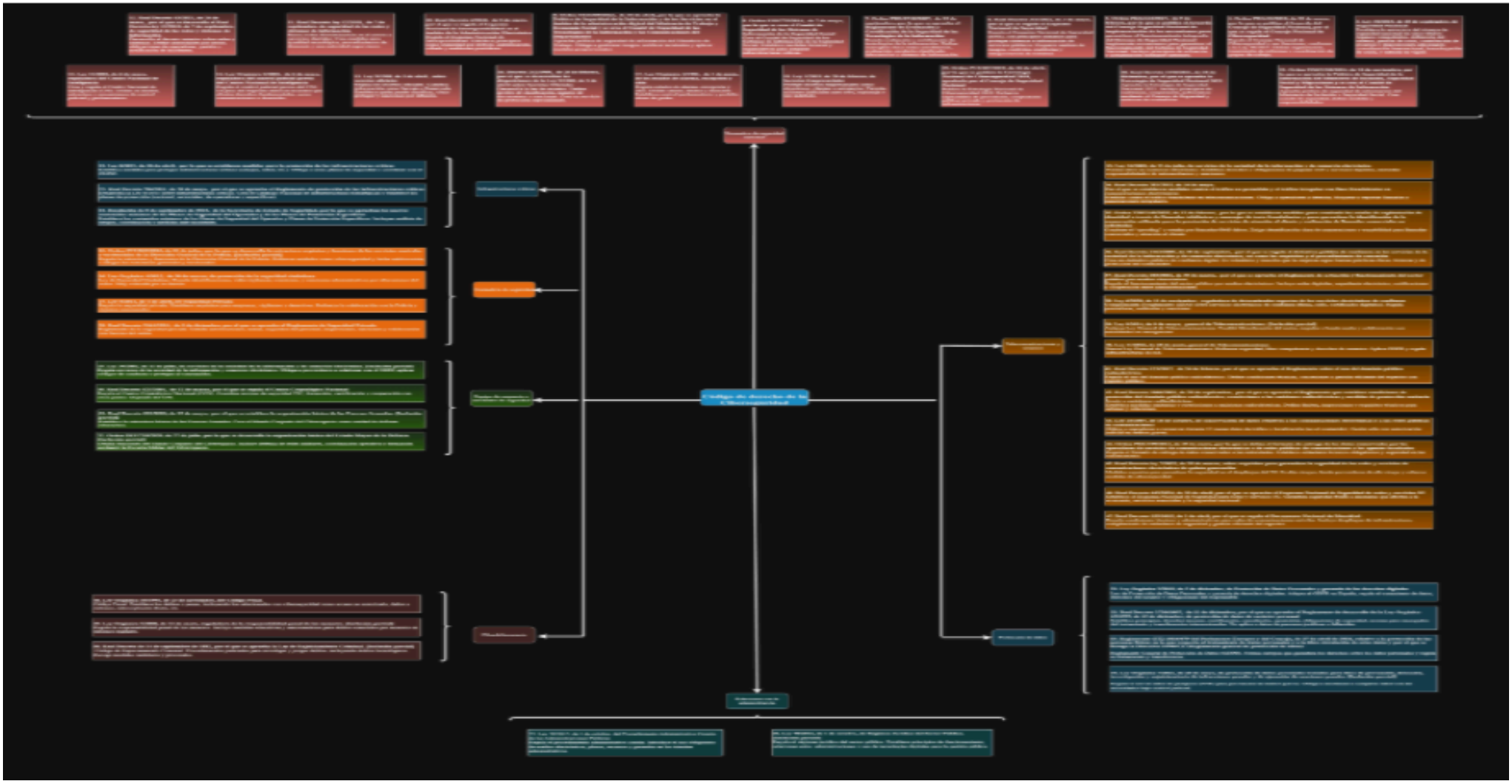
Normativa

Código de derecho de la Ciberseguridad

Jennifer

Contenido

Esquema



Código de derecho de la Ciberseguridad

3. Ley 36/2015, de 28 de septiembre, De Seguridad Nacional

Estructura de la ley donde se explican los formatos, a quienes afectan y porque se ha realizado. La estructura son cincos partes en la que hemos encontrado:

Título I: Detallan los órganos competentes de la Seguridad Nacional y que competencias se les asignan.

Título II: Creación, definición del sistema de seguridad nacional.

Título III: Gestión de crisis.

Título IV: Regulación de la contribución de recursos a la seguridad nacional.

Título V: En esta parte tenemos cuatro disposiciones adicionales que consta de:

Coordinación con instrumentos internacionales.

Homologación de instrumentos de gestión de crisis y comunicación pública respectivamente

Disposición transitoria relativa a la actividad de los comités especializados

Regulación de los títulos competenciales, desarrollo reglamentario, mandamiento legislativo y entrada en vigor.

4. Orden PRA/33/2018, de 22 de enero, Por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad

Mediante la ley transitoria 36/2015 de 28 de septiembre, se realizó la entrada en vigor de la Ley de Seguridad Nacional para asignar funciones concretas a los órganos competentes dentro de la Seguridad Nacional, donde podemos encontrar a las Cortes Generales, el Gobierno, el Presidente del Gobierno, los Ministros, el Consejo de Seguridad Nacional, los Delegados del Gobierno de las Comunidades Autónomas y en las ciudades con Estatuto de Autonomía de Ceuta y Melilla.

Además ponemos en acuerdo la modificación del marco regulador del consejo nacional de ciberseguridad, y la comunicación del mismo en el boletín oficial del Estado (BOE).

Acuerdo por el que se regula el Consejo Nacional de Ciberseguridad

Se intenta establecer el marco regulador del Consejo Nacional de Ciberseguridad

Viene previsto por el artículo 20.3 de la Ley 36/2015 de 28 de septiembre.

Se especifican las funciones específicas del Consejo de Seguridad Nacional

Organización del Consejo de Seguridad Nacional

Método de transmisión de los informes

Utilización de los mecanismos de enlace y coordinación

Grupos de trabajo

5. Orden PRA/116/2017,

De 9 de febrero, por la que se publica el Acuerdo del Consejo Seguridad Nacional de implementación de los mecanismos para garantizar el funcionamiento integrado del Sistema de Seguridad Nacional

Debido a lo dispuesto en los artículos 18.2, 25.1, 21.1c, 22 y Disposición Transitoria única, apartado 2, conjunto al artículo 11.1, todos correspondientes a la ley 36/2015, de 28 de septiembre, se ha acordado:

Aprobar la implementación de mecanismos para garantizar el funcionamiento del Sistema Seguridad Nacional

Para ello se ha realizado lo siguiente:

- Descripción del funcionamiento óptico, integrado y flexible del Sistema de Seguridad Nacional
- Las clases de mecanismos pertenecientes al sistema de seguridad nacional
- Principios y procedimientos de actuación
- Informes periódicos para la actualización de esta orden.

6. Real Decreto 311/2022, de 3 de mayo,

Por el que se regula el Esquema Nacional de Seguridad

El decreto regula el Esquema Nacional de Seguridad (ENS), estableciendo principios básicos y requisitos mínimos para proteger adecuadamente la información y los sistemas utilizados en la prestación de servicios públicos. Se aplica tanto al sector público como privado cuando manejan datos sensibles.

Los sistemas que traten datos personales deben cumplir con el Reglamento Europeo 2016/679 (GDPR), identificando al responsable del tratamiento y aplicando medidas según el análisis de riesgos.

El objetivo principal es asegurar que las organizaciones usen los sistemas de información de forma segura y eficiente, mediante un enfoque integral que combina aspectos humanos, técnicos, jurídicos y organizativos.

Se requiere:

- Análisis y gestión de riesgos.
- Protocolos de prevención, detección, respuesta y conservación.
- Evaluación periódica de sistemas y vigilancia continua.
- Claras responsabilidades y políticas de seguridad formalmente aprobadas por cada administración.

También se incluyen medidas como:

- Control de accesos y privilegios mínimos.
- Protección de instalaciones y sistemas.
- Adquisición segura de productos y servicios.
- Integridad de sistemas, protección de la información en tránsito y almacenamiento.
- Registro de actividades y detección de código dañino.
- Auditorías al menos cada dos años y elaboración de informes de seguridad coordinados por el CCN.

- Cumplimiento de normas según los ciclos de vida de sistemas y servicios.

Finalmente, el ENS debe mantenerse actualizado y se exige la categorización de los sistemas en función del impacto de la información y servicios que manejan.

7. Orden PRE/2740/2007,

De 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información

Se aprueba el reglamento de evaluación y certificación de la seguridad de las tecnologías de la información, por el que se definen:

- **Acreditación:** Declaración de conformidad de los laboratorios solicitantes, emitidas por el Organismo de Certificación
- **Acreditación de competencia de técnica:** Acreditación que concede una entidad de acreditación reconocida a un laboratorio, por donde se aprueba un Reglamento de la infraestructura para la calidad y seguridad industrial
- **Certificación:** Es la determinación, obtenida mediante un proceso metodológico de evaluación.
- **Declaración de seguridad:** Conjunto de requisitos y especificaciones de las propiedades de seguridad de un producto.
- **Evaluación:** Análisis realizado mediante un proceso metodológico de un producto o sistema.
- **Información de las evaluaciones:** Es todo aquello relacionado con la actividad de evaluación de la seguridad de un producto.
- **Producto a evaluar:** Producto que solicita una certificación
- **Producto clasificado:** Productos con requisitos específicos para manejar con seguridad materias clasificadas.
- **Laboratorio de evaluación:** Laboratorio de ensayo.
- **Sistema de Información:** Conjunto de elementos hardware, software, datos y usuarios.
  A su vez se explica la estructura de la emisión del certificado.

Por último se exponen los fines, donde se vigila que la normativa de organismo de certificación se corresponda y equipare con términos y referencias de esquemas de certificación equivalentes. Asesorar al organismo de certificación en la evolución de sus procedimientos y asesorar al organismo la identificación de esquemas.

Por finalizar, se explicará todas en esta orden se explican todas las pautas respecto a las visitas de laboratorio, como para la acreditación de laboratorio homologado con su correspondiente sello de calidad.

8. Orden ESS/775/2014,

De 7 de mayo, por la que se crea el Comité de Seguridad de los Sistemas de Información de la Seguridad Social

El objetivo es aplicar las obligaciones de la Directiva NIS a entidades críticas para asegurar su infraestructura digital.

Estructura legal destacada:

- **Cap. I (Art. 1-2):** Define operadores esenciales (OSE) y servicios digitales, establece ámbito de aplicación.
- **Cap. II (Art. 3-9):** Obliga a adoptar medidas técnicas y organizativas (gestión de riesgos, seguridad por diseño, etc.).
- **Cap. III (Art. 10-14):** Regula la notificación de incidentes al CSIRT.
- **Cap. IV (Art. 15-19):** Establece la obligación de auditorías de seguridad periódicas (mínimo cada 2 años).
- **Cap. V (Art. 20-22):** Impulsa la cooperación nacional e internacional.
- **Punto clave:** Refuerza el control de seguridad en sectores estratégicos (energía, sanidad, transporte, etc.).

9. Orden TES/369/2023,

De 10 de abril, por la que se aprueba la Política de Seguridad de la Información y de los Servicios en el ámbito de la administración digital del Ministerio de Trabajo y Economía Social y se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Departamento

El objetivo es proteger las redes y servicios frente a incidentes que afecten a su integridad, disponibilidad y confidencialidad.

Estructura legal destacada:

- **Título VII (Art. 95-100):** Seguridad
    - **Art. 95:** Obligación de aplicar medidas proporcionadas al riesgo.
    - **Art. 96:** Evaluación y gestión de riesgos.
    - **Art. 97:** Notificación de incidentes relevantes al Ministerio.
    - **Art. 100:** Facultad del Gobierno para intervenir por razones de seguridad nacional.
- **Punto clave:** Integra la seguridad cibernética como pilar obligatorio en todos los operadores de redes y servicios.

10. 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

El objetivo es garantizar un nivel adecuado de protección en los sistemas de las administraciones públicas y sector privado que presta servicios públicos.

Estructura legal destacada:**Cap. I (Art. 1-5):** Define principios básicos como seguridad por defecto, prevención y vigilancia continua.

- **Cap. II (Art. 6-10):** Establece requisitos mínimos: autenticación robusta, control de accesos, continuidad del servicio, cifrado, etc.
- **Cap. IV (Art. 12):** Obliga a auditorías periódicas de seguridad.
- **Cap. V (Art. 13-14):** Detalla cómo validar el cumplimiento del ENS (certificaciones, declaraciones responsables).
- **Punto clave:** Mejora la ciberresiliencia del sector público y privado, ajustándose al marco europeo.

11. Real Decreto-ley 12/2018,

De 7 de septiembre, de seguridad de las redes y sistemas de información

El objetivo es evitar la discriminación, también en el acceso digital a servicios, inteligencia artificial, algoritmos y plataformas.

Estructura legal destacada:

- **Título I (Art. 1-8):** Reconocimiento del derecho a no sufrir discriminación por ningún motivo.
- **Título II (Art. 9-16):** Medidas activas para fomentar la igualdad en el uso de tecnología y servicios digitales.
- **Título III (Art. 17-32):** Establece procedimientos para denunciar discriminaciones digitales.
- **Título IV (Art. 33-37):** Crea una autoridad independiente que supervisa estos derechos.
- **Punto clave:** Relaciona el derecho a la ciberseguridad con el respeto a la igualdad en entornos tecnológicos y digitales.

12. Real Decreto 43/2021, de 26 de enero,

Por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

Desarrolla reglamentariamente el RDL 12/2018, que traspuso la Directiva NIS (UE 2016/1148) sobre seguridad de redes y sistemas de información.

Establece el marco estratégico e institucional, las obligaciones de seguridad de los Operadores de Servicios Esenciales (OSE) y Proveedores de Servicios Digitales (PSD), y la gestión y notificación de ciberincidentes.

- **Capítulo II. Autoridades y coordinación (arts. 3–5)**
  Designa autoridades competentes por sector (transporte, energía, salud, alimentación, etc.) para supervisión y coordinación.

Regula la cooperación entre CSIRT de referencia, Autoridad Nacional (Consejo de Seguridad Nacional) y punto de contacto único para intercambio transfronterizo.

- **Capítulo III. Requisitos de seguridad (arts. 6–7)**
  OSE/PSD deben implantar políticas integrales de seguridad (gestión de riesgos, medidas organizativas y técnicas, continuidad, registro de actividad…).
  Deben documentar sus medidas en una "Declaración de aplicabilidad" firmada por el Responsable de Seguridad de la Información, revisable cada 3 años.
  Designación y funciones del Responsable de Seguridad de la Información (coordinación con CSIRT, notificación de incidentes, elaboración de políticas…).
- **Capítulo IV. Gestión y notificación de incidentes (arts. 8–11)**
  Obligación de gestionar internamente y, según niveles de impacto/peligrosidad (anexo), notificar a CSIRT y autoridades a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.
    - **Plazos:** notificación inicial "inmediata" (según nivel), intermedias y final (20 días para críticos; 40 días para muy altos).

  Detalla contenidos mínimos de notificación (fecha, descripción, taxonomía, impacto, plan de acción, etc.).
- **Capítulo V. Supervisión (art. 15)**
  Autoridades competentes pueden inspeccionar, recabar auditorías externas y colaborar con CSIRT para verificar cumplimiento de obligaciones de seguridad y notificación.

13. Ley 11/2002, de 6 de mayo, Reguladora del Centro Nacional de Inteligencia

- **Naturaleza y misión (arts. 1–2)**

Crea el CNI (antes Centro Superior de Información de la Defensa) como organismo especial adscrito a Defensa.
Su misión es obtener y analizar información para prevenir riesgos a la independencia, integridad territorial, intereses nacionales y estabilidad del Estado de derecho.

- **Organización (arts. 6–10)**

La Comisión Delegada del Gobierno para Asuntos de Inteligencia (VP, Exteriores, Defensa, Interior, Economía, Presidencia, Dirección del CNI) fija y supervisa objetivos.
Estructura: Secretario de Estado Director (rango Secretario de Estado, nombrado por RD, mandato 5 años), Secretaría General (rango Subsecretario) y unidades operativas.

- **Control y coordinación (arts. 3, 11–12)**

Coordinación con otros servicios de inteligencia y CSIRT.
Control parlamentario: la Comisión de gastos reservados del Congreso conoce objetivos e informe anual—sesiones secretas.

- **Control judicial previo (remite a la Ley Orgánica 2/2002)**

Sobre medidas que afecten a derechos fundamentales (domicilio, comunicaciones).

14. Ley Orgánica 2/2002,
De 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia

Autoridad judicial competente

Designa un Magistrado del TS (Sala 2ª o 3ª) para autorizar, a petición del Director del CNI, intervenciones que afecten a la inviolabilidad del domicilio y secreto de comunicaciones.

Procedimiento (art. 1)

Solicitud motivada (qué, por qué, a quién, duración).

Plazo de resolución: 72 h (o 24 h en urgencia).

Reserva secreta de la resolución.

Obligación de destruir la información obtenida que no guarde relación con el fin autorizado.

15. Ley 9/1968, de 5 de abril,
Sobre secretos oficiales

- **Objeto y ámbito (arts. 1–3)**

Regula la clasificación y protección de "materias clasificadas" cuya divulgación perjudique la seguridad del Estado.

Categorías: Secreto (máxima protección) y Reservado.

- **Competencia y procedimiento (arts. 4–10)**

Solo Consejo de Ministros y Junta de Jefes de Estado Mayor pueden clasificar; no delegable.

Debe notificarse a medios si puede trascender; documentos llevan marca de clasificación.

Excepción: Congreso y Senado siempre tienen acceso, incluso en sesión secreta.

- **Obligaciones y sanciones (arts. 8–14)**

Prohibición de acceso, copia o difusión por no autorizados; obligación de entrega a la autoridad más cercana.

Personal con acceso debe cumplir medidas de custodia, traslado, archivo y destrucción que se desarrollarán reglamentariamente.

Incumplimientos: responsabilidad penal (Código Penal) y disciplinaria (falta muy grave).

16. Decreto 242/1969,
De 20 de febrero, por el que se desarrollan las disposiciones de la Ley 9/1968, de 5 de abril sobre Secretos Oficiales

Un secreto oficial son informaciones o documentos cuyo conocimiento por personas no autorizadas podría perjudicar la seguridad del Estado. Este Decreto establece las reglas prácticas para proteger esa información clasificada.

Clasificación de la información:

- Se determinan los niveles de clasificación "reservado" y "secreto".
- Se consideran clasificables no solo documentos escritos, sino también planos, grabaciones, mapas, etc.

Definiciones:

- **Asunto:** Tema relacionado con materias de defensa, política exterior, seguridad, etc.

- **Acto:** Toda acción o decisión oficial relacionada con dichos asuntos.
- **Documento:** Toda representación gráfica, sonora o visual que contenga información clasificada.
- **Control y manejo:** Se regula cómo debe custodiarse, trasladarse y destruirse la información clasificada. Todo acceso, incluso dentro de la Administración, debe justificarse. Se crea el Servicio de Protección de Materias Clasificadas, encargado de supervisar estas tareas.
- **Responsabilidades y sanciones:** Difundir o usar información clasificada sin autorización se considera falta muy grave. Se aplican sanciones disciplinarias y, si procede, penales.
- **Adaptación internacional:** Se inspira en normativas de países industrializados, para homogeneizar los estándares de protección de secretos.
- **Disposiciones especiales**: Las Fuerzas Armadas y el servicio diplomático pueden establecer normativas internas adicionales para adaptarse a sus funciones específicas.

17. Ley Orgánica 4/1981,
De 1 de junio, de los estados de alarma, excepción y sitio

Estado excepcional son situaciones extraordinarias en las que el Estado puede limitar ciertos derechos y libertades para restaurar la normalidad, siempre dentro del marco constitucional.

Tres tipos de estado:

1. **Estado de alarma:**

Causas: catástrofes, epidemias, paralización de servicios esenciales, desabastecimiento.
Duración: hasta 15 días, prorrogables con autorización del Congreso.
Afecta: circulación, abastecimiento, servicios esenciales, etc.

2. **Estado de excepción:**

Causas: alteración grave del orden público.
Competencia: el Gobierno, con autorización previa del Congreso.
Permite suspender ciertos derechos fundamentales (manifestación, expresión, etc.).
Las medidas deben ser estrictamente necesarias y proporcionadas.

3. **Estado de sitio:**

Causas: insurrección o acto que amenace gravemente la soberanía nacional o el orden constitucional.
Competencia: el Congreso lo declara a propuesta del Gobierno.
Se otorgan poderes extraordinarios a la Autoridad Militar.
El Congreso puede decidir qué delitos pasan a la jurisdicción militar.

Otras características comunes:

Las decisiones deben publicarse de inmediato en el Boletín Oficial del Estado.
Los poderes públicos siguen funcionando con normalidad.
Los actos administrativos durante estos estados pueden impugnarse judicialmente.
Prohibición del abuso de poder: las medidas deben cesar una vez finaliza el estado excepcional.

18. Ley 1/2019, de 20 de febrero,
De Secretos Empresariales

Secreto empresarial es cualquier información valiosa para una empresa (como fórmulas, estrategias, algoritmos o listas de clientes) que no sea conocida públicamente y que la empresa haya protegido razonablemente.

- **Ámbitos protegidos:**

Conocimientos técnicos o científicos.
Datos sobre proveedores, clientes, estrategias de mercado o de negocio.
Información organizativa o financiera confidencial.
Protección frente a conductas ilícitas:

- **Prohíbe acciones como:**

Robo, espionaje o hackeo.
Incumplimiento de acuerdos de confidencialidad.
Copia no autorizada de documentos internos.

- **Medidas judiciales disponibles:**

Una empresa víctima de uso indebido de su secreto puede solicitar:
Indemnizaciones económicas.
Medidas cautelares, como la paralización del uso del secreto o la destrucción del material ilegalmente obtenido.
Confidencialidad durante el juicio, para no agravar la exposición del secreto.

- **Relación con otras leyes:**

Modifica la Ley de Competencia Desleal: toda violación de secreto empresarial se considera conducta desleal.
Alinea el derecho español con la Directiva (UE) 2016/943, armonizando la protección de secretos en toda la UE.

- **Importancia práctica:**

Esta ley refuerza el derecho de las empresas a innovar y competir sin temor al espionaje o uso indebido de su know-how, especialmente en un entorno digitalizado y globalizado.

19. Orden PCI/487/2019, de 26 de abril,
Por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional

La Orden PCI/487/2019, de 26 de abril, publica oficialmente la Estrategia Nacional de Ciberseguridad 2019 de España, que fue aprobada por el Consejo de Seguridad Nacional. Esta estrategia establece el marco general para proteger los derechos y libertades de los ciudadanos, garantizar la seguridad nacional en el ciberespacio y asegurar el funcionamiento de servicios esenciales e infraestructuras críticas frente a amenazas y ataques cibernéticos.
Sus principales objetivos son:

- Fortalecer las capacidades de prevención, detección y respuesta a ciberataques.

- Fomentar la cooperación público-privada y la coordinación entre organismos nacionales e internacionales.
- Impulsar una cultura de ciberseguridad en la sociedad.
- Promover la resiliencia tecnológica e industrial del país.
- Mejorar la protección de las infraestructuras críticas.
- Garantizar un marco normativo y legal actualizado y adecuado a las amenazas actuales.

20. Real Decreto 1150/2021,
De 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021

1. Objetivos Estratégicos
    - Protección del ciberespacio nacional: Garantizar la seguridad de infraestructuras críticas y servicios esenciales.
    - Fortalecimiento de capacidades: Desarrollar habilidades y recursos en ciberseguridad.
    - Colaboración público-privada: Fomentar la cooperación entre sectores para una respuesta eficaz ante amenazas.
2. Principios Rectores
    - Enfoque integral: Abordar la ciberseguridad desde múltiples dimensiones (tecnológica, organizativa, legal).
    - Resiliencia: Capacidad de anticipación, resistencia y recuperación ante incidentes cibernéticos.
    - Adaptabilidad: Actualización continua frente a la evolución de amenazas y tecnologías.
3. Líneas de Acción
    - Desarrollo normativo: Implementación de leyes y regulaciones específicas en ciberseguridad.
    - Educación y concienciación: Programas formativos para ciudadanos y profesionales.
    - Cooperación internacional: Participación en iniciativas y organismos globales de ciberseguridad.
4. Estructura de Gobernanza
    - Consejo de Seguridad Nacional: Órgano principal de coordinación y supervisión.
    - Comités especializados: Grupos de trabajo centrados en áreas específicas de ciberseguridad.
    - Centros de respuesta a incidentes: Entidades encargadas de gestionar y mitigar ciberataques.
5. Evaluación y Seguimiento
    - Indicadores de rendimiento: Métricas para medir la eficacia de las acciones implementadas.
    - Revisión periódica: Actualización de la estrategia en función de nuevos desafíos y avances tecnológicos.

21. Orden ISM/1320/2024,

De 18 de noviembre, por la que se aprueba la Política de Seguridad de la Información del Ministerio de Inclusión, Seguridad Social y Migraciones y se crea el Comité de Seguridad de los Sistemas de Información

Política de Seguridad de la Información (PSI) sus objetivos principales es proteger la confidencialidad, integridad y disponibilidad de la información gestionada por el Ministerio.

Cumplir con las normativas vigentes en materia de protección de datos y seguridad de la información.

- **Marco Normativo:**

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

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

Reglamento (UE) 2016/679, General de Protección de Datos (RGPD).

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

- **Principios Rectores**

Proporcionalidad: Las medidas de seguridad deben ser proporcionales a los riesgos identificados.

Mejora continua: Revisión y actualización periódica de las medidas de seguridad para adaptarse a la evolución de los riesgos y tecnologías.

- **Ámbito de Aplicación**

Obligatorio para todo el personal del Ministerio, incluyendo órganos superiores y directivos, así como organismos adscritos y dependientes.

Comité de Seguridad de los Sistemas de Información (CSSI)

- **Funciones Principales**

Coordinar las actividades relacionadas con la seguridad de los sistemas de información del Ministerio.

Aprobar y supervisar las normas y procedimientos en materia de seguridad de la información.

Establecer criterios comunes de actuación en todos los órganos del Ministerio para el cumplimiento de las normas de seguridad.

Revisar el estado global de la seguridad en cada uno de los órganos superiores y directivos del Ministerio.

Promover la concienciación y formación en materia de seguridad para el personal del Ministerio.

22. Ley 8/2011, de 28 de abril,

Por la que se establecen medidas para la protección de las infraestructuras críticas

1. Objeto y Finalidad

Establecer estrategias y estructuras para coordinar las acciones de las Administraciones Públicas en la protección de infraestructuras críticas.

Mejorar la prevención, preparación y respuesta frente a amenazas que puedan afectar a estas infraestructuras.

2. Definiciones Clave

Infraestructura Crítica: Instalaciones, redes, sistemas o equipos físicos y tecnológicos cuya interrupción o destrucción tendría un impacto significativo en la seguridad nacional, la salud, el bienestar económico o el funcionamiento efectivo del Estado.

Operador Crítico: Entidad pública o privada responsable de una infraestructura crítica.

3. Sistema de Protección de Infraestructuras Críticas (SPIC)

Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC): Órgano encargado de coordinar y supervisar las actividades relacionadas con la protección de infraestructuras críticas.

Comisión Nacional para la Protección de las Infraestructuras Críticas: Órgano colegiado que asesora y apoya al CNPIC en la elaboración de políticas y estrategias.

4. Instrumentos de Planificación

Plan Nacional de Protección de las Infraestructuras Críticas (PNPIC): Documento que establece las directrices generales para la protección de infraestructuras críticas a nivel nacional.

Planes Estratégicos Sectoriales (PES): Desarrollados por sectores específicos para identificar y proteger infraestructuras críticas dentro de su ámbito.

Planes de Seguridad del Operador (PSO): Elaborados por cada operador crítico para detallar las medidas de seguridad aplicables a sus infraestructuras.

Planes de Protección Específicos (PPE): Planes detallados para cada infraestructura crítica, basados en los PSO.

5. Obligaciones de los Operadores Críticos

Designar un Responsable de Seguridad y Enlace con el CNPIC.

Elaborar y mantener actualizados los PSO y PPE.

Colaborar con las autoridades en la implementación de medidas de protección y en la gestión de incidentes

6. Ámbito de Aplicación

Aplica a infraestructuras críticas ubicadas en territorio español, tanto públicas como privadas, que prestan servicios esenciales en sectores como energía, transporte, agua, salud, tecnologías de la información, entre otros.

7. Colaboración Internacional

Promueve la cooperación con otros Estados y organizaciones internacionales para la protección de infraestructuras críticas transnacionales.

23. Real Decreto 704/2011, de 20 de mayo,

Por el que se aprueba el Reglamento de protección de las infraestructuras críticas

1. Objeto y Ámbito de Aplicación

Objeto: Desarrollar el marco previsto en la Ley 8/2011, concretando las actuaciones de los órganos del Sistema de Protección de Infraestructuras Críticas y los instrumentos de planificación correspondientes.
Ámbito de aplicación: Infraestructuras críticas ubicadas en territorio español, tanto públicas como privadas, que prestan servicios esenciales para la sociedad.

2. Catálogo Nacional de Infraestructuras Estratégicas (CNIE)

Definición: Registro administrativo que contiene información completa y actualizada de todas las infraestructuras estratégicas en España, incluyendo las críticas y las críticas europeas que afecten al país.
Finalidad: Gestionar datos para diseñar mecanismos de planificación, prevención, protección y reacción ante amenazas.
Contenido: Descripción, ubicación, titularidad, servicios prestados, nivel de seguridad requerido y otra información relevante.

3. Sistema de Protección de Infraestructuras Críticas (SPIC)

Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC):
Órgano dependiente de la Secretaría de Estado de Seguridad.
Funciones: asistencia en ejecución de funciones, mantenimiento del Plan Nacional de Protección, determinación de criticidad, coordinación de análisis de riesgos, recopilación y análisis de información, participación en ejercicios y simulacros, y coordinación con organismos internacionales.

- Comisión Nacional para la Protección de las Infraestructuras Críticas:

Presidida por el Secretario de Estado de Seguridad.
Funciones: promover la cultura de seguridad, aplicación efectiva de la Ley 8/2011, aprobación de Planes Estratégicos Sectoriales, designación de operadores críticos y creación de grupos de trabajo.

- Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas:

Participación de representantes de distintos ministerios y organismos.
Funciones: elaboración y revisión de Planes Estratégicos Sectoriales, verificación del cumplimiento de planes, asesoramiento técnico y colaboración en acciones derivadas del cumplimiento de la Directiva 2008/114/CE.

4. Instrumentos de Planificación

Plan Nacional de Protección de las Infraestructuras Críticas (PNPIC):
Instrumento de programación del Estado para mantener seguras las infraestructuras que proporcionan servicios esenciales.
Establece criterios y directrices para movilizar capacidades operativas y medidas preventivas.
Revisión cada cinco años o cuando se modifiquen datos o instrucciones relevantes.
Planes Estratégicos Sectoriales (PES):
Instrumentos de estudio y planificación para conocer los servicios esenciales proporcionados en cada sector, su funcionamiento, vulnerabilidades y medidas estratégicas necesarias.
Planes de Seguridad del Operador (PSO):

Documentos elaborados por operadores críticos que detallan las medidas de seguridad aplicables a sus infraestructuras.
Incluyen análisis de riesgos, medidas preventivas y protocolos de actuación.
Planes de Protección Específicos (PPE):
Planes detallados para cada infraestructura crítica, basados en los PSO.
Definen medidas concretas para garantizar la seguridad integral de las infraestructuras.

5. Designación de Operadores Críticos

Una empresa u organismo es designado como operador crítico si al menos una de sus infraestructuras es considerada crítica.
El CNPIC elabora una propuesta de resolución y la notifica al titular o administrador correspondiente.

6. Interlocución con Operadores Críticos

Sector Privado: El CNPIC actúa como punto directo de interlocución con la Secretaría de Estado de Seguridad.
Sector Público: El órgano competente de la Administración puede constituirse en interlocutor con el Ministerio del Interior a través del CNPIC.

7. Colaboración y Coordinación Territorial

Delegaciones del Gobierno en Comunidades Autónomas y Ciudades con Estatuto de Autonomía:
Coordinan la actuación de las Fuerzas y Cuerpos de Seguridad del Estado ante alertas de seguridad.
Colaboran con otros órganos y organismos públicos en acciones para el cumplimiento de los Planes Sectoriales.

24. Resolución de 8 de septiembre de 2015, De la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos

Resolución de 8 de septiembre de 2015 (Contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos)
Finalidad: Homogeneizar los requisitos de seguridad que deben cumplir los operadores críticos para proteger las infraestructuras estratégicas.

- **Planes de Seguridad del Operador (PSO):**

Incluyen un análisis de los servicios esenciales prestados, identificación de activos críticos y los riesgos asociados.
Deben contener políticas de gobierno de la seguridad, programas de formación y concienciación, y mecanismos de coordinación con autoridades públicas.
Prevé la implantación de medidas técnicas, organizativas y físicas específicas según riesgos detectados.

- **Planes de Protección Específicos (PPE):**

Son planes derivados, más concretos y adaptados a infraestructuras específicas.
Deben realizar un análisis de vulnerabilidades particulares y establecer protocolos de respuesta ante incidentes.
Importante: El cumplimiento de estos planes es obligatorio para operadores críticos designados según la legislación de protección de infraestructuras.

25. Orden INT/859/2023, de 21 de julio,

Por la que se desarrolla la estructura orgánica y funciones de los servicios centrales y territoriales de la Dirección General de la Policía. [Inclusión parcial]

Orden INT/859/2023 (Estructura y funciones de la Dirección General de la Policía)

Propósito: Adaptar la estructura de la Policía Nacional a los nuevos desafíos de seguridad, como el cibercrimen, terrorismo internacional o delincuencia organizada.

- Organización Central:

La Dirección General se estructura en comisarías generales especializadas (Judicial, Información, Científica, Seguridad Ciudadana, etc.).

Se refuerzan unidades clave como ciberseguridad y lucha antiterrorista.

- Unidades Territoriales:

Las jefaturas superiores, comisarías provinciales, locales y de distrito dependen funcionalmente de los órganos centrales.

- Funciones:

Prevención y persecución del delito, protección de altas personalidades, control de fronteras, extranjería y cooperación internacional.

Se establecen competencias claras para cada comisaría, mejorando la coordinación.

26. Ley Orgánica 4/2015,

De 30 de marzo, de protección de la seguridad ciudadana

Ley Orgánica 4/2015 (Protección de la Seguridad Ciudadana)

Objeto: Proteger la convivencia ciudadana y asegurar el ejercicio pacífico de los derechos fundamentales.

- Aspectos principales:

Identificación: La policía puede requerir la identificación en casos de prevención de delitos o alteraciones de seguridad.

Espacios Públicos: Regula el uso de videocámaras fijas y móviles para preservar la seguridad, con garantías de respeto a los derechos fundamentales.

- Manifestaciones y Reuniones:

Se regulan notificaciones previas y la actuación policial ante alteraciones del orden público.

Se sanciona la resistencia a la autoridad o desórdenes públicos.

Catálogo de Infracciones:

Clasificación en muy graves, graves y leves, con sanciones que van desde advertencias hasta multas económicas considerables.

Críticas:

Algunos sectores sociales y políticos la consideran restrictiva de libertades públicas.

27. Ley 5/2014, de 4 de abril,
De Seguridad Privada

Ley 5/2014(Ley de Seguridad Privada)

Objetivo: Reconocer la seguridad privada como complemento esencial de la seguridad pública y regular detalladamente.

- Aspectos clave:

Ámbito de actuación:
Empresas de seguridad (vigilancia, transporte de fondos, protección de bienes).
Detectives privados y servicios de investigación.
Servicios de videovigilancia y sistemas de alarmas.

- Personal:

Exige formación específica, habilitación profesional, acreditaciones, y respeto estricto a los derechos fundamentales.
Refuerza la profesionalización y el control de las actividades de seguridad privada.
Colaboración público-privada:
Se obliga a los profesionales de seguridad privada a cooperar activamente con las Fuerzas y Cuerpos de Seguridad del Estado.

- Control e Inspección:

Inspecciones periódicas, registros administrativos obligatorios y un régimen sancionador proporcional a las infracciones cometidas.

- Impacto:

Reforzamiento de la vigilancia en espacios privados de uso público (centros comerciales, eventos, infraestructuras críticas).

28. Real Decreto 2364/1994,
De 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada

- Objeto y ámbito del reglamento

Regula el funcionamiento de las empresas y el personal de seguridad privada en España.
Desarrolla la Ley 23/1992 y la Ley Orgánica 1/1992.
Distingue competencias del Estado (habilitación armada, ámbito nacional) y Comunidades Autónomas (autorización, inspección y sanción a nivel autonómico).

- Actividades autorizadas

Las empresas pueden:
Vigilar personas, bienes y eventos.
Transportar y custodiar dinero, valores y explosivos.
Instalar y mantener sistemas de seguridad (alarmas, CCTV).
Asesorar en materia de seguridad (no fabricar ni comercializar).

- Autorización y requisitos

Autorización en tres fases: documentación legal, medios/técnicos, garantías y personal.
Obligación de estar inscritas en el Registro del Ministerio del Interior.

Necesario jefe de seguridad, seguro de responsabilidad civil y garantía financiera.
Subcontratación permitida sólo con empresas autorizadas.

- Colaboración con fuerzas de seguridad

Obligación de informar sobre delitos, altas/bajas de personal y servicios especiales.
Coordinar servicios con la policía y Guardia Civil.
Los contratos y servicios deben notificarse con antelación.

- Armas y uso

Solo determinadas actividades pueden usar armas (transporte de valores, escoltas, vigilancia armada).
Las armas deben estar registradas y custodiadas en armeros.
Pruebas de tiro y psicotécnicas obligatorias y periódicas.

- Personal de seguridad

Incluye vigilantes, escoltas, guardas del campo, jefes y detectives.
Requisitos: mayor de edad, sin antecedentes, formación y habilitación profesional.
Formación inicial y continua obligatoria, en centros autorizados.

- Obligaciones operativas

Evaluar riesgos antes de prestar servicios.
Comunicación con personal operativo.
Registro de actividades, contratos y revisiones en libros-registro.
Cumplir requisitos técnicos de instalación y mantenimiento.

- Servicios técnicos

Solo empresas autorizadas pueden instalar sistemas de seguridad.
Prohibido conectar directamente a las Fuerzas de Seguridad.
Centrales de alarmas: verificación previa, registro de alarmas, respuesta con vigilantes si aplica.

- Departamentos de seguridad

Obligatorios en empresas con 24 vigilantes o servicios de alto riesgo.
Funciones: planificación, coordinación con policía, control de armas y formación.
Director de seguridad: enlace con autoridades.

- Control e inspección

Competencia del Ministerio del Interior y Gobiernos Civiles.
Revisión de documentación, armas y servicios.
Inspecciones rutinarias y por denuncia.
Informes y memorias anuales obligatorias.

- Infracciones y sanciones

Clasificadas en:

  - Muy graves: operar sin autorización, uso indebido de armas, revelar información confidencial.
  - Graves: falta de formación, personal sin habilitación, uso de sistemas no homologados.
  - Leves: fallos administrativos, documentación incompleta.
  - Sanciones: desde multas hasta cierre de la empresa o cancelación de habilitaciones.

29. Ley 34/2002, de 11 de julio,

De servicios de la sociedad de la información y de comercio electrónico. [Inclusión parcial]

La Ley 34/2002 (modificada en 2025) establece obligaciones para proveedores de servicios, registros de dominio y entidades públicas en España para colaborar con el CERT (equipo de respuesta a ciberseguridad) en la gestión de incidentes en Internet.

Puntos clave:

- Colaboración obligatoria: Proveedores y entidades públicas deben ayudar al CERT, compartiendo información (como direcciones IP comprometidas) y siguiendo recomendaciones de seguridad.
- Códigos de conducta: El Gobierno creará normas para una cooperación público-privada, con medidas para prevenir y mitigar ataques.
- Acción contra usuarios negligentes: Si un usuario no soluciona un incidente en el plazo indicado, los proveedores deben aislar el equipo o servicio afectado.
- Coordinación institucional: Se garantiza el intercambio de información entre la Secretaría de Telecomunicaciones y la de Seguridad para una respuesta coordinada.

Objetivo: Garantizar una gestión eficaz de ciber incidentes y proteger a usuarios y terceros en España.

30. Real Decreto 421/2004,

De 12 de marzo, por el que se regula el Centro Criptológico Nacional

El objeto es regular el Centro Criptológico Nacional (CCN), adscrito al Centro Nacional de Inteligencia (CNI), para garantizar la seguridad de la información y sistemas tecnológicos de la Administración.

Motivación:

- Necesidad de proteger información sensible y sistemas ante amenazas cibernéticas.
- Coordinar adquisición de material criptológico, homologación y formación especializada.
- Garantizar confidencialidad, integridad y disponibilidad de la información clasificada.

Funciones del CCN:

- Elaborar normas y recomendaciones de seguridad TIC.
- Formar a personal en ciberseguridad.
- Certificar productos/sistemas de cifrado.
- Evaluar tecnologías de seguridad.
- Velar por el cumplimiento de la normativa de información clasificada.
- Cooperar con organismos internacionales afines.

Director del CCN:

- Lo dirige el Secretario de Estado Director del CNI.
- Actúa como autoridad de certificación en seguridad TIC y criptología.
- Ámbito: Sistemas que procesan, almacenan o transmiten información protegida o clasificada.
- Entrada en vigor: Al día siguiente de su publicación en el BOE (20/03/2004).

31. Real Decreto 521/2020, de 19 de mayo,

Por el que se establece la organización básica de las Fuerzas Armadas. [Inclusión parcial]

Título II: Estructura operativa de las Fuerzas Armadas

Capítulo II: El Estado Mayor de la Defensa (EMAD)

El EMAD es el órgano que apoya al Jefe de Estado Mayor de la Defensa (JEMAD) en funciones estratégicas y operativas.

Funciones principales:

- Desarrollo de políticas de seguridad de la información y telecomunicaciones en las Fuerzas Armadas.
- Apoyo al JEMAD en la Infraestructura de Información para la Defensa y en la supervivencia de sistemas críticos.
- Planificación y dirección de la información geoespacial en su ámbito.
- Dirección y coordinación de la sanidad operativa.

Estructura del EMAD:

- Cuartel General.
- Mando de Operaciones.
- Centro de Inteligencia de las Fuerzas Armadas (CIFAS).
- Mando Conjunto del Ciberespacio.
- Centro Superior de Estudios de la Defensa Nacional (CESEDEN).
- Organizaciones operativas permanentes y órganos militares vinculados a organizaciones internacionales.

Capítulo IV: Órganos del EMAD

Mando Conjunto del Ciberespacio: Responsable de garantizar la libertad de acción de las Fuerzas Armadas en el ciberespacio.

Funciones:

- Planificación y ejecución de operaciones militares en el ciberespacio.
- Protección de infraestructuras críticas (físicas, lógicas y virtuales) para la Defensa.

32. Orden DEF/710/2020, de 27 de julio,

Por la que se desarrolla la organización básica del Estado Mayor de la Defensa. [Inclusión parcial]

El objeto es regular la organización básica del Estado Mayor de la Defensa, centrándose en el papel del Mando Conjunto del Ciberespacio, elemento esencial en la estrategia de defensa nacional.

Estructura y contenido:

- **Artículo 13: Define y estructura el Mando Conjunto del Ciberespacio como responsable de:**

Ejecutar operaciones militares en el ciberespacio.

Defender redes, sistemas, servicios y recursos digitales de las Fuerzas Armadas.

Coordinar el planeamiento operativo de ciberdefensa en contextos nacionales y de coalición.

Funciones específicas del Comandante del Mando Conjunto (Disposición adicional segunda):

Dirigir operativamente los Centros de Operaciones de Seguridad (COS) de los Ejércitos.

Coordinar con el CESTIC (Centro de Sistemas y Tecnologías de la Información y las Comunicaciones).
Supervisar la preparación y disponibilidad del personal ciberdefensivo.
Garantizar la coherencia de la actividad ciber con el resto de capacidades operativas (como el espectro electromagnético).

Escuela Militar del Ciberespacio (EMCO):

Encargada de la formación especializada en operaciones cibernéticas.
Vinculada al CESEDEN para definir currículo, convocatorias, criterios y perfiles docentes.
Esta orden marca la formalización del ámbito militar del ciberespacio como dominio de operaciones, integrando la ciberdefensa en la estructura militar permanente.

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

El objeto del Art. 1 es establecer el marco jurídico de los servicios de la sociedad de la información (páginas web, comercio electrónico, comunicaciones electrónicas comerciales) y definir la responsabilidad de los intermediarios.
Estructura y artículos clave:

- **TÍTULO I – Disposiciones generales:**

Art. 2–4: Ámbito territorial, principios de coordinación con otras normas.

- **TÍTULO II – Obligaciones de los prestadores:**

Art. 5–12: Información obligatoria que debe aparecer en las webs.
Obligaciones sobre contratos electrónicos (precio, condiciones, procedimiento de contratación).
Transparencia en las comunicaciones comerciales.

- **TÍTULO III – Comunicaciones comerciales por vía electrónica:**

Art. 13–16: Se prohíbe el envío de publicidad sin consentimiento previo.
Requisitos de identificación del remitente y contenido comercial.

- **TÍTULO IV – Responsabilidad de los prestadores de servicios:**

Art. 17–23: Limita la responsabilidad de intermediarios como proveedores de hosting, buscadores, enlaces, etc.
Establece cuándo son responsables por contenidos ilegales o actividades ilícitas.

- **TÍTULO V – Solución de conflictos:**

Cap. I – Art. 30–31: Acción judicial de cesación frente a infracciones.
Cap. II – Art. 32: Posibilidad de utilizar sistemas extrajudiciales de resolución de conflictos (mediación, arbitraje).

- **TÍTULO VI – Información y control:**

Art. 33–36 bis: Supervisión administrativa.
Registro nacional de organizaciones de datos con fines altruistas (Art. 35 bis).
Deber de colaboración con la Administración.

- **TÍTULO VII – Infracciones y sanciones (Art. 37–45):**

Clasifica infracciones en leves, graves y muy graves.
Define el régimen sancionador, cuantías de multas y plazos de prescripción.

- **Disposiciones adicionales y finales:**

Fomento del uso del español en Internet.
Protección de menores.
Accesibilidad para personas con discapacidad.
Modificaciones en otras leyes (propiedad intelectual, telecomunicaciones, etc.).
Esta ley es clave en el comercio electrónico, establece derechos y obligaciones de todos los que operan en la red, y define la responsabilidad legal sobre los contenidos.

34. Real Decreto 381/2015, de 14 de mayo,
Por el que se establecen medidas contra el tráfico no permitido y el tráfico irregular con fines fraudulentos en comunicaciones electrónicas

El objeto es regular medidas contra el tráfico no permitido e irregular con fines fraudulentos en el ámbito de las comunicaciones electrónicas.
Contenido detallado:

- Art. 1 – Objeto: Luchar contra fraudes que se aprovechan del uso ilegítimo de numeraciones telefónicas, como el tráfico gris o llamadas internacionales disfrazadas.
- Art. 2 – Definiciones: Tráfico no permitido, tráfico irregular, tráfico con fines fraudulentos, spoofing.
- Art. 3 – Medidas de detección y prevención: Los operadores deben implementar sistemas para identificar y bloquear llamadas fraudulentas.
- Art. 4 – Acceso a información: La CNMC y otros órganos reguladores podrán solicitar datos para investigaciones.
- Art. 5 – Procedimientos de actuación: Se establece un protocolo de detección y reacción ante actividades sospechosas.
- Art. 6 – Obligación de bloqueo: Los operadores deberán bloquear el tráfico identificado como fraudulento.
- Art. 7 – Colaboración internacional: Se promueve cooperación con autoridades extranjeras y organismos multilaterales.
- Art. 8 – Derechos del usuario: Establece mecanismos de reclamación y reparación para los usuarios afectados.
- Art. 9 – Registro de numeraciones: La CNMC mantendrá un listado de numeraciones bloqueadas por fraude.
- Art. 10 – Régimen sancionador: Las infracciones podrán ser sancionadas conforme a la Ley General de Telecomunicaciones.

Este decreto protege al consumidor frente a llamadas o conexiones fraudulentas y obliga a los operadores a ser proactivos en la lucha contra el fraude telefónico.

35. Orden TDF/149/2025, de 12 de febrero,

Por la que se establecen medidas para combatir las estafas de suplantación de identidad a través de llamadas telefónicas y mensajes de texto fraudulentos y para garantizar la identificación de la numeración utilizada para la prestación de servicios de atención al cliente y realización de llamadas comerciales no solicitadas

El objeto es establecer medidas técnicas y regulatorias para frenar las estafas por suplantación de identidad telefónica y SMS (spoofing) y garantizar la correcta identificación de las numeraciones usadas en llamadas comerciales y atención al cliente.

Desarrollo por capítulos y artículos:

- **Capítulo I – Disposiciones generales**

Art. 1-4: Aplica a operadores y plataformas de SMS, establece definiciones y principios rectores como la trazabilidad y transparencia.

- **Capítulo II – Identificación de línea**

Art. 5-8: Prohíbe la manipulación del número visible para el receptor (caller ID), establece la obligación de verificación de identidad por parte de los operadores. Registro de intentos de suplantación detectados. Permite excepciones justificadas (por ej., líneas de emergencia).

Capítulo III – Mensajes fraudulentos

Art. 9-12: Regulación del uso de remitentes alfanuméricos (ej. "BancoX"). Exige verificación de identidad para usar remitentes personalizados. Procedimientos de denuncia ciudadana y actuación rápida.

- **Capítulo IV – Atención al cliente y llamadas comerciales**

Art. 13-15: Se establece que todas las llamadas comerciales deben provenir de numeraciones claramente identificables. Las llamadas no podrán hacerse desde números ocultos. Las líneas de atención al cliente deberán emplear numeración asignada y validada.

Disposiciones adicionales y finales:

- Se promueve la colaboración intersectorial.
- El cumplimiento será supervisado por la Secretaría de Estado de Telecomunicaciones.
- Entrada en vigor: 20 días desde su publicación.

36. Real Decreto 1163/2005, de 30 de septiembre,

Por el que se regula el distintivo público de confianza en los servicios de la sociedad de la información y de comercio electrónico, así como los requisitos y el procedimiento de concesión

Distintivo público de confianza en servicios de la sociedad de la información y comercio electrónico

Este Real Decreto crea un distintivo público oficial, voluntario, que pueden utilizar las entidades que ofrecen servicios digitales y se adhieran a un código de conducta aprobado.

Ejes principales:

- Objeto: Fortalecer la confianza del usuario en el entorno digital, mostrando que la entidad adherida cumple estándares éticos y de calidad.

- Requisitos de los códigos de conducta: Deben contener principios de protección al consumidor, transparencia, confidencialidad, y resolución de conflictos.
- Obligaciones de las entidades promotoras:
  - Supervisar el cumplimiento del código.
  - Informar sobre su contenido y alcance.
  - Contar con sistemas eficaces de reclamaciones.
- Procedimiento de concesión y retirada del distintivo: Evaluación por parte del órgano competente y posibilidad de revocación si se incumplen las condiciones.
- Control público: La Administración puede hacer inspecciones y requerir informes sobre el funcionamiento del código.

Este distintivo tiene un diseño gráfico propio y debe colocarse en sitios web de forma visible, transmitiendo confianza al consumidor digital.

37. Real Decreto 203/2021, de 30 de marzo,
Por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos

Reglamento de actuación del sector público por medios electrónicos.

Este reglamento desarrolla la Ley 39/2015 y regula cómo deben actuar las administraciones públicas en el entorno digital, garantizando derechos digitales de ciudadanos y empresas.

Contenido relevante:

- Identificación y firma electrónica: Determina qué medios de autenticación son válidos (certificados cualificados, sistemas de clave concertada, etc.).
- Sedes electrónicas y portales: Toda administración debe tener sede electrónica propia, segura y accesible, donde se publiquen servicios e información oficial.
- Expediente administrativo electrónico: Incluye normas sobre creación, archivo, acceso, trazabilidad y conservación digital de documentos.
- Notificaciones electrónicas: Regula cómo se notifican electrónicamente los actos administrativos.
- Colaboración interadministrativa: Fomenta la interoperabilidad entre administraciones para compartir tecnologías y simplificar trámites.

Este decreto supone un avance clave en la digitalización de la administración y busca eficiencia, transparencia y accesibilidad universal.

38. Ley 6/2020, de 11 de noviembre,
Reguladora de determinados aspectos de los servicios electrónicos de confianza

Reguladora de determinados aspectos de los servicios electrónicos de confianza.

Complementa el Reglamento eIDAS de la UE, que establece las bases para la identificación electrónica y los servicios de confianza, como la firma digital.

Aspectos principales:

- Ámbito de aplicación: Abarca la regulación nacional de los servicios electrónicos de confianza no armonizados directamente por el reglamento europeo.

- Prestadores de servicios de confianza: Se regulan sus obligaciones, registro, auditorías, y condiciones técnicas, especialmente si son prestadores cualificados.
- Tipos de servicios regulados:
- Firma electrónica (simple, avanzada, cualificada).
- Sellos electrónicos y de tiempo
- Servicios de entrega electrónica certificada
- Certificados de autenticación de sitios web
- Supervisión y sanciones: Establece la figura de supervisión (normalmente el Ministerio competente) y un régimen sancionador para incumplimientos.

Esta ley garantiza la seguridad jurídica y técnica en las transacciones electrónicas, fomentando la confianza en los entornos digitales tanto públicos como privados.

39. Ley 9/2014, de 9 de mayo,
General de Telecomunicaciones. [Inclusión parcial]

Ley General de Telecomunicaciones

Aunque fue parcialmente derogada por la Ley 11/2022, esta norma fue fundamental para liberalizar y modernizar el sector de las telecomunicaciones.

Claves principales:

- Objetivos: Facilitar el despliegue de redes, eliminar barreras administrativas, y fomentar la inversión en infraestructuras de banda ancha.
- Dominio público radioeléctrico: Se regula como bien de dominio público estatal, garantizando acceso flexible y eficiente a los operadores.
- Acceso universal: Garantiza que todos los ciudadanos puedan acceder a servicios de calidad, en línea con la Agenda Digital para Europa (acceso de al menos 30 Mbps).
- Reducción de costes de despliegue: Se incorporan medidas para compartir infraestructuras y reducir obstáculos urbanísticos.
- Seguridad y colaboración: Obliga a los operadores a colaborar con la Administración en situaciones de seguridad y emergencia.

A pesar de su derogación parcial, la ley consolidó principios clave que todavía son aplicados en la regulación actual del sector.

40. Ley 11/2022, de 28 de junio,
General de Telecomunicaciones

Establece el marco regulador para las telecomunicaciones en España refuerza el despliegue de redes y servicios asegurando la libre competencia obliga a operadores a mantener la seguridad de las redes y notificar violaciones de datos personales.

Aplica el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018.

Se remite a la Ley 25/2007 en materia de conservación y cesión de datos a autoridades.

Estructura y puntos clave:

- **Título I – Disposiciones Generales**

Art. 1-4: Define el objeto, ámbito, principios y servicios esenciales (defensa, seguridad, protección civil).
Título II – Redes y Servicios en Régimen de Libre Competencia
Art. 5-13: Regula requisitos, registro de operadores, suministro de información, acceso e interconexión.

- **Título III – Obligaciones Públicas y Derechos de Usuarios**

Incluye: Obligaciones de planeamiento urbano, acceso a infraestructuras públicas, servicio universal, seguridad de redes, derechos del usuario (portabilidad, transparencia, calidad del servicio).
Anexos: Incluyen tasas, definiciones técnicas y servicios mínimos de acceso a Internet

41. Real Decreto 123/2017,
De 24 de febrero, por el que se aprueba el Reglamento sobre el uso del dominio público radioeléctrico

Regula la utilización de bandas de frecuencias en dominio público, establece procedimientos electrónicos obligatorios con la administración, define bandas con limitaciones y servicios reservados, prevé medidas sin incremento de gasto público.
Crea un registro público de concesiones actualizado automáticamente.
Puntos clave:

- Marco legal: Desarrolla aspectos clave de la Ley 9/2014 y la Ley 11/2022.
- Concesiones y autorizaciones: Define procedimientos para solicitud, renovación, revocación y condiciones técnicas de uso.
- Gestión eficiente del espectro: Facilita la asignación ordenada, promueve la neutralidad tecnológica y fomenta el uso compartido.
- Control e inspección: Establece mecanismos de control del cumplimiento técnico y jurídico de los titulares

42. Real Decreto 1066/2001, de 28 de septiembre,
Por el que se aprueba el Reglamento que establece condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a emisiones radioeléctricas

Detalla obligaciones para garantizar la protección frente a emisiones radioeléctricas.
Establece criterios para evaluación de exposición y medidas correctivas.
Exige el cumplimiento de normas técnicas específicas.
Las condiciones se adaptan según la ubicación (urbano, rural, etc.).
Impone inspecciones y autorización de instalaciones con base en límites legales.
Puntos clave:

- Límites de exposición: Basados en recomendaciones europeas, aplicables a antenas, estaciones base, etc.
- Medidas de protección sanitaria: Incluyen niveles de referencia y restricciones específicas.
- Compatibilidad de instalaciones: Facilita la coexistencia de múltiples emisores.
- Autorizaciones e inspecciones: Regula la instalación, control e inspección técnica de estaciones radioeléctricas

43. Ley 25/2007, de 18 de octubre,

De conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones

Obliga a los operadores a conservar datos de tráfico y localización (no contenido) hasta 12 meses.

Cesión sólo con autorización judicial para investigación de delitos graves.

Regula el formato electrónico obligatorio para la entrega de datos a autoridades.

Introduce régimen sancionador por incumplimiento.

Obliga a registrar compradores de tarjetas prepago para prevenir usos delictivos.

Contenido principal:

- Art. 1-4: Define los datos que deben conservarse: tráfico, localización, identificadores de usuario y equipo, duración, tipo de servicio, entre otros.
- Finalidad: Investigación, detección y enjuiciamiento de delitos graves, previa autorización judicial.
- Exclusiones: No incluye el contenido de las comunicaciones ni la información consultada.
- Regulación de prepago: Registro obligatorio de compradores de tarjetas SIM prepago.
- Importante: Transposición de la Directiva 2006/24/CE, aunque anulada por el TJUE en 2014, sigue en vigor en parte en España

44. Orden PRE/199/2013, de 29 de enero,

Por la que se define el formato de entrega de los datos conservados por los operadores de servicios de comunicaciones electrónicas o de redes públicas de comunicaciones a los agentes facultados

- Finalidad de la Orden

  Desarrolla la disposición final cuarta de la Ley 25/2007, sobre conservación de datos de comunicaciones electrónicas.

  Establece el formato y protocolo para entregar los datos conservados a autoridades facultadas (Gobierno, Fuerzas y Cuerpos de Seguridad, Justicia, Inteligencia).
- Datos afectados

Incluyen:

Identificación de llamadas (origen/destino) de telefonía fija, móvil e Internet.

Localización de dispositivos móviles, incluso prepago.

Llamadas infructuosas.

Entrega sólo con autorización judicial, y para la persecución de delitos graves.

- Estándar técnico obligatorio

Adopta el estándar ETSI TS 102 657 como base técnica.

Los operadores con más de 2.000 solicitudes anuales están obligados a usar:

- Flujo de información, protocolos y formatos definidos por este estándar.
- Con las adaptaciones del anexo I de la Orden.

- Operadores con menos de 2.000 solicitudes

Pueden usar un formato alternativo, de los recogidos en el anexo III.
Debe acordarse con las autoridades y garantizar la seguridad y confidencialidad.
Si luego superan el umbral de 2.000 solicitudes, deben migrar al estándar ETSI.

- Interfaces de intercambio

Se definen dos interfaces lógicas:

- HI-A: para peticiones y respuestas administrativas.
- HI-B: para la entrega de datos conservados.

Pueden compartir canal físico, pero deben operar en territorio nacional y con seguridad y trazabilidad (ver anexo II).

- Aplicación a operadores

Operadores ya existentes: tienen el plazo fijado por la Ley 25/2007 para adaptarse.

Nuevos operadores: deben cumplir desde el inicio, salvo que puedan usar transitoriamente el formato alternativo.

- Actualización de anexos

Los secretarios de Estado de Seguridad, Hacienda y CNI pueden actualizar los anexos para adaptarlos a la evolución tecnológica.

45. Real Decreto-ley 7/2022, de 29 de marzo,
Sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación

Este Real Decreto-ley establece medidas urgentes para garantizar la seguridad del despliegue del 5G en España, en línea con las recomendaciones de la UE.
Objetivos principales:

- Proteger infraestructuras críticas y servicios esenciales frente a amenazas cibernéticas.
- Evitar dependencias tecnológicas peligrosas limitando el uso de proveedores de “alto riesgo”.
- Asegurar un despliegue seguro del 5G, clave para la economía y la administración

Medidas Clave:

- Evaluación de riesgos obligatoria para operadores.
- Restricción de proveedores considerados de alto riesgo.
- Requisitos de ciberseguridad reforzados para operadores (planes, notificaciones, etc.).
- Supervisión y control por parte de las autoridades competentes.
- Colaboración institucional nacional e internacional en ciberseguridad.

Importancia:
El 5G será esencial para sectores estratégicos (energía, transporte, salud, defensa). Este decreto busca garantizar su seguridad frente a riesgos tecnológicos y geopolíticos.

46. Real Decreto 443/2024,

De 30 de abril, por el que se aprueba el Esquema Nacional de Seguridad de redes y servicios 5G

El objetivo es establecer el Esquema Nacional de Seguridad (ENS) para redes y servicios 5G, cuyo propósito es garantizar un nivel adecuado de seguridad frente a amenazas que puedan afectar a la seguridad nacional, la economía o los servicios esenciales, en el contexto del despliegue y explotación de las redes 5G.

Ámbito de aplicación es el ENS 5G se aplica a:

- Los operadores de redes y servicios 5G establecidos en España.
- Entidades que gestionen infraestructuras críticas o esenciales que utilicen redes 5G.
- Organismos del sector público que dependan del 5G para funciones clave.
- Proveedores que participen en el suministro de equipos, software o servicios esenciales para el funcionamiento de las redes 5G.

Principales componentes del ENS 5G

a) Clasificación y protección de activos

Los operadores deben identificar y clasificar los activos de la red en función de su criticidad.

Se deben adoptar medidas de protección específicas en función del nivel de riesgo asociado a cada activo.

b) Evaluación de riesgos y amenazas

Se establece la obligación de realizar evaluaciones de riesgos periódicas, teniendo en cuenta amenazas técnicas, económicas, organizativas y geopolíticas.

Debe prestarse especial atención a las amenazas vinculadas a agentes externos que puedan actuar de forma hostil o con fines de espionaje o sabotaje.

c) Gestión de proveedores

Se incorpora un mecanismo de evaluación y control de proveedores, en especial aquellos considerados de alto riesgo.

La selección de proveedores debe basarse en criterios técnicos y de seguridad, incluyendo su sede, control gubernamental y comportamiento previo.

d) Certificación y auditoría

Los operadores deben someterse a auditorías externas independientes con una periodicidad determinada.

Se exige la certificación de productos, servicios y procesos críticos conforme a normas de seguridad reconocidas a nivel nacional o europeo.

e) Obligaciones en caso de incidentes

Establecimiento de procedimientos de detección, notificación y respuesta ante incidentes de seguridad.

Cooperación con las autoridades competentes y con los CSIRT (equipos de respuesta a incidentes).

Supervisión y régimen sancionador

El cumplimiento del ENS 5G será supervisado por el Ministerio para la Transformación Digital y de la Función Pública, con la colaboración de otros órganos competentes en materia de ciberseguridad.

Se establece un régimen sancionador específico, en el marco de la Ley General de Telecomunicaciones, para los casos de incumplimiento.

Objetivos generales del ENS 5G

Fortalecer la seguridad nacional frente a ciberamenazas asociadas a redes 5G.
Fomentar la resiliencia y continuidad de los servicios esenciales.
Promover la confianza en la infraestructura digital nacional.
Garantizar la autonomía estratégica frente a dependencias tecnológicas externas.

Entrada en vigor

El Real Decreto entra en vigor a los 20 días de su publicación en el BOE, es decir, el 20 de mayo de 2024.

Normativa relacionada

- Ley 11/2022, de Telecomunicaciones.
- Estrategia Nacional de Ciberseguridad.
- Recomendaciones de la **Comisión Europea sobre la seguridad de las redes 5G.
- Normas técnicas y marcos internacionales de gestión de riesgos.

47. Real Decreto 255/2025, de 1 de abril,

Por el que se regula el Documento Nacional de Identidad

El objeto es la regulación del proceso de expedición, gestión y desarrollo del DNI en formato físico y digital. La motivación es la adaptación tecnológica, refuerzo de la seguridad jurídica e identificación digital dentro del marco nacional y europeo.

Fundamento legal:

- Ley Orgánica 4/2015, de protección de la seguridad ciudadana.
- Ley 6/2020 sobre servicios electrónicos de confianza.
- Constitución Española (Art. 149.1.8ª, 18ª, 21ª y 29ª).
- Reglamentos UE 2019/1157 y 910/2014.

Capítulos principales:

- Disposiciones Generales: Naturaleza jurídica, funciones y finalidad del DNI.
- Derechos y Obligaciones: Titularidad, obligatoriedad desde los 14 años, intransferibilidad, deber de custodia.
- Tramitación y Renovación: Procedimientos, validez, duplicados, entrega.
- Versión Digital: Requisitos técnicos y funcionales para uso en móviles.
- Protección de Datos: Conformidad con RGPD y legislación española.
- Disposiciones relevantes adicionales:
- Sustitución temporal del DNI.
- Regulación para menores de edad.
- DNI en el extranjero.

Transitorias:

- Validez de DNIs anteriores.
- Medidas antes de la plena implantación del Registro Civil.
- Adaptación obligatoria del sector público y privado a la versión digital en 12 meses.
- Derogatoria: Queda derogado el RD 1553/2005.

Finales:

- Modificaciones normativas asociadas.
- Entrada en vigor inmediata desde su publicación en el BOE.

48. Ley Orgánica 10/1995, de 23 de noviembre, Del Código Penal.

Disposiciones Generales sobre Responsabilidad Penal (Libro I, Título II)

Artículos 27-30: Establecen quiénes son responsables penalmente (autores y cómplices). Los autores incluyen a quienes ejecutan el hecho directamente, inducen a otros, o cooperan de manera esencial. Los cómplices participan con actos anteriores o simultáneos. Se excluye la responsabilidad de cómplices en delitos cometidos mediante medios de difusión mecánicos.

Artículos 31-31 quinquies: Detallan la responsabilidad penal de las personas jurídicas por delitos cometidos en su nombre o beneficio, con excepciones para entidades públicas. Se especifican condiciones para eximir responsabilidad (ej. implementación de modelos de prevención eficaces).

Responsabilidad Civil (Título V)

Artículos 109-122: Regulan la reparación de daños derivados de delitos, incluyendo restitución, indemnización por perjuicios materiales/morales, y responsabilidad subsidiaria del Estado por daños causados por funcionarios. También se menciona la responsabilidad civil solidaria de aseguradores y titulares de medios de comunicación.

Delitos Relacionados con Amenazas y Coacciones (Capítulos II-III)

Artículos 169-171: Penas por amenazas condicionales (1-5 años de prisión) o no condicionales (6 meses-2 años), agravadas si se realizan por escrito, teléfono, o en nombre de grupos.

Artículos 172-172 quater: Castigan coacciones (6 meses-3 años), acoso (3 meses-2 años), y matrimonios forzados (6 meses-3.5 años). Se agravan si afectan a menores, víctimas vulnerables, o se cometen en el domicilio.

Delitos Sexuales y contra la Libertad (Capítulos IV-V)

Artículos 185-189 ter: Penalizan la explotación sexual, prostitución forzada, pornografía infantil (1-9 años), y corrupción de menores. Se incluyen penas para personas jurídicas (multas y disolución) y medidas para retirar contenido ilegal de internet.

Delitos contra la Intimidad y Propiedad Intelectual (Títulos X-XI)

Artículos 197-201: Protegen secretos y datos personales. Penas por acceder, difundir o modificar datos sin autorización (1-7 años), con agravantes si afectan a menores o datos sensibles (ideología, salud, etc.).

Artículos 270-277: Sancionan la violación de derechos de propiedad intelectual (6 meses-4 años) e industrial (6 meses-2 años), con penas mayores por beneficios económicos significativos o uso de menores.

Delitos Informáticos y contra el Patrimonio (Títulos XIII-XIV)

Artículos 248-251 bis: Estafas, incluyendo fraudes informáticos (6 meses-6 años), con agravantes por daños a servicios esenciales o uso de organizaciones criminales.

Artículos 264-264 quater: Daños a sistemas informáticos (6 meses-8 años), especialmente si afectan infraestructuras críticas o emplean malware. Responsabilidad penal para personas jurídicas (multas del triple al décuplo del perjuicio).

Delitos contra los Animales (Título XVI bis)

Artículos 340 bis-340 quinquies: Penalizan maltrato (3-24 meses), abandono (multa o trabajos comunitarios), y causar la muerte de animales (hasta 2 años). Incluyen inhabilitación para tenencia de animales y responsabilidad de personas jurídicas.

Falsedades y Secretos de Estado (Títulos XVIII y Disposiciones Especiales)

Artículos 401, 598-603: Usurpación de estado civil (6 meses-3 años) y revelación de secretos de defensa nacional (1-5 años), con agravantes para funcionarios o uso de medios de comunicación.

Conclusiones Clave

Enfoque integral: Abarca desde delitos tradicionales hasta delitos digitales, con adaptaciones a la era tecnológica.

Responsabilidad ampliada: Incluye a personas jurídicas y figuras como intermediarios en redes.

Protección de grupos vulnerables: Agravantes para delitos contra menores, víctimas de violencia de género, y personas con discapacidad.

Sanciones proporcionales: Penas variables según gravedad, beneficio económico, y daño social causado.

49. Ley Orgánica 5/2000, de 12 de enero, Reguladora de la responsabilidad penal de los menores. [Inclusión parcial]

Esta ley combina responsabilidad penal con un enfoque educativo y rehabilitador para menores, priorizando su reinserción social. Establece medidas proporcionales a la gravedad del delito, protege los derechos de las víctimas y adapta el proceso a la edad y circunstancias del menor. Incluye modificaciones recientes (2025) para reforzar la protección de víctimas vulnerables.

Se aplica a personas mayores de 14 años y menores de 18 que cometan delitos o faltas tipificados en el Código Penal o leyes penales especiales.

Los menores de 14 años no son penalmente responsables; se les aplican medidas de protección conforme al Código Civil y la Ley Orgánica 1/1996.

Los menores gozan de todos los derechos reconocidos en la Constitución, tratados internacionales (como la Convención sobre los Derechos del Niño) y normas de protección.

- Competencia judicial

Los Jueces de Menores son competentes para:

- Conocer de los hechos delictivos cometidos por menores.
- Resolver sobre responsabilidades civiles derivadas de dichos hechos.
- Ejecutar las sentencias.

La Audiencia Nacional (Juzgado Central de Menores) es competente para delitos graves como terrorismo (artículos 571 a 580 del Código Penal) o delitos cometidos en el extranjero con jurisdicción española.

- Derechos de las víctimas

Las víctimas tienen derecho a:

- Ser informadas de medidas de asistencia y protección.

- Personarse en el expediente y nombrar abogado (incluyendo asistencia jurídica gratuita).
- Declarar de forma telemática en casos de violencia de género, sexual, trata, o si son menores/discapacitados.
- Recibir notificaciones de resoluciones y medidas cautelares.

- Medidas aplicables a menores
  - Las medidas, ordenadas por gravedad, incluyen:
  - Internamiento (cerrado, semiabierto, abierto o terapéutico).
  - Tratamiento ambulatorio (para adicciones o trastornos psíquicos).
  - Libertad vigilada (seguimiento educativo y social).
  - Prestaciones en beneficio de la comunidad (hasta 200 horas).
  - Prohibición de aproximación/comunicación con la víctima.
  - Amonestación (reprimenda judicial).
  - Privación de permisos (conducir, armas, etc.).
  - Inhabilitación absoluta (para delitos graves como terrorismo).
- Reglas clave:

Las medidas de internamiento en régimen cerrado solo aplican para delitos graves, violencia, o actos cometidos en grupo.

Las medidas no pueden superar los límites máximos:

- 2 años para delitos menos graves.
- 6 años para mayores de 16 en casos de extrema gravedad (ej., homicidio, terrorismo).
- 8 años para delitos con pena de prisión ≥15 años.
- Principio acusatorio y modificación de medidas

El juez no puede imponer medidas más graves ni de mayor duración que las solicitadas por el Ministerio Fiscal o acusador.

Las medidas pueden modificarse (reducirse, sustituirse o suspenderse) si beneficia al menor y cumple los objetivos educativos.

- Mayoría de edad y prescripción

Si el menor cumple 18 años durante el cumplimiento de una medida:

Continúa aplicándose hasta su finalización, salvo que se requiera traslado a un centro penitenciario (por incumplimiento de objetivos).

Prescripción:

- Delitos graves: 3 a 5 años.
- Faltas: 3 meses.
- Medidas: 1 a 3 años según su duración.

- Disposiciones especiales

Para delitos sexuales o de violencia de género, se impone obligatoriamente educación sexual y en igualdad.

En casos de pluralidad de infracciones, se aplica la medida más grave, con límites acumulativos (hasta 10 años para mayores de 16).

50. Real Decreto de 14 de septiembre de 1882,

Por el que se aprueba la Ley de Enjuiciamiento Criminal. [Inclusión parcial]

Los Artículos 1º al 5º y partes seleccionadas del Libro II y Títulos siguientes establecen el marco normativo del proceso penal, desde la denuncia y querella, pasando por las funciones de la Policía Judicial, la recogida de pruebas, hasta las medidas de investigación tecnológicas. Se abordan medidas específicas para delitos digitales y tecnológicos, con un equilibrio entre eficacia investigativa y protección de derechos fundamentales.

Disposiciones Generales (Art. 1–5)

Aprueban el Código y fijan fechas y procedimientos para su aplicación.

Regulan el papel del Ministerio Público y la creación de nuevos tribunales.

Las Salas de Gobierno resolverán dudas interpretativas.

Denuncia y Querella (Art. 259–281)

Obligación de denunciar delitos públicos (salvo excepciones familiares/profesionales).

Profesionales como médicos y funcionarios tienen deber de denuncia.

Entrega vigilada (Art. 263 bis): permite rastrear delitos como narcotráfico y ciberdelitos.

Policía Judicial (Art. 282–298)

Funciones: proteger víctimas, recoger pruebas, redactar atestados.

Agentes encubiertos (Art. 282 bis): se autoriza su uso en casos de ciberdelincuencia y crimen organizado.

Pruebas y Peritajes

Recogida de pruebas: conservación de evidencias materiales y digitales.

Informe pericial (Art. 456–472): intervención de peritos para valorar pruebas, incluidos soportes electrónicos.

Medidas intrusivas (Tít. VIII, Art. 545–588 septies)

Entrada y registro en domicilios y lugares cerrados con auto judicial.

Interceptación de comunicaciones (teléfono, internet, email) requiere autorización judicial.

Registro de dispositivos y equipos informáticos: incluye registros remotos y acceso masivo a datos.

Captación de comunicaciones orales con dispositivos electrónicos.

Colaboración obligatoria de proveedores de servicios (telecomunicaciones, internet).

Conservación de datos (Art. 588 octies): proveedores deben guardar datos hasta 180 días.

6. Celebración del juicio (Art. 723–727)

Presentación y valoración de pruebas digitales y periciales en juicio oral.

Se regulan inspecciones oculares y recusación de peritos.

Procedimiento abreviado (Art. 769–773)

Obligaciones de la Policía Judicial:

Recoger pruebas.

Informar derechos a víctimas y detenidos.

Colaborar con el Ministerio Fiscal.

Publicaciones y delitos digitales (Art. 816–823 bis)

Secuestro de publicaciones (impresas, audiovisuales o digitales) usadas para cometer delitos.

Posibilidad de prohibir la difusión digital de contenidos ilícitos.

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

La Ley Orgánica 3/2018:

Adapta el ordenamiento jurídico español al Reglamento General de Protección de Datos (RGPD).

Refuerza los derechos digitales de los ciudadanos, en línea con el artículo 18.4 de la Constitución Española.

Aplica a todo tratamiento de datos personales, automatizado o no, con ciertas exclusiones (personas fallecidas, materias clasificadas, etc.).

Principios del tratamiento

Exactitud y actualización de los datos.

Confidencialidad: obligación de secreto para todos los involucrados.

Consentimiento: libre, informado e inequívoco (mayores de 14 años o con tutela).

Prohibición de tratar categorías especiales de datos salvo excepciones legales.

Tratamiento por interés público o legal debe estar expresamente habilitado por norma.

Derechos de los ciudadanos

Acceso, rectificación, supresión y limitación del tratamiento.

Portabilidad y oposición, especialmente en marketing directo.

Transparencia informativa, con esquemas de información por capas (ej. videovigilancia, cookies).

Tratamientos específicos

Videovigilancia: legal con límites claros (no grabar domicilios privados, guardar solo 1 mes).

Datos de contacto profesional y sistemas de solvencia: uso lícito bajo condiciones.

Protección de denunciantes e investigación estadística: permitidos con garantías.

Listas Robinson: exclusión voluntaria de publicidad no deseada.

Responsables y encargados

Responsabilidad proactiva: medidas técnicas, evaluación de riesgos y documentación.

Delegado de Protección de Datos (DPD) obligatorio en sectores sensibles (salud, educación, banca).

Registro de actividades y bloqueo de datos ante disputas legales.

Autoridades de control

AEPD: supervisa, inspecciona, sanciona y emite directrices.

Puede realizar auditorías preventivas y emitir circulares vinculantes.

Autoridades autonómicas: actúan sobre entidades públicas regionales; deben cooperar con la AEPD.

Régimen sancionador

Infracciones:

- Muy graves: tratamiento sin consentimiento, transferencias ilegales.
- Graves: falta de medidas de seguridad o transparencia.
- Leves: errores formales o incumplimiento parcial.
- Sanciones: hasta 20 millones € o el 4% del volumen de negocio.

Entidades públicas: sin multa económica, pero con obligación de corregir.

Garantía de los derechos digitales (Título X)

Neutralidad y acceso universal a Internet.
Seguridad digital y educación en competencias digitales.
Protección de menores, incluido el derecho a la intimidad digital.
Derecho a la desconexión digital laboral y limitaciones al control empresarial.
Derecho al olvido en buscadores y redes sociales.

Disposiciones adicionales relevantes

Esquema Nacional de Seguridad: medidas específicas para datos en el sector público.
Investigación en salud: tratamiento legal con seudonimización y evaluación de impacto.
Régimen transitorio: contratos previos al RGPD válidos hasta 2022 (salvo adaptación).

52. Real Decreto 1720/2007,
De 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

Su principal objetivo es complementar la Ley Orgánica 157/1999 que trata temas de Protección de datos de carácter personal de medidas de seguridad de los ficheros automatizados que contengan datos personales. Aplica a todos los tipos de datos de carácter personal registrados en soportes físico y digital de modo que pudiesen ser utilizados para su procesamiento en el sector privado y público. Este reglamento no va a ser aplicable a los tratamientos de datos de personas jurídicas, ni ficheros que mencionen nombres y apellidos, teléfonos, fax o dirección postal de terceros, ni datos de empresarios individuales ni personas fallecidas mientras los datos no involucren a sus familiares.

Principios y títulos

- El título I contempla el objeto y ámbito de aplicación del reglamento. Se fija el criterio a seguir en materia de cómputo de plazos para unificar la cuestión del tratamiento de datos en ficheros tanto públicos como privados
- El título II trata los principios de protección de datos relacionados con el ámbito del real decreto. Se hace especial hincapié en los aspectos de los servicios de comunicaciones electrónicas y la recopilación de datos de los menores.

Presenta los principios de legitimidad de los datos, de legítimo interés y los derechos de modificación, cese y olvido del tratamiento de los datos.
Se presenta en el mismo título un estatuto sobre el encargado del tratamiento estableciendo sus funciones y regulaciones, así como la posibilidad de subcontratación del mismo.

- El título III explica los derechos del ciudadano para el acceso, rectificación, cancelación, y oposición al tratamiento de sus datos y que constituyen el derecho fundamental a la protección de datos.
- Los títulos IV a VII clarifican criterios específicos a determinado tipo de ficheros de titularidad privada que por su trascendencia lo requerían -los relativos a la solvencia patrimonial y crédito y los utilizados en actividades de publicidad y prospección comercial-, el conjunto de obligaciones materiales y formales que deben conducir a los responsables a la creación e inscripción de los ficheros, los criterios y procedimientos para la realización de las transferencias internacionales de datos, y, finalmente, la regulación de un instrumento, el código tipo

- El título VIII regula la seguridad, que repercute sobre múltiples aspectos organizativos, de gestión y aún de inversión, en todas las organizaciones que traten datos personales. El reglamento trata de ser particularmente riguroso en la atribución de los niveles de seguridad, en la fijación de las medidas que corresponda adoptar en cada caso y en la revisión de las mismas cuando ello resulte necesario. Por otra parte, ordena con mayor precisión el contenido y las obligaciones vinculadas al mantenimiento del documento de seguridad
- Finalmente en el título IX, dedicado a los procedimientos tramitados por la Agencia Española de Protección de Datos, se ha optado por normar exclusivamente aquellas especialidades que diferencian a los distintos procedimientos tramitados por la Agencia de las normas generales previstas para los procedimientos en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, cuya aplicación se declara supletoria al presente reglamento.

53. 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

El objetivo es proteger los datos personales de las personas físicas y regular su libre circulación dentro y fuera de la UE.

Se aplica a tratamientos automatizados y no automatizados de datos personales, incluso fuera de la UE si afectan a residentes europeos.

No se aplica a actividades domésticas, seguridad pública o justicia penal (reguladas por la Directiva UE 2016/680).

Sus principios son la licitud, lealtad, finalidad, minimización, exactitud, limitación de conservación, integridad/confidencialidad.

El consentimiento es libre, informado y verificable.

Capítulos relevantes:

Capítulo 4: Deberes de responsables y encargados, incluyendo evaluación de impacto y certificaciones.

Capítulo 5: Transferencia internacional de datos solo con garantías adecuadas.

Capítulo 6: Autoridades de control independientes y con poder sancionador.

Capítulos finales: cooperación entre autoridades, coherencia regulatoria y protección del ciudadano.

54. Ley Orgánica 7/2021,

De 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. [Inclusión parcial]

El objetivo es regular el tratamiento de datos personales por autoridades competentes para fines penales y de seguridad pública.

Puntos clave:

- Aplicación: Policía, Fiscalía, Jueces, Prisiones, Aduanas, Antiblanqueo y Antiterrorismo.
- Principios: proporcionalidad, conservación limitada, colaboración interinstitucional, y respeto a los derechos del afectado.
- Prohibición de decisiones automatizadas sin intervención humana.
- Derechos post mortem: familiares pueden ejercer derechos de acceso, rectificación o supresión

55. Ley 39/2015, de 1 de octubre,

Del Procedimiento Administrativo Común de las Administraciones Públicas.

El objetivo es regular la relación entre ciudadanos y administraciones públicas.

Puntos clave:

- Establece el uso obligatorio de medios electrónicos para empresas, profesionales colegiados y empleados públicos.
- Las personas físicas pueden elegir el medio de comunicación (electrónico o no).
- Refuerza la seguridad jurídica, participación ciudadana y eficiencia administrativa.

56. Ley 40/2015, de 1 de octubre,

De Régimen Jurídico del Sector Público. [Inclusión parcial]

El objetivo es regular la organización, relaciones internas y responsabilidades del sector público.

Puntos clave:

- Complementa a la Ley 39/2015: incluye sede electrónica, identificación digital, y relaciones interadministrativas.
- Regula la potestad sancionadora, la responsabilidad patrimonial y la actuación administrativa automatizada.
- Fomenta la transparencia, coordinación y cooperación entre administraciones.