Programa de Jornadas Escolares

Promoción del uso seguro y responsable de Internet entre los menores

---

Privacidad, identidad digital y reputación

Charla de sensibilización al 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

Esta guía servirá como orientación al profesorado a la hora de desarrollar en el aula una charla de sensibilización sobre **Privacidad, identidad digital y reputación**, apoyándose en la presentación **Privacidad, identidad digital y reputación. Sesión de sensibilización dirigida al alumnado.**

La guía (y la presentación anexa a ella) tratarán de responder al objetivo: Conocer los conceptos de privacidad, identidad digital y reputación online y sus implicaciones para la vida personal y profesional presente y futura. Se incidirá en la necesidad de sensibilizar al alumnado sobre el papel que la privacidad y la identidad digital están cobrando en la sociedad actual que afecta a todos los aspectos de la vida, comprendiendo tanto los beneficios como los riesgos con la finalidad de promover las buenas prácticas necesarias para una construcción y gestión positiva de la identidad digital.

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.

Trabajará los fundamentos teóricos y principales características sobre privacidad, identidad digital y reputación online. Explicará las consecuencias que se pueden derivar de la falta de privacidad y de la construcción de una identidad digital negativa, ofreciendo ejemplos concretos y cercanos al alumnado. A su vez expondrá la importancia de la construcción y gestión positiva de la identidad digital proporcionando pautas concretas.

1.1. Objetivos didácticos

- Tomar conciencia sobre la importancia de la privacidad en Internet.
- Conocer las oportunidades y las repercusiones de nuestra imagen en Internet.
- Aprender a construir nuestra identidad digital de forma positiva

1.2. Contenidos

- Conceptos de privacidad propia y de terceros.
- Concepto de identidad digital
- Concepto de reputación online.
- Factores determinantes de la identidad-reputación digital.
- Riesgos vinculados a la falta de privacidad.
- Pautas para la construcción y gestión de una identidad digital positiva.

1.3. Metodología

A lo largo de esta presentación el docente realizará la exposición de contenido, combinando el método **expositivo**[1] y el **interrogativo**[2].

Actuará también como facilitador de una sesión participativa utilizando el **debate**[3] y la visualización de los vídeos, con objeto de animar a compartir información, ideas, inquietudes, dudas, buscando en todo momento promover un entorno que favorezca la motivación del alumnado.

Esta metodología promoverá también 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. El formador utilizará un lenguaje acorde con el nivel de conocimientos previstos en el alumnado destinatario con objeto de un entendimiento claro de las actividades propuestas, contribuyendo a su buen desarrollo.

2. Fundamentos teóricos sobre privacidad, identidad digital y reputación online

TRANSPARENCIA 3: ¿Quién sabe qué es?

A modo de introducción y como elemento de motivación iniciaremos la charla con una imagen de una botella de Coca-Cola vacía y preguntaremos: **¿quién sabe qué es?**

El formador deberá abordar la reflexión haciéndonos conscientes de que todos identificamos perfectamente una marca. Esta empresa ha invertido muchos años y dinero en fabricar esta imagen, una botella diferente, un logo, anuncios originales, atractivos, diferentes…

De la misma manera que identificamos esta marca, ahora, gracias a la tecnología cada uno de nosotros es perfectamente identificable en Internet.

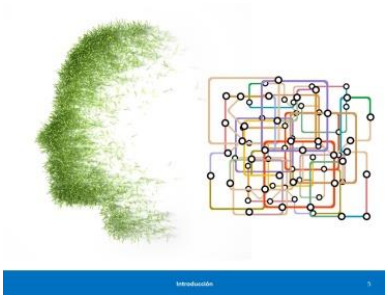
[1] **METODOLOGÍA EXPOSITIVA:** centrada en la transmisión de información, posibilita la transmisión de conocimientos ya estructurados, facilitando demostraciones de tipo verbal y la transmisión de información y conocimiento, de manera rápida y generalizada.

[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.

[3] **El DEBATE EN EL AULA**: nos permite estimular el análisis y el cambio de actitudes por medio de la presentación de distintos puntos de vista.

TRANSPARENCIA 4: Identidad digital

La **identidad digital** es el conjunto de información sobre una persona expuesta en Internet y, por tanto, que le caracteriza y le diferencia de los demás.



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

El formador solicitará aportaciones por parte del alumnado. **¿Qué información voy dejando en la red sobre mí?**

TRANSPARENCIA 5: ¿Desde cuándo tenemos identidad digital?

Los pasos que vamos dando por Internet van construyendo una imagen sobre nosotros que podría llegar a identificarnos plenamente.

Muchas veces antes de que nosotros comencemos a utilizar Internet, esa imagen ya se ha ido creando porque alguien (generalmente los padres) han subido imágenes nuestras con nuestro nombre y apellidos.

Pregunta al alumnado: **¿A qué años comenzaste a utilizar Internet?**

TRANSPARENCIA 6: ¿Qué información voy dejando sobre mí en la red?

En esta diapositiva, se ofrecerá más en detalle las formas en las que podemos ir dejando información sobre nosotros en Internet. Y por tanto, información que puede ir formando parte de nuestra identidad digital.

¿Qué forma parte de nuestra identidad digital?

- Lo que pienso, 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 7: Interacciones que realizamos en Internet cada minuto

Preguntaremos al alumnado si saben que es una infografía[4] y en cualquier caso daremos su definición y les pediremos que observen la imagen de la diapositiva elaborada en 2016 por **Domo.com,** una empresa especializada en la extracción de datos.

Con objeto de tomar conciencia de la cantidad de información que vamos dejando en Internet, el formador comentará el número de interacciones que realizamos en Internet cada minuto de cada día.

Algunos datos que se observan en la infografía: 3.400 millones de personas conectadas que cada minuto:

- Comparten 216.300 fotos en Facebook.
- Ponen 2.400.000 de "Me gustas" en post en Instagram.
- Visualizan casi 7.000.000 de vídeos en Snapchat

Pregunta de reflexión al alumnado: **¿Cuántos comentarios haces al día?, ¿Cuántos likes?**

Es conveniente que el alumnado entienda que todos estos datos tienen un valor incalculable. Además de reflejar nuestra identidad digital son utilizados para muchas otras actividades.

La información de los usuarios es un activo valiosísimo sobre todo para aquellas empresas que utilizándolos les permite, por ejemplo, ser más competitivas o generar nuevos negocios y servicios.

Pero también para las personas, para nosotros como individuos, como usuarios personales tenemos que darnos cuenta de que la información que generamos va a permanecer a lo largo del tiempo en Internet y parte de esa información que nosotros mismos hemos generado en un momento dado podría llegar tanto a favorecernos como a perjudicarnos.

TRANSPARENCIA 8: ¿Cuántas identidades utilizamos en Internet?

Las personas utilizamos diferentes identidades en función de las diferentes actividades que desarrollamos online. Por ejemplo, podemos tener nuestro perfil en Facebook o Twitter, subir fotos a Instagram, crear vídeos en YouTube, participar en diferentes foros o blog del colegio…

En cada uno de estos servicios vamos creando una identidad digital parcial de nosotros, que pueden estar o no relacionadas con el resto.

La suma de todas estas identidades parciales permite construir una identidad digital y una imagen de la persona en Internet.

En base a esta información, proyectamos una imagen que es como nos ven los demás. Y esta imagen puede resultar positiva o negativa, es lo que se conoce como **reputación online.**

[4] **INFOGRAFÍA**: Método para representar la información de forma icónica y textual de manera que el usuario pueda comprenderla fácilmente empleando para ello herramientas informáticas.

(Adelantamos así el concepto de reputación online, aunque más adelante volveremos a incidir en él).

TRANSPARENCIA 9: Lo que otros publican sobre mí

¡Ojo! Lo que otros publican sobre nosotros también forma parte de nuestra identidad digital. Esta información es más difícil de gestionar, porque en Internet es muy complicado eliminar contenidos publicados (por ejemplo, información que hable sobre nosotros y que no se ajuste a la verdad o que de una imagen negativa sobre nosotros o sencillamente que no nos guste) pero por lo general, según nos comportemos, así opinarán de nosotros.

Obviamente, todos queremos que se hable bien de nosotros, tener una buena imagen en Internet. Parece extraño que alguien quisiese lo contrario ¿no?

A continuación, el formador puede lanzar la siguiente pregunta:

¿Cómo se puede construir una identidad digital que perjudique a una persona? ¿Alguien construiría una identidad digital negativa sabiendo que le puede perjudicar?

TRANSPARENCIA 10: Qué entendemos los usuarios por privacidad

Tras interactuar con los alumnos, comentaremos las noticias que se muestran en la presentación y visualizaremos los vídeos.

Tanto las 2 noticias como los vídeos evidencian el desconocimiento en torno al concepto de privacidad y por tanto sobre las consecuencias que se derivan de la falta de privacidad. Si no se dispone de tiempo suficiente, sólo se recomienda la visualización de uno de los vídeos.

Noticias de ejemplo

- La noticia "**Paula Váquez publica por error su teléfono y dirección en Twitter**" hace referencia a una popular presentadora que tuiteó un parte médico con sus datos en el que se podía leer su número de teléfono y su dirección, pocos minutos después, y gracias a los retuits de sus casi 200.000 seguidores, esa imagen circulaba por Twitter como la pólvora, recibiendo multitud de llamadas de fans y curiosos.

  Poco después, la presentadora dándose cuenta de su error borraba el mensaje pero el daño ya estaba hecho. La presentadora amenazó en un nuevo tuit con publicar los teléfonos de quien siguiera llamándola y así lo hizo pese a ser advertida por otros usuarios que publicar el número de móvil de otras personas podía ser constitutivo de delito.

- La segunda noticia: "**Detienen a un ladrón que se dejó abierto su Facebook en la casa en la que entró a robar**". El ladrón no cerró su sesión, más tarde fue reconocido en la calle por la foto de su perfil de Facebook.

Como decíamos estas dos noticias muestran el desconocimiento que tenemos en torno a la privacidad.

Vídeos de ejemplo

La visualización de los siguientes vídeos incide en este aspecto:

- **El adivino Dave.** Este vídeo forma parte de una campaña publicitaria con el objetivo de llamar la atención del 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 micrófono 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: **¿Qué información se podría descubrir sobre nosotros en función de la información que publicamos en nuestras redes sociales?**

- **Si todo estaba perfecto… ¿qué falló?** Vídeo desarrollado por chicos y chicas de 12 a 18 años en el marco de un concurso "Tecnología Sí. Conéctate con responsabilidad" que tiene por objetivo premiar cortos que aborden aspectos relacionados con el uso seguro de la tecnología.

  Este vídeo en concreto aborda la importancia de la entrevista de trabajo y como la imprudencia, la ignorancia sobre privacidad, identidad digital y reputación online y la falta de conocimiento a la hora de utilizar la tecnología puede perjudicarnos seriamente ante la posibilidad de obtener un empleo.

  Se puede orientar hacia la reflexión de otro tipo de situaciones más próximas a la realidad del alumnado, por ejemplo, en lugar de una entrevista de trabajo la misma situación puede darse para entrar en un equipo de fútbol, baloncesto para entrar en un coro o en cualquier otro tipo de asociación que realice una mínima selección de sus miembros e incluso a la hora de ligar o buscar pareja.

  ***Observaciones:** el sonido de este vídeo no es óptimo pero el hecho de que tanto su guionaje como realización esté elaborado por menores y dirigido precisamente a menores hace que consideremos relevante incluirlo. Es un ejemplo de cómo los propios menores pueden participar de manera activa en el desarrollo de materiales dirigidos a ellos mismos, observando cómo son capaces de dar consejos certeros cuando se les pide reflexión y análisis, utilizando su propio lenguaje, de forma que los resultados pueden llegar a ser mejor acogidos por sus iguales.

Por otro lado, hay que tener en cuenta otro factor de influencia, **la falsa sensación de privacidad** que nos produce interactuar a través de nuestro smartphone o cualquier otro dispositivo a través de las aplicaciones que manejamos. Más adelante será necesario destacar este último factor con el alumnado.

TRANSPARENCIA 11: ¿Qué es la privacidad?

La **privacidad** se puede definir como el ámbito de la vida personal que se tiene derecho a proteger de cualquier intromisión.

Nosotros elegimos el grado de privacidad que queremos mantener. No nos comportamos de la misma manera con nuestros amigos que con nuestros profesores, nuestros padres o nuestra pareja. Con cada uno compartimos ciertas cosas (a veces incluso con nadie, lo guardamos para nosotros). Gracias a esto, podemos tener relaciones sociales enriquecedoras y variadas que nos permiten desarrollarnos como personas.

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 positivos en algunos casos, pero que nos pueden perjudicar en otros. 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 le hemos pedido permiso.

TRANSPARENCIA 12: ¿Qué forma parte de nuestra privacidad?

La información que hace referencia a nuestros gustos, aficiones, creencias, etc. También forman parte de nuestra privacidad.

Un ejemplo: las imágenes que se ven a través de la webcam de mi habitación (sin que se me vea) forman parte de mi privacidad.

Se pueden lanzar a los alumnos varias preguntas para ver qué cosas perciben ellos como privadas:

- ¿Publicarías una foto tuya en la entrada del colegio o en la puerta de tu casa?
- ¿Publicarían una foto de tu habitación en Internet?
- ¿Publicarías en Internet tus creencias religiosas?

- ¿Y tus pensamientos más íntimos?

La diversidad de respuestas nos demuestra que la privacidad es algo subjetivo.

TRANSPARENCIA 13: Datos personales

Nuestros **datos personales** también forman parte de **nuestra privacidad** y dicen mucho sobre nosotros. Por ejemplo, nuestro DNI, la dirección donde vivimos, nuestro número de móvil, dirección de correo electrónico, nuestra imagen (vídeos, fotos), incluso nuestra voz, son datos personales.

También, son datos personales los relacionados con la salud -enfermedades, pruebas médicas o tratamientos-, los datos bancarios como el número de cuenta o de tarjeta, los datos asociados a nuestra vida laboral, como por ejemplo, el salario, los datos biométricos como las huellas dactilares, 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.

TRANSPARENCIA 14: Protege tus datos personales

Los datos personales están protegidos por la **LOPD** (Ley Orgánica de Protección de Datos 5/1999), nadie puede hacer un uso indebido de ellos. Toda persona tiene derecho a decidir sobre quién tiene datos personales suyos y a saber para qué los van a utilizar.

Todo aquel que incumpla esto, podrá acogerse a los derechos **"ARCO":**

- **Derecho de Acceso**. Tenemos derecho a saber qué información tiene una organización sobre nosotros.
- **Derecho de Rectificación**. Tenemos derecho a rectificar nuestra información si está desactualizada o es incorrecta.
- **Derecho de Cancelación**. Tenemos derecho a cancelar el uso de nuestra información si ya no utilizamos ningún servicio de una empresa. Pueden mantener información nuestra por motivos legales, pero ya no pueden usar nuestros datos para nada más.
- **Derecho de Oposición**. Si una organización ha obtenido nuestra información sin nuestro consentimiento o queremos que deje de utilizarla, este derecho nos permite oponernos a que utilicen nuestros datos.

Para registrarnos en algunos servicios de Internet, en ocasiones nos piden diversos datos personales: nombre y apellidos, teléfono, fecha de nacimiento, correo electrónico, etc. Al proporcionar estos datos corremos un riesgo, ya que no podemos controlar con exactitud quién va a acceder a ellos ni para qué.

La ley española obliga a las empresas a proteger estos datos, pero a algunas no les aplica por estar ubicadas en otros países. Por este motivo, debemos valorar antes de darnos de alta en algún servicio, qué datos nos piden y qué uso van a hacer de ellos. Para ello es importante que leamos las condiciones de uso y la política de privacidad del servicio antes de facilitar cualquiera de nuestros datos.

A tener muy en cuenta, la LOPD también establece que los **datos personales de los menores de 14 años** sólo pueden ser tratados por terceras personas con el **consentimiento de los padres o tutor legal**.

TRANSPARENCIA 15: Facilitar información privada nos hace ser más vulnerables

En función de la cantidad de datos que facilitemos expondremos en mayor o menor medida nuestra vida privada. Además, esta información puede ser utilizada para fines que nos pueden perjudicar.

Facilitar un exceso de información nos hace más vulnerables, por ejemplo, podemos ser víctimas de ciberacoso o suplantación de la identidad.

Ejemplo que se puede utilizar: Robo de Identidad: **"Detenida una joven de 18 años por usurpar el perfil de otra persona en una red social"**. Una joven de 18 años fue arrestada acusada de usurpar el perfil de una persona en una red social, publicar fotos íntimas suyas y extorsionarle, en concreto fue acusada de acusados de los delitos de **usurpación de estado civil, contra la intimidad, extorsión y amenazas**.

La víctima descubrió los hechos cuando al intentar acceder a una red social de Internet, vio que no podía hacerlo utilizando sus claves habituales y al entrar desde otra cuenta constató que alguien había usurpado su perfil, colgando además fotos íntimas suyas acompañadas de comentarios desagradables, por lo que presentó una denuncia.

Los agentes comprobaron además que una persona exigía dinero para devolverle las claves de su perfil, además de amenazarle si no se atenía a sus pretensiones.

TRANSPARENCIA 16: ¿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. En concreto se contemplan 7 tipos delictivos (Delitos relativos a la intromisión en la intimidad y descubrimiento y revelación de secretos).

En la presentación observaremos cómo sólo hemos incluido alguno de estos delitos, aquellos que pueden ser más comprensibles y/o cercanos al perfil del alumnado, por ejemplo por el auge que está teniendo el ciberacoso en la actualidad.

- **Descubrimiento de secretos o vulneración de la intimidad de otro. (Por ejemplo, cuando una persona se apodera sin consentimiento de mensajes de correo electrónico o de**

información privada extraída al entrar en la red social de un compañero/a al haberse dejado esta persona la sesión abierta*).*

- Apoderamiento, utilización o modificación de información reservada en perjuicio de un tercero. (ej. Vulnerando sistemas de seguridad o a través de engaños que permitan hacerse con la contraseña sin la autorización del titular).
- **Difusión, revelación o cesión a terceros de datos, hechos o imágenes. (Cuando sin autorización del titular se comparte dicha información con terceros. ¡Ojo! La ley señala que también 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 y se reenvía).**
- **Difusión, revelación o cesión a terceros de imágenes o grabaciones que menoscaben gravemente la intimidad (incluso cuando se obtuvieron con anuencia de su titular, en un entorno íntimo y fuera de la mirada de terceros).**
- Intrusión. Si una persona accede o permite el acceso a un sistema de información protegido.
- Intercepción de transmisiones o datos. Como el anterior pero sin necesidad de entrar en el sistema sino interceptando datos por ejemplo utilizando un software que intercepte toda la información que recibe o envía otro móvil.
- Uso de programas informáticos o contraseñas para fines ilícitos. Se sanciona a quien lo cometa o brinde herramientas para ello.

TRANSPARENCIA 17: Falsa sensación de privacidad en Internet

También es necesario que el alumnado observe que es relativamente sencillo interceptar las comunicaciones a través de la red, y que esto puede afectar igualmente a nuestra privacidad.

Por ejemplo, cuando utilizamos una wifi pública, cualquier persona que esté conectado a la misma podría capturar los datos que salen de nuestro dispositivo, a no ser que estemos conectándonos a páginas seguras, es decir, aquellas que cuando enviamos información ésta circula cifrada (la URL empieza por https) de manera que aunque fuera capturada, no sería legible.

Por otra parte, los agujeros de seguridad o vulnerabilidades, son fallos en el diseño y programación del software y aplicaciones que permiten comprometer su seguridad.

Sólo es necesario hacer una búsqueda en Google sobre fallos o agujeros de seguridad y comprobaremos la existencia en redes sociales, como en sistemas operativos, reproductores multimedia…

Estos fallos, podrían permitir a los ciberdelincuentes acceder a nuestros dispositivos y en consecuencia a nuestra información privada si no tenemos el equipo correctamente configurados y actualizados.

Comentaremos algunos ejemplos:

- Detectan un agujero de seguridad en 12 millones de routers.

- Descubren un fallo en Facebook que permitía acceder a cualquier cuenta
- El fallo de seguridad por el que Facebook paga más de 6.000 euros si lo detectas.
- Descubren un fallo de seguridad que podría afectar al 95% de los usuarios de Android.
- Fallo de seguridad en el reproductor multimedia VLC
- Vulnerabilidad crítica en Adobe Flash Player

TRANSPARENCIA 18: Nuestros pasos por Internet dejan un rastro

Debemos dejar claro que, pese a la sensación de privacidad que nos puede dar realizar algún tipo de actividad a través de nuestros dispositivos electrónicos sin que nadie nos vea, todos los pasos que damos al utilizar nuestros dispositivos digitales y/o al acceder a Internet dejan rastro, aunque intentemos borrarlo. Y esto tiene sus aspectos positivos y negativos.

- Cuando nos arrepentimos de haber subido alguna foto nuestra, por ejemplo en redes sociales, y la quitamos enseguida, podrían ser recuperadas a través de los buscadores que se dedican a registrar todo lo que aparece en Internet.
- Almacenamos fotos privadas en nuestro dispositivo móvil, sin darnos cuenta que lo podemos perder o nos lo pueden robar y con él nuestra intimidad.
- Cuando se acosa a alguien a través de Internet pensando que nadie nos ve, y aunque se utilice un perfil falso, la navegación deja un rastro imborrable.
    - **Caso Eva Hache:**

      La presentadora recibió amenazas de muerte a través de su cuenta de Twitter. Eva H. lo puso en conocimiento de la Policía y la Guardia Civil precisamente a través de las cuentas oficiales online de estos organismos:

      "Hola, buenas noches, señor agente", escribió la presentadora en un tuit en el que mencionaba ambas cuentas (@policia y @Guardiacivil062) y añadía un enlace al pantallazo de las amenazas

      La respuesta por parte de las fuerzas de seguridad del Estado fue inmediata, le indicaban también la necesidad de presentar denuncia. Así lo hizo la popular presentadora. Poco después era detenido el acosador.

      La Policía Nacional detiene al acosador de Eva Hache en Twitter

      La humorista recibió amenazas de muerte a través de la red social

      "No hay ningún sistema que garantice al cien por cien la eliminación de un archivo en soporte digital"

- Cuando borramos un documento lo que estamos haciendo realmente es ocultar un indicador que identifica este archivo en la memoria del dispositivo, pero no estamos borrando el documento, que permanece en el disco duro siendo posible su recuperación. Da igual que sea un documento, una foto, una conversación de chat, el historial de navegación o un correo electrónico.

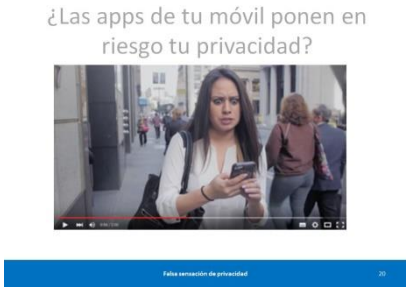
Por ejemplo, cuando borramos mensajes de correo electrónico de nuestra cuenta y ya no los vemos, no desaparecen, se siguen conservando en nuestro ordenador y en la empresa que ofrece el servicio de correo. Los servidores de Gmail, por ejemplo, guardan los correos que borramos durante 18 meses.

- **Caso incendio Horta de San Juan**:

> **Uno de los detenidos por el incendio de Horta aparece en una foto de espaldas al fuego**
>
> Uno de los detenidos por el incendio de Horta de Sant Joan (Tarragona) aparece en una quincena de fotografías que los Mossos de Esquadra recuperaron de la tarjeta de memoria de una cámara, también se puede ver a uno de los arrestados recogiendo hojas secas para hacer el fuego.
>
> Días después del incendio, los detenidos borraron las fotos de la tarjeta de memoria de la cámara fotográfica, pero los técnicos de los Mossos consiguieron recuperar las imágenes. En el incendio murieron cinco bomberos.

- Hace unos años un estudiante austriaco que hizo su tesis sobre la privacidad, solicitó a Facebook todos los datos que tenían sobre él, Facebook le envió un CD con 1200 páginas donde además de los datos de su perfil aparecían referencias sobre sus gustos, sus intereses, sus opiniones religiosas y hasta sus conversaciones privadas, y notas que había eliminado. Tras varias quejas a Facebook presentó diversas denuncias a las autoridades de su país. Se formó un colectivo **"Europa contra Facebook"** buscan que no todo lo que se comparta pueda ser utilizado por la empresa sin pedir el previo consentimiento del usuario.

TRANSPARENCIA 19: ¿Las apps de tu móvil ponen en riesgo tu privacidad?



Cuando navegamos por Internet, simplemente realizando búsquedas, dejamos un rastro. También cada like, comentario o retweet generan innumerables cantidades de información, y mucha de ella estará disponible en Internet si hacemos uso de servicios como Google. Éste por ejemplo, podría saber qué buscamos (intereses personales o profesionales), gustos, nuestra localización geográfica, horarios... Incluso nuestros correos electrónicos, ya que sus términos y condiciones del servicio indican que **lee y escanea los mensajes que enviamos por Gmail para ofrecernos publicidad relacionada** con los temas que tratamos en nuestros correos.

En definitiva, es el negocio de muchas empresas. Nos ofrecen productos muy buenos y gratuitos con el objetivo de poder construir perfiles detallados del uso que hacemos de ellos y ofrecer a los anunciantes la posibilidad de exponer sus mensajes publicitarios ante nosotros.

"Si algo es gratis el producto eres tú"

Pero evidentemente, un trato de "productos por información" no tiene por qué ser necesariamente malo, si se ejecuta con los términos claros y las garantías adecuadas.

- Visualizar video **Derechos de las aplicaciones móviles**.

El formador incidirá en la importancia de que el usuario sea responsable de la lectura de todas las políticas de servicio de las aplicaciones para no poner en peligro su privacidad en servicios tan personales, porque una vez que lo aceptamos, damos nuestro total consentimiento.

Será necesario evidenciar que las intercepciones de información ("hackeos del servicio"), los fallos de seguridad, etc. están ahí, pero en cualquier caso **somos nosotros** quienes debemos poner todos los medios para velar por nuestros datos y por nuestra privacidad y seguridad.

Se puede sugerir unos "deberes" al alumnado:

- Usuarios de Android: revisar los permisos a los que puede acceder cada aplicación que tienen descargada en su smartphone desde el menú **Ajustes > Aplicaciones**.
- Los usuarios de iPhone pueden comprobar las aplicaciones que tienen acceso a las distintas funcionalidades del teléfono como la Localización, Calendario, Contactos, etc. desde el menú a **Ajustes > Privacidad**.

TRANSPARENCIA 20: Reputación online

Como ya explicamos al principio de la presentación, la suma de todas las informaciones que se van publicando sobre nosotros en Internet construye nuestra identidad digital. Esta información será **cómo los demás nos ven en Internet**, y es lo que llamamos reputación online.

Cuando somos conscientes de que alguien nos está conociendo, bien porque entablamos una conversación o bien porque se establece un contacto visual, es decir, el hecho de ser conscientes de que una persona se está formando una impresión de nosotros, nos anima a cuidar al máximo nuestra imagen. En determinadas situaciones, incluso extremamos este cuidado. Por ejemplo, pensemos que tenemos la oportunidad de conocer a alguien muy importante para nosotros y que podemos estar con esa persona media hora. Seguro que dedicaremos un tiempo a pensar qué ropa ponernos, y cuando estemos delante de esa persona trataremos de causarle buena impresión, por ejemplo hablando de un tema que sabemos que le gusta.

En Internet ocurre lo mismo, solo que yo no sé cuando alguien me puede buscar por Internet para saber de mí, (por tanto no tengo tiempo de ponerme mi mejor ropa), sencillamente la información que esté en Internet sobre mí tiene que ofrecer buena impresión en cualquier momento. Esta facilidad de acceso es una característica de la identidad digital que afecta directamente a la reputación online.

TRANSPARENCIA 21: ¿Qué pasa si alguien nos busca por Internet?

Cada vez es más habitual que te hablen de alguien y en un segundo lo busques en Internet para saber de quién se trata, saber más sobre esa persona, lo hacemos incluso por simple curiosidad.

Igual que lo hacemos nosotros, lo pueden hacen los demás, sobre todo cuando se tiene que seleccionar a alguien de entre varios candidatos. Por ejemplo, para entrar en el equipo de

fútbol o en una residencia universitaria, etc. En muchos sitios antes de aceptarnos, tal vez miren en Internet para saber más de nosotros y dependiendo de la impresión que les causemos, nos admitirán o no.

TRANSPARENCIA 22: Lo que publicamos en Internet perdura en el tiempo

Lo que es seguro es que dentro de unos años alguien buscará a nuestros alumnos para saber más sobre ellos y darles quizá o no el trabajo que están buscando (7 de cada 10 empresas lo hace) y el 95% de los profesionales de RRHH[5] reconocen la importancia de las redes sociales como aliado perfecto, ya que, además de los estudios o experiencia de la persona candidata, permiten conocer detalles acerca de cómo es esta en su día a día y cómo se muestra a los demás.

Este ejemplo es importante porque es necesario que el alumnado empiece a darse cuenta de que lo que publicamos en Internet puede perdurar en el tiempo y afectar a nuestra vida personal y profesional en un futuro. Y es que, mientras que en la vida offline una persona puede, con mayor o menor facilidad, poner fin o modificar alguno de los rasgos diferenciadores que conforman su identidad, en Internet borrar el rastro que van dejando nuestras decisiones no es fácil. La identidad digital perdura y cuanto más tiempo pasa, más difícil es eliminarla por completo o modificar sus raíces: **"lo que publicamos hoy puede pasarnos factura dentro de unos años".**

TRANSPARENCIA 23: Recomendaciones (I)

Finalizaremos el taller con un **resumen de las principales recomendaciones**.

Recomendaciones para cuidar nuestra privacidad y construir una identidad y reputación online positiva.

- **Utilizar contraseñas seguras y no compartirlas**. A pesar de ser una recomendación básica que deberíamos conocer, todos los años se publican las 25 contraseñas más utilizadas y siguen apareciendo contraseñas totalmente inseguras (1234; password; qwerty; 111111;…)

  La contraseña es personal e intransferible, no debemos decírsela a nadie. 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.

[5] IV Informe 2015 Infoempleo-Adecco Redes Sociales y Mercado de Trabajo. http://iestatic.net/infoempleo/documentacion/Informeempleoyredes2015.pdf

Es muy importante igualmente que utilicemos diferentes contraseñas para los diversos servicios y/o aplicaciones de los que somos usuarios.

- **Utilizar patrones de seguridad.** Parémonos a pensar la cantidad de datos que llevamos simplemente en nuestro smartphone (datos/imágenes personales, datos que afectan a nuestra privacidad, incluso datos e imágenes que pueden afectar a la privacidad de terceros).

- **Revisar los permisos que solicitan las aplicaciones que se instalan en el smartphone**: tengo que poner en una balanza el servicio que me hace esa aplicación y los permisos que cedo.

TRANSPARENCIA 24: Recomendaciones (II)

- **Informarse sobre las condiciones y políticas de privacidad, antes de aceptar crear un perfil al abrir una cuenta en una red social.** Tómate el tiempo necesario para comprender los términos, la información que encuentres te indicará que información comparten y como protegen tu privacidad frente a terceros.

- **Configurar adecuadamente las opciones de privacidad al crear el perfil**. Si tienes cualquier duda, las principales redes sociales tienen los llamados **centros de seguridad,** donde puedes encontrar información para resolverlas. Es tan fácil como poner en el buscador "centro seguridad" facebook/twitter/Instagram.

- **Revisar periódicamente las opciones de privacidad de nuestro perfil.** Las redes sociales cambian sus parámetros de privacidad o su política de privacidad y no siempre avisan por lo que podemos pensar que tenemos bien configurada las opciones de privacidad y no ser así. **Es una buena práctica revisar cada cierto tiempo las opciones de privacidad de nuestras redes sociales.**

TRANSPARENCIA 25: Recomendaciones (III)

- **Conectarse a páginas seguras para transacciones importantes o informaciones sensibles.** Son aquellas páginas cuya URL empiezan por HTTPS para que la información viaje cifrada por la red y nadie pueda interceptar la información que se intercambia. Todos los bancos utilizan este protocolo pero también las redes sociales y los servicios de mensajería instantánea más conocidos también lo utilizan para proteger la información de sus usuarios.

- **Valorar cuando tener activado servicios como la 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.

- **No publicar excesiva información personal. Y tener presente: "pensar antes de publicar".** No por aparecer esta recomendación la última es la menos importante todo lo contrario, como hemos visto a lo largo de la exposición 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.

TRANSPARENCIA 26: Recomendaciones que se convierten en hábitos

Es importante incidir que si logramos aplicar estas recomendaciones y lo convertimos en hábitos, podremos andar mucho más tranquilos por Internet.

Como hemos visto a lo largo de la exposición nuestra identidad digital nos puede ayudar a abrir puertas o cerrarlas. Observar la importancia de "estar" en Internet, de forma activa, aportando, participando, construyendo red… una identidad digital bien gestionada no sólo repercute en una vida más activa, también es facilitadora de consolidar un entramado social más sólido dentro y fuera de la red.

Además de seguir las pautas de prevención en relación a nuestra privacidad, se puede aportar alguna idea que contribuya a la construcción positiva de la identidad digital del alumnado y por tanto a su reputación online:

- **Buscar apoyo en el Centro Educativo y en sus profesores para que publiquen aquellos trabajos de calidad realizados por el alumnado a lo largo del curso escolar en el blog y/o canales del centro.**

Además de atender las dudas que puedan haber surgido a lo largo de la charla, al finalizar este se abrirá de nuevo un tiempo que permita aclarar todos aquellos interrogantes o dudas que hayan podido permanecer.

TRANSPARENCIA 27: 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 28: 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