

Tratamiento de la Información y Competencia Digital (TICD)

Acceso Ciclos Formativos de Grado Superior (ACFGS)

Tema 2. Seguridad y ética informática

Tema 2. Parte 3. Criptografía y Protección intelectual.

Resumen

Paco Aldarias.8/11/2023



1. INTRODUCCIÓN

Elementos indispensables para implementar un sistema seguro.

CRIPTOGRAFÍA

- Disciplina muy antigua
- Objetivo = **ocultar la información** a personas no deseadas.
- Base = cifrado de textos, aunque se ha desarrollado ampliamente desde la aparición de los primeros ordenadores.

AUTENTICACIÓN

- Proceso para el establecimiento o confirmación de algo (o alguien) como real.
- La autenticación de un objeto = **confirmación de su procedencia**
- La autenticación de una persona = verificar su identidad.

2. CRIPTOGRAFÍA

Ejemplo de uso del cifrado para transmitir un mensaje en una red no segura (ej. Internet).

1. El emisor cifra su mensaje utilizando una clave y un algoritmo de cifrado.
2. Este mensaje cifrado es transmitido por la red al receptor.
3. Utilizando la clave y un algoritmo de descifrado puede obtener el mensaje original.

Si un intruso intercepta el mensaje no lo podrá descifrar si no sabe el algoritmo de descifrado y la clave.

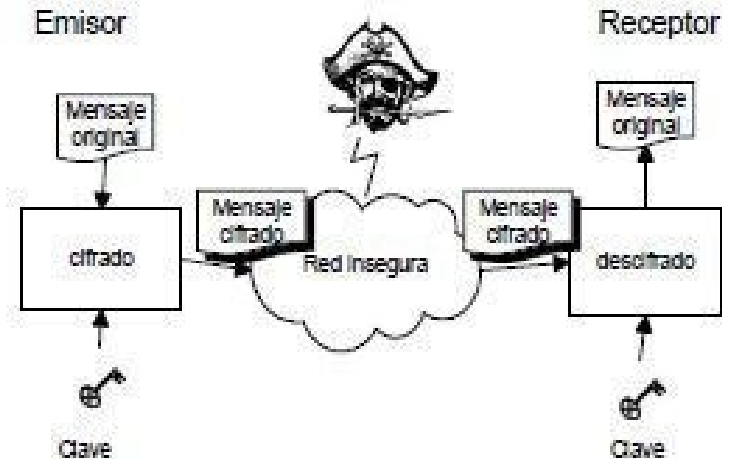


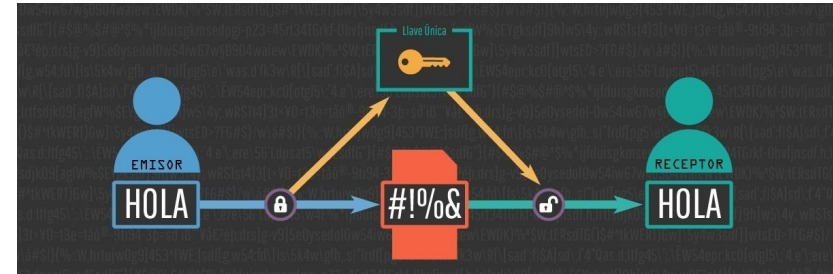
Figura 3: Cifrado y descifrado de un mensaje

2. CRIPTOGRAFÍA

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

OBJETIVOS

- **Confidencialidad:** el mensaje no puede ser leído por personas no autorizadas.
- **Integridad:** el mensaje no puede ser alterado sin autorización.
- **Autenticación:** 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



2. CRIPTOGRAFÍA

El cifrado es necesario entre otras funciones para:

- Proteger la información almacenada en un ordenador
- Proteger la información transmitida desde un ordenador a otro.

Artículos sobre cifrado:

Cifrado del disco usando el sistema operativo. [Link](#)

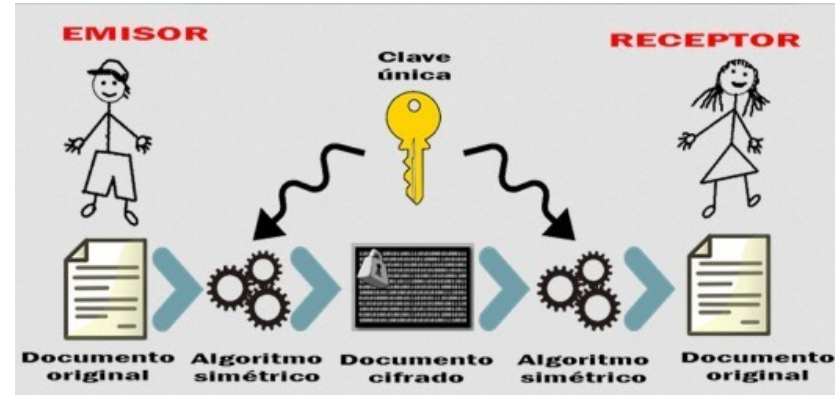
Cifrado de documentos con libre office. [Link](#)

Cifrar antes de subir a la nube mediante app: [Link](#)

2. CRIPTOGRAFÍA

Tipos de algoritmos de cifrado

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

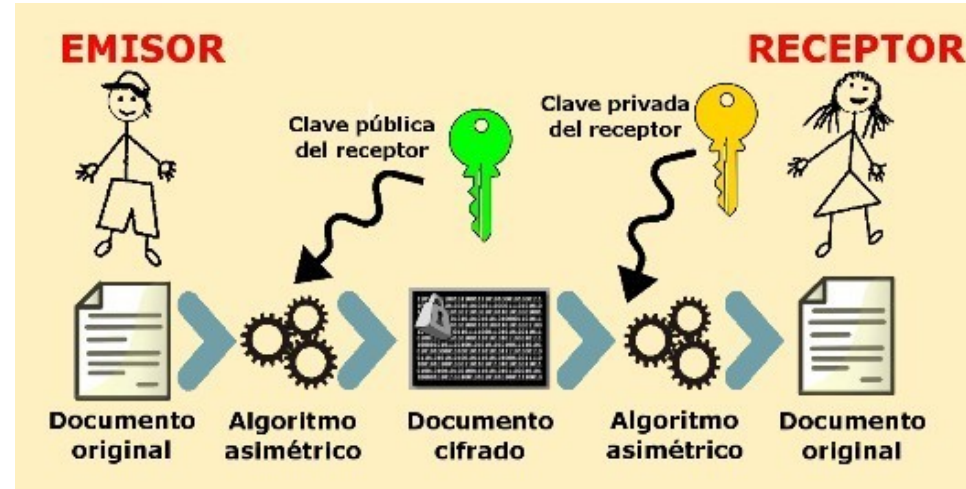


Como ejemplo de sistema simétrico está [Enigma](#). Este fue un sistema empleado por [Alemania](#) durante la [Segunda Guerra Mundial](#), en el que las claves se distribuían a diario en forma de [libros de códigos](#). Cada día, un operador de [radio](#), receptor o transmisor, consultaba su copia del 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. CRIPTOGRAFÍA

Tipos de algoritmos de cifrado

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).



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.

3. AUTENTICACIÓ

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.

- Por lo que uno sabe (ej. una contraseña)
- Por lo que uno tiene (ej. una tarjeta magnética)
- Por lo que uno es (ej. 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. AUTENTICACIÓN

3.1. Mecanismos de autenticación por lo que sabes

Autenticación por lo que sabes →

Contraseñas.

- Es la técnica más usual.
- Mayor complejidad → mayor dificultad.
- Debe ser confidencial.

EJEMPLOS DE CONTRASEÑAS QUE **NO** DEBEMOS UTILIZAR



CONSEJOS

- **No compartas** tus contraseñas con nadie.
- Asegúrate de que son **robustas** → formadas por al menos 8 caracteres (mayúsculas, minúsculas, números y caracteres especiales).
- Utiliza alguna **regla sencilla** para recordarlas.
- **No utilices la misma contraseña** en diferentes servicios.
- Cuidado con las **preguntas** de seguridad (que nadie 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.

3. AUTENTICACIÓN

3.2. Mecanismos de autenticación

Autenticación por lo que tienes.

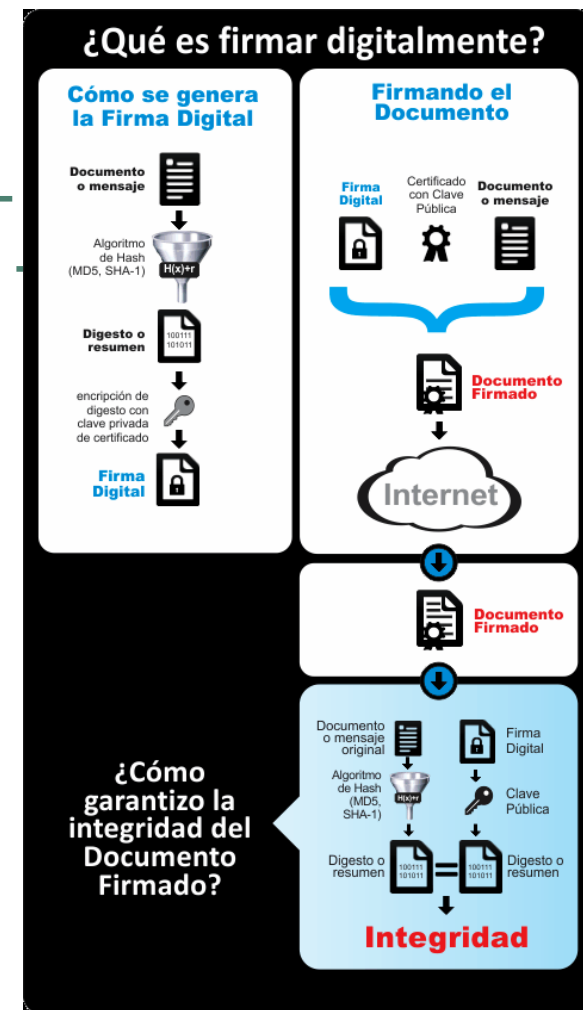
- **Tarjeta inteligente** (o smartcard) resistente a la adulteración, que ofrece funciones para un almacenamiento seguro de información y también para su procesamiento.
- Actuales = chip inteligente
- Antiguas = banda magnética.
- Lector + PIN = Acceso.



3. AUTENTICACIÓN

3.2.1. Firma con Certificado 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.



3. AUTENTICACIÓN

3.3. Mecanismos de autenticación

Autenticación por lo que eres → **sistemas biométricos.**

- Sistemas a usar próximamente para la identificación de usuarios.
- Más amigables (no passwords o tarjeta de identificación).
- Son mucho más difíciles de falsificar.
- Precio elevado.
- Dificultad de mantenimiento.
- Basados en características físicas del usuario:
 - Voz: identificación de sonidos y sus características.
 - Escritura: Característica no estrictamente biométrica. Autenticar al autor de un escrito basándose en ciertos rasgos tanto de la firma como de su rúbrica.
 - Huellas: dos dedos nunca poseen huellas similares (ni gemelos ni dedos de la misma persona).



1. CRIPTOGRAFÍA Y AUTENTICACIÓN

1.2. Mecanismos de autenticación

Sistemas de autenticación biométrica (II)

- Patrones oculares: Análisis de patrones retinales o del iris. Son los más efectivos:
 - Coincidencias casi 0
 - Muerto el individuo los tejidos oculares degeneran rápidamente → dificulta la falsa aceptación de atacantes que puedan robar este órgano de un cadáver.
 - Desventaja → incomodidad y desconfianza.
- Geometría de la mano: Son los más rápidos con una probabilidad de error aceptable. Son capaces de aprender (actualizan su base de datos con los cambios) → un pequeño crecimiento, adelgazamiento, el proceso de cicatrizado de una herida...)



1. CRIPTOGRAFÍA Y AUTENTICACIÓN

1.2. Mecanismos de autenticación

Sistemas de autenticación biométrica (II)

- Patrones oculares: Análisis de patrones retinales o del iris. Son los más efectivos:
 - Coincidencias casi 0
 - Muerto el individuo los tejidos oculares degeneran rápidamente → dificulta la falsa aceptación de atacantes que puedan robar este órgano de un cadáver.
 - Desventaja → incomodidad y desconfianza.
- Geometría de la mano: Son los más rápidos con una probabilidad de error aceptable. Son capaces de aprender (actualizan su base de datos con los cambios) → un pequeño crecimiento, adelgazamiento, el proceso de cicatrizado de una herida...)



4. PROPIEDAD INTELECTUAL

¿Qué es?

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?

Persona que crea alguna obra.

Todas las creaciones originales en cualquier medio actual o futuro, son objeto de propiedad intelectual.

La propiedad intelectual corresponde al autor solo por haberla creado.

La condición de autor tiene **carácter irrenunciable.**

¿Cómo puede protegerse?

Legislación/Normativa:

- Patentes
- Derechos de autor
- Marcas

Organismos:

- OMPI = Organización Mundial de la Propiedad Intelectual.
- A nivel nacional, el Registro General de la Propiedad Intelectual.

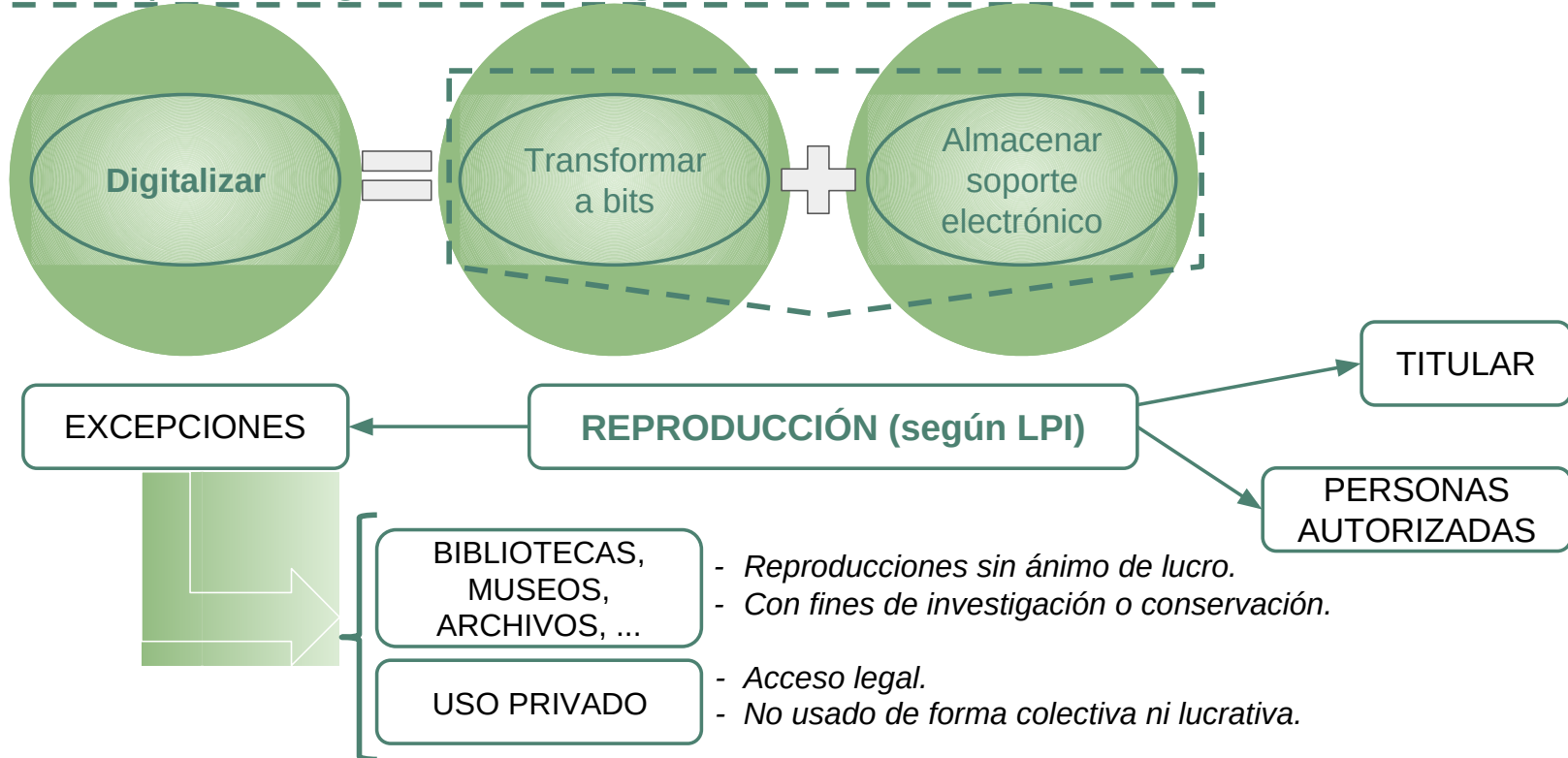
4. PROPIEDAD INTELECTUAL

4.1. Aspectos digitales en la legislación sobre P.I.



4. PROPIEDAD INTELECTUAL

4.1. Aspectos digitales en la legislación sobre P.I.



4. PROPIEDAD INTELECTUAL

4.1. Aspectos digitales en la legislación sobre P.I.

Canon digital

- 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.
- 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.

4. PROPIEDAD INTELECTUAL

4.1. Aspectos digitales en la legislación sobre P.I.

Uso de contenidos libremente en internet

- Alojar contenidos libremente en internet → si somos los titulares o tenemos autorización (Respetar los derechos de autor).
- La carga de contenidos protegidos en una red de difusión abierta = acto de comunicación pública (uno de los cuatro derechos básicos de explotación que pertenecen con exclusividad a su titular).
- La navegación en Internet no es explotación de derechos de propiedad intelectual → su uso posterior deberá respetar lo que el titular de los derechos establezca.
- Contenido protegido (copyright © + “todos los derechos reservados”) → sólo uso permitido por ley.
- Contenidos con licencias de uso más permisivas (libres o abiertas) → Ej. licencias Creative Commons.

4. PROPIEDAD INTELECTUAL

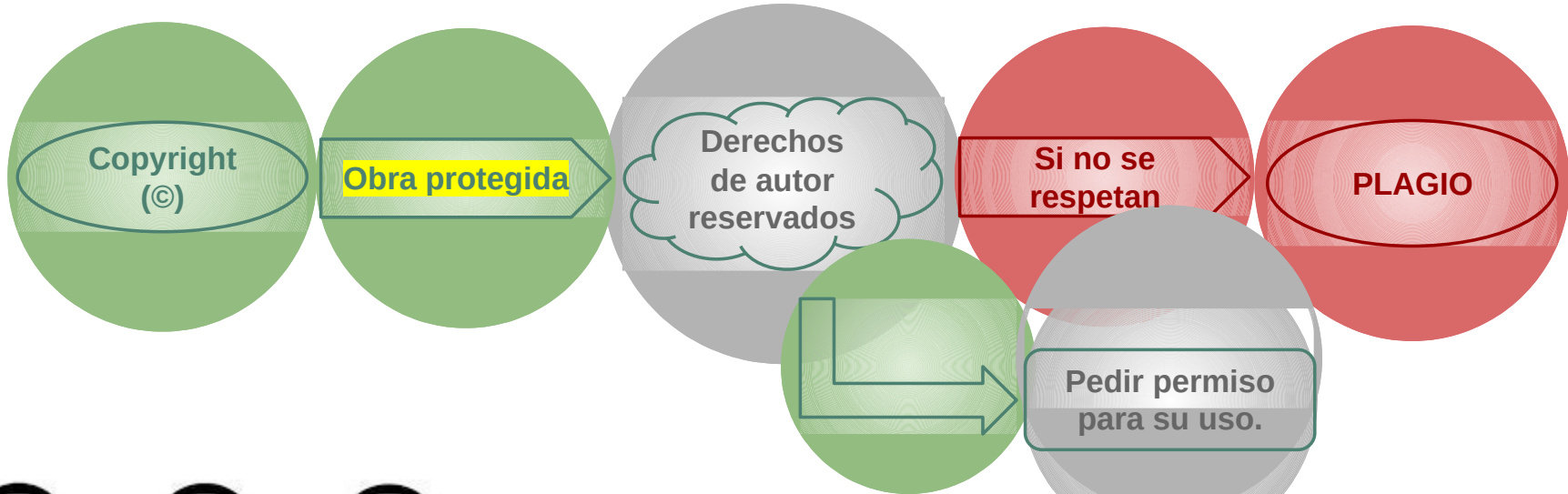
4.1. Aspectos digitales en la legislación sobre P.I.

Protección de medidas tecnológicas a los derechos de propiedad intelectual

- Otorgan al titular el control de los **derechos de explotación** sobre su obra (tanto dispositivos técnicos como a 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,

4. PROPIEDAD INTELECTUAL

4.2. Derechos de autor (copyright /copyleft)



Copyright



Copyleft



Creative
Commons



4. PROPIEDAD INTELECTUAL

4.2. Derechos de autor (copyright /copyleft)

Copyleft Derecho de autor que permite la alteración de una obra y la libre distribución de sus copias garantizando los mismos derechos libres para esas versiones modificadas.
Símbolo Copyright invertido .



Copyright



Copyleft



Creative
Commons



4. PROPIEDAD INTELECTUAL

4.3 Licencia Creative commons

Licencias CC actuales:

- *Permiten diferentes usos*
- **Símbolos identificativos**

Dominio público (CC0):



Esta es la opción más abierta.
Es 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.

TIPOS DE LICENCIAS CREATIVE COMMONS (CC)	
<p>Reconocimiento (BY)</p> <p>Permite cualquier explotación de la obra, incluyendo una finalidad comercial, así como la creación y distribución de obras derivadas sin ninguna restricción.</p>	<p>Reconocimiento - NoComercial (BY-NC)</p> <p>Permite la generación de obras derivadas sin uso comercial de la obra original.</p>
<p>Reconocimiento - NoComercial - CompartirIgual (BY-NC-SA)</p> <p>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.</p>	<p>Reconocimiento - NoComercial - SinObrasDerivadas (BY-NC-ND)</p> <p>No se permite un uso comercial de la obra original ni la generación de obras derivadas.</p>
<p>Reconocimiento - CompartirIgual (BY-SA)</p> <p>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.</p>	<p>Reconocimiento - SinObrasDerivadas (BY-ND)</p> <p>Se permite el uso comercial de la obra pero no la generación de obras derivadas.</p>

4. PROPIEDAD INTELECTUAL

4.3 Licencia Creative commons

Dominio público (CC0):




<https://pixabay.com/es/>

Fotos, ilustraciones, vectores y vídeos libres de derechos autor bajo la licencia Creative Commons CC0

4. PROPIEDAD INTELECTUAL

4.4 Obras de dominio público (Public Domain)

- Situación en la que quedan las creaciones cuando termina el periodo de protección que les otorgan los derechos de autor (entre 20 y 50 años según creación).
- Pueden ser utilizadas sin permiso y sin generar contraprestación para el creador original o sus herederos.
- Se puede por tanto copiarlas, distribuirlas, adaptarlas, etc... 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. 
- Ejemplos:
 - 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. Actividades y Webgrafía

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

- Obras en dominio público o con CC0 ó CC (by).
- Reconocer la fuente y la autoría en este segundo caso “CC (by)”
- Si no necesitas retocar la creación original y/o el uso no va a ser comercial → resto de licencias Creative Commons “CC” y cumplir sus requisitos.
- Si estás dispuesto a pagar al autor por el uso → webs de venta de imágenes.

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

- Misma situación legal que en el apartado anterior.
- En las redes sociales mismas condiciones legales que en cualquier otro sitio de Internet, además de las propias normas de uso de cada una de esas plataformas sociales.
- En caso de vulneración de la propiedad intelectual → posible denuncia del autor + sanciones (retirada de la publicación o expulsión del usuario).

3. Actividades y Webgrafía

1. <https://www.aepd.es/>
2. <http://www.ceice.gva.es/es/web/deposito-legal-propiedad-intelectual/oficina-de-reg.-de-lapropiedad>
3. [https://www.ecured.cu/Gesti%C3%B3n_de_Derechos_Digitales_\(DRM_\)](https://www.ecured.cu/Gesti%C3%B3n_de_Derechos_Digitales_(DRM_))
4. <https://www.xataka.com/legislacion-y-derechos/preguntas-y-respuestas-sobre-el-nuevocanon-digital-quien-tendra-que-pagarlo-cuanto-y-por-que>
5. <https://es.khanacademy.org/computing/computer-science/cryptography>
6. <https://tecnologia-informatica.com/que-es-la-criptografia/>
7. <https://www.evidian.com/pdf/wp-strongauth-es.pdf>
8. <https://creativecommons.org/>