Seguridad en los Sistemas Informáticos
Tema 2: Legislación y normativa en materia de seguridad

Grado en Ingeniería Informática

Departamento de Ingeniería Informática
Universidad de Cádiz

Curso 2019–2020

Índice

Definiciones

- Ley En el régimen constitucional, es una disposición votada por las Cámaras y sancionada por el Jefe del Estado.
- Ley Orgánica Es aquella que tiene por objeto precisar las bases de organización y funcionamiento de una institución determinada.
- Decreto Es una norma jurídica emanada del poder ejecutivo (Gobierno) en virtud de las competencias al mismo atribuidas por la legislación vigente.
- Real Decreto Similar a la anterior, pero es sancionada por el Jefe del Estado.

Introducción

- Derecho Informático: es la parte del Derecho que regula el mundo informático.
  - Protección de datos personales
  - Protección jurídica de los programas de ordenador
  - Delitos informáticos
  - Documento electrónico
  - Comercio electrónico
  - Contratación electrónica e informática

LO15/1999 – LOPD (I)

- Su objetivo es garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y, especialmente, de su honor e intimidad personal y familiar.
- Consta de:
  - Siete títulos
  - Seis disposiciones adicionales
  - Tres disposiciones transitorias
  - Una disposición derogatoria única
  - Tres disposiciones finales

LO15/1999 – LOPD (II)

Se tratan entre otros los siguientes términos:

- Ámbito de aplicación de la LO
- Consentimiento del afectado
- Datos especialmente protegidos
- Seguridad de los datos y deber de secreto
- Derecho a indemnización
- Tratamientos con fines de publicidad y prospección comercial
- Creación de la Agencia de Protección de Datos (AEPD)
- Infracciones y sanciones: responsable, tipos y cuantías
- Modificación de la Ley General Tributaria
- Derogación de LO5/1992

LO15/1999 – LOPD (III)

- Ámbito de aplicación: Datos de carácter personal registrados en soporte físico, que los haga susceptibles de ser tratados, y utilizados tanto por entidades privadas como públicas.
- La ley no es aplicable:
  - A ficheros mantenidos por personas físicas para actividades personales.
  - A ficheros sometidos a la normativa sobre protección de materias clasificadas.
  - A ficheros relacionados con la investigación del terrorismo y de formas graves de delincuencia organizada.

LO15/1999 – LOPD (IV)

Derecho de información

Cuando se recogen datos de carácter personal, los interesados deben ser informados de:

- De que esos datos se van a almacenar en un fichero, que puede ser posteriomente tratado.
- De la finalidad para la que se recogen los datos y el destinatario de la información.
- Del carácter obligatorio o no de su respuesta a las preguntas que se le hacen.
- De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- De la posibilidad de ejercer su derecho de acceso, rectificación, cancelación y oposición.
- De la identidad y dirección del responsable del tratamiento, o en su caso de su representante.

L59/2003 (I)

- Su objetivo es regular la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.
- Consta de:
  - Exposición de motivos para justificar la promulgación de dichar ley
  - Seis títulos
  - Diez disposiciones adicionales
  - Dos disposiciones transitorias
  - Una disposición derogatoria única
  - Tres disposiciones finales

L59/2003 (II)

Se tratan entre otros los siguientes términos:

- Firma electrónica y documentos firmados electrónicamente
- Certificados electrónicos
- DNI electrónico
- Prestación de servicios de certificación
- Responsabilidad
- Dispositivos de firma electrónica
- Supervisión y control
- Infracciones y sanciones
- Derogación de RD14/1999
- La ley se dicta al amparo de varios artículos de la Constitución Española

RD3/2010 (I)

- RD por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la administración electrónica.
- Su objetivo es establecer la política de seguridad en la utilización de medios electrónicos.
- Está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información.
- Su contenido está inspirado en otros documentos de la Administración: Criterios SNC, Guías CCN-STIC, MAGERIT, Esquema Nacional de Interoperabilidad...
- Tiene en cuenta:
  - Recomendaciones de la Unión Europea.
  - Situación tecnológica de las Administraciones Públicas.
  - Servicios electrónicos ya existentes.
  - Estándares abiertos.

RD3/2010 (II)

- ENS define sus **principios básicos**:
  - Seguridad integral.
  - Gestión de riesgos.
  - Prevención, reacción y recuperación.
  - Líneas de defensa.
  - Reevaluación periódica.
  - Función diferenciada: responsable de la información, responsable del servicio y responsable de la seguridad.
- Todos los órganos superiores de las Administraciones públicas deberán disponer de su política de seguridad.
- Esta política debe incluir unos **requisitos mínimos**:
  - Organización e implantación del proceso de seguridad.
  - Análisis y gestión de los riesgos.
  - Gestión de personal.
  - Profesionalidad.
  - Autorización y control de los accesos.

RD3/2010 (cont.)

- La política de seguridad debe incluir unos **requisitos mínimos** (cont.):
  - Protección de las instalaciones.
  - Adquisición de productos (muy valorados los productos certificados).
  - Seguridad por defecto.
  - Integridad y actualización del sistema.
  - Protección de la información almacenada y en tránsito: entornos inseguros (portátiles. . .)
  - Prevención ante otros sistemas de información interconectados.
  - Registro de actividad (garantizar la protección de los derechos relacionados con los datos personales).
  - Incidentes de seguridad.
  - Continuidad de la actividad.
  - Mejora continua del proceso de seguridad.

Reglamento General de Protección de Datos (RGPD) 2016/679 (I)

- En vigor desde el 25 de mayo de 2016.
- Se empezó a aplicar el 25 de mayo de 2018.
- A responsables de tratamiento de datos establecidos en la UE, y responsables no establecidos en la UE que traten bienes o servicios destinados a ciudadanos de la UE.
- **Derecho al olvido**:
  - Los ciudadanos tienen derecho a solicitar, y obtener de los responsables, que los datos personales sean suprimidos cuando estos ya no sean necesarios para la finalidad con la que fueron recogidos.
  - El interesado puede solicitar que se bloqueen en las listas de resultados de buscadores los vínculos que conduzcan a informaciones que le afecten que resulten obsoletas, incompletas, falsas o irrelevantes y no sean de interés público.

Reglamento General de Protección de Datos (RGPD) 2016/679 (II)

- **Derecho a la portabilidad**:
  - Implica que el interesado que haya proporcionado sus datos a un responsable que los esté tratando de modo automatizado podrá solicitar recuperar esos datos en un formato que le permita su traslado a otro responsable.
  - Cuando ello sea técnicamente posible, el responsable deberá trasferir los datos directamente al nuevo responsable designado por el interesado.
- La edad en la que los menores pueden prestar por sí mismos su consentimiento para el tratamiento de sus datos personales (redes sociales...) es de 16 años, aunque cada Estado miembro puede establecer la suya propia (con límite inferior de 13 años). En España, por debajo de 14 años es necesario el consentimiento de padres o tutores.

Reglamento General de Protección de Datos (RGPD) 2016/679 (III)

- Prevención por parte de las organizaciones (públicas o privadas) que tratan datos.
- El Reglamento prevé una batería completa de medidas:
  - Protección de datos desde el diseño.
  - Protección de datos por defecto.
  - Medidas de seguridad.
  - Mantenimiento de un registro de tratamientos.
  - Realización de evaluaciones de impacto sobre la protección de datos.
  - Nombramiento de un delegado de protección de datos.
  - Notificación de violaciones de la seguridad de los datos.
  - Promoción de códigos de conducta y esquemas de certificación.
- La información que se proporcione debe ser fácil de entender y presentarse en un lenguaje claro y conciso.

Reglamento General de Protección de Datos (RGPD) 2016/679 (IV)

- El consentimiento, con carácter general, debe ser libre, informado, específico e inequívoco. No puede deducirse del silencio o de la inacción de los ciudadanos.
- Es importante revisar los sistemas de registro del consentimiento para que sea posible verificarlo ante una auditoría.
- Datos sensibles: se incluyen además los datos genéticos y biométricos, y las infracciones y condenas penales (no las administrativas).
- Sanciones: hasta los 20 millones de euros o el 4 % de la facturación global anual (no se excluye de las multas a las Administraciones Públicas, aunque los Estados Miembros pueden acordarlo así).

LO 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPD-GDD) (I)

- Adaptación del ordenamiento jurídico español al Reglamento UE 2016/679.
- Se permite que las personas vinculadas al fallecido por razones familiares o de hecho o sus herederos puedan solicitar el acceso a los mismos, así como su rectificación o supresión.
- El consentimiento ha de proceder de una declaración o de una clara acción afirmativa del afectado.
- Se mantiene en 14 años la edad a partir de la cual el menor puede prestar su consentimiento.
- Principio de transparencia en el tratamiento del reglamento europeo, que regula el derecho de los afectados a ser informados acerca del tratamiento y recoge la denominada "información por capas".

LO 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPD-GDD) (II)

- Derechos de acceso, rectificación, supresión, oposición, derecho a la limitación del tratamiento y derecho a la portabilidad.
- Regula el régimen de la Agencia Española de Protección de Datos.
- Modelo de "ventanilla única" en el que existe una autoridad de control principal y otras autoridades interesadas.
- Procedimiento de cooperación entre autoridades de los Estados miembros y decisión vinculante del Comité Europeo de Protección de Datos.
- Neutralidad de la Red y el acceso universal, derechos a la seguridad y educación digital así como los derechos al olvido, a la portabilidad y al testamento digital.

RD-ley 12/2018 de seguridad de las redes y sistemas de información

- Medidas para garantizar un nivel común de seguridad de las redes y Sistemas de Información (SI) en UE.
- Se aplicará a las entidades que presten servicios esenciales para la comunidad y dependan de las redes y SI para el desarrollo de su actividad.
- También se aplicará a los proveedores de determinados servicios digitales.
- Deberán adoptar medidas para gestionar los riesgos que se planteen para la seguridad de las redes y SI.
- Deberán notificar los incidentes sufridos (se protege a la entidad notificante y se reserva la información confidencial).
- Los CSIRT (*Computer Security Incident Response Team*) analizan riesgos y supervisan incidentes a escala nacional, difunden alertas sobre ellos y aportan soluciones para mitigar sus efectos.

Conclusiones

- Reflexión
  - ¿Son correctas las formulaciones de las leyes?
  - ¿Abarcan todos los temas?
  - ¿Es fácil controlar el cumplimiento?
- *El desconocimiento de la ley no exime de su cumplimiento*
- ¿Es o debe ser una competencia del Graduado en Ingeniería Informática?

Tareas I

1. Lectura de las leyes y reglamentos explicados en esta presentación.
2. Búsqueda de respuestas (en grupo) a las siguientes preguntas:
   1. ¿A qué tipos de ficheros no es aplicable la LOPD? ¿A cuáles sí?
   2. ¿Cuáles son los datos especialmente protegidos por la LOPD?
   3. ¿Qué establece la LOPD en cuanto al "deber de secreto" y la "comunicación de datos"?
   4. ¿Cuáles son algunas de las funciones de la Agencia de Protección de Datos?
   5. ¿Qué tipos de infracciones distingue la LOPD? ¿Cuál es la sanción para cada una de ellas?
   6. ¿Cuál es la función del "responsable de fichero" y "responsable de seguridad"?

Tareas II

7. ¿Cuáles son los niveles de seguridad?
8. ¿En qué consiste la "función diferenciada" según RD 3/2010?
9. ¿En qué se basa la "determinación de la categoría" de un sistema según RD 3/2010?
10. ¿Cuáles son las dimensiones definidas por RD 3/2010?
11. ¿Cuáles son los niveles que pueden ser requeridos en una dimensión de seguridad según RD 3/2010?
12. ¿Qué elementos son considerados redes y sistemas de información según el Real Decreto-ley 12/2018?
13. ¿Qué es un CSIRT? ¿Cuáles son los CSIRT de referencia en España?
14. ¿En qué entidades deberán designarse un delegado de datos?
15. ¿Qué tipos de infracciones existen según la Ley Orgánica 3/2018?
16. ¿A qué se denomina "información por capas"?

Tareas III

17. ¿En qué consiste la neutralidad de la red?
18. ¿En qué consiste el modelo de "ventanilla única"?
19. ¿En qué consiste el derecho a la portabilidad?
20. ¿En qué consiste el testamento digital?
21. Desde la óptica de la LOPD y de las instrucciones de la AEPD:
    - código postal, sexo y fecha de nacimiento,
    - direcciones de correo electrónico,
    - imágenes captadas por una cámara de TV,
    - grabaciones de voz y vídeo,
    - telefonía fija y móviles, y
    - SMS

    ¿son datos de carácter personal?

Referencias electrónicas

- BOE: `https://www.boe.es/`
- Agencia Española de Protección de Datos: `https://www.aepd.es/`
- Reglamento General de Protección de Datos: `http://rgpd.es/`
- Grupo de Delitos Telemáticos de la Guardia Civil: `https://www.gdt.guardiacivil.es`
- Data protection officer – European Commission: `https://ec.europa.eu/info/departments/data-protection-officer_en`
- Derecho: `http://www.derecho.com`
- El otro lado: `https://www.elotrolado.net/`
- Informática jurídica: `http://www.informatica-juridica.com`
- Delitos informáticos: `http://www.delitosinformaticos.com`
- Noticias jurídicas: `http://noticias.juridicas.com`