

Por tanto, es necesario verificar aquella información de nuestro interés, por ejemplo acudiendo a otras fuentes de referencia y a ser posible, de nuestra confianza (páginas web oficiales, instituciones educativas, organismos públicos, etc.).

TRANSPARENCIA 7: Bulos, mitos y fraudes

Frecuentemente llegan a nuestro buzón de correo, redes sociales y mensajería instantánea, noticias falsas, e incluso fraudes, que son difundidos con gran rapidez y viralidad a través de Internet.

Comentaremos con el alumnado algunos de los ejemplos más conocidos:

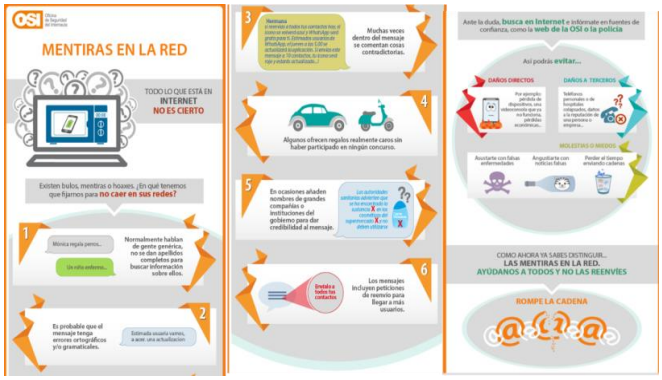
- **Falso anuncio de Zara**, refiriéndose a vales descuento que no tienen validez. Aunque la presentación muestra como ejemplo éste, indicar a los alumnos que han circulado por Internet **otros supuestos vales descuento/cupones falsos** que afectaban a otras empresas como Mercadona, Lidl, H&M, etc.
- **Mensajes falsos, propagados a través de WhatsApp**: "*WhatsApp te cobrará 37 céntimos por cada mensaje que envíes a menos que reenvíes esto a todos tus contactos*"

> *Hola, soy Germán Menafre, director de WhatsApp. Este mensaje es para informarles a todos nuestros usuarios de que sólo nos quedan 530 cuentas disponibles para nuevos teléfonos, y que nuestros servidores han estado recientemente muy congestionados, por lo que estamos pidiendo su ayuda para solucionar este problema. Necesitamos que nuestros usuarios activos reenvíen este mensaje (…) Mañana empiezan a cobrar los mensajes por WhatsApp a 0,37 centavos. Reenvía este mensaje a más de 9 personas de tus contactos y te será gratuito de por vida.*

- El **bulo sobre los cartones de leche**, que afirma que los números del fondo del envase de los cartones de leche, indican las veces que la leche caducada ha vuelto a ser reciclada para su venta y consumo, cuando en realidad, e**sas cifras** identifican el lote de la materia prima usada para fabricar los briks.
- Y otros muchos, que pueden verse en páginas especializadas en la temática, como: la **recopilación de bulos recogida por la OCU (Organización de Consumidores y Usuarios)** y **Cazahoax** o los canales en Twitter de **Policía Nacional** y **Guardia Civil**, con información permanentemente actualizada sobre ellos.

Son sólo algunos de los ejemplos más conocidos, que podemos encontrar fácilmente a través de mensajería, correo electrónico y/o redes sociales. Por ello, es importante analizar, tanto las posibles consecuencias de este tipo de contenido y su propagación masiva a través de la red, como la capacidad de muchos de ellos para **infectar dispositivos**, **robar de éstos información personal**, **enviar correo spam**, etc.

TRANSPARENCIA 8-9-10: Mentiras en la red



A modo de resumen sobre las mentiras, bulos y fraudes que circulan por la Red y a los que los menores y jóvenes pueden tener fácil acceso, abordaremos algunas interesantes recomendaciones de la Oficina de Seguridad del Internauta, recogidas en la infografía **"Mentiras en la Red"**.

El formador hará hincapié en el mensaje de que efectivamente, 'no todo es cierto en

Internet', e identificar los bulos, fraudes y mentiras que viajan a través de la Red, pasa por reconocer algunas de las reiteradas características de sus mensajes:

- Falta de concreción en el mensaje. No hablan de nadie ni nada en particular, sino de forma generalista.
- Probablemente contenga errores ortográficos y/o gramaticales y mensajes contradictorios.
- Ofrecen regalos de alto valor económico, desproporcionados en relación a la oferta que presentan.
- Añaden la referencia de conocidas y grandes empresas u organizaciones, con objeto de dar credibilidad a la oferta.
- Solicitan el reenvío masivo de la oferta a través de nuestros usuarios, con el objeto de extenderla rápida y cómodamente, al mayor número posible de usuarios.

TRANSPARENCIA 11: ¿Qué conoces de los virus?

Otro de los riesgos vinculados al uso de las TIC es el *malware* o **virus informático**: aquel programa malicioso capaz de colarse en un dispositivo con fines como:

- Robar datos privados.
- Hacer que el dispositivo deje de funcionar correctamente.
- Tomar su control para llevar a cabo otras acciones maliciosas.

Son muchos los ejemplos que los usuarios de dispositivos electrónicos encuentran cada día sobre alertas y casos reales de virus informáticos que infectan éstos causando la pérdida de información, el bloqueo del dispositivo, el robo de datos personales, etc.

En esta diapositiva, el formador buscará la participación del alumnado en torno a su conocimiento sobre los virus y sus estrategias de defensa.

Algunas de las preguntas que se pueden realizar:

- ¿Qué tipos de virus conocéis?
- ¿Os habéis visto amenazados en alguna ocasión por alguno de ellos?
- ¿Cuál ha sido el 'detonante', la acción que ha activado y extendido ese virus?
- ¿Cuáles creéis que son los métodos más habituales de infección?
- ¿Qué crees que se podría haber hecho para evitarlos?
- ¿Afectan sólo a ordenadores? ¿Habéis detectado algún virus en vuestros dispositivos móviles?
- ¿Tenéis instalado y configurado un antivirus en vuestro Smartphone o Tablet?

Si necesitamos más información para poder guiar adecuadamente este interrogatorio, podemos acudir por ejemplo a la **web de OSI sobre virus** y al **monográfico de Red.es sobre protección ante virus y fraudes**.

TRANSPARENCIA 12: Posibles vías de infección

Principales vías de infección:

- **Correo electrónico.** Es una de las principales vías de entrada de virus, a través de ficheros adjuntos peligrosos o enlaces a páginas web maliciosas.
- **Dispositivos de almacenamiento externo** (USB, discos duros, tarjeta de memoria), al copiar archivos infectados de un USB a nuestro equipo. En ocasiones, simplemente por el hecho de conectar un USB a nuestro equipo podemos resultar infectados, ya que algunos virus tienen la capacidad de auto-ejecutarse.
- **Descarga de ficheros desde Internet**. Al abrir o ejecutar ficheros (programas, contenido multimedia, documentos, etc.) pueden traer camuflado/escondido algún tipo de malware. Hay que tener especial precaución con lo que descargamos mediante programas de compartición de ficheros (P2P) u obtenemos en las distintas páginas web de descarga de contenidos, ya que pueden ser más propensos a contener virus.
- **Páginas web maliciosas,** preparadas para infectar al usuario que las visita aprovechando **problemas de seguridad de un navegador no actualizado** o de los complementos instalados: Java, Flash, etc. También a través de páginas web legítimas, que han sido manipuladas por ciberdelincuentes, **redirigiéndonos a webs maliciosas o fraudulentas**. Una forma de llegar a éstas podría ser, por ejemplo, haciendo clic en **enlaces acortados** en Twitter (u otras redes sociales) o en enlaces facilitados en correos electrónicos fraudulentos.
- **Redes sociales,** utilizadas para infectar los dispositivos debido a la gran cantidad de usuarios que las frecuentan y el alto grado de propagación que facilitan. Hay que ser precavidos frente a publicaciones con enlaces a páginas web con mensajes o titulares llamativos que resulten "raros" o poco fiables, solicitudes para instalar programas para poder acceder o visualizar un contenido, o aplicaciones que solicitan autorización no justificada para el acceso a nuestra **información personal**.
- **Vulnerabilidades y fallos de seguridad** en los sistemas operativos, navegadores, aplicaciones, plugins o programas instalados en el dispositivo. Son aprovechadas por los ciberdelincuentes para infectar los equipos, a veces, sin que el usuario tenga que realizar una acción que le haga consciente de ello. El ejemplo comentado en este caso por el formador puede ser el **Fallo de seguridad de Abobe Flash Player**. A través de este fallo de seguridad, un atacante puede tomar el control remoto de un dispositivo y realizar cualquier acción, como por ejemplo instalar malware**.** Para evitarlos, es importante mantener actualizados nuestros dispositivos.
- **Descarga de apps de mercados de aplicaciones no oficiales.** Un ejemplo reciente lo podemos encontrar en el enorme éxito del juego de aventura de realidad aumentada **Pokemon-Go.** Muchas personas no esperaron a que la app estuviese publicada en los mercados de aplicaciones oficiales y se descargaron algunas de las numerosas versiones que circulaban por Internet, sin ser conscientes de que muchas de éstas estaban manipuladas para llevar a cabo acciones maliciosas en el dispositivo en el que se instalase. En este artículo de OSI podemos encontrar más información **"¿Vas a jugar a Pokémon Go? Sigue nuestros consejos de seguridad".**

TRANSPARENCIA 13: Ransomware. Un ejemplo de virus

El **virus de la Policía** nos puede servir como ejemplo de malware clasificado como **Ransomware** que "secuestra" el ordenador, smartphone o los ficheros que contiene pidiendo un "rescate" para permitirnos usar de nuevo el dispositivo y recuperar los ficheros.

En este caso el virus bloquea o toma el control del ordenador infectado, y haciéndose pasar generalmente por una organización, empresa o entidad conocida con cierta reputación y prestigio solicita un ingreso económico para desbloquearlo.

Nunca se debe ceder ante este tipo de chantaje, puesto que rara vez se devuelve el acceso a la información. Ante una situación de este tipo la recomendación es ponerlo en conocimiento de OSI, la Policía Nacional o la Guardia Civil.

TRANSPARENCIA 14: Conociendo algunos fraudes

El **phishing** es una de las técnicas más usadas por los ciberdelincuentes, sobre la que puedes saber más a través de **este artículo**. Consiste básicamente en que los ciberdelincuentes, haciéndose pasar por una compañía o empresa conocida, intenta robar información privada de los usuarios como son, por ejemplo, las claves de acceso a los servicios online o datos bancarios.

Independientemente del medio utilizado, el objetivo final siempre es obtener información confidencial: nombres y apellidos, direcciones de correo electrónico, números de identificación personal, número de tarjeta de crédito, etc. Para obtener esta información, los ciberdelincuentes generalmente se valen de la ingeniería social y de un enlace que redirige al usuario a una página web fraudulenta que simula ser la web legítima, en algunas ocasiones pueden utilizar documentos adjuntos maliciosos para perpetrar el hurto de datos.

Para saber más sobre las estrategias que éstos usan para 'captar' a sus víctimas, veremos a continuación varios ejemplos.

- La **Falsa factura electrónica de Endesa**: ejemplo de una conocida campaña fraudulenta, de tipo phishing, que suplanta la identidad de la empresa Endesa y cuyo propósito es instalar malware (conocido como Ransomware) en el equipo de la víctima y cifrar los ficheros del equipo para impedir su acceso y posteriormente pedir un rescate (una cantidad de dinero) a cambio de la clave de descifrado que permita recuperar los datos.
- El **Fraude de Correos y Telégrafos:** una campaña masiva de correos fraudulentos que se propagó por email bajo el **falso aviso** de la imposibilidad de "Correos y Telégrafos" de entregar una carta certificada. En este caso, el objetivo del phishing fue infectar los equipos de los usuarios con el fin de poder controlarlos de forma remota para después llevar a cabo distintas actividades maliciosas.
- el **Virus de la Policía**, ya presentado anteriormente como ejemplo de 'Ransomware' y cuyo efecto provoca el bloqueo del ordenador del usuario, solicitando a éste un ingreso de dinero para desbloquearlo, con la excusa del pago de una multa.

Otros ejemplos reales de este tipo de fraude son:

- Phishing al **servicio de iCloud de Apple**
- Phishing a **PayPal**
- Phishing a **Dropbox**
- Phishing a **Iberia**

Otra manera de engañar a los usuarios es poniendo en circulación **fraudes a través de redes sociales**. Un ejemplo son los **falsos vídeso virales en Facebook:** se trata de vídeos que se propagan a través de los muros de los usuarios de Facebook, infectando el dispositivo afectado con un virus de tipo "troyano". Éste permite el robo de información y la instalación de una extensión en el navegador para publicar en Facebook de forma automática y seguir propagando el contenido malicioso entre más usuarios.

Finalmente, **a través de la descarga de contenidos de Internet**, también los usuarios podemos ser engañados, no sólo porque podemos instalar de manera involuntaria malware sino que también porque podemos ser timados. Un ejemplo real: **Videollamadas de WhatsApp**. Los mensajes de esta campaña fraudulenta ofrecen a los usuarios activar las videollamadas para el sistema de mensajería instantánea WhatsApp (a día de hoy esta funcionalidad no la ofrece la app). La promoción fraudulenta se propaga a través de redes sociales en teléfonos móviles, con mensajes que contienen un enlace que redirige a una web que trata de suplantar la identidad de WhatsApp, desde la que le anima al usuario a "descargar la funcionalidad de videollamadas", remitiéndole a otra web desde la que se intentará **subscribir al usuario a un servicio SMS Premium**.

TRANSPARENCIA 15: El adivino Dave

Uno de los riesgos más habituales viene derivado de no dar la debida importancia a la privacidad en la red. Por este motivo debemos sensibilizar sobre la necesidad de una apropiada gestión de la privacidad, que facilite la creación de una identidad y reputación de provecho para el desarrollo personal y profesional del menor.

Debemos concienciar a los menores sobre la **importancia de una búsqueda de equilibrio entre las virtudes de mostrarse públicamente y los riesgos que conlleva**.

La visualización del vídeo **El adivino Dave** nos ayudará a introducir los conceptos de privacidad, identidad digital y reputación online. Este vídeo forma parte de una campaña publicitaria con el objetivo de llamar la atención sobre el peligro que conlleva compartir la vida privada en Internet. Se invitó a participar a personas anónimas que paseaban por la calle, Dave, un supuesto adivino con dotes paranormales iba a hablarles sobre su vida. En realidad se trataba de un actor que a través de un minúsculo auricular en su oído recibía información de un grupo de hackers que buscaban información sobre la vida de los visitantes a través de lo que ellos mismos habían publicado en sus redes sociales.

- ¿Cuál fue el precio de su casa?
- ¿Cuánto dinero hay en su cuenta bancaria?
- ¿Cuánto gastó en ropa y en bebida el mes pasado?

- ¿Cuál es el número de su tarjeta bancaria?

Son algunas de las preguntas que el adivino Dave sabe responder de las personas que tiene delante.

Pregunta de reflexión para realizar al alumnado: **¿Qué información se podría descubrir sobre nosotros en función de la información que publicamos en nuestras redes sociales?**

TRANSPARENCIA 16: Información sobre nosotros

Información que vamos dejando sobre nosotros en la red:

- Lo que pienso: lo que digo, publico.
- Lo que comparto: mis aficiones, lo que me gusta.
- Lo que compro.
- Con quien me relaciono: mis contactos/grupos de amigos.
- Fotos que muestran mi apariencia: (mis imágenes).
- Vídeos que muestran mi forma de divertirme, o mis intereses, mis inquietudes…

TRANSPARENCIA 17: Privacidad en Internet

La **Privacidad** se puede definir como el ámbito de la vida personal que se tiene derecho a proteger de cualquier intromisión. La privacidad nos proporciona seguridad, nos resguarda de la mirada de los otros.

La privacidad es necesaria, las personas tenemos diferentes facetas y en cada una de ellas nuestra privacidad es diferente, es decir no nos comportamos de la misma manera con nuestros amigos, que con nuestros profesores, nuestros padres o nuestra pareja.

Nosotros elegimos el grado de privacidad de cada una de nuestras relaciones y gracias a esto podemos tener relaciones sociales enriquecedoras y variadas que nos permiten desarrollarnos como personas.

La privacidad también tiene que ver con aquello que se comparte sólo con uno mismo.

La privacidad nos da seguridad, nos permite tener parcelas de intimidad para hacer cosas que no haríamos en público, estar relajados, no tener que cuidar nuestra apariencia.

En definitiva, nuestra información privada dicen mucho sobre nosotros o sobre nuestra familia, entorno, etc. En función de la cantidad de datos que facilitemos expondremos en mayor o menor medida nuestra vida privada, que puede ser utilizada para fines que nos pueden perjudicar.

Es decir, un exceso de información sobre nosotros nos hace más vulnerables.

De la misma manera que debemos ser cuidadosos con la gestión de nuestra privacidad, deberemos serlo con la privacidad de los demás. Reflexionar sobre la cantidad de veces que publicamos imágenes en las que junto a nosotros aparecen otras personas a las que no les hemos pedido permiso.

TRANSPARENCIA 18: Identidad digital y reputación online

Por su vinculación con la privacidad y aunque no lo abordemos en profundidad es conveniente dejar claro el significado del término **identidad digital**: conjunto de información sobre una persona expuesta en Internet y que le caracteriza y le diferencia de los demás.

Por tanto, nuestra identidad digital se puede formar con la información que sobre **nosotros mismos** vamos dejando en la red.

Según lo que publicamos y lo que publican los demás, la gente con la que nos relacionamos, lo que nos "gusta", etc. creamos (consciente o inconscientemente) una imagen de nosotros en Internet (identidad digital) que provoca en los demás una valoración, **reputación digital**. No se trata de que sea mejor o peor, sino de que seamos conscientes de que todo lo que hacemos en Internet (o dicen de nosotros) contribuye a nuestra imagen y reputación.

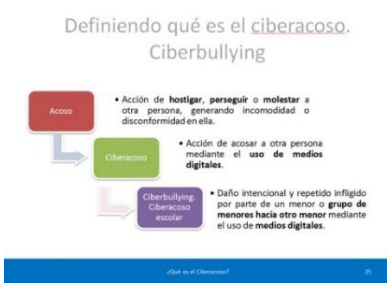
TRANSPARENCIA 19: ¿Qué pasa si alguien vulnera nuestra privacidad?

Si alguien vulnera nuestro derecho a la privacidad puede ser constitutivo de delito. En la actual reforma del Código Penal se amplía la protección de la intimidad al adoptar un enfoque orientado a impedir delitos a través de las TIC. Vamos a comentar algunos relacionados con la intromisión en la intimidad y descubrimiento y revelación de secretos.

- **Descubrimiento de secretos o vulneración de la intimidad de otro.** Por ejemplo cuando una persona se apodera sin consentimiento de mensajes de correo electrónico, información privada extraída al entrar en la red social de un compañero/a al haberse dejado esta persona la sesión abierta.
- **Difusión, revelación o cesión a terceros de datos, hechos o imágenes.** Cuando sin autorización del titular divulga dicha información a terceros. ¡Ojo! La ley dice que será sancionado quien realice la divulgación sin intervenir en su obtención pero conociendo su origen ilícito. Por ejemplo cuando se recibe una foto íntima de un compañero/a y se reenvía.
- **Difusión, revelación o cesión a terceros de imágenes o grabaciones que menoscaben gravemente la intimidad.** Incluso cuando se obtuvieron con consentimiento de su titular, en un entorno íntimo y fuera de la mirada de terceros.

TRANSPARENCIA 20: Definiendo el Ciberacoso

Otro riesgo que abordaremos en esta charla es el ciberacoso. Daremos las definiciones de acoso, ciberacoso y ciberacoso escolar o ciberbullying.



Deberemos dejar claro que debemos entender el ciberacoso como una conducta ligada a la violencia y la privación de derechos hacia otra persona, que con independencia del formato en el que se manifiesta (a través de la tecnología o de forma física, en persona), genera inseguridad e indefensión en la/s víctima/s y que desde el centro educativo (tanto profesorado, como el propio alumnado espectador de este tipo de conductas) se puede y debe reorientar.

TRANSPARENCIA 21: Características del Ciberacoso

Debemos tener en cuenta el "efecto desinhibidor" que las tecnologías de la información facilitan sobre los comportamientos, propiciando que se actúe de manera impulsiva, sin pensar en las consecuencias de nuestros actos.

Su capacidad para **ocultar la identidad** (aunque es una falsa sensación), para **extender un mensaje** masivamente a una gran velocidad y de **conexión permanente**: 24 horas, 7 días de la semana, son características del ciberbullying que se convierten en **factores de riesgo,** aumentando el impacto del agresor/a sobre la víctima.

TRANSPARENCIA 22: Rol de las personas implicadas - agresor

Hablaremos de algunas características y motivaciones que pueden darse en los perfiles implicados, pero dejando claro que no hay un perfil único y estas son sólo características manifiestas en un determinado número de casos. El perfil del agresor/a:

CARACTERÍSTICAS	MOTIVACIONES INTERNAS	MOTIVACIONES EXTERNAS
• Necesidad de dominar • Bajo rendimiento • Baja tolerancia a la frustración • Dificultad para asumir normas	• Frustración • Venganza • Búsqueda de aprobación • Aburrimiento • Necesidad de excluir a la víctima de un grupo/ estatus	• Intolerancia. Prejuicio ante las diferencias • Cierta sensación de seguridad (a través de las TIC) • No implica enfrentamiento físico

TRANSPARENCIA 23: Rol de las personas implicadas - víctima

El perfil de la víctima suele presentar estas características:

VÍCTIMA
• Pocos amigos • Bajo concepto de sí mismo/a • Dificultades de interacción social • Víctima de acoso off-line

Pero al igual que decíamos en el caso del perfil del agresor, no hay un perfil único, cualquiera puede ser 'el elegido', sin un motivo o causa aparente.

TRANSPARENCIA 24: Rol de las personas implicadas - observador

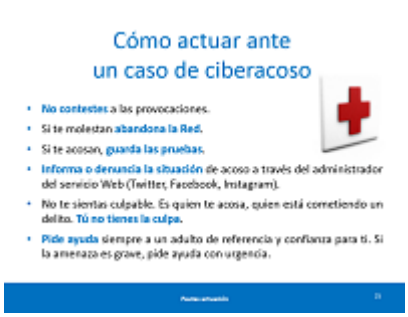
El tercer perfil implicado es el de los observadores (personas que dentro de su entorno, callan y no denuncian el acoso, consintiendo pasivamente sus consecuencias).

OBSERVADORES
Colaboradores pasivos: • No manifiestan su rechazo al acoso. • En algunos casos, difunden las acciones de acoso llevadas a cabo, sin denunciar esta situación.

El docente hará hincapié en este perfil, porque es precisamente desde la toma de conciencia de las situaciones de ciberacoso que suceden a nuestro alrededor, desde donde se puede hacer una gran labor por mediar y luchar contra el ciberacoso.

En muchas ocasiones las medidas de acción ante el ciberacoso pasan por "dar un paso al frente" y manifestar nuestro rechazo y repulsa a este tipo de acciones y nuestro apoyo a las víctimas, ya sea de manera pública o en privado (por ejemplo comentándoselo a un adulto de referencia padres, educadores).

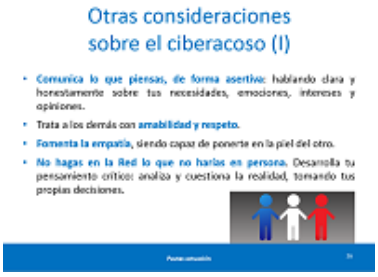
TRANSPARENCIA 25: Cómo actuar ante el ciberacoso



Y ante el ciberacoso destacaremos la necesidad de seguir las siguientes pautas:

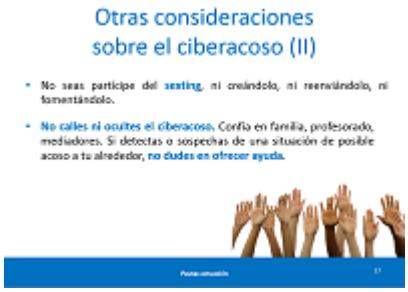
- No contestes a las provocaciones.
- Si te molestan abandona la Red.
- Si te acosan guarda las pruebas.
- Informa o denuncia la situación de acoso a través del administrador del servicio Web (Twitter, Facebook, Instagram).
- No te sientas culpable. Es quien te acosa, quien está cometiendo un delito. Tú no tienes la culpa.
- Pide ayuda siempre a un adulto de referencia y confianza para ti. Si la amenaza es grave, pide ayuda con urgencia.

TRANSPARENCIA 26: Cómo actuar ante el ciberacoso (I)



- Comunica lo que piensas, de forma asertiva: hablando clara y honestamente sobre tus necesidades, emociones, intereses y opiniones.
- Trata a los demás con amabilidad y respeto.
- Fomenta la empatía, en tus relaciones, siendo capaz de ponerte en la piel del otro.
- No hagas en la Red lo que no harías en persona. Desarrolla tu pensamiento crítico: analiza y cuestiona la realidad, tomando tus propias decisiones.

TRANSPARENCIA 27: Cómo actuar ante el ciberacoso (II)

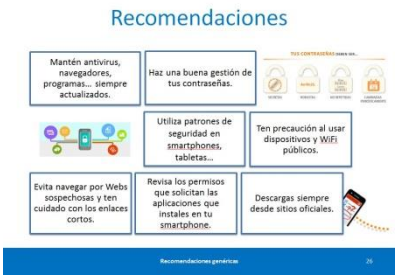


- No seas partícipe del sexting, ni creándolo, ni reenviándolo, ni fomentándolo.
- No calles ni ocultes el ciberacoso. Confía en familia, profesorado, mediadores. Si detectas o sospechas de una situación de posible acoso a tu alrededor, no dudes en ofrecer ayuda.

TRANSPARENCIA 28: Qué podemos hacer para un uso seguro y responsable

Las transparencias 28 y 29 tratan de responder a la pregunta ¿Qué podemos hacer nosotros para que nuestra experiencia con las TIC sea segura y responsable?

El formador hará hincapié en la importancia de que estas sencillas pautas se conviertan en hábitos en nuestra relación diaria con las TIC.



- Mantén **siempre actualizados antivirus, sistema operativo, navegadores, programas…** tanto en ordenadores como en tabletas y smartphones, y siempre desde la web oficial del fabricante.
- Lleva a cabo una **buena gestión de contraseñas**, es decir, estas deben ser secretas y robustas. A pesar de ser una recomendación básica que todos conocemos, todos los años se publican las 25 contraseñas más utilizadas y siguen apareciendo en los primeros puestos contraseñas como: 1234; password; qwerty; 111111;…

  Una contraseña segura no debe contener ninguna información relacionada con nosotros, es decir, no debe contener nuestro nombre, ni nuestra edad, año de nacimiento, nombre de nuestro perro…, debe tener un mínimo de 8 caracteres incluyendo mayúsculas, minúsculas, dígitos y caracteres especiales. Además, la contraseña es personal e intransferible, no debemos decírsela a nadie. Es muy importante igualmente que utilicemos diferentes contraseñas para los diversos servicios y/o aplicaciones de los que somos usuarios y que la cambiemos periódicamente.
- **Activa patrones de seguridad** en tus smartphones y tabletas. Párate a pensar la cantidad de datos que llevas simplemente en tu smartphone (datos/imágenes personales, datos que afectan a tu privacidad, incluso datos que pueden afectar a la privacidad de terceros).
- **Toma precauciones al utilizar dispositivos y redes wifi públicas** (procura no realizar transacciones o intercambio de información sensible e importante).
- **Evita navegar por webs sospechosas (programas y juegos gratuitos, fotos de famosos, etc.). y ten mucha precaución con los enlaces cortos** (tipo bit.ly; goo.gl;) analízalos antes de acceder a ellos, sobre todo desde pantallas móviles, Twitter y otras redes sociales, donde se usan para ahorrar caracteres que pueden dirigirnos a páginas web fraudulentas, que contienen malware.
- **Revisa los permisos que solicitan las aplicaciones que instales en tus Smartphone**… Pon en una balanza el servicio que hace esa aplicación y los permisos que cedes.
- Realiza las **descargas siempre desde sitios oficiales**.

TRANSPARENCIA 29: Qué podemos hacer para un uso seguro y responsable

- **Siempre que puedas, más aún para transacciones importantes o informaciones sensibles conéctate a través de páginas seguras.** Son aquellas que empiezan por https Todos los bancos tienen este protocolo pero ahora también las redes sociales lo van incorporando. Así, tienen, al activar el cifrado, toda la información que enviemos será encriptada y en caso de ser interceptada no será legible. Es muy útil cuando nos conectamos desde fuera de casa.

- **Configura adecuadamente las opciones de privacidad de tus redes sociales y revísalas periódicamente**. Si tienes cualquier duda las principales redes sociales tienen centros de seguridad donde puedes encontrar información para resolver tus dudas, es tan fácil como poner en el buscador centro seguridad Facebook/Twitter/Instagram.
- **No publiques excesiva información personal**. Subir una fotografía comprometida o realizar un comentario polémico tal vez pueda pasar desapercibido en el presente pero puede pasarnos factura en el futuro. Es necesario que pensemos siempre en las consecuencias que puede suponer tanto para nuestra reputación online como para la de los demás.
- **Valora cuando tener activados los servicios de geolocalización**. Ya que estaríamos transmitiendo nuestra ubicación e incluso hábitos de desplazamiento. Además los Smartphone y la mayoría de las cámaras digitales actuales registran la posición GPS del lugar donde se toma una determinada foto y esa información se añade a los metadatos de la misma, quedando accesible a cualquiera a quien hagamos llegar la foto. La mejor solución pasa por deshabilitar en general la conexión GPS cuando no se esté utilizando.
- Haz **copias de seguridad** de la información que te interesa, para impedir, por ejemplo, que la acción de algún virus nos haga perderla.

TRANSPARENCIA 30: Dónde localizar más información

Recomendaremos dos páginas imprescindibles para saber más y estar perfectamente actualizado:

La página de OSI Oficina de Seguridad del Internauta **https://www.osi.es** Destacar las siguientes secciones con información de interés:

- **Ponte al día (sección de actualidad):**
  - **Avisos de seguridad**
  - **Blog**
  - **Historias reales**
- **¿Qué deberías saber?**
  - Sobre tus dispositivos
  - Sobre tu información
  - Sobre el fraude
  - Sobre tus conexiones
  - Sobre tu actividad online

Y la página Internet Segura for Kids **http://www.is4k.es** con:

- La información que "**necesitas saber**" sobre privacidad, ciberacoso escolar, sexting, contenido inapropiado, uso y configuración segura, mediación parental.
- Artículos de interés y actualidad en el "**blog**".

- Guías, juegos, herramientas de control parental y otros recursos "**de utilidad**".
- Información de "**programas**" de sensibilización para un uso seguro y responsable de Internet por los menores.
- Una "**línea de ayuda**" con una serie de preguntas frecuentes y un contacto para resolver dudas.

TRANSPARENCIA 31: Despedida

Siempre podéis poneros en contacto con nosotros a través de la web:

- https://www.is4k.es

Internet Segura for Kids (IS4K), es el nuevo Centro de Seguridad en Internet para menores en España. Allí podéis encontrar información, guías, juegos y otros recursos de utilidad sobre los principales riesgos de Internet, cómo prevenirlos y afrontarlos. Además disponéis de una línea de ayuda con una serie de preguntas frecuentes y un contacto para resolver vuestras dudas.

Recordad que podéis seguir nuestros perfiles públicos de redes sociales:

- Facebook, buscando "Internet Segura for Kids"
- Twitter, usuario @is4k