Universidad de Oviedo

Departamento de Informática

Campus de Gijón

Legislación relativa a la Seguridad de la Información

Presentación

Daniel F. García

Para informarse…

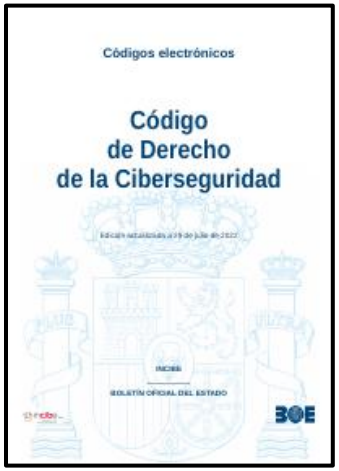
incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

Inicio > Protege tu empresa > ¿Qué te interesa?
> Cumplimiento legal

https://www.incibe.es/protege-tu-empresa/que-te-interesa/cumplimiento-legal

BOLETÍN OFICIAL DEL ESTADO



Inicio > Biblioteca Jurídica Digital > Pestaña “Códigos”
> Defensa y Seguridad > Código de Derecho de la Ciberseguridad

Actualizado a 25-julio-2023 contiene 1281 páginas

https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=173&modo=2&nota=0&tab=2

Legislación básica sobre seguridad informática

1. Reglamento General de Protección de Datos (**RGPD**) *27-Abr-2016*
   Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (**LOPDP**) *5-Dic-2018*
2. Ley de Servicios para la Sociedad de la Información y del Comercio Electrónico (**LSSI-CE**) *11-Jul-2002*
3. Reglamento de Identificación y Firma Electrónicas (**eIDAS**) *23-Jul-2014*
   Ley 6/2020 de regulación de los servicios-e de confianza *12-Nov-2020*
   RD de expedición del DNI y certificados *24-Dic-2005*
4. Ley del Procedimiento Administrativo Común de las Administraciones Públicas (**LPACAP**) *1-Oct-2015*
5. Ley de Medidas de Impulso para la Sociedad de la Información (**LISI**) *29-Dic-2007*
6. Ley de Protección de las Infraestructuras Críticas (**LPIC**) *28-Abr-2011*
7. RDL de Seguridad de las Redes y Sistemas de Información (**SRSI**) *8-Sep-2018*

Reglamento General de Protección de Datos (RGPD)

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

DOUE núm. 119 del Miércoles 4 mayo 2016

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

Reglamentos Europeos → Aplicación directa en los estados miembros

Objeto del RGPD:

Establece las normas relativas a la protección de las personas en relación con el tratamiento de los datos personales Art 1

Aplicado al tratamiento (semi)automatizado de datos personales Art 2
Y al tratamiento no automatizado de datos personales que serán incluidos en ficheros

El ámbito territorial de aplicación es la toda la UE
Pertenecen a la UE el responsable/encargado, los interesados, etc. Art 3

Ley Orgánica de Protección de Datos Personales

Ley Orgánica 3/2018, de 5 de diciembre,
de Protección de Datos Personales y garantía de los derechos digitales

BOE núm. 294 del Jueves 6 diciembre 2018

https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf

---

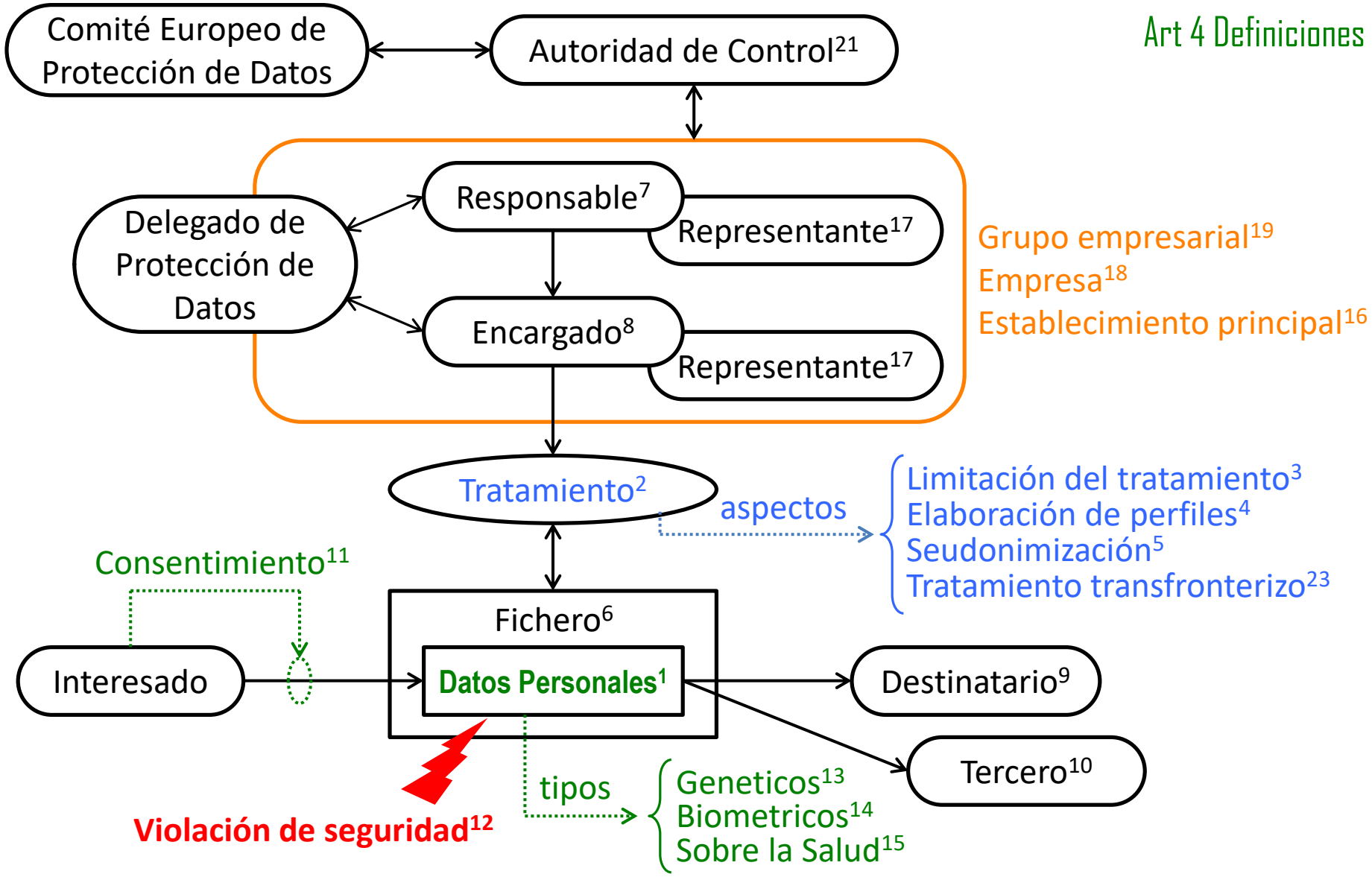
Objeto de la LOPDP:

a) Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679
LOPDP Títulos I-IX Artículos 1-78

b) Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución
LOPDP Título X Artículos 79-97

El RGPD permite que sus directrices puedan ser especificadas adicionalmente o restringidas por cada estado miembro → Esto se hace en España con la LOPDP

RGPD: Entidades involucradas



RGPD: Principios – Cap. II

Verde: Art. RGPD

Rojo: Art. LOPDP

Principios relativos al tratamiento Art 5 4-5

Los datos personales serán:

a) **Tratados** de manera lícita, leal y transparente para el interesado

b) Recogidos con **fines** determinados, explícitos y legítimos

c) Adecuados, pertinentes y limitados a lo **necesario**

d) **Exactos** y, si fuera necesario, actualizados

e) Mantenidos para permitir la identificación de los interesados durante justo el **tiempo** necesario

f) Tratados de tal manera que se garantice una **seguridad** adecuada

Licitud del tratamiento Art 6-8 6-8

Consentimiento del interesado, Cumplir un contrato/obligación legal, Proteger intereses vitales, …

Tratamiento de categorías especiales de datos personales Art 9 9

Esta prohibido tratar datos personales que revelen el origen étnico, opinión política, religión, etc., o datos genéticos, biométricos, etc., dirigidos a identificar una persona física unívocamente

PERO HAY EXCEPCIONES Ej. El interesado da su consentimiento explícito

Tratamiento de datos penales Art 10 10

El tratamiento de datos penales sólo podrá realizarse bajo la supervisión de autoridades públicas

LOPDP Titulo IV Disposiciones aplicables a tratamientos concretos → Art 19-27 + Ley Org 7/2021

RGPD: Derechos del interesado – Cap. III

Información Art 13-14 Al recabar datos personales, el responsable debe informar al interesado 11

Acceso Art 15 El interesado tendrá acceso a sus datos e información sobre su tratamiento 13

Rectificación Art 16 El interesado podrá corregir sus datos personales inexactos 14

Supresión Art 17 El interesado puede solicitar la supresión de sus datos en algunas circunstancias
(Derecho al olvido) → Pero hay circunstancias que **IMPIDEN** la supresión 15

Limitación del tratamiento Art 18 El interesado debe autorizar cada tratamiento 16
El responsable conserva los datos, que se pueden usar para ejercitar acciones legales 17

Portabilidad Art 20 El interesado puede transferir sus datos de un responsable a otro responsable

Oposición Art 21 El interesado puede oponerse al tratamiento de sus datos (hay excepciones) 18

No ser objeto de decisiones individuales automatizadas Art 22
El interesado no debe ser objeto de decisiones tomadas automáticamente con efectos jurídicos

---

Antiguamente se consideraban los derechos **ARCO** → Acceso, Rectificación, Cancelación y Oposición
El RGPD los mantiene y establece otros

LOPDP Titulo III Derechos de las personas

RGPD: Tratamiento de los datos 1 – Cap. IV

Entidades y personas involucradas

Responsable del tratamiento Art 24 28-30

Es la persona física o jurídica que determina los fines y medios del tratamiento

Debe aplicar las medidas para que el tratamiento cumpla el RGPD

Encargado del tratamiento Art 28 33

Es la persona física o jurídica que trata los datos personales por cuenta del responsable

El tratamiento se realiza según un **contrato jurídico** ente el responsable y el encargado

Delegado de Protección de datos Art 37-39 34-37

Es un profesional con conocimientos especializados en derecho y en protección de datos

Funciones →
- Asesora al Responsable y al Encargado (ej. evaluación de impacto)
- Supervisa el cumplimiento del RGPD
- Atiende a los interesados y coopera con la Autoridad de Control

Designación OBLIGATORIA por Responsable y Encargado cuando el tratamiento

- Lo hace un organismo público
- Requiere observación habitual y sistemática de interesados a gran escala
- Es a gran escala de categorías especiales de datos personales

RGPD: Tratamiento de los datos 2 – Cap. IV

Actividades a realizar

Registro de las actividades de tratamiento Art 30 31

Cada RESPONSABLE llevará un registro de Actividades de tratamiento

Cada ENCARGADO llevará un registro de Categorías de Actividades de tratamiento

Seguridad de los Datos Personales Art 32

El Responsable y el Encargado aplicarán Medidas Técnicas y Organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo
considerando: las técnicas, los costes, el tratamiento, los riesgos para derechos y libertades

Requiere 4 tipos de medidas: garantizar CIA

Para demostrar su cumplimiento sirve la adhesión a →
- Código de conducta Art 40
- Mecanismo de certificación Art 42

Notificar Violaciones de Seguridad a la Autoridad de Control Art 33

El Responsable debe notificar la violación a la Autoridad de Control en un plazo de 72 horas
El Encargado notificará la violaciones al Responsable sin dilación

Comunicar Violaciones de Seguridad al Interesado Art 34

El Responsable debe comunicar la violación al interesado
cuando entrañe un alto riesgo para los derechos y libertades de las personas

Actividades a realizar 2

Evaluación de impacto relativa a la protección de datos Art 35

El responsable evaluará el impacto del tratamiento antes de realizarlo
SI el tratamiento entraña un alto riesgo para los derechos y libertades de las personas

La evaluación es OBLIGATORIA en 3 casos:

1.-Elaboración de perfiles personales usados para tomar decisiones con efectos jurídicos
2.-Tratamiento a gran escala de categorías especiales de datos
3.-Observación sistemática a gran escala de una zona de acceso público

La Autoridad de Control publicará Listas de Tipos de Tratamiento que
SI y NO requieren una evaluación de impacto

La evaluación INCLUIRÁ como mínimo:

a) Descripción del tratamiento: fines, legitimidad, operaciones
b) Evaluación de la necesidad y proporcionalidad de las operaciones respecto a su finalidad
c) Evaluación de los riesgos del tratamiento para los derechos y libertades de los interesados
d) Medidas previstas para afrontar los riesgos

Consulta Previa Art 36

El responsable consultara a la Autoridad de Control antes de realizar un tratamiento
CUANDO la evaluación muestre un riesgo alto y NO se apliquen medidas para mitigarlo

RGPD: Tratamiento de los datos 4 – Cap. IV

Códigos de conducta Art 40 38

Los CC son guías de aplicación del RGPD en sectores específicos

Promoverán la elaboración de CC:
- Estados miembros de la UE
- Autoridades de Control
- Comité Europeo de Protección de Datos (Comité)
- Comisión Europea

Pueden elaborar CC las Asociaciones de Responsables o Encargados

Las entidades que se adhieran a un CC están obligadas a cumplirlo

Un CC tendrá mecanismos que permitan a un organismo de supervisión verificar su cumplimiento

Aprobación de CC que afecten a:
- 1 Estado → Autoridad del Control
- N Estados → Comité + Comisión Europea

Supervisión de códigos de conducta aprobados Art 41

Un Organismo de Supervisión **acreditado** puede supervisar el cumplimiento de un CC

La Autoridad de Control concede y revoca la acreditación a los Organismos de Supervisión

La AC debe someter los "Criterios de Acreditación de los Organismos de Supervisión" al Comité

RGPD: Tratamiento de los datos 5 – Cap. IV

Certificación Art 42

Los estados, las AC, el Comité y la Comisión …
Promoverán la creación de certificaciones y sellos/marcas de protección de datos

La certificación será voluntaria y la expedirá un Organismo de Certificación o la AC

El periodo de validez de la certificación es de 3 años y se podrá renovar

El Comité archivará y publicará todos los mecanismos de certificación y sellos/marcas

Organismo de Certificación Art 43 39

Los OdC expedirán y renovarán las certificaciones, después de informar a la AC

Los OdC serán acreditados por { La Autoridad de Control (AC) competente
La Entidad Nacional de Acreditación (ENAC)

Para acreditarse, un OdC debe cumplir los requisitos definidos en este articulo
Y los criterios aprobados por la AC o el Comité, que serán públicos y accesibles

La acreditación se expide por un período mínimo de 5 años y se podrá renovar

RGPD: Resto de la ley

Cap. V Transferencias de datos personales a terceros países u organizaciones internacionales

Art 44-50 40-43

Se pueden hacer las transferencias si el nivel de protección de las personas no es menoscabado

Mecanismos de la ley:
- Decisión de adecuación de la Comisión
- Garantías adecuadas del Responsable y/o Encargado
- Normas corporativas vinculantes

Cap. VI Autoridades de control independientes

Art 51-59

Define el establecimiento, funciones, etc., de la ACs en cada estado de la UE

LOPDP Art 40-43: La Agencia Española de Protección de Datos (AEPD)

LOPDP Art 57-62: Agencias autonómicas de protección de datos

Cap. VII Cooperación y coherencia

Art 60-76

Establece los mecanismos de cooperación entre autoridades de control

Define las funciones del Comité Europeo de Protección de Datos

Cap. VIII Recursos, responsabilidad y sanciones

Art 77-84 63-69

Establece derechos: a reclamar ante una AC, a la tutela judicial contra una AC, etc.

Establece las condiciones generales para la imposición de multas administrativas Art 83

RGPD: Infracciones y sanciones

Condiciones generales definidas en el RGPD: Art 83

Infracciones con multa **hasta** 10M€ ó 2% Volumen de negocio (empresas)

a) Obligaciones del Responsable o Encargado Art 8 11 25-39 42 43
b) Obligaciones de los Organismos de Certificación Art 42 43
c) Obligaciones de la Autoridad de Control Art 41.4

Infracciones con multa **hasta** 20M€ ó 4% Volumen de negocio (empresas)

a) Principios básicos para el tratamiento Art 5 6 7 9
b) Derechos de los interesados Art 12-22
c) Transferencias de datos personales Art 44-49
d) Obligaciones definidas por los estados Art 85-91
e) Incumplimientos de resoluciones Art 58

La cuantía de la multa se impondrá en cada caso individual considerando sus circunstancias

---

LOPDP clasifica las infracciones y pone ejemplos: 70-78

- Muy graves (prescriben en 3 años) Hasta 20M€ Art 83.5 72
- Graves (prescriben en 2 años) Hasta 10 M€ Art 83.4 73
- Leves (prescriben en 1 año) 74

Ley de Servicios de la Sociedad de la Información

LEY 34/2002, de 11 de julio,
de servicios de la sociedad de la información y de comercio electrónico (**LSSI-CE**)

BOE núm. 166 del Viernes 12 julio 2002

https://www.boe.es/boe/dias/2002/07/12/pdfs/A25388-25403.pdf

Información en la página web del Ministerio de Asuntos Económicos y Transformación Digital

https://lssi.mineco.gob.es

La LSSI-CE Regula:

- La prestación de los servicios de Sociedad de la Información
- La contratación por vía electrónica

Aplicable a prestadores de servicios:

- Establecidos en España
- Establecidos en el extranjero y que proveen servicios en España

NO Aplicable a (por tener normativa específica):

- Servicios de notarios y registradores de la propiedad y mercantiles
- Servicios de abogados y procuradores

LSSI-CE Aspectos de la ley 1 – Prestación de servicios

Obligaciones de los prestadores de servicios vía Internet

Comunicar al Registro Mercantil su nombre de dominio LSSI Art 9

Mostar la información (web): nombre, dirección, datos registrales, NIF LSSI Art 10

Mostrar de forma clara y exacta el precio de los productos y servicios

Sobre los prestadores de servicios ISP, Hosting, etc. LSSI Art 16

Colaborar con los órganos públicos para la resolución de incidencias: LSSI Art 12
almacenamiento de datos y eventos para rastreo

No son responsables de contenidos ilícitos si no los elaboran LSSI Art 16 (13-17)
Sí son responsables si los conocen y no los retiran o no lo comunican

Sobre la publicidad por Internet

Prohíbe la publicidad por correo electrónico no solicitada LSSI Art 21

Posibilidad de borrarse de las listas de correo informativo LSSI Art 22

LSSI-CE Aspectos de la ley 2 – Contratación electrónica

Contratación por vía electrónica

LSSI Art 23-29

Los contratos celebrados por vía electrónica tendrán plena efectividad jurídica siempre que cumplan los requisitos legales necesarios para que sean válidos

La prueba de celebración se rige por lo establecido en la Ley de Firma Electrónica
(El soporte electrónico con el contrato será admisible en juicios como prueba documental)

Las partes pueden pactar que un tercero archive en soporte informático los documentos y comunicaciones electrónicas (con fecha y hora) usadas en la contratación durante un tiempo estipulado (mínimo: 5 años)

Antes de contratar

El prestador (oferente) del servicio informará al destinatario de:

Trámites de celebración / Archivo, accesibilidad y lenguas del documento electrónico

La información no será necesaria en estas circunstancias:

1.- Los contratantes lo acuerdan y ninguno de ellos es consumidor

2.- El contrato se ha celebrado exclusivamente mediante intercambio de correos-e

Después de contratar

El oferente debe confirmar la recepción de la aceptación

La confirmación no es necesaria en las mismas 2 circunstancias anteriores

LSSI-CE Infracciones y sanciones

Tipos de infracciones y sanciones: leves, graves, y muy graves LSSI Art 38-39

Infracciones **muy graves** (multa de 150.000€ a 600.000€)

- Incumplimiento de las órdenes de un órgano administrativo en casos de
  - Orden púbico
  - Seguridad pública
  - Defensa nacional
  - Salud pública
- No suspender el servicio cuando lo ordena un órgano administrativo
- No retener los datos de las comunicaciones el periodo mínimo
- Usar los datos retenidos para fines no previstos

Infracciones **graves** (multa de 30.000€ a 150.000€)

- No proveer información registral y/o de precios de productos y servicios
- Enviar >3 anuncios a un destinatario en <1 año sin su consentimiento
- No facilitar las condiciones de contratos o confirmar las aceptaciones de condiciones
- Resistencia o dilación de acciones de inspección

Infracciones **leves** (multa < 30.000€)

- No comunicar al registro mercantil el nombre de dominio
- No proveer información (aparte de la registral y precios)
- Incumplir artículos sobre envío de publicidad (infracción no grave)
- Incumplir la obligación de confirmar la recepción de peticiones (aceptaciones)

Reglamento de Identificación y Firma Electrónicas

Reglamento UE 910/2014 de 23 de julio de 2014 **eIDAS**

DOCE vol.57, L 257, Jueves 28 agosto 2014

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32014R0910&from=ES

LEY 6/2020, de 11 de noviembre, de regulación de los servicios electrónicos de confianza **LRSEC**

BOE núm. 258 del Jueves 12 noviembre 2020

https://www.boe.es/boe/dias/2020/11/12/pdfs/BOE A 2020 14046.pdf

---

Establece los medios de identificación electrónica eIDAS Art 6-12

Regula los certificados electrónicos Art 4-7

Regula los Servicios de Confianza eIDAS Art 13-24 Art 8-13
(Autoridades de certificación)

Regula Firmas y Sellos Electrónicos eIDAS Art 25-40

Ley 6/2020 Infracciones y sanciones

Tipos de infracciones y sanciones: leves, graves, y muy graves LRSEC Art 18-20

Infracciones **muy graves** (multa de 150.001€ a 300.000€)

- Infracción grave repetida en un plazo de dos años
- Expedir certificados cualificados sin realizar las comprobaciones pertinentes

Infracciones **graves** (multa de 50.001€ a 150.000€)

- Resistencia u obstrucción a las acciones de inspección
- Actuar como prestador cualificado de servicios de confianza sin tener la cualificación
- No proteger adecuadamente los datos de creación de firma o sello
- Incumplir la obligación de notificación de incidentes
- Adoptar medidas insuficientes o nulas para resolver incidentes de seguridad
- Incumplimiento de resoluciones dictadas por el Ministerio, etc.

Infracciones **leves** (multa < 50.000€)

- Publicar información no veraz o no acorde con la ley
- No comunicar el inicio, cese o modificación de actividad, etc.

Real Decreto sobre expedición del DNI

REAL DECRETO 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica

BOE núm. 307 del Sábado 24 diciembre 2005

https://www.boe.es/boe/dias/2005/12/24/pdfs/A42090-42093.pdf

Portal oficial sobre el DNI electrónico:

https://www.dnielectronico.es/

El chip incrustado en el soporte del DNI incluye RD Art 11

- Certificados reconocidos de autenticación y de firma
- Certificado electrónico de la autoridad emisora

} Con sus períodos de validez

- Claves privadas necesarias para la activación de los certificados

Validez de los certificados electrónicos RD Art 12

- Periodo de vigencia de 30 meses → Extendido a 60 meses (máximo)
- A la extinción solicitar nuevos certificados, para el mismo DNI
- La pérdida de validez del DNI → Perdida de validez de sus certificados

Ley del Procedimiento Administrativo Común de AAPP

LEY 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las administraciones Públicas (**LPACAP**)

BOE núm. 236 del Viernes 2 octubre 2015

https://www.boe.es/boe/dias/2015/10/02/pdfs/BOE-A-2015-10565.pdf

---

La ley 39/2015 deroga la Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos de 2007
Pues integra el uso de medios electrónicos en el procedimiento administrativo común

Reconoce el derecho y la obligación de los ciudadanos de relacionarse electrónicamente con las Administraciones Públicas (AAPP) LPACAP Art 14

- Identificación y firma de los interesados LPACAP Art 9-12
  - Mediante Certificados o Claves concertadas y Sistemas de Firma Electrónica
- Establecimiento de registros electrónicos LPACAP Art 16
  - Para la recepción y remisión de solicitudes, escritos y comunicaciones
- Archivo electrónico de documentos LPACAP Art 17
  - Garantizando la integridad, autenticidad y conservación
- Notificaciones LPACAP Art 40-46
  - Preferentemente por medios electrónicos (obligatorios para algunos interesados)

Ley del Procedimiento Administrativo Común de AAPP

REAL DECRETO 203/2021, de 30 de marzo, de Reglamento de actuación y funcionamiento del sector público por medios electrónicos

BOE núm. 77 del Miércoles 31 marzo 2021

https://www.boe.es/boe/dias/2021/03/31/pdfs/BOE-A-2021-5032.pdf

RD Esquema Nacional de Seguridad - 1

REAL DECRETO 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad

BOE núm. 106 del Miércoles 4 mayo 2022

https://www.boe.es/boe/dias/2022/05/04/pdfs/BOE-A-2022-7191.pdf

---

Su objeto es regular el Esquema Nacional de Seguridad (ENS)

RD Art 1-4

Establece los principios básicos y los requisitos mínimos para gestionar la seguridad de la información manejada en las Administraciones Públicas

Principios básicos del ENS: RD Art 5-11

a) Seguridad como proceso integral
b) Gestión basada en los riesgos
c) Prevención, detección, respuesta y conservación
d) Líneas de defensa
e) Vigilancia continua
f) Reevaluación periódica
g) Diferenciación de responsabilidades

RD Esquema Nacional de Seguridad - 2

Política de seguridad y Requisitos mínimos de seguridad: RD Art 12-27

a) Organización e implantación del proceso de seguridad
b) Análisis y gestión de los riesgos
c) Gestión de personal
d) Profesionalidad
e) Autorización y control de los accesos
f) Protección de las instalaciones
g) Adquisición de productos de seguridad
h) Mínimo privilegio
i) Integridad y actualización del sistema
j) Protección de la información almacenada y en tránsito
k) Prevención ante otros sistemas de información interconectados
l) Registro de actividad y detección de código dañino
m) Incidentes de seguridad
n) Continuidad de la actividad
ñ) Mejora continua del proceso de seguridad

Cumplimiento de los requisitos mínimos RD Art 28-30

El Centro Criptológico Nacional elabora las "Guías de Seguridad de las TICs" (*Serie 800*)
https://www.ccn.cni.es/

RD Esquema Nacional de Seguridad - 3

Auditoría de seguridad RD Art 31 y ANEXO III Cada 2 años

La "Comisión Sectorial de Administración Electrónica" recogerá información para realizar informes sobre el estado de la seguridad de los SIs RD Art 32

Respuesta a incidentes de seguridad RD Art 36-37

Apoyo del CCN-CERT: Centro Criptológico Nacional - Computer Emergency Response Team

Normas de conformidad RD Art 35-38

Actualización RD Art 39

Categorización de los SIs RD Art 40-41 y ANEXO I

Confidencialidad [C]
Integridad [I]
Trazabilidad [T]
Autenticidad [A]
Disponibilidad [D]

Nivel requerido en cada dimensión: Bajo, Medio, Alto

Medidas de Seguridad → ANEXO II

- Disposiciones generales
- Selección de medidas
- Marco organizativo
- Marco operacional
- Medidas de protección
- Desarrollo de las medidas
- Interpretación

RD Esquema Nacional de Interoperabilidad

REAL DECRETO 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica

BOE núm. 25 del Viernes 29 enero 2010

https://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1331.pdf

---

Su objeto es regular el Esquema Nacional de Interoperabilidad (ENI) RD Art 1-3

Principios básicos del ENI: RD Art 4-7

- a) La interoperabilidad como cualidad integral
- b) Carácter multidimensional de la interoperabilidad →
  - Organizativa RD Art 8-9
  - Semántica RD Art 10
  - Técnica RD Art 11
- c) Enfoque de soluciones multilaterales

Aspectos del ENI:
- Infraestructuras y servicios comunes RD Art 12
- Comunicaciones (Red SARA) RD Art 13-15
- Reutilización y transferencia de tecnología RD Art 16-17
- Firma electrónica y certificados RD Art 18-20
- Recuperación y conservación de documentos electrónicos RD Art 21-24

Normas de conformidad RD Art 25-28

Actualización RD Art 29

Ley de Impulso de la Sociedad de la Información

LEY 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información (**LISI**)

BOE núm. 312 del Sábado 29 diciembre 2007

https://www.boe.es/boe/dias/2007/12/29/pdfs/A53701-53719.pdf

Integra un conjunto de medidas orientadas a impulsar la Sociedad de la Información en el sector privado

Las medidas se agrupan en 3 líneas fundamentales

- Facturación electrónica LISI Art 1
  - Promueve el uso de medios electrónicos para la facturación
- Obligación de disponer de un medio de interlocución telemática LISI Art 2
  - Para las empresas presten servicios al público de especial trascendencia económica
- Ofertas públicas de contratación electrónica entre empresas LISI Art 3
  - Una empresa compra/vende productos a otras usando un proceso electrónico abierto

LISI: Aspectos básicos

El resto de artículos de la LISI recogen modificaciones de otras leyes

20 Modificaciones de la Ley 34/2002 LISI Art 4
Servicios de la SI y de CE

6 Modificaciones de la Ley 59/2003 LISI Art 5
Firma electrónica

1 Modificación de la Ley 59/2003 LISI Art 6
Ordenación del comercio minorista

5 Modificaciones de la Ley 32/2003 LISI Art 7
General de Telecomunicaciones

2 Modificaciones de la Ley 11/1998 LISI Art 8
General de Telecomunicaciones

Incluye Disposiciones importantes:

Uso de caracteres de las lenguas oficiales de España en ".es" LISI DA 1ª

Extensión de servicios de banda ancha LISI DA 2ª

Mejora de los niveles de seguridad y confianza en Internet LISI DA 3ª

Necesidades de información para fines estadísticos y de análisis LISI DA 4ª

Acceso de las personas con discapacidad a las TIC LISI DA 11ª

Transferencia tecnológica a la sociedad → CENATIC LISI DA 14ª http://www.cenatic.es/

Cesión de contenidos para ponerlos a disposición de la sociedad LISI DA 17ª

Regulación del juego y las apuestas por Internet LISI DA 20ª

Ley de Protección de Infraestructuras Críticas (LPIC)

LEY 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (**LPIC**)

BOE núm. 102 del Viernes 29 abril 2011

https://www.boe.es/boe/dias/2011/04/29/pdfs/BOE-A-2011-7630.pdf

REAL DECRETO 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas

BOE núm. 121 del Sábado 21 mayo 2011

https://www.boe.es/boe/dias/2011/05/21/pdfs/BOE-A-2011-8849.pdf

---

Establece las estrategias y las estructuras adecuadas que permiten dirigir y coordinar las actuaciones de las AAPP para proteger infraestructuras críticas

LPIC Art 1

Define múltiples conceptos: LPIC Art 2

- Servicio esencial, Sector estratégico, Infraestructura
- Criterios horizontales de criticidad, etc., …

{ Estratégica
Crítica
Crítica Europea

Zona crítica
Análisis de riesgos

Establece el "**Catálogo** Nacional de Infraestructuras Críticas" LPIC Art 4 RPIC Art 3-5

LPIC Elementos básicos

Establece el "**Sistema** de Protección de Infraestructuras Críticas"

Agentes del Sistema: Ministerio del Interior, Los Operadores Críticos, …, y LPIC Art 5-13, RPIC Art 6-15

El centro Nacional de Protección de Infraestructuras Críticas — LPIC Art 7, RPIC Art 7
https://cnpic.interior.gob.es/

Establece los "Instrumentos de **Planificación** del Sistema" LPIC Art 14

- El Plan Nacional de Protección de las Infraestructuras Críticas RPIC Art 16-18
- Los Planes Estratégicos Sectoriales RPIC Art 19-21
- Los Planes de Seguridad del Operador RPIC Art 22-24
- Los Planes de Protección Específicos RPIC Art 25-29
- Los Planes de Apoyo Operativo RPIC Art 30-32

Establece las "**Comunicaciones** en el Sistema" LPIC Art 15-18, RPIC Art 33-36

RDL de Seguridad de las Redes y Sist de Información

RDL 12/2018, de 7 de septiembre, de Seguridad de las Redes y Sistemas de Información (**SRSI**)

BOE núm. 218 del Sábado 8 septiembre 2018

https://www.boe.es/boe/dias/2018/09/08/pdfs/BOE-A-2018-12257.pdf

Este RDL transpone la Directiva (UE) 2016/1148 de la UE de 6 de julio de 2016 a la legislación española

Objeto: Regular la seguridad de las Redes y SI usados para proveer **Servicios Esenciales** Art 1-2

Los **Servicios Esenciales** están definidos por la Ley 8/2011 LPIC Art 6-7

Afecta principalmente a los Operadores Críticos

Define las **autoridades** competentes y los equipos de respuesta a incidentes Art 8-15

CSIRT (Computer Security Incident Response Team) https://www.csirt.es/

Especifica las **obligaciones** de seguridad de los operadores Críticos Art 16-18

Son desarrolladas en el RD 43/2021

Promueven la aplicación de regulaciones y normas → **Estrategia Nacional de Ciberseguridad**
https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019

Indica las obligaciones al **notificar los incidentes** de seguridad Art 19-31

Define la **supervisión** de los operadores y las sanciones Art 32-42

Legislación de la Unión Europea 1 - DEROGADA

Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995

Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

DOCE núm. L281/31 del 23 noviembre 1995

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046&rid=1

La directiva se aplicó en España mediante la LOPD

Directiva 1999/93/CE del parlamento europeo y del consejo de 13 de diciembre 1999

Por la que se establece un marco comunitario para la firma electrónica

DOCE núm. L13/12 del 19 enero 2000

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31999L0093&from=ES

Directiva 2002/58/CE del parlamento europeo y del consejo de 12 de julio de 2002

Relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)

DOCE núm. L201/37 del 31 julio 2002

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32002L0058&from=ES

Legislación de la Unión Europea 2 - VIGENTE

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

DOUE núm. 119 del Miércoles 4 mayo 2016

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

Deroga la Directiva 95/46/CE (Reglamento general de protección de datos) con efecto a partir del 25 de mayo de 2018

Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016

Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos

DOUE núm. 119 del Miércoles 4 mayo 2016

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L0680&from=ES

Legislación de la Unión Europea 3 - VIGENTE

Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019

Relativo a ENISA (Agencia de la UE para la ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación

DOUE núm. 151 del viernes 7 junio 2019

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0881&from=ES

Deroga el Reglamento (UE) 526/2013 (Reglamento sobre la ciberseguridad)

Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 diciembre 2022

Relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión

DOUE núm. L333/80 del 27 diciembre 2022

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32022L2555

Deroga la Directiva (UE) 2016/1148 (Medidas de seguridad de Redes y SI)