Fundamentos de las TICs y la Ciberseguridad

Eduardo Díaz-Mayordomo
Francisco de Santos
Facultad de CC. Jurídicas y Empresariales

Ética y Marco Legal de las TICs.

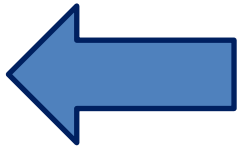
1. Principios de la Sociedad Digital.
2. Ética en las TICs.
3. Las cookies.
4. Legislación y normativa en TICs.

Principios de la Sociedad digital:

- Potenciar el desarrollo, uso y empleo de la sociedad digital mediante los medios e instrumentos necesarios.
- Garantizar los valores fundamentales recogidos en el artículo primero de la Constitución.
- Garantizar la dignidad humana con sus derechos inherentes.
- Disminución de la brecha digital. → Búsqueda de la igualdad.
- Permitir el acceso y el conocimiento a todos los individuos.

ÉTICA Y MARCO LEGAL DE LAS TICS. Índice.

1. Principios de la Sociedad Digital.
2. Ética en las TICs.
3. Las cookies.
4. Legislación y normativa en TICs.



Principios Éticos:

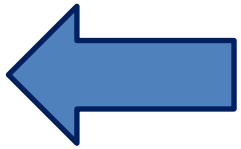
- Privacidad → Control de la información → Protección.
- Autonomía → Decisión por parte del individuo cuales son los fines para los que se utiliza la tecnología.
- Integridad y dignidad → No violación de dignidad como seres humanos.
- Fiabilidad → Para el propósito establecido → No amenazar la salud.
- E-inclusión → los servicios deben ser accesibles a todos los individuos.

La sociedad debe hacer un uso de la tecnología aumentando la calidad de vida y no dañando a ningún Individuo.

Las TICs y la informática carecen de valor ético, es su uso el que debe ser juzgado.

ÉTICA Y MARCO LEGAL DE LAS TICS. Índice.

1. Principios de la Sociedad Digital.
2. Ética en las TICs.
3. Las cookies.
4. Legislación y normativa en TICs.



ÉTICA Y MARCO LEGAL DE LAS TICs. Las Cookies.

¿Qué son las Cookies?

Información almacenada en un fichero que se instala en el navegador del cliente una vez que se realiza una petición a un servicio web con el objetivo de almacenar y recolectar ciertos datos.

- Permiten gestionar el flujo de usuarios de un sitio web.
- Mejoran la experiencia de navegación.

En algunas ocasiones, estos ficheros (cookies) pueden vulnerar la privacidad del usuario, recopilando información del usuario con una finalidad distinta:

- Información de los hábitos de navegación del usuario.
- Utilizar datos personales o no personales sin el consentimiento.
- Ceder información a una entidad externa.

¿Regulación de las Cookies?

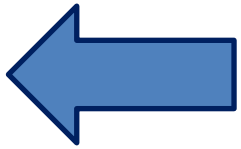
La Directiva 2002/58 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones.

Traspuesta a nuestro ordenamiento jurídico mediante la Ley 34/2002, de Servicios de la Sociedad de la Información y el Comercio Electrónico.

- Para proceder a la instalación de cookies en los navegadores de los usuarios, se requiere además de haberles informado, el **consentimiento previo** a la instalación de las mismas.

ÉTICA Y MARCO LEGAL DE LAS TICS. Índice.

1. Principios de la Sociedad Digital.
2. Ética en las TICs.
3. Las cookies.
4. Legislación y normativa en TICs.



Código Penal.

Según redacción de Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal

- Amenazas y coacciones.
- Abusos sexuales.
- Delitos contra el honor.
- Descubrimiento y revelación de secretos.
- Defraudaciones
- Daños.
- Delitos relativos a la propiedad intelectual e industrial.
- Delitos contra la salud pública.

Código Penal.

Delito	Artículos	Bien Jurídico Protegido
Amenazas y coacciones	169 a 172	Libertad Individual
Abusos sexuales	181 a 189	Libertad /Indemnidad sexual
Delitos contra el honor	205 a 210	Honor
Descubrimiento y revelación de secretos	197 a 201	Intimidad
Mercado empresarial	278	Secreto de empresa
Violación secreto empresarial	279	Secreto de empresa
Consumidores	281-286	Intereses (económicos) de los consumidores y principio de veracidad a la actividad publicitaria.
Fraude informático	248	Patrimonio
Daños	263 a 267	Propiedad pública y privada
Propiedad intelectual	270 a 277	El patrimonio de los titulares de derechos de la propiedad intelectual
Propiedad industrial	270 a 277	El patrimonio de los titulares de derechos de la propiedad intelectual
Delitos contra la salud pública	359 a 371	Salud pública

Propiedad Intelectual e Industrial.

La propiedad es un derecho reconocido en el artículo 33 de nuestra Constitución (se reconoce el derecho a la propiedad privada y a la herencia).

El régimen jurídico de la propiedad está regulado básicamente en el Código Civil: Libro Segundo: Títulos Primero y Segundo.

Contrato: acuerdo entre partes para realizar un intercambio de bienes o servicios de carácter patrimonial, es decir, susceptibles de valoración económica.

Las TICs son considerados bienes inmateriales o intangibles, siendo la vía esencial para la protección jurídica, los denominados derechos de propiedad intelectual:

- Derechos de propiedad intelectual y su materialización en derechos de autor.
- Derechos de propiedad industrial. Patentes y marcas.

Propiedad Intelectual e Industrial.

En nuestro sistema jurídico los bienes inmateriales o intangibles, están regulados básicamente en:

Texto refundido de la ley de Propiedad Intelectual	Ley de Patentes y Marcas	Código Penal
• En los artículos 1 a 40 se establece el régimen general de protección jurídica de la propiedad intelectual.	• En lo relativo a la propiedad industrial.	• En lo relativo a delitos en materia de propiedad intelectual e industrial y secreto profesional e industrial.

El artículo 10 del Texto Refundido de la Ley de Propiedad intelectual: "son objeto de propiedad intelectual todas las creaciones originales, literarias artísticas o científicas expresadas en cualquier medio o soporte.

RGPD y LOPDGDD

Reglamento (UE) 2016 / 679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

¿Qué es un dato personal? → Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Datos especialmente sensibles: tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

RGPD y LOPDGDD

Principios:

- Licitud, lealtad y transparencia.
- Para fines determinados, explícitos y legítimos.
- Adecuados, pertinentes y no excesivos.
- Exactos y actualizados.
- Limitados en el tiempo (política de retención/conservación).
- Seguridad (protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental).

Bases jurídicas de tratamiento:

- Consentimiento:
  - Trazable
  - Diferenciado y con lenguaje claro y sencillo
  - Rectificable (retirada en cualquier momento)
- Ejecución de contrato
- Cumplimiento obligación legal
- Protección intereses vitales
- Misión realizada en interés público
- Interés legítimo

RGPD y LOPDGDD

Derechos: ARSOPOL → ARCO +

- Acceso
- Rectificación
- Supresión (“derecho al olvido”)
- Oposición
- Portabilidad
- No ser objeto de decisiones individualizadas
- Limitación del tratamiento

- Su ejercicio es gratuito.
- Si las solicitudes son infundadas o excesivas pueden ser cobradas las consultas.
- Se deben responder en el plazo de un mes.
- El responsable está obligado a informar sobre los medios para ejercitar estos derechos.
- Puede atender la solicitud el encargado del tratamiento. Según contrato.

LSSI

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Servicios de la sociedad de la información: "[…] todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario. El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios»"

Ejemplos de servicios de la sociedad de la información

- La contratación de bienes o servicios por vía electrónica.
- La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.
- La gestión de compras en la red por grupos de personas.
- El envío de comunicaciones comerciales.
- El suministro de información por vía telemática.

LSSI

Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico

LSSI. Información en la página web.

- **Datos:** nombre o denominación social; residencia o domicilio o, en su defecto, la dirección de uno de sus establecimientos permanentes en España; dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.
- **Inscripción**: Los datos de su inscripción en el Registro mercantil.
- **Autorización administrativa:** En el caso de que su actividad estuviese sujeta a un régimen de autorización administrativa previa.
- **Profesión regulada:** Si ejerce una profesión regulada (ej. Abogados) deberá indicarse ciertos datos adicionales.
- **Identificación fiscal:** El número de identificación fiscal que le corresponda.
- **Precios**: información clara y exacta sobre el precio del producto o servicio.
- **Códigos de conducta:** Los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente.

Firma Electrónica.

Firma electrónica (firma digital en algunos países) es el conjunto de datos en forma electrónica, consignados a otros o asociados con ellos, que pueden ser utilizados **como medio de identificación del firmante** (Ley de Firma electrónica 59/2003 española).

- **Integridad**: los mensajes o documentos no han sido alterados.
- **Autenticidad de origen**: la fuente de datos recibidos es alegada.
- **No repudio en origen**: un documento firmado no puede repudiarse.

Un **certificado digital** es un documento electrónico que establece una asociación entre una persona o entidad y su clave pública y está firmado por un tercero de confianza.

El tercero de confianza se conoce como **Prestador de Servicios de Confianza** (PSC).

Certificado Digital

dni electrónico

Firma Electrónica.

Directiva europea 1999 / 93 / CE de firma electrónica.

Define la firma electrónica avanzada como la que cumple los siguientes requisitos:

- Está vinculada al firmante de manera única.
- Permite la identificación del firmante.
- Ha sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control.
- Está vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable.

El tipo de firma que será admisible como prueba en procedimientos judiciales: **la firma cualificada (*qualified*)** que es una firma avanzada basada en un Certificado reconocido y creada por un dispositivo seguro de creación de firma. En la ley española se denomina firma reconocida.

Ley 59 / 2003 de firma electrónica

Se establece la **firma reconocida** (*qualified signature* según Directiva) como la **firma avanzada** basada en un **certificado reconocido** y generada mediante un **dispositivo seguro de creación de firma**.

Esquema Nacional de Seguridad. Introducción

Real Decreto 311/2022 3 Mayo por el que se regula el Esquema Nacional de Seguridad.

- Generar confianza en la ciudadanía en el uso de medios electrónicos en el ámbito de las administraciones públicas.
- Ley 11/2007 de 22 de junio de acceso electrónico de los ciudadanos a los servicios públicos mediante la creación del Esquema Nacional de Seguridad.
- Medidas para garantizar la seguridad de los sistemas, datos, comunicaciones y servicios electrónicos para el ejercicio de derechos y deberes por parte de los ciudadanos en las Administraciones Públicas.
- Establece los principios básicos y requisitos mínimos que permiten una protección adecuada de la información y los servicios.
- Se determinan las dimensiones de seguridad y sus niveles, se categorizan los sistemas, las medidas de seguridad adecuadas y la auditoría periódica de la seguridad.
- Seguridad como actividad o proceso integral.

Será aplicado por las Administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias

Esquema Nacional de Seguridad. Principios

En las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

Principio	Descripción
Seguridad Integral	Proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema.
Gestión de riesgos	• El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado. • La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad.
Prevención, reacción y recuperación	• La seguridad del sistema debe conseguir que las amenazas sobre el mismo no se materialicen en la información y servicios que maneja. • Las medidas deben conseguir que el sistema garantizará la conservación de los datos e informaciones en soporte electrónico. • De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital.

Esquema Nacional de Seguridad. Principios

Principio	Descripción
Vigilancia continua	El sistema ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad que, cuando una de las capas falle, permita: Ganar tiempo. • Reducir la probabilidad de que el sistema sea comprometido en su conjunto. • Minimizar el impacto final sobre el mismo. • Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.
Reevaluación periódica	Para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.
Diferenciación de responsabilidades	• En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad. • El responsable de la información determinará los requisitos de la información tratada; el responsable del servicio determinará los requisitos de los servicios prestados; y el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. • La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios. • La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

Fundamentos de las TICs y la Ciberseguridad

¡Muchas gracias!