

Tema 2: "Ciberseguridad y derechos de autor"

Introducción.....	2
Seguridad en internet.....	3
Cosas que no debes compartir o hacer en internet.....	3
Peligros de internet.....	5
Consejos de seguridad en internet.....	7
Los derechos de autor en internet.....	9
Fuente de los contenidos y otra información.....	12

Introducción.

Esta unidad es una guía para el uso responsable de internet. También será un referente cuando creamos un blog o página web, además del uso correcto de las redes sociales.

Para ello tenemos que conocer por una parte qué no debemos hacer, que derechos y obligaciones tenemos, que están estipulados por ley.

También tenemos que conocer los peligros que existen en la red, y no exponernos a estas situaciones que nos pueden llevar a peligrar nuestra integridad psíquica y económica. También no debemos exponer a otras personas a estas situaciones, por el material que podamos **colgar** sobre ellos.

La precaución, el conocimiento y nuestra intuición nos indicará como movernos por la red de forma segura. No todo es lo que parece, ni todo es cierto, por lo menos para tomarlo en serio.

Aplicando una serie de principios navegaremos seguro por la red.

Seguridad en internet

Internet tiene muchas ventajas para muchas cosas. Desde trabajar sin el uso de papel a través de archivos que quedan registrados digitalmente, la compra de forma sencilla y rápida desde nuestro ordenador para que nos llegue a casa, la comunicación con nuestro amigos y familiares, el ocio a través de muchas plataformas y un largo etcétera.

Por todo lo mencionado en el párrafo anterior es también un lugar donde habrá gente que romperá las normas para sacar algún beneficio, desprestigiar a personas o cualquiera sabe la finalidad. Las red es tan compleja e intervienen tantas instituciones y personas que es muy difícil regular su funcionamiento y normas de una forma clara y efectiva. Con esta idea podemos llegar a la conclusión de que hay que tomar medidas para protegernos. Para esto tenemos que conocer los peligros de la red.

Los bancos, instituciones y empresas en general se toman muy en serio su protección con software y medidas que los protegen.

Las personas debemos hacer lo mismo porque van a intentar engañarnos de una forma u otra. Si conocemos los riesgos es más fácil protegernos. Hay que **desconfiar de los chollos, de los correos desconocidos** y sobre todo **no dar datos personales a cualquiera, aunque parezca que sean fiables**, porque no sabemos por donde viene el engaño y quién es la persona que está detrás, muchas veces con información muy personal y que nos puede confundir.

Tampoco hay que ser un paranoico, pero siempre usar el sentido común, porque internet tiene muchos ventajas y beneficios.

Cosas que no debes compartir o hacer en internet.

Hay muchas cosas que se pueden compartir en internet, ya sea en las redes o información para crear una cuenta de algo. Siempre vamos a tener que compartir algún dato, pero hay que valorar si es necesario y no hacerlo de forma sistemática e irreflexiva.

Tenemos que valorar el compartir la siguiente información:

Correo electrónico y número telefónico.

Estos dos datos son muy importantes, si lo damos nos pueden llenar el correo de **spams** de forma generalizada. Lo del número de teléfono es peor porque nos pueden acosar con llamadas a cualquier hora intentando vendernos cualquier cosa a precios de chollo.

Lo peor de esto es que nos intenten engañar con cualquier estrategia con los datos que sabe de ti. Tu al ver lo que saben de ti, te confías y te engañan.

Dirección y ubicación.

No sabemos que intenciones tiene el que nos pide saber donde vivimos o la ubicación en tiempo real. Puede sonar un poco raro a veces el que nos pidan estos datos. Si permitimos la ubicación, siempre que sea necesario, solo en el momento de usar la aplicación.

Fotos de menores.

¿A qué personas dejarías entrar a tu casa a observar a tus hijos, que vayan pasando y los observen?” Los que observan son miles de ojos mirando a tus hijos y no con los ojos con los que los miras tú... Hay quien relata su vida con pelos y señales; desde una operación, a un cumpleaños, hasta sus avances en los estudios. Uno de las claves es no mostrar en estas redes la información a todo el mundo, sino a la gente de confianza.

Fotos o vídeos comprometidas

Nunca hay que compartir algo que pueda ser morboso para los demás, incluido a los amigos. No puedes saber si compartes algo hasta donde puede llegar. Lo que te parece natural, normal, o de la vida misma para ti no lo es para los demás. Piénsalo antes de compartir.

Luego si compartes fotos de personas sin su permiso es peor, porque puedes estar cometiendo un delito.

Lo peor es que aunque te arrepientes puede ser imposible borrar estas fotos o vídeos de la red. Puede que sea imposible evitar su expansión e incluso borrar sus registros en las bases de datos donde pueda estar. Es la realidad.

DNI, carné de conducir, datos bancarios.

Nuestro DNI, el número o una foto del documento, el carné de conducir, un contrato de trabajo o los datos bancarios son muy personales. Si revelamos alguna de ellos estamos expuestos a una suplantación de identidad y el uso de nuestros datos de manera fraudulenta.

Luego nos buscará la justicia por haber cometido un delito que no hemos hecho.

Conversaciones privadas.

Al igual que las fotos podemos estar comprometiendo a los demás. Revelando cosas de la intimidad de los demás. Esto es un ataque a la intimidad o la revelación de secretos. No todo vale, se puede estar cometiendo un delito.

Peligros de internet.

Algunos de estos peligros vienen de ser demasiado confiados y poco críticos con lo que vemos en la pantalla. Hay analizar lo que vemos. También como hemos leído en el apartado anterior no hay que compartir de forma irreflexiva datos personales.

Robo de identidad.

Hay muchas forma de robar la identidad de otra persona. Una es como hemos visto en el apartado anterior obteniendo los documentos mediante el engaño, proporcionando directamente datos del perjudicado. El otro es conseguir datos mediante malware y meterse en nuestro sistema, buscarlo y robarlo. Un ejemplo son los **Keyloggers**, es un tipo de software que consiguen leer nuestra contraseñas cuando las ponemos.

Filtraciones de datos.

Mediante el software adecuado se filtran en un ordenador o base de datos y la usan para sus fines. Por ejemplo las cuentas de los usuarios de un banco.

Software malicioso y virus.

Se pueden meter en tu ordenador, a través de un correo, una página web, un software que te hayas descargado para robarte información, chantajearte o simplemente fastidiarte tus archivos porque si.

Correos electrónicos de phishing y estafas;

Mediante correo electrónico te solicitan información para engañarte y estafarte. No te fíes de alguien que te pida tus datos personales ni pinches en ningún enlace de correos sospechosos.

Sitios web falsos.

En algunos casos suplantan a sitios oficiales u otros que parecen reales, con una estética similar. Puede que vendan algo a un precio muy bueno. Luego pagas, no consigues nada y ya tienen tus datos. Tendrás que cancelar tu tarjeta si no te han **desplumado** antes.

Estafas románticas.

Son personas con las que contactas ya sea por amistad o buscar pareja, y te engañan. Primero se ganan tu confianza y luego te piden cosas. Puede que incluso con la información que sacan de la víctima intenten chantajearla. De forma que te sacan tu dinero si pueden. Es difícil de demostrar sobre todo si lo haces voluntariamente. Hay personas que se ganan la vida con esto y obtienen denuncias de muchas personas.

Contenido inapropiado.

Hay páginas de diferente ámbito, como el de pornografía o material pirata de todo tipo. Ganan dinero con la propaganda que ponen, de diferente estilo. Sus problemáticas son diferentes, por ejemplo el de los derechos de autor en páginas con material con copyright o un material inadecuado para menores.

Ciberacoso.

El acoso a personas mediante el insulto y el desprestigio. Se esconden detrás de la pantalla para transmitir su odio, muchos de ellos sin dar la cara. Algunos crean cuentas falsas para que no sepan quienes son.

Configuración de privacidad defectuosa.

No se debe dar información personal en abierto, esto es a todo el mundo. Corremos un gran riesgo, sobre todo si estamos en el punto de vista de los demás. Hay que configurar bien nuestros navegadores y redes sociales para prevenir. Aparte de la precaución y sentido común que debemos tener al publicar información personal.

Debemos borrar los cookies y no dejar registradas las contraseñas en ordenadores que no son seguros. Todo esto se consigue con una buena configuración de los programas que usamos.+

<https://www.kaspersky.es/resource-center/preemptive-safety/top-10-preemptive-safety-rules-and-what-not-to-do-online>

Consejos de seguridad en internet

Del apartado anterior, los peligros de la red, nos hace pensar en que debemos tomar una serie de medidas para que no nos perjudique. Así debemos estar atentos y configurar nuestros equipos adecuadamente.

Usar una conexión de internet segura.

Las redes públicas son inseguras y por ello si las usamos no debemos hacer transacciones personales importantes. Si usamos las nuestras debemos poner claves que no sean evidentes y que las claves sean largas. Así no tendremos intrusos. Luego hay software de control de nuestra red.

Por otro lado es seguro usar y configurar redes VPN que son más complicadas de identificar sus contenidos.

Poner contraseñas seguras.

Si ponemos claves cortas, fáciles de descifrar y claves repetidas corremos el riesgo de que averigüen nuestras claves. Esto es peligroso, sobre todo si son cuentas importantes para nosotros.

Activar la autenticación múltiples.

Esto es que además de la clave nos pidan otro dato o que se verifique a través del móvil.

Por ejemplo yo tengo asociado la cuenta de “Google” a mi móvil. Cada vez que me meto en mi cuenta en un ordenador no habitual tengo que confirmar con el móvil.

Sistemas operativos y software actualizados.

Los sistemas operativos que no se actualizan, no se corrigen las brechas de seguridad del sistema y pueden ser vulnerables. Aparte los navegadores y diferente software van evolucionando y es necesaria su actualización para que funcionen correctamente.

Usar usuarios personales en los sistemas operativos.

Si cada vez que accedo a un sistema operativo tengo que meter mi clave propia estaremos en un entorno de confianza y por ello será más seguro porque nadie más puede acceder al software que hay instalado con una configuración concreta. Esto no excluye que tengamos que configurar correctamente nuestro software.

Mirar si las webs son de confianza

Si sabemos que una web o entorno de internet es de confianza es algo positivo. Pero cuando entramos en un sitio nuevo debemos desconfiar en un principio. Sobre todo si debemos usar datos personales y por ejemplo usar nuestra tarjeta bancaria.

Podemos investigar y ver que dicen sobre la página nueva que queremos usar.

Pagar en internet con sistemas seguros como PayPal o tarjetas virtuales.

Hoy existen sistemas de pago seguros o que minimicen nuestras pérdidas. Yo por ejemplo uso una tarjeta virtual donde pongo una cantidad adecuada de dinero para que si me roban sea la mínima cantidad.

Configurar el software adecuadamente.

En los navegadores no debemos guardar nuestras claves, sobre todo si es usado por más de una persona. Todo se puede configurar. Si no sabemos hacerlo en un navegador podemos usar otro navegador que sea más fácil o que te lo permita.

Los navegadores podemos configurarlos para borrar los cookies de forma sistemática cuando acabe nuestra sesión. Esto evitará que nos rastreen. Ya que los cookies registran cuáles son nuestros gustos en internet, de forma que nos pueden colar spams, entre otros.

Todos los navegadores te permiten borrar los cookies de forma manual, pero no de forma automática.

No pinchar en enlaces sospechosos

Cuando nos envían correos sospechosos o páginas webs que no nos dan confianza no pinches en ningún enlace, simplemente deja esa página o borra ese correo.

Haz copias de seguridad

Cuando tienes en tu ordenador cosas que para ti son realmente importantes hay que sacarles copia. Ya sea un pen-drive, la nube, otros disco duro, servidores nas, etc.

Todas las empresas lo hacen o ponen en peligro el trabajo realizado durante un día, semanas, mese e incluso años.

Por ejemplo un programador que haya estado trabajando un día completo para el es muy importante sacarle copia, no solo porque te puedan robar tu trabajo, que no es lo normal, sino que el archivo se puede romper, al igual que lo hacen muchas cosas.

Tener cuidado con lo que te descargas.

A todo el mundo le gusta lo gratis, pero en internet puede ser un peligro. Si no es un sitio de confianza infórmate o no lo hagas. Se te pueden instalar virus o cualquier tipo de malware.

Nunca se sabe hasta que te sucede.

Tener cuidado con qué personas te relacionas en la web

La red es un sitio donde se mueve todo tipo de personas y no sabes quién está detrás.

En un sitio de confianza puedes pensar que no te van a engañar, pero la precaución es algo muy importante que tenemos que tener siempre presente.

Las estafas y engaños están al día, casi todos los días salen nuevas formas de engaño, más sofisticadas y que dan muy bien el pego de fiables. Sólo lo sabe al que le pasa.

Usar en general software de protección.

Existe software gratuito y de pago para proteger nuestros dispositivos electrónicos. El mismo sistema operativo suele tener medios de protección. Por ello tenemos que tenerlos actualizados.

Muchos antivirus hacen que nuestros dispositivos vayan más lentos. Es un precio que hay que pagar.

La mejor prevención es no meternos en sitios que pueden ser peligrosos.

No dejar rastros digitales

Esto es todo lo que se puede ver o no en la red que tu has dejado. Por ejemplo fotos, comentarios, datos personales, etc. Es mejor pasar desapercibido.

<https://www.kaspersky.es/resource-center/preemptive-safety/top-10-preemptive-safety-rules-and-what-not-to-do-online>

Los derechos de autor en internet.

En este apartado se clarifica lo que podemos **colgar** en internet, o más bien, que es **lo que no podemos** o debemos poner en nuestras páginas webs, blogs, redes sociales, etc.

Los derechos de autor en la red son aquellos derechos que protegen el contenido creado por el autor original de la obra, tal y como están recogidos en las leyes de propiedad intelectual de cada país. Reconocen su autoría y sus derechos a la explotación si lo quiere así su creador.

“Todos los días millones de personas comparten contenido propio y ajeno en la red, y todos los días se producen infracciones a los derechos de autor en Internet.”

¿Existen los derechos de autor en la red?

Mucha gente piensa que lo que hay en internet se puede usar libremente. Esto claramente es un error, porque siempre existe alguien que lo ha creado y por esto tiene un autor.

De aquí surge una pregunta:

¿todo lo que tiene derechos de autor debe estar registrado?

Pues no, por el hecho de crear una obra ya tiene derechos de autor. Ahora sí, el hecho de estar registrado te da una seguridad, que de otra forma puede ser difícil de demostrar la autoría.

Si creamos algo y está en un artículo de una página web desde hace por ejemplo 5 años, esta página será la prueba de que lo hemos creado nosotros.

¿Qué tiene derechos de autor?

Todo tipo de información, esto es: imágenes, textos, vídeos, diseños, etc.

El que ha hecho una foto podrá determinar si quiere cederla gratuitamente para su uso, pagar por ella o sencillamente que reconozcan la foto como suya en la red.

Esto es lo mismo con artículos, cuentos, opiniones, vídeos, software, diseños de cualquier tipo. Es muy amplio.

¿Qué son los derechos de imagen?

Una foto no es sólo la imagen, sino también si hay alguna persona reconocible. No puedes usar la imagen de otra persona sin que te haya dado permiso para compartirla. Menos derecho a difundirla de forma masiva.

Cada persona tiene derecho a decidir sobre el uso de su propia imagen. La cosa cambia cuando hablamos de menores. En este caso son sus tutores los que pueden decidir.

Sin embargo unos padres que deciden colgar de forma masiva de sus hijo puede poner en riesgo por ejemplo su intimidad.

¿Qué pasa con los vídeos?

Exactamente lo mismo.

¿En qué ámbitos se aplica este derecho?

Como he dicho anteriormente en todos los ámbitos de internet: páginas webs, blogs, redes sociales, plataformas de “Google”, por ejemplo “Youtube”, etc.

¿Cómo podemos proteger nuestros derechos de autor?

Podemos usar el “Registro de la propiedad intelectual”.

En Andalucía:

<https://www.cultura.gob.es/cultura/areas/propiedadintelectual/mc/rpi/que-es/organizacion/oficinas-provinciales/andalucia.html>

En el ámbito digital:

<https://creativecommons.org/>

Creative commons: es una organización sin ánimo de lucro dedicada a promover el acceso y el intercambio de cultura. Tiene un registro gratuito para establecer que tu obra es de tu propiedad.

¿Cómo saber si una imagen tiene derechos de autor?

En principio todo tiene derechos de autor.

Existen plataformas gratuitas de todo tipo de material, como pueden ser de imágenes, vídeos, audios, diseños 3D, tutoriales, etc. De esta forma nos aseguramos de forma segura. Aunque muchas tienen condiciones.

Algunas personas usan marcas de agua y el símbolo del copyright © para indicarnos que no vas a poder usar la foto libremente.

Algunas webs que ofertan material gratuito son:

Fotos:	https://www.pexels.com/es-es/
Fotos	https://unsplash.com/es/
Música	https://uppbear.io/
Diseños 3D:	https://www.thingiverse.com/

De cualquier forma, aunque sean gratuitas hay que consultar las condiciones de uso, porque están registradas por una persona.

Si no se respetan mis derechos de autor, ¿qué puedo hacer?

Sin ningún tipo de dudas lo primero es ponernos en contacto con la persona o entidad que ha usado mi material e instarles a que deje de usarlo y lo retire de su plataforma.

Muchas plataformas tienen la posibilidad de denunciar el uso indebido de un artículo por ejemplo, indicando las razones de dicha denuncia.

También nos queda la **vía judicial**, que suele salir bastante caro, ya que meterse en **pleitos** es costoso, en **tiempo, dinero y energía**. Todo lo que se pueda resolver con la palabra es más beneficioso, incluso para nuestra **salud**.

Hay que saber que quién pierde el juicio **paga** el juicio.

¿Cuánto tiempo podemos tener la propiedad de nuestra obra?

Depende del país y sus leyes, pero dura de media toda la vida del autor más unos 70 años. Así lo podrán disfrutar sus descendientes.

Luego el beneficio económico no lo es todo. El autor tiene derecho a que se reconozca su autoría, que se respete la integridad de su obra, esto es que no puede ser modificada, o que se le reconozca incluso por un seudónimo. También tiene derecho a que no se le reconozca, por ejemplo su nombre, aunque si sus beneficios.

Otros aspecto que se pueden observar en la protección de datos.

La **piratería en internet** es la práctica de copiar, vender, reproducir o distribuir contenidos o productos sin la autorización de los titulares de sus derechos de autor, derechos de explotación o propietarios de los mismos.

Todos sabemos como funciona. En España se persigue a las páginas webs que permiten el acceso a contenido pirata, pero tiene muchas brechas en la legislación que hace que no funcione bien. Además hay que tener en cuenta la complejidad de la red mundial. Unas páginas desaparecen y otras aparecen. Estas páginas con acceso a contenido ilícito viven de la propaganda.

El acceso “**fácil**” a este material hace pensar a muchas personas que todo es gratis.

El mayor delito verdaderamente penado es que tu vendas la obra de otro. Hasta el momento esto es así, porque hay muchas páginas webs donde se consigues enlaces a todo tipo de material con derechos de autor.

Fuente de los contenidos y otra información.

Protección de datos

<https://protecciondatos-lopd.com/>

<https://protecciondatos-lopd.com/empresas/derechos-autor-internet/#:~:text=autor%20en%20internet%3F-,%C2%BFQu%C3%A9%20son%20los%20derechos%20de%20autor%20en%20internet%3F,propiedad%20intelectual%20de%20cada%20pa%C3%ADs>

<https://es.semrush.com/blog/que-son-derechos-autor-internet/>

Compartir en internet

<https://www.lavanguardia.com/tecnologia/20211006/7767188/7-cosas-debes-compartir-nuncainternet-pmv.html>

Reglas de seguridad en internet

<https://www.kaspersky.es/resource-center/preemptive-safety/top-10-preemptive-safety-rules-andwhat-not-to-do-online>

Redes sociales

<https://www.heraldo.es/noticias/aragon/2019/06/09/cuando-compartir-es-delito-no-todo-vale-enredes-sociales-1319213.html>

Ley de propiedad intelectual. Real decreto:

<https://www.boe.es/buscar/pdf/1996/BOE-A-1996-8930-consolidado.pdf>

Registro de la propiedad intelectual.

<https://www.boe.es/eli/es/rd/2023/07/11/611/dof/spa/pdf>