Normativas y Seguridad en la Era Digital

Claves sobre Propiedad Intelectual, Licencias y Gestión de Riesgos

Propiedad Intelectual

Licencias

Gestión de Riesgos

Creado por:

Esteban, Marqués, Ricardo, Kevin y Aitor

Agenda

En esta presentación abordaremos tres pilares fundamentales sobre normativas y seguridad digital:

Marco Legal de la Propiedad Intelectual

Exploraremos la Ley de Propiedad Intelectual y su relevancia en el entorno digital.

Modelos de Licenciamiento

Analizaremos los diferentes tipos de licencias (Copyright, Copyleft, Creative Commons) y su impacto en el uso de obras.

Gestión de Riesgos con MAGERIT v3

Detallaremos la metodología para identificar, analizar y tratar riesgos informáticos.

Marco Normativo de Propiedad Intelectual

Real Decreto Legislativo 1/1996

Aprueba el Texto Refundido de la Ley de Propiedad Intelectual (LPI)

Establece el marco jurídico para salvaguardar los rights de los autores sobre sus obras

Objetivo Principal

Proteger las creaciones originales literarias, artísticas o científicas, expresadas por cualquier medio o soporte

Principales Características

Protección Automática

La propiedad intelectual corresponde al autor por el solo hecho de su creación

Registro No Requerido

No necesidad de registro formal para obtener protección

Derechos Integrados

La propiedad intelectual integra derechos de carácter personal (morales) y patrimonial (de explotación)

Derechos del Autor

La Ley de Propiedad Intelectual distingue claramente entre dos categorías de derechos que corresponden al autor: los derechos morales y los derechos patrimoniales.

Derechos Morales

Inherentes a la persona del autor. Son **irrenunciables e inalienables** , acompañan al autor durante toda su vida y a sus herederos tras su fallecimiento.

Según el Artículo 14 de la LPI:

- Derecho de divulgación: Decidir si la obra ha de ser divulgada y en qué forma
- Derecho de paternidad: Exigir el reconocimiento de su condición de autor
- Derecho a la integridad de la obra: Impedir deformaciones o alteraciones
- Derecho de modificación: Modificar la obra respetando los derechos de terceros
- Derecho de retirada del comercio: Retirar la obra por cambio de convicciones

Derechos Patrimoniales

Permiten al autor obtener beneficio económico. Son **transmisibles** y comprenden las facultades de autorizar o prohibir el uso de la obra.

Derechos de explotación:

- Reproducción: Fijación de la obra en un medio que permita su comunicación
- Distribución: Puesta a disposición del público del original o copias
- Comunicación Pública: Acceso a la obra por una pluralidad de personas
- Transformación: Traducción, adaptación o cualquier otra modificación

Protección en el Entorno Digital

Activos Protegidos

Software

Aplicaciones móviles y programas de ordenador considerados obras literarias debido a su código fuente.

Bases de Datos

Colecciones de obras o datos que, por su selección o disposición, constituyan creaciones intelectuales.

Contenido Multimedia

Elementos visuales, audiovisuales y textuales integrados en aplicaciones o plataformas digitales.

Excepciones y Limitaciones

Copia Privada

Reproducción de obras divulgadas para uso privado, no profesional ni empresarial, sin fines comerciales.

Usos Educativos

Reproducción parcial, distribución y puesta a disposición de obras en universidades y centros de investigación para fines docentes.

Dominio Público

Obras cuyos derechos de autor han expirado (generalmente 70 años después de la muerte del autor) o aquellas que el autor ha decidido liberar.

Espectro de Licencias

Las licencias son mecanismos que regulan cómo se puede usar, distribuir y modificar una obra protegida por propiedad intelectual. Existen diferentes modelos que se encuentran en un espectro que va desde lo más restrictivo hasta lo más permisivo.

Copyright Restrictivo
Todo derecho reservado

Creative Commons
Licencias híbridas

Copyleft
Permisos compartidos

Copyright Restrictivo

- Derechos de autor protegidos por defecto
- Uso exclusivo del autor
- Prohibición de reproducción

Creative Commons

- Licencias híbridas flexibles
- Permisos personalizables
- Attribution, NonCommercial, ShareAlike

Copyleft

- Permisos compartidos y derivados
- Software libre y código abierto
- GPL y licencias similares

Tipos de Licencias Creative Commons

Six combinaciones principales de licencias CC con diferentes niveles de restricción y permisos de uso:

CC BY

Reconocimiento: Se debe atribuir la obra correctamente.

CC BY-SA

Reconocimiento + Igualar: Atribución y misma licencia.

CC BY-ND

Reconocimiento + SinDerivadas: Atribución y no modificar.

CC BY-NC

Reconocimiento + NoComercial: Atribución y uso no comercial.

CC BY-NC-SA

Reconocimiento + NoComercial + Igualar: Atribución, no comercial y misma licencia.

CC BY-NC-ND

Reconocimiento + NoComercial + SinDerivadas: Atribución, no comercial y no modificar.

Atribución Igualar SinDerivadas NoComercial

MAGERIT v3: Gestión de Riesgos

Metodología sistemática desarrollada por el Gobierno español para el análisis y la gestión de riesgos en sistemas de información.

Objetivo Principal

Conciliar a los responsables de las organizaciones sobre la existencia de riesgos y la necesidad de gestionarlos.

Marco Regulador

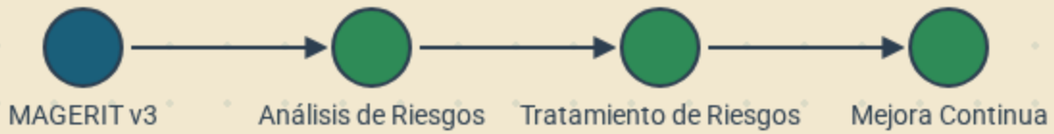
Fundamental en el ámbito de la Administración Pública española y alineado con el Esquema Nacional de Seguridad (ENS).

Soporte para SGSI

Complementa y apoya la implementación de Sistemas de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001.

Marco Práctico

Proporciona un marco práctico para el análisis y tratamiento de riesgos en el contexto de la implementación de los SGSI.



Fases del Análisis de Riesgos

El Método de Análisis de Riesgos (MAR) de MAGERIT v3 proporciona una estructura clara para evaluar los riesgos asociados a los activos de información. Este proceso se estructura en los siguientes pasos clave:

1. Identificación de Activos

Se identifican todos los elementos valiosos para la organización que soportan su misión. Esto incluye datos, software, hardware, redes de comunicaciones, instalaciones y personal.

2. Identificación de Amenazas

Se analizan los eventos que pueden causar daño a los activos, ya sean de origen natural, industrial, errores no intencionados o ataques intencionados.

3. Evaluación del Riesgo

Se determina el impacto potencial que tendría la materialización de una amenaza sobre un activo y la probabilidad de que ocurra. El riesgo se calcula combinando estos dos factores.

Cálculo del Riesgo: Riesgo = Impacto × Probabilidad

Tratamiento del Riesgo

Una vez identificados y evaluados los riesgos, MAGERIT v3 propone diversas estrategias para su tratamiento, buscando reducir el riesgo a un nivel aceptable para la dirección de la organización:

Mitigar

Consiste en reducir la probabilidad de ocurrencia de una amenaza o el impacto que esta causaría. Esto se logra mediante la implementación de salvaguardas o contramedidas.

Aceptar

Implica asumir conscientemente el riesgo residual, es decir, el riesgo que permanece después de aplicar las medidas de seguridad existentes o planificadas, cuando el coste de mitigarlo supera el beneficio.

Transferir

Se refiere a la delegación o compartición del riesgo con un tercero, por ejemplo, a través de pólizas de seguro.

Eliminar

Consiste en suprimir la fuente del riesgo, lo que puede implicar dejar de realizar una actividad o eliminar un activo que genera un riesgo inaceptable.

Ciclo de Mejora Continua

MAGERIT v3 se integra en un ciclo de mejora continua, siguiendo el modelo PDCA (Plan-Do-Check-Act), también conocido como ciclo de Deming. Este enfoque iterativo asegura que la gestión de riesgos sea un proceso dinámico y adaptable a la evolución de los sistemas de información y su entorno.

Planificar (Plan)

Se establecen los objetivos de seguridad y se realiza el análisis de riesgos para identificar dónde se encuentra la organización y dónde quiere estar.

Hacer (Do)

Se implementan los planes de seguridad y las salvaguardas definidas para tratar los riesgos.

Verificar (Check)

Se evalúan los resultados obtenidos y la efectividad de las medidas implementadas para determinar si se han alcanzado los objetivos propuestos.

Actuar (Act)

Se actualizan los planes y se realizan ajustes para mejorar continuamente la postura de seguridad, aprendiendo de la experiencia y adaptándose al nuevo contexto.

Síntesis y Conexión

En esta presentación, hemos explorado tres pilares fundamentales para la gestión de la información en la era digital:

Propiedad Intelectual

Establece quién es el titular de una creación y qué derechos (morales y patrimoniales) le corresponden. Es el punto de partida que define la titularidad de los activos digitales.

Tipos de Licencias

Regulan cómo se pueden usar, distribuir y modificar las creaciones. Actúan como un puente entre el creador y el usuario, permitiendo un control flexible sobre los derechos de explotación.

MAGERIT v3

Proporciona un marco sistemático para el análisis y la gestión de los riesgos informáticos. Es el método práctico para proteger la información y los sistemas que la contienen.

Interrelación

La interrelación entre estos elementos es crucial: la Propiedad Intelectual define **qué** proteger, las Licencias determinan **cómo** se puede usar y compartir lo protegido, y MAGERIT v3 establece **cómo** salvaguardar esos activos frente a posibles amenazas.