

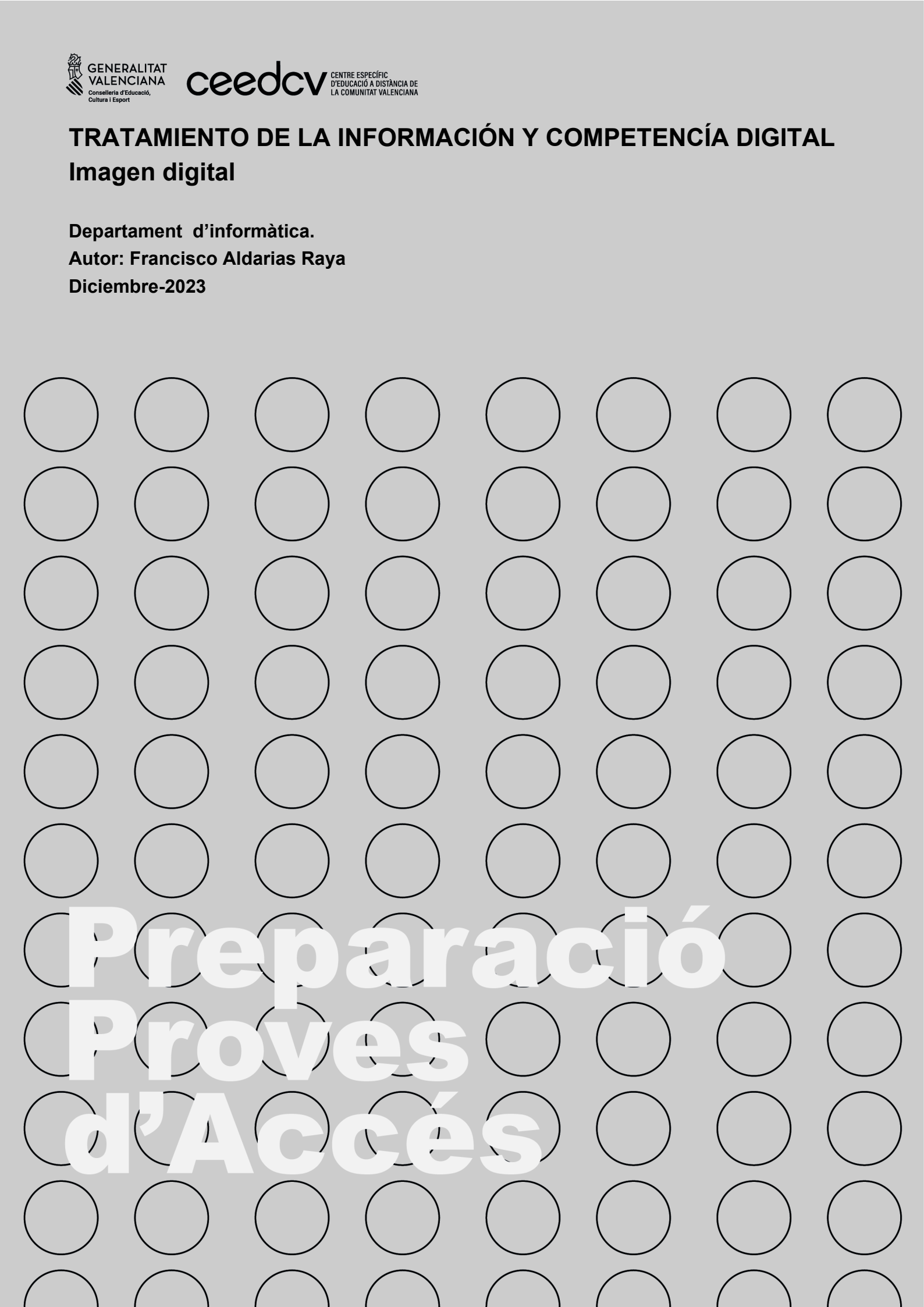
TRATAMIENTO DE LA INFORMACIÓN Y COMPETENCIA DIGITAL

2.3 CRIPTOGRAFIA Y PROTECCIÓN INTELECTUAL

Departament d'informàtica.

Autor: Francisco Aldarias Raya

8-Noviembre-2023



**Preparació
Proves
d'Accés**

ÍNDICE

1 INTRODUCCIÓN	2
2 CRIPTOGRAFÍA	2
3 AUTENTICACIÓN	5
3.1 Autenticación mediante lo que sabes	5
3.2 Autenticación mediante lo que tienes	6
3.3 Autenticación mediante lo que eres.	9
4 PROPIEDAD INTELECTUAL	10
4.1 Aspectos digitales en la legislación sobre la propiedad intelectual	10
4.2 Derechos de autor o Copyright	13
4.3 Obras de dominio público (Public Domain)	14
4.4 Licencia Creative commons	14
5 BIBLIOGRAFÍA	17

1 INTRODUCCIÓN

La criptografía y los mecanismos de autenticación son elementos indispensables para implementar un sistema seguro.

La criptografía es una disciplina muy antigua cuyo objeto es la de ocultar la información a personas no deseadas. La base de la criptografía ha sido el cifrado de textos, aunque se ha desarrollado ampliamente desde la aparición de los primeros ordenadores.

La autenticación (mejor que autentificación) es el acto o proceso para el establecimiento o confirmación de algo (o alguien) como real. La autenticación de un objeto puede significar la confirmación de su procedencia, mientras que la autenticación de una persona a menudo consiste en verificar su identidad.

2 CRIPTOGRAFÍA

El cifrado es el proceso por el que un texto es transformado en otro texto cifrado usando una función matemática (también denominado algoritmo de encriptación) y una clave. El descifrado es el proceso inverso.

Su objetivo se puede resumir en asegurar la:

- **Confidencialidad:** el mensaje no puede ser leído por personas no autorizadas.
- **Integridad:** el mensaje no puede ser alterado sin autorización.
- **Autentificación:** se puede verificar que el mensaje ha sido enviado por una persona, y recibido por otra.
- **No repudio:** significa que después de haber enviado un mensaje, no se puede negar que el mensaje no es tuyo.

El cifrado es necesario entre otras funciones para:

- Proteger la información almacenada en un ordenador
- Proteger la información transmitida desde un ordenador a otro.
- Asegurar la integridad de un fichero.

El cifrado también tiene sus límites, ya que no puede prevenir el borrado de información ni el acceso al documento antes de su cifrado, por lo que un plan de seguridad no se puede basar simplemente en el cifrado de la información.

No todas las formas de cifrado tienen la misma seguridad. Hay cifrados muy simples que son fáciles de romper (se denomina romper un cifrado a la obtención del mensaje descifrado o la clave) y otros muchos más complejos que requieren de técnicas muy complejas para su descifrado.

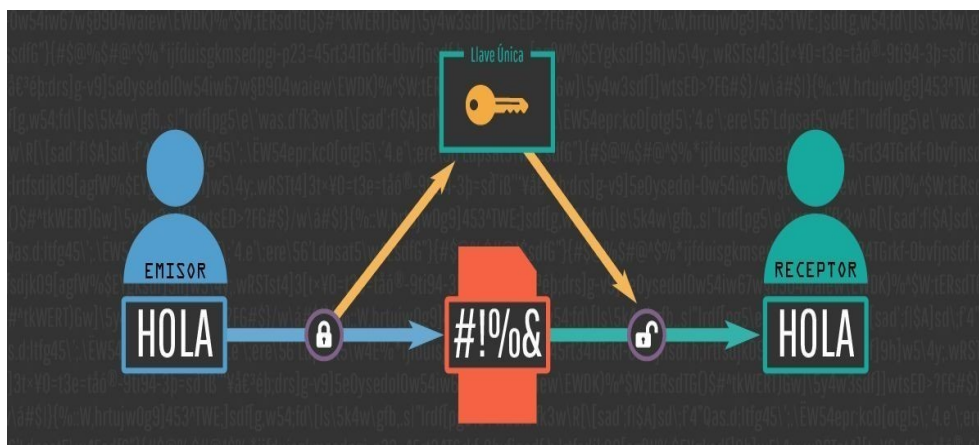


Cifrar tus documentos con libreoffice:

<https://ubunlog.com/como-cifrar-tus-documentos-con-libreoffice/>

No existen mecanismos de cifrado totalmente seguros, ya que con un ordenador lo suficientemente potente (o muchos a la vez) y el tiempo necesario (años o siglos) siempre será posible romper el cifrado. Por lo tanto, el objetivo de la criptografía es obtener mecanismos de cifrado que sean lo suficientemente complejos para evitar su descifrado usando la tecnología actual.

En la figura se puede ver un ejemplo de uso del cifrado para transmitir un mensaje en una red no segura (por ejemplo Internet).



El emisor cifra su mensaje utilizando una clave y un algoritmo de cifrado. Este mensaje cifrado es transmitido por la red al receptor. Este, utilizando la clave y un algoritmo de descifrado puede obtener el mensaje original. De esta forma, aunque un intruso intercepte el mensaje no lo podrá descifrar si no sabe el algoritmo de descifrado y la clave.

Hay dos tipos básicos de algoritmos de cifrado:

1. **Clave simétrica:** utiliza la misma clave para cifrar y descifrar un mensaje. Estos métodos de cifrado se usan principalmente para proteger información que se almacena en un disco duro o para transmisión de datos entre ordenadores.



El algoritmo de encriptación más usado de este tipo es el DES (Data Encryption Standard) que usa una clave de 56-bits. Un mensaje cifrado con este algoritmo es bastante seguro aunque ya puede ser descifrado con máquinas muy potentes en menos de un día, por lo que su uso está restringido a ámbitos civiles. Otros algoritmos comúnmente usados son el RC2, RC4, RC5 e IDEA. La mayoría de estos tienen patente, aunque su uso público está permitido.

Como ejemplo de sistema simétrico está Enigma. Este fue un sistema empleado por Alemania durante la Segunda Guerra Mundial, en el que las claves se distribuían a diario en forma de libros de códigos. Cada día, un operador de radio, receptor o transmisor, consultaba su copia del libro de códigos para encontrar la clave del día. Todo el tráfico enviado por ondas de radio durante aquel día era cifrado y descifrado usando las claves del día.

2. **Clave asimétrica:** que utiliza una clave pública para cifrar el mensaje y una clave privada para descifrarlo. De esta forma cualquiera puede cifrar un mensaje pero solo quien tenga la clave privada puede descifrarlo. Esto sirve para poder enviar un mensaje a un determinado destino sin que otro pueda descifrarlo. El objeto de estos métodos es la de asegurar la integridad y la autenticación del origen de los datos (por ejemplo, usando firmas digitales).



RSA es el algoritmo de encriptación más conocido de clave pública. RSA utiliza una clave pública que es usada para cifrar el mensaje y una clave privada que es usada para descifrar el mensaje.

Estos dos métodos de encriptación funcionan muchas veces conjuntamente. Por ejemplo, el protocolo SSL, que se utiliza como conexión segura en Internet (el que usa el navegador cuando está en modo seguro y en la URL nos sale https), utiliza primero una clave pública para enviar de forma cifrada la clave secreta DES que posteriormente utilizarán en la comunicación. De esta forma la clave DES utilizada sólo la podrá descifrar el destino. Este método en general se denomina OTP (One Time Password) ya que para cada sesión se genera una nueva clave DES.

Cifrar documentos antes de subirlos a la nube:

<https://enfocuenomada.com/cryptomator-encryptar-archivos-nube/>

3 AUTENTICACIÓN

Definimos la Autenticación como la verificación de la identidad del usuario, generalmente cuando entra en el sistema o la red, o accede a una base de datos.

Normalmente para entrar en el sistema informático se utiliza un nombre de usuario y una contraseña. Pero, cada vez más se están utilizando otras técnicas más seguras.

Es posible autenticarse de tres maneras:

- Por lo que uno sabe (una contraseña, permanente o temporal)
- Por lo que uno tiene (una tarjeta inteligente o token usb)
- Por lo que uno es (las huellas digitales)

La utilización de más de un método a la vez aumenta las probabilidades de que la autenticación sea correcta. Pero la decisión de adoptar más de un modo de autenticación por parte de las empresas debe estar en relación al valor de la información a proteger.

3.1 Autenticación mediante lo que sabes

La técnica más usual es la autenticación utilizando contraseñas ya sean permanentes o temporales.

Este método será mejor o peor dependiendo de las características de la contraseña. En la medida que la contraseña sea más grande y compleja para ser adivinada, más difícil será burlar esta técnica.

Además, la contraseña debe ser confidencial. No puede ser conocida por nadie más que el usuario.

Poner contraseña a un archivo pdf

<https://www.xataka.com/basics/como-poner-contrasena-a-archivo-pdf>

Para evitar riesgos derivados de las contraseñas, es conveniente seguir estos consejos:

- No compartas tus contraseñas con nadie. Si lo haces, dejará de ser secreta y estarás dando acceso a otras personas a tu privacidad.
- Asegúrate de que son robustas. Están formadas por al menos 8 caracteres: con mayúsculas, minúsculas, números y caracteres especiales. Utiliza alguna regla sencilla para recordarlas.
- No utilices la misma contraseña en diferentes servicios. Siempre claves diferentes para servicios diferentes. O al menos no uses la misma de tu correo electrónico en otro sitio.
- Cuidado con las preguntas de seguridad. Si las utilizas, que nadie más sepa las respuestas.
- Utiliza gestores de contraseñas si te cuesta memorizar las contraseñas o utilizas muchas.
- Utiliza la autenticación de dos pasos siempre que sea posible y el servicio lo merezca.

EJEMPLOS DE CONTRASEÑAS QUE **NO** DEBEMOS UTILIZAR



3.2 Autenticación mediante lo que tienes

Desde un punto de vista formal una tarjeta inteligente (o smartcard) es un dispositivo de seguridad del tamaño de una tarjeta de crédito, resistente a la adulteración, que ofrece funciones para un almacenamiento seguro de información y también para su procesamiento.

En la práctica, las tarjetas inteligentes pueden ser de diversos tipos. Pueden poseer un chip inteligente que es el que las diferencia de las antiguas tarjetas de crédito, que sólo incorporaban una banda magnética donde iba almacenada cierta información del propietario de la tarjeta. Otras se basan en tecnologías inalámbricas como el NFC y RFID (como las tarjetas del metro y autobús). Y otras en generadores de contraseñas que se sincronizan con servidores de autenticación.



Cuando el usuario poseedor de una smartcard desea autenticarse necesita introducir la tarjeta en un hardware lector; los dos dispositivos se identifican entre sí. Tras identificarse las dos partes, se lee la identificación personal de la tarjeta, y el usuario teclea su PIN. Si la respuesta es correcta el usuario obtiene acceso al recurso pretendido.

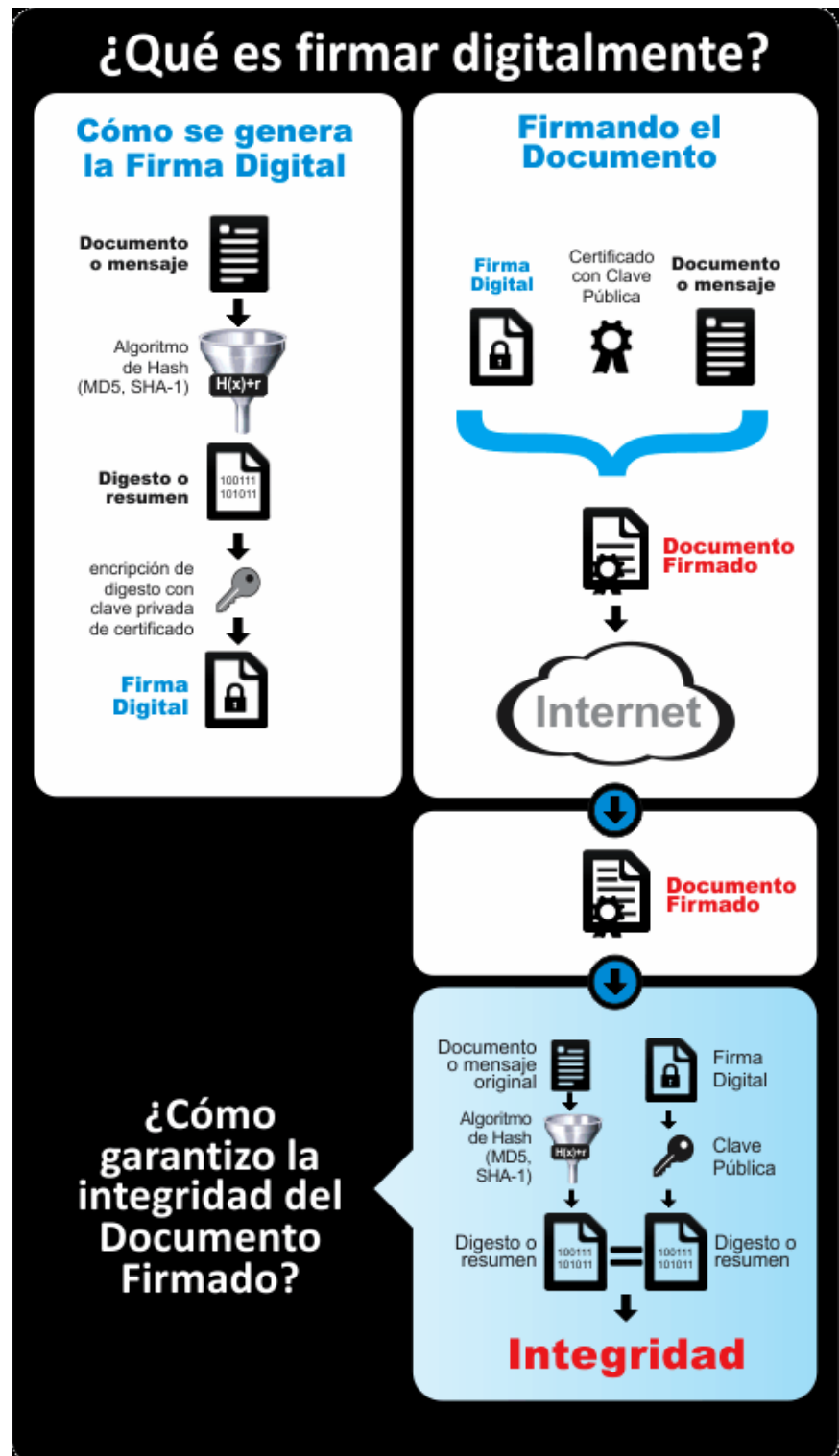
3.2.1 La firma digital

El objetivo de la firma digital es la de certificar los contenidos de un mensaje. En este caso el mensaje original no es necesario que vaya cifrado, sino que contiene (o va en un fichero aparte) un código que identifica el mensaje y que va cifrado con una clave privada. A este proceso de certificar el mensaje con una firma digital se denomina firmado. Esta firma digital nos sirve para asegurar la integridad, autenticación y el no repudio. En este caso, el mensaje original no es necesario que vaya cifrado, aunque si lo va también, garantizamos la confidencialidad del mensaje. El algoritmo de firma digital más usado actualmente es el **MD5**.

La firma digital funciona mediante complejas operaciones matemáticas que relacionan el documento firmado con información propia del firmante. Estas operaciones permiten que terceras personas puedan **reconocer la identidad del firmante** y asegurarse de que los contenidos no han sido modificados.

El firmante genera o aplica un algoritmo matemático llamado "función hash", el cual se cifra con la clave privada del firmante. El resultado es la firma digital,

que se enviará adjunta al mensaje original. De esta manera el firmante adjuntará al documento una marca que es única para dicho documento y que sólo él es capaz de producir.



Para realizar la verificación del mensaje, el receptor generará la huella digital del mensaje recibido, luego descifrará la firma digital del mensaje utilizando la clave pública del firmante y obtendrá de esa forma la huella digital del mensaje original; si ambas huellas digitales coinciden, significa que no hubo alteración y que el firmante es quien dice.

Firma digital avanzada:

La firma digital avanzada además incluye una marca de tiempo e información de validación que permiten determinar una fecha y hora en el que la firma digital existía y el certificado era válido. La marca de tiempo es generada por una autoridad de estampado de tiempo y sirve para determinar el momento en el cual la firma digital y el respectivo certificado fueron validados.

3.3 Autenticación mediante lo que eres.

Parece que en un futuro no muy lejano estos serán los sistemas que se van a imponer en la mayoría de situaciones en las que se haga necesario autenticar un usuario: son más amigables para el usuario (no va a necesitar recordar passwords o números de identificación complejos, y, como se suele decir, el usuario puede olvidar una tarjeta de identificación en casa, pero nunca se olvidará de su mano o su ojo) y son mucho más difíciles de falsificar que una simple contraseña o una tarjeta magnética; las principales razones por la que no se han impuesto ya en nuestros días es su elevado precio, fuera del alcance de muchas organizaciones, y su dificultad de mantenimiento.

Estos sistemas son los denominados biométricos, basados en características físicas del usuario:

- **Verificación de voz.** En estos sistemas no se intenta reconocer lo que el usuario dice, sino identificar una serie de sonidos y sus características para decidir si el usuario es quien dice.
- **Verificación de escritura.** Aunque la escritura (generalmente la firma) no es una característica estrictamente biométrica, se suele agrupar dentro de esta categoría. El objetivo es autenticar al autor de un escrito basándose en ciertos rasgos tanto de la firma como de su rúbrica.
- **Verificación de huellas.** Es un patrón bastante bueno para determinar la identidad de forma inequívoca, ya que está aceptado que dos dedos nunca poseen huellas similares, ni siquiera entre gemelos o entre dedos de la misma persona.
- **Verificación de patrones oculares.** Los modelos de autenticación biométrica basados en patrones oculares se dividen en dos tecnologías diferentes: o bien analizan patrones retinales, o bien analizan el iris. Estos métodos se suelen considerar los más efectivos: la probabilidad de coincidencia es casi 0, y además una vez muerto el individuo los tejidos oculares degeneran rápidamente, lo que dificulta la falsa aceptación de atacantes que puedan robar este órgano de un cadáver.

La principal desventaja de los métodos basados en el análisis de patrones oculares es su escasa aceptación por la incomodidad de tener que mirar a través de un binocular (o monocular), por la desconfianza del usuario ante el hecho de que un haz de rayos analice su ojo, y porque un examen de este órgano puede revelar enfermedades o características médicas que a muchas personas les puede interesar mantener en secreto, como el consumo de alcohol o de ciertas drogas.

- **Retina.** La forma de los vasos sanguíneos de la retina humana es un elemento característico de cada individuo, por lo que numerosos estudios en el campo de la autenticación de usuarios se basan en el reconocimiento de esta característica.

- Iris. El iris humano (el anillo que rodea la pupila, que a simple vista diferencia el color de ojos de cada persona) es una estructura única por individuo inalterable durante toda la vida de la persona. La probabilidad de una falsa aceptación es la menor de todos los modelos biométricos.
- Verificación de la geometría de la mano. Son los más rápidos dentro de los métodos biométricos con una probabilidad de error aceptable en la mayoría de ocasiones. Quizás uno de los elementos más importantes del reconocimiento mediante analizadores de geometría de la mano es que éstos son capaces de aprender: a la vez que autentican a un usuario, actualizan su base de datos con los cambios que se puedan producir en la muestra (un pequeño crecimiento, adelgazamiento, el proceso de cicatrizado de una herida...); de esta forma son capaces de identificar correctamente a un usuario cuya muestra se tomó hace años, pero que ha ido accediendo al sistema con regularidad.

Interesante. CURSO GRATUITO SOBRE CRIPTOGRAFÍA : Khan Academy.
<https://es.khanacademy.org/computing/computer-science/cryptography>

4 PROPIEDAD INTELECTUAL

¿Qué es la propiedad intelectual?

Es el conjunto de derechos que corresponden a los autores y a otros titulares (artistas, productores, organismos de radiodifusión...) respecto de las obras y prestaciones fruto de su creación.

¿Quien es el autor de una obra con protección de la propiedad intelectual?

Se considera autor a la persona natural que crea alguna obra literaria, artística o científica. Son objeto de propiedad intelectual todas las creaciones originales literarias, artísticas o científicas expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro. La propiedad intelectual de una obra literaria, artística o científica corresponde al autor por el solo hecho de su creación.

La condición de autor tiene un carácter irrenunciable; no puede transmitirse “inter vivos” ni “mortis causa”, no se extingue con el transcurso del tiempo así como tampoco entra en el dominio público ni es susceptible de prescripción.

¿Como puede protegerse la propiedad intelectual?

La legislación protege la Propiedad Intelectual, por ejemplo, mediante las patentes, los derechos de autor y las marcas, que permiten obtener reconocimiento o ganancias por las invenciones o creaciones.

Dentro de la normativa de la propiedad intelectual existe una serie de mecanismos de protección de los derechos de propiedad intelectual, existiendo la posibilidad de acudir a acciones administrativas, civiles o penales.

Para proteger la Propiedad Intelectual existe la OMPI (Organización Mundial de la Propiedad Intelectual) y, a nivel nacional, el Registro General de la Propiedad Intelectual.

4.1 Aspectos digitales en la legislación sobre la propiedad intelectual

La irrupción de las nuevas tecnologías en la sociedad de la información y del conocimiento ha revolucionado los modos y maneras de crear y difundir contenidos y de acceder y compartir los

misimos. Las normas reguladoras de la propiedad intelectual aplicables a entornos analógicos se han visto obligadas a adaptarse a los nuevos entornos digitales.

La legislación de la propiedad intelectual contempla expresamente algunos **aspectos digitales**.

Los más destacados podrían ser:

- la digitalización como acto de reproducción,
- la compensación por copia privada a través del llamado “canon digital”,
- la puesta a disposición del público de contenidos a través de Internet o intranets como acto de comunicación pública, y
- las medidas tecnológicas y la DRM (gestión digital de derechos “digital rights management”)

4.1.1 La digitalización como acto de reproducción

Digitalizar es convertir contenidos en series de bits y almacenarlos en soportes electrónicos tangibles (CDR, DVD, USB, etc.) o intangibles (memoria del ordenador). Ejemplo de digitalización es el escaneo de documentos impresos.

La digitalización da lugar a una nueva copia del contenido y por tanto es un acto de reproducción en el sentido de la Ley de Propiedad Intelectual, lo cual a su vez significa que es un acto de explotación que corresponde en exclusiva a su titular y no puede realizarse por otras personas salvo autorización legal o expresa del mismo.

Existen ciertas excepciones a esta consideración:

- A favor de las bibliotecas, museos, archivos... para realizar reproducciones (sean analógicas o digitales) sin ánimo de lucro y con fines de investigación o conservación.
- Se permite también la copia para uso privado, aunque requiere que el acceso a la obra sea legal y la copia no se utilice de forma colectiva ni lucrativa.

4.1.2 Canon digital

Técnicamente se trata de una compensación por la copia privada que la ley permite hacer para uso personal. Se considera que dicha copia conlleva una pérdida económica para el titular de los derechos de autor. En contrapartida se establece un gravamen sobre los equipos, aparatos y soportes susceptibles de ser usados para realizar reproducciones. La compensación existe en nuestra legislación desde el año 1987. La novedad consiste en su extensión al ámbito digital.

La remisión de contenidos protegidos a través de correo electrónico a una pluralidad de personas puede considerarse “puesta a disposición del público” en el sentido legal, y requerir autorización de su titular. Si el envío es individual y la copia digital se ha realizado de forma lícita puede considerarse una extensión o entrega de la reproducción, que no constituye un nuevo acto de explotación, y por tanto ser también lícita.

4.1.3 Uso de contenidos libremente en internet

No siempre podemos alojar contenidos libremente en internet. Sólo si quien realiza la carga es el titular de los derechos o cuenta con autorización para ello. En otro caso hay que respetar los derechos de autor.

La carga de contenidos protegidos en un servidor conectado a una red de difusión abierta constituye un acto de explotación de derechos de propiedad intelectual; para ser exactos, es un supuesto de “puesta a disposición interactiva” contemplado por la ley como acto de comunicación pública (uno de los cuatro derechos básicos de explotación que pertenecen con exclusividad a su titular).

La mera navegación y ojeo de contenidos en Internet no suele implicar una explotación de derechos de propiedad intelectual. Sin embargo, un uso posterior de dichos contenidos, aunque estén libremente accesibles, deberá respetar lo que el titular de los derechos establezca.

Si el contenido aparece protegido por el símbolo del copyright © acompañado de la expresión “todos los derechos reservados”, no se puede dar a tal contenido más uso que el permitido por ley.

Sin embargo, cada vez con más frecuencia se pueden encontrar contenidos con licencias de uso más permisivas, llamadas licencias libres o abiertas. En esos casos se debe respetar la voluntad del titular en cuanto a usos consentidos y condiciones establecidas. Ejemplos de ello son las licencias Creative Commons, que veremos a continuación.

Uso de contenidos en Aulas Virtuales

Un Aula virtual no suele ser una red abierta y pública sino una red o intranet de acceso restringido.

No obstante, la carga de contenidos en la misma mantiene la calificación de puesta a disposición interactiva y por tanto “comunicación pública” a los efectos de la Ley. En consecuencia, y sin perjuicio de las excepciones legales, requiere autorización del titular.

Los recursos docentes que los profesores ponen a disposición de los alumnos en su aula virtual están sujetos a derechos de autor como cualquier otro contenido perteneciente a la propiedad intelectual.

4.1.4 Protección de medidas tecnológicas a los derechos de propiedad intelectual

Las normas de protección de medidas tecnológicas pretenden otorgar al titular el control de los derechos de explotación sobre su obra y se extienden tanto a los dispositivos técnicos como a los mecanismos de gestión de derechos. La ley establece acciones contra los actos de supresión o elusión de unos u otros.

DRM (Digital Right Management) son las siglas que designan a los sistemas de gestión digital del derecho de autor. Un archivo protegido con la tecnología DRM permite al distribuidor controlar, que, quién, cuándo y cómo, va a ver ese archivo en base a la licencia de distribución que haya diseñado el autor o distribuidor de la obra. Esto ha ocasionado bastante controversia.

4.1.5 Licencias sobre la propiedad intelectual

La OMPI (Organización Mundial de la Propiedad Intelectual) explica que la propiedad intelectual se refiere a las creaciones de la mente: invenciones, obras literarias y artísticas, etc. Así como a los símbolos, logotipos, nombres e imágenes utilizados en el comercio.

Todos esos textos, fotografías, dibujos, música, vídeos... tienen dueños. A éstos se les conceden derechos y la Ley de Propiedad Intelectual los regula. Son de dos tipos:

- Los morales, con los que se les reconoce la autoría de la obra, se les otorga el poder negarse a que se realicen modificaciones en ella y en cualquier obra derivada.
- Los patrimoniales, con los que se estipula las ganancias a percibir por la obra. Éstos no suelen pertenecer al autor sino a los propietarios: productores, editores, sellos discográficos...

Estas creaciones necesitan además un soporte o medio para ser transmitidas, y en estos tiempos Internet resulta ser uno de los métodos de difusión más habituales. Y todo lo que está en Internet es para muchos “free” en el doble sentido del término: gratis y libre. Pero no es así.

Los autores de una obra pueden decidir en qué condiciones permiten a los demás usarla y esta concesión puede ser muy variada:

1. Vigencia de los derechos de autor.
2. Dominio público.
3. Creative Commons.

4.2 Derechos de autor o Copyright

Los autores pueden reservarse para ellos todos los derechos y en este caso se dice que la obra está sometida a derechos de autor y está protegida, tiene copyright. Por lo que si alguien no respeta estos derechos estará cometiendo plagio.

Si se quiere hacer uso de una obra con derecho de autor para una nueva creación se debe pedir permiso para ello. Hay pequeñas excepciones y algunas están en la enseñanza.

La legislación sobre derechos de autor (también conocida con el término anglosajón Copyright, aunque no son exactamente lo mismo) es relativamente moderna en Occidente, y no se inició legalmente hasta el siglo XVIII.

A nivel gráfico se reconoce al Copyright © por el uso de un símbolo regulado según el artículo 146 del Real Decreto Legislativo 1/1996, que es la Ley de Propiedad Intelectual.

Es importante señalar que para generar los derechos de autor no se exige ninguna inscripción en un registro, sino que nacen con la creación de la obra en si. Se debe recordar también que aunque existen armonizaciones o convenios internacionales, las leyes de cada país pueden diferir en algunos puntos en especial respecto al plazo de protección tras el cual los derechos de autor expiran.

El Copyright también dispone de una variante relacionada: el Copyleft es un tipo de derecho de autor que permite la alteración de una obra y la libre distribución de sus copias, pero que también garantiza los mismos derechos libres para esas versiones modificadas. Se representa con un símbolo de Copyright invertido.

4.3 Obras de dominio público (Public Domain)

Se trata de la situación en la que quedan las creaciones cuando termina el periodo de protección que les otorgan los derechos de autor. A partir de ese momento pueden ser utilizadas sin permiso y sin generar contraprestación para el creador original o sus herederos.

Se puede por tanto copiarlas, distribuirlas, adaptarlas, etc... Pero sin olvidar que al hacerlo se pueden crear nuevas imágenes o una obra derivada que sí estará protegida por los derechos de autor. Se representa con un símbolo de Copyright tachado.

Por ejemplo habrás visto en muchas ocasiones reproducciones modificadas de cuadros famosos. El cuadro original puede estar en dominio público, pero la nueva obra creada no. Es decir, la obra nueva ahora posee una propiedad intelectual propia.

Tampoco el hecho de que se fotografíe un monumento histórico o paisaje convierte la imagen resultante en dominio público.

4.4 Licencia Creative commons

Estas licencias se publicaron en 2002 por Creative Commons, una corporación sin ánimo de lucro fundada en 2001 en los Estados Unidos.

A diferencia de los derechos de autor, las licencias Creative Commons no se generan por sí mismas, sino que necesitan la voluntad expresa del autor para su nacimiento.

Su finalidad es que autores y creadores puedan compartir voluntariamente su trabajo con herramientas libres, pero manteniendo ciertos derechos en función de la licencia elegida.

Estas licencias “**Creative Commons**” se construyen basándose en cuatro condiciones:

- **Reconocimiento (BY)**

Puedes compartir y adaptar la imagen u obra con cualquier finalidad, incluso comercial, con la única condición de reconocer la autoría original (normalmente con un enlace al original).

- **No Comercial (NC)**

Se permite cualquier explotación de la obra siempre que no se haga con uso comercial.

- **Sin obras derivadas (ND)**

No se permite hacer transformaciones para hacer otra nueva.

- **Compartir (SA)**

Se permite crear obras derivadas que mantengan la misma licencia si se divulgan.

Combinándolas generan los siete tipos de licencias CC que podemos encontrar en la actualidad y que permiten diferentes usos y se reconocen por estos símbolos:

1. Dominio público (CC0)

Esta es la opción más abierta. Es consecuencia en realidad de la ausencia de las cuatro condiciones, de forma que el creador ha renunciado por completo a sus derechos de autor equiparando la situación legal a la del dominio público.



Banco de imágenes: <https://pixabay.com/es/>

Fotos, ilustraciones, vectores y vídeos libres de derechos autor bajo la licencia Creative Commons CC0 es lo que ofrece este site. El material está organizado por categorías: animales, deportes, educación, música, ciencia...y se puede acceder a él con sólo registrarse. Es uno de los servicios de bancos de imágenes gratis más completo. El banco de imágenes tiene más de 1 millón de imágenes y videos compartidos.

2. Reconocimiento (BY)

Puedes compartir y adaptar la imagen u obra con cualquier finalidad, incluso comercial, con la única condición de reconocer la autoría original (normalmente con un enlace al original).

3. Reconocimiento – Compartir Igual (BY-SA)

Añade la condición de que si remezclas, editas, transformas o creas algo nuevo a partir de ese material fotográfico, deberás difundir el resultado con la misma licencia que tenía el original.

4. Reconocimiento – No Comercial (BY-NC)

En este caso además no puedes usar esa imagen para una finalidad comercial o lucrativa.

5. Reconocimiento – Sin Obra Derivada (BY-ND)

No se permite un uso comercial de la imagen original ni la generación de obras derivadas de la misma

6. Reconocimiento – No Comercial – Compartir Igual (BY-NC-SA)

No está autorizado el uso comercial de la obra original ni de las posibles derivadas, que además deben compartirse con la misma licencia y derechos de autor que la original.

7. Reconocimiento – No Comercial – Sin Obra Derivada (BY-NC-ND)

Se trata de la más restrictiva de todas las licencias de las imágenes en Internet, puesto que no permite obras derivadas ni el uso comercial de las mismas.

TIPOS DE LICENCIAS CREATIVE COMMONS (CC)	
Reconocimiento (BY)  Permite cualquier explotación de la obra, incluyendo una finalidad comercial, así como la creación y distribución de obras derivadas sin ninguna restricción.	Reconocimiento - NoComercial (BY-NC)  Permite la generación de obras derivadas sin uso comercial de la obra original.
Reconocimiento - NoComercial - CompartirIgual (BY-NC-SA)  No se permite uso comercial de la obra original ni de las posibles obras derivadas, cuya distribución debe hacerse con una licencia igual a la que regula la obra original.	Reconocimiento - NoComercial - SinObraDerivada (BY-NC-ND)  No se permite un uso comercial de la obra original ni la generación de obras derivadas.
Reconocimiento - CompartirIgual (BY-SA)  Se permite el uso comercial de la obra y de las posibles obras derivadas, cuya distribución debe hacerse con una licencia igual a la que regula la obra original.	Reconocimiento - SinObraDerivada (BY-ND)  Se permite el uso comercial de la obra pero no la generación de obras derivadas.

Fuente: Proyecto CECARM

¿Qué fotos pueden utilizarse libremente en un blog o sitio web según sus derechos de autor o licencia Creative Commons?

- Si no quieres tener que preocuparte de si vas a hacer un uso comercial o vas a transformar la imagen original, entonces debes limitarte a buscar para tu blog o página web contenido visual y obras en dominio público o con CC0 ó CC (by).

Recuerda, eso sí, siempre reconocer la fuente y la autoría en este segundo caso “CC (by)” en algún lugar de ese artículo de tu blog o sitio web (en el que se publicara la foto).

- Si tienes claro que no necesitas retocar la creación original y/o el uso no va a ser comercial, entonces puedes ampliar la búsqueda entre el resto de licencias Creative Commons “CC” y cumplir sus requisitos al publicar la imagen en tu blog o página web.
- Finalmente, si estás dispuesto a pagar al autor o comercializador por el uso de su obra puedes acudir a los sitios web que venden imágenes y por el precio marcado adquirir el derecho de uso de la fotografía en las condiciones que allí se marquen.

¿Qué pasa con los derechos de autor de una imagen al compartirla en redes sociales?

Si en vez de incluir la imagen en una página web o blog propios vamos a compartirla en una red social, la situación legal no se modifica respecto a lo explicado en el apartado anterior sobre los derechos de propiedad intelectual de las imágenes en Internet.

En las redes sociales funcionan las mismas condiciones legales sobre los derechos de autor de las imágenes que en cualquier otro sitio de Internet, además de las propias normas de uso de cada una de esas plataformas sociales.

Esto significa que en caso de vulneración de la propiedad intelectual de esas imágenes o de los derechos de autor de las fotografías en redes sociales además de la posible denuncia del autor,

podríamos encontrarnos con sanciones que vayan desde la retirada de la publicación o mensaje hasta la expulsión del usuario de esa plataforma social.

¿Y si la imagen la encontramos en la web de un organismo público como un ayuntamiento o gobierno local?

Pues, nuevamente, tampoco se modifica la situación legal. Como ya he indicado, no es el soporte el que marca la situación legal de la obra fotográfica.

Por tanto si en la web del ayuntamiento encontramos una imagen de nuestro interés, deberemos averiguar la situación legal de esa foto, sin suponer que por el mero hecho de estar colgada en una web municipal ya es de dominio público.

5 BIBLIOGRAFÍA

- <https://www.aepd.es/>
- <http://www.ceice.gva.es/es/web/deposito-legal-propiedad-intelectual/oficina-de-reg.-de-lapropiedad>
- [https://www.ecured.cu/Gesti%C3%B3n_de_Derechos_Digitales_\(DRM\)](https://www.ecured.cu/Gesti%C3%B3n_de_Derechos_Digitales_(DRM))
- <https://www.xataka.com/legislacion-y-derechos/preguntas-y-respuestas-sobre-el-nuevocanon-digital-quien-tendra-que-pagarlo-cuanto-y-por-que>
- <https://es.khanacademy.org/computing/computer-science/cryptography>
- <https://tecnologia-informatica.com/que-es-la-criptografia/>
- <https://www.evidian.com/pdf/wp-strongauth-es.pdf>
- <https://creativecommons.org/>
- <http://www.firma-digital.cr/como%20funciona/>
- <https://www.xataka.com/seguridad/autenticacion-en-dos-pasos-que-es-como-funciona-y-por-que-deberias-activarla>
- <https://nuoplanet.com/blog/que-es-rfid/>
- <http://www.rtve.es/noticias/20121023/como-descifran-hackers-seguridad-tarjetastransporte-publico/571371.shtml>
- <https://www.redeszone.net/2019/02/16/comprobar-contrasenas-no-filtradas-keepass/>