

Resúmenes OPE 5/22

# Temario para el Cuerpo Superior de Ingenieros Informáticos de la Administración de la Generalitat

A1-06

SALVADOR CARRION PONZ  
Dic2022-Ene2023



## Prólogo

Este documento recoge el temario que utilicé para aprobar las oposiciones al **Cuerpo Superior Técnico de Ingeniería en Informática de la Administración de la Generalitat (A1-06)**. El contenido ha sido elaborado íntegramente por mí, basándome en fuentes públicas disponibles en internet, como documentos, wikis y otros recursos de acceso libre.

El objetivo de este material es proporcionar una **referencia, clara, estructurada y gratuita**, para quienes estén preparándose oposiciones de informática o similares.

---

### ¿Te ha sido útil este material?

Si valoras este trabajo y deseas apoyarlo, puedes invitarme a un café virtual a través del siguiente enlace:

 [ko-fi.com/salvacarrion](https://ko-fi.com/salvacarrion)

---

### Aviso Legal

Estos temas reflejan mi criterio personal en cuanto a la estructuración y el formato del contenido. Aunque he procurado la máxima precisión, no puedo garantizar la exactitud, exhaustividad o ausencia de errores en la información presentada. **Por lo tanto, el uso de este material queda bajo tu propia responsabilidad.**

Si detectas errores, tienes sugerencias o deseas contribuir a mejorar este temario, estaré encantado de recibir tu colaboración. ¡Toda ayuda es bienvenida!

---

### Licencia

Este contenido está protegido bajo la licencia **Creative Commons BY-NC 4.0**, lo que permite compartir y adaptar el material bajo las siguientes condiciones:

- **Atribución:** Debes dar crédito al autor original.
- **No comercial:** No puedes utilizar este material con fines comerciales.

## Contenido

Jerarquía Normativa.....	11
Constitución Española .....	14
Constitución Española.....	14
Estructura y Datos relevantes .....	30
Estatuto de Autonomía de la Comunidad Valenciana .....	34
Ley Orgánica 5/1982, de 1 de julio, de Estatuto de Autonomía de la Comunidad Valenciana.	
.....	34
Estructura y Datos relevantes .....	45
Gobierno Valenciano.....	46
Ley 5/1983, de 30 de diciembre, de Gobierno Valenciano.....	46
Unión Europea.....	54
Características del Ordenamiento Jurídico de la Unión Europea .....	54
Leyes de Igualdad .....	59
Ley Orgánica 3/2007, para la igualdad efectiva de mujeres y hombres .....	59
Ley 9/2003, de igualdad entre mujeres y hombres (Comunidad Valenciana).....	63
Leyes contra de Violencia de Género.....	66
Ley Orgánica 1/2004, de medidas de protección integral contra la violencia de género.....	66
Gobierno Abierto, Transparencia, y Buen gobierno .....	70
Ley 19/2013 de Transparencia, Acceso a la Información Pública y Buen Gobierno .....	70
Ley 1/2022, de Transparencia y Buen Gobierno de la Comunitat Valenciana.....	77
Régimen Jurídico del Sector Público .....	81
Ley 40/2015 - Régimen Jurídico del Sector Público .....	81
Procedimiento Administrativo Común de las Administraciones Públicas .....	89
Ley 39/2015 - Procedimiento Administrativo Común de las Administraciones Públicas .....	89
Ley 9/2017 - Contratos del Sector Público .....	106
Ley 9/2017 - Contratos del Sector Público .....	106
Función pública .....	115
RDL 5/2015 - Ley del Estatuto Básico del Empleado Público (TREBEP) .....	115
Ley 4/2021 - Función Pública Valenciana.....	120
Decreto 42/2019 - Condiciones de trabajo del personal funcionario de la Administración de la Generalitat.....	141
Decreto 49/2021 - Regulación del teletrabajo como modalidad de prestación de servicios del personal empleado público de la Administración de la Generalitat.....	144
Hacienda Pública .....	146
Ley 1/2015 - de Hacienda Pública, del Sector Público Instrumental y de Subvenciones.....	146

Sociedad Digital.....	151
Tecnología y desarrollo en la Sociedad Digital.....	151
Agenda Digital .....	154
Agenda Digital de la Comunitat Valenciana (ADCV) .....	154
Gestión de los servicios TIC.....	156
Guías ITIL .....	156
Gestión y Dirección de Proyectos .....	159
Metodología PM2.....	159
GvLOGOS .....	161
Planificación Estratégica y Metodologías Ágiles .....	163
Metodologías Ágiles .....	163
Calidad del Software .....	165
Análisis de Requisitos .....	165
Aseguramiento de la Calidad .....	168
DevOps .....	171
Fundamentos del Testeo (ISTQB).....	174
Familia de Normas ISO/IEC 25000 (SQuaRE).....	177
Esquema Nacional de Seguridad (ENS) .....	180
Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.....	180
Medidas de Seguridad.....	184
Gestión de Riesgos .....	185
Análisis de riesgos en la gestión de proyectos.....	185
Metodología MAGERIT .....	188
Desarrollo Seguro de Aplicaciones.....	192
OWASP 4.0 (Open Web Application Security Project) .....	192
Seguridad y protección de redes de comunicaciones.....	195
Gestión de Ciberincidentes .....	200
Seguridad de la Información en la Generalitat Valenciana.....	204
Decreto 130/2012 - Organización de la seguridad de la información de la Generalitat .....	204
Decreto 66/2012 - Política de Seguridad de la Información de la Generalitat .....	206
Orden 19/2013 - Uso Seguro de Medios Tecnológicos en la Administración de la Generalitat .....	209
Inteligencia Artificial.....	212
Inteligencia Artificial: Conceptos Básicos, Tecnologías Fundamentales y Aplicaciones Prácticas .....	212
Gestión de datos corporativos .....	220

Gestión de Datos Corporativos .....	220
Big Data .....	223
Minería de Datos.....	225
Casos prácticos sobre clasificación .....	231
Tabla de nomenclaturas comunes .....	233
Gobernanza del dato.....	234
Gobernanza del dato y metodologías .....	234
Modelo estratégico, operativo y organizativo del dato .....	236
APIs (Application Programming Interface).....	239
Apificación.....	239
Automatización Robótica de Procesos (RPA).....	241
Automatización Robótica de Procesos (RPA).....	241
Tecnología Blockchain .....	244
Tecnología blockchain, funcionamiento, tipos, estructura y aplicaciones .....	244
Organizaciones descentralizadas (OD) .....	248
Centros de Procesamiento de Datos (CPD).....	250
Diseño de un Centro de Procesamiento de Datos (CPD) .....	250
Infraestructura Convergente e Hiperconvergente.....	259
Centro de Datos Definido por Software (SDDC).....	258
Hiperconvergencia en el Centro de Proceso de Datos.....	259
Tendencias (i): Impacto Ambiental, Escalabilidad, Automatización y Gestión Remota .....	260
Casos Prácticos .....	263
Virtualización de recursos .....	265
Virtualización.....	265
Contenedores Docker.....	268
Plataforma de Kubernetes .....	269
Sistemas de almacenamiento .....	270
Sistemas de almacenamiento .....	270
Computación en la Nube (Cloud Computing) .....	275
Computación en la Nube.....	275
Infraestructuras, Plataformas y Software como Servicio (IaaS, PaaS, SaaS).....	278
Aspectos varios de la computación en la Nube .....	279
Puesto de trabajo TIC .....	281
El puesto de trabajo TIC en una organización.....	281
Infraestructura del puesto de trabajo virtual (VDI) .....	282
Protección de datos personales .....	286

Reglamento (UE) 2016/679 (RGPD) .....	292
Administración Electrónica .....	299
Real Decreto 203/2021, de 30 de marzo, Reglamento de actuación y funcionamiento del sector público por medios electrónicos .....	299
Decreto 220/2014, de 12 de diciembre, del Consell, por el que se aprueba el Reglamento de Administración Electrónica de la Comunitat Valenciana.....	301
Desarrollo web .....	303
Arquitectura de Desarrollo en la Web .....	303
Tecnologías Web: HTML, CSS, Javascript, AngularJS.....	307
HTML .....	307
Desarrollo de Aplicaciones Móviles .....	308
Diseño y Desarrollo de Aplicaciones Móviles.....	308
Aplicaciones Web para Móviles .....	311
Aplicaciones Nativas: Android.....	312
Aplicaciones Nativas: iOS .....	314
Aplicaciones Nativas: Windows .....	315
Aplicaciones Híbridas .....	315
Accesibilidad y Usabilidad .....	317
Arquitectura Orientada a Servicios (SOA) .....	321
Arquitectura Orientada a Servicios (SOA) .....	321
Arquitectura de Servicios Web.....	325
Modelo de desarrollo de aplicaciones basado en microservicios.....	328
Formatos usados para interoperabilidad de servicios: JSON y XML.....	330
JSON (JavaScript Object Notation) .....	330
Programación sin código .....	332
Programación Low-Code y No-Code .....	332
Gestión Documental.....	334
Gestión Documental.....	334
Esquema Nacional de Interoperabilidad (ENI) .....	339
Esquema Nacional de Interoperabilidad.....	339
Normas Técnicas de Interoperabilidad (NTI) .....	344
Interoperabilidad Europea, Nacional y Autonómica.....	348
Plataforma Autonómica de Interoperabilidad de la Generalitat Valenciana (PAI).....	351
Infraestructuras de interoperabilidad.....	354
Identificación y firma electrónica.....	357

Identificación y firma electrónica. Marco europeo y nacional. Certificados digitales. Claves privadas, públicas y concertadas. Formatos de firma electrónica. Servicios de directorio. Mecanismos de identificación y firma biométricos .....	357
Sistemas de Información Geográfica (SIG).....	367
Sistemas de Información Geográfica (SIG).....	367
Infraestructuras de Datos Espaciales (IDE) .....	370
Definición y Componentes. Arquitectura y Servicios Web de una IDE .....	370
Redes de computadores.....	375
Red de computadores: Componentes, Categorías, dispositivos,... .....	375
Cálculo de redes .....	378
Redes de Área Extensa (WAN) .....	379
Modelos de interconexión de sistemas abiertos: Modelo OSI vs Modelo TCP/IP .....	383
Modelo de Referencia OSI (Open Systems Interconnection) .....	383
Modelo TCP/IP o Internet Protocol Suite.....	385
Comparativa entre modelos .....	387
Virtualización de redes.....	388
Virtualización de redes.....	388
Redes definidas por software (SDN) .....	389
Redes de área amplia definidas por software (SD-WAN) .....	391
Orquestación y Gestión Centralizada de Dispositivos de Comunicaciones .....	392
Redes de emergencia .....	394
Redes de emergencia .....	394
Red COMDES (Comunicaciones Móviles Digitales de Emergencias y Seguridad de la Comunitat Valenciana).....	397
Estándar TETRA (Terrestrial Trunked Radio).....	399
Internet de las Cosas (IoT).....	401
Internet de las Cosas (IoT).....	401
Redes de Sensores.....	404
Ciudades Inteligentes (Smart Cities) .....	405
Ciudades Inteligentes (Smart Cities) .....	405
Redes inalámbricas.....	408
Redes inalámbricas.....	408
Redes 5G y Programa ÚNICO-Banda Ancha .....	412
Redes 5G .....	412
Seguridad en las Comunicaciones .....	415
Seguridad en las Comunicaciones .....	415
Seguridad Inalámbrica.....	418

Acceso seguro a redes corporativas.....	419
Acceso seguro a redes corporativas.....	419

# BLOQUE GENERAL (Legislación)

## Jerarquía Normativa

### Rango de Ley

- **Constitución:**
  - Es la ley fundamental del Estado y tiene la máxima jerarquía normativa.
- **Reformas:**
  - **Total, Derechos Fundamentales o Corona:** Requiere la aprobación de 2/3 de ambas Cámaras y referéndum.
  - **Parcial:** Requiere 3/5 de ambas Cámaras. Si el Senado la rechaza, el Congreso puede aprobarla por 2/3. Es posible someterla a referéndum.
- **Tratados Internacionales:**
  - Incorporados al ordenamiento jurídico según lo establecido en la Constitución.
- **Leyes Orgánicas:**
  - Regulan el desarrollo de derechos fundamentales, libertades públicas, Estatutos de Autonomía y régimen electoral general.
  - Se aprueban por **mayoría absoluta del Congreso**.
- **Leyes Ordinarias:**
  - Regulan materias no reservadas a leyes orgánicas.
  - Se aprueban por **mayoría simple del Congreso**, salvo veto absoluto del Senado, en cuyo caso requerirían mayoría absoluta.
- **Decretos Legislativos (Real Decreto Legislativo):**
  - Dictados por el poder ejecutivo mediante delegación de las Cortes Generales, excepto en materias reservadas a leyes orgánicas.
  - **Tipos de delegación:**
    - **Ley de Bases:** Permite elaborar un texto articulado.
    - **Ley Ordinaria:** Permite elaborar textos refundidos (armonización normativa).
- **Decretos Leyes (Real Decreto Ley):**
  - Normas provisionales con rango de ley dictadas por el poder ejecutivo en casos de extraordinaria y urgente necesidad.
  - Excluyen materias reservadas a leyes orgánicas.
  - Deben ser convalidadas o derogadas por el Congreso en un plazo de 30 días.

## Rango Reglamentario

- **Decreto:** Norma jurídica con rango de reglamento aprobada por órganos ejecutivos de las comunidades autónomas.
- **Real Decreto:** Norma jurídica emitida por el Gobierno Central y formalizada por el Rey según la Constitución.

## Iniciativas Legislativas

- **Proyecto de Ley:** Propuesta presentada por el Gobierno, aprobada previamente en el Consejo de Ministros.
- **Proposición de Ley:** Propuesta presentada por el Congreso, el Senado, Asambleas Legislativas de las CCAA o mediante iniciativa legislativa popular (excluye materias de leyes orgánicas).
- **Anteproyecto de Ley:** Documento elaborado por uno o varios ministerios para ser elevado al Consejo de Ministros como proyecto de ley.
- **Leyes Marco:** Emanadas de las Cortes Generales, otorgan a las CCAA la facultad de dictar normas legislativas dentro del marco fijado por el Estado.

## Ordenamientos Jurídicos

- **Jerarquía en el Estado:**
  1. Decretos.
  2. Órdenes de Comisiones Delegadas del Gobierno.
  3. Órdenes Ministeriales.
  4. Disposiciones de órganos inferiores según su jerarquía.
- **Jerarquía en las CCAA:**
  - Similar al Estado, pero adaptada a las consejerías y órganos colegiados autonómicos.
  - En la Comunidad Valenciana:
    1. Decretos del Consell.
    2. Decretos del President.
    3. Órdenes de Comisiones Delegadas del Consell.
    4. Órdenes de Conselleria.
    5. Disposiciones de órganos inferiores.
- **Jerarquía en Entidades Locales:**

1. Reglamento Orgánico.
2. Ordenanzas.

## Fuentes del Derecho

- **La Ley:** Principal fuente del Derecho.
- **La costumbre:** Aplica en defecto de ley aplicable.
- **Principios generales del Derecho:** Supletorios en ausencia de ley o costumbre.

## Constitución Española

# Constitución Española de 1978

### Título Preliminar

#### Art. 1: Valores / Soberanía / Forma política

- España es un **Estado social y democrático de Derecho** que tiene como valores superiores: **libertad, justicia, igualdad y pluralismo político**.
- La **soberanía nacional reside en el pueblo español**, de quien emanan los poderes del Estado.
- Su forma política es la **Monarquía parlamentaria**.

#### Art. 2: Unidad / Autonomía / Solidaridad

- La Constitución se basa en la **indisoluble unidad de la Nación española**.
- Reconoce el derecho a la **autonomía de nacionalidades y regiones** y garantiza la **solidaridad entre todas ellas**.

#### Art. 3: Lenguas

- El **castellano es la lengua oficial del Estado**.
- Las demás lenguas españolas serán también oficiales en sus respectivas comunidades autónomas según los estatutos.
- Se protege la **riqueza lingüística** como patrimonio cultural.

#### Art. 4: Bandera de España

- Formada por **tres franjas horizontales**: roja, amarilla (doble de ancha) y roja.
- Las banderas autonómicas podrán utilizarse junto a la bandera nacional.

#### Art. 5: Capital del Estado

- La capital de España es la **villa de Madrid**.

#### Art. 6: Partidos políticos

- Representan el **pluralismo político** y son instrumentos fundamentales para la **participación política**.
- Su funcionamiento debe ser **democrático**.

#### Art. 7: Sindicatos y asociaciones empresariales

- Contribuyen a la **defensa de intereses económicos y sociales**.
- Funcionamiento democrático.

#### Art. 8: Fuerzas Armadas

- Compuestas por **Ejército de Tierra, Armada y Ejército del Aire**.
- Su misión es garantizar la **soberanía, independencia, integridad territorial y el orden constitucional**.

#### **Art. 9: Sujeción a la ley / Garantías judiciales**

- Todos están **sujetos a la Constitución y leyes**.
- Los poderes públicos deben promover **igualdad y participación real y efectiva**.
- Garantías: **principio de legalidad, jerarquía normativa, publicidad, irretroactividad, seguridad jurídica, y responsabilidad pública**.

### **Título I: De los derechos y deberes fundamentales**

#### **Art. 10: Dignidad y derechos de la persona**

- Fundamento del orden político y paz social: **dignidad, libre desarrollo de la personalidad y respeto a la ley y derechos ajenos**.
- Interpretación conforme a la **Declaración Universal de Derechos Humanos**.

#### **Art. 11: Nacionalidad**

- Regulada por ley: **adquisición, conservación y pérdida**.

#### **Art. 12: Mayoría de edad**

- Alcanzada a los **18 años**.

#### **Art. 13: Extranjeros / Extradición / Asilo**

- Los extranjeros tienen los **mismos derechos y libertades** que los españoles, salvo restricciones.
- **Extradición**: conforme al principio de reciprocidad, excluyendo delitos políticos.
- Derecho de **asilo** para ciudadanos extranjeros y apátridas.

#### **Art. 14: Igualdad ante la ley**

- Todos son **iguales ante la ley** sin discriminación por nacimiento, raza, sexo, religión, opinión u otra circunstancia.

#### **Art. 15: Derecho a la vida y a la integridad física y moral**

- **Abolición de la pena de muerte**, excepto en tiempos de guerra según leyes militares.

#### **Art. 16: Libertad ideológica, religiosa y de culto**

- Garantizada sin más limitación que el orden público protegido por la ley.

#### **Art. 17: Derecho a la libertad y seguridad**

- **Detención preventiva**: máximo 72 horas.
- Obligación de informar al detenido de forma inmediata, con **asistencia de abogado**.

- Garantía de procedimiento de **habeas corpus**.

**Art. 18: Derecho al honor, intimidad y propia imagen**

- Inviolabilidad del domicilio y secreto de las comunicaciones protegidos.

**Art. 19: Libertad de residencia y circulación**

- Derecho a moverse y residir en cualquier lugar del territorio español.

**Art. 20: Libertad de expresión**

- Incluye producción, creación, y difusión sin censura previa.

**Art. 21: Derecho de reunión**

- Reuniones pacíficas y sin armas no requieren autorización previa.

**Art. 22: Derecho de asociación**

- Prohibidas asociaciones secretas y paramilitares.

**Art. 23: Participación en asuntos públicos**

- Directa o por representantes elegidos mediante **sufragio universal**.

**Art. 24: Tutela judicial efectiva**

- Derecho a juicio justo, **presunción de inocencia** y a no declarar contra sí mismo.

**Art. 25: Principio de legalidad penal**

- Nadie será sancionado por actos que no sean delito en el momento de cometerse.
- Las penas deben orientarse a la **reinserción y reeducación social**.

**Art. 26: Prohibición de Tribunales de Honor**

- En la administración civil y organizaciones profesionales.

**Art. 27: Derecho a la educación**

- **Educación básica obligatoria y gratuita**.
- Fomenta el respeto a los principios democráticos y derechos fundamentales.

**Art. 28: Derecho de sindicación y huelga**

- Derecho a huelga limitado para las **FFAA y cuerpos disciplinados**.

**Art. 29: Derecho de petición**

- Ejercido por escrito, individual o colectivamente, salvo fuerzas armadas (solo individual).

**Art. 30: Defensa de España**

- Derecho y deber de defensa regulados por ley.

**Art. 31: Sistema tributario**

- Basado en **igualdad y progresividad**, sin carácter confiscatorio.

#### **Art. 32: Matrimonio**

- Derecho a contraer matrimonio con **plena igualdad jurídica** entre los cónyuges.

#### **Art. 33: Propiedad privada y herencia**

- Derecho a la **propiedad privada y a la herencia**, limitada por la función social.
- Expropiación solo mediante **indemnización y utilidad pública** conforme a la ley.

#### **Art. 34: Derecho de fundación**

- Para fines de **interés general**.

#### **Art. 35: Derecho al trabajo**

- Derecho y deber de trabajar, con libertad de elección de profesión.
- Se garantizan **condiciones dignas y remuneración suficiente**.

#### **Art. 36: Colegios profesionales**

- Su estructura y funcionamiento serán **democráticos**.

#### **Art. 37: Negociación colectiva y huelga**

- Derecho a **negociar convenios colectivos** y adoptar medidas de conflicto colectivo, incluido el derecho a huelga.

#### **Art. 38: Libertad de empresa**

- Garantizado dentro de las exigencias de la **economía general** y, en su caso, planificación estatal.

#### **Art. 39: Protección a la familia e infancia**

- **Protección integral a los hijos, madres y familias**.
- Igualdad ante la filiación, independientemente de su naturaleza.

#### **Art. 40: Redistribución y empleo**

- Los poderes públicos promoverán:
  - **Redistribución de la renta equitativa**.
  - **Política de pleno empleo**.

#### **Art. 41: Seguridad social**

- Garantizada para todos los ciudadanos.

#### **Art. 42: Protección de emigrantes**

- Velará por los derechos económicos y sociales de trabajadores españoles en el extranjero.

#### **Art. 43: Protección de la salud**

- Salud pública organizada y tutelada por los poderes públicos.
- Fomento de la **educación física y el deporte**.

#### **Art. 44: Cultura y ciencia**

- Acceso a la **cultura y promoción de la ciencia e investigación** como derecho de todos.

#### **Art. 45: Medio ambiente**

- Derecho a disfrutar de un medio ambiente adecuado.
- **Deber de conservarlo** y uso racional de recursos naturales.

#### **Art. 46: Patrimonio cultural**

- Protección y promoción del patrimonio histórico, cultural y artístico.

#### **Art. 47: Derecho a la vivienda**

- Todos los españoles tienen derecho a una **vivienda digna**.
- Se evitará la **especulación del suelo**.

#### **Art. 48: Juventud**

- Promoción de la **participación libre y eficaz** en desarrollo político, social y cultural.

#### **Art. 49: Atención a personas con discapacidad**

- Políticas de **integración y accesibilidad** para personas con discapacidades.

#### **Art. 50: Tercera edad**

- Garantía de **suficiencia económica** y servicios sociales específicos para ancianos.

#### **Art. 51: Consumidores y usuarios**

- Protección de sus derechos a la **seguridad, salud e intereses económicos**.

#### **Art. 52: Organizaciones profesionales**

- Su funcionamiento será **democrático** y representarán intereses económicos y sociales.

#### **Art. 53: Garantías de derechos**

- Tutela de derechos fundamentales mediante:
  - Procedimiento basado en **preferencia y sumariedad**.
  - Recurso de amparo ante el Tribunal Constitucional.

#### **Art. 54: Defensor del Pueblo**

- Es un **alto comisionado de las Cortes Generales** encargado de defender los derechos fundamentales.
- **Supervisa la actividad administrativa** y da cuenta a las Cortes Generales.
- Regulación mediante **ley orgánica**.

#### **Art. 55: Suspensión de derechos y libertades**

- Derechos susceptibles de suspensión durante los **estados de excepción o sitio**:
  - **Libertad personal (17.1, 17.2, 17.3, 17.4), inviolabilidad del domicilio (18.2), secreto de las comunicaciones (18.3), libertad de circulación (19), reunión (21)**, entre otros.
- En investigaciones contra **bandas armadas o terrorismo**, se pueden suspender derechos individualmente con **intervención judicial**.

### **Título II: De la Corona**

#### **Art. 56: El Rey**

- Jefe del Estado, **símbolo de unidad y permanencia**.
- Representa a España en relaciones internacionales y **arbitra/modera el funcionamiento de las instituciones**.
- Su persona es **inviolable y no está sujeta a responsabilidad**.

#### **Art. 57: Sucesión al trono**

- Orden de **primogenitura y representación**, con preferencia del varón sobre la mujer en el mismo grado.
- Las **Cortes Generales regulan vacantes o conflictos sucesorios** mediante ley orgánica.

#### **Art. 58: Reina consorte o consorte del Rey**

- No podrá asumir funciones constitucionales, salvo **regencia**.

#### **Art. 59: Regencia**

- Durante la minoría o incapacidad del Rey.
- Ejercida por el parente más próximo; si no los hubiera, será designada por las **Cortes Generales**.

#### **Art. 60: Tutela del Rey menor**

- Nombrada por el Rey en su testamento o, de no existir, ejercida por el progenitor viudo.

#### **Art. 61: Juramento del Rey**

- "**Guardar y hacer guardar la Constitución y respetar los derechos de los ciudadanos y CCAA**".

#### **Art. 62: Funciones del Rey**

- **Sancionar/promulgar leyes**, convocar elecciones, proponer candidato a Presidente del Gobierno, expedir decretos, y mando supremo de las Fuerzas Armadas, entre otras.

#### **Art. 63: Relaciones internacionales**

- Acredita embajadores, manifiesta consentimiento en tratados internacionales, y declara la guerra o la paz con autorización de las Cortes Generales.

#### **Art. 64: Refrendo de los actos del Rey**

- Actos refrendados por el Presidente del Gobierno o los ministros, quienes son responsables de ellos.

#### **Art. 65: Casa Real**

- El Rey recibe un presupuesto asignado por el Estado y lo distribuye libremente.

### **Título III: De las Cortes Generales**

#### **Art. 66: Funciones de las Cortes Generales**

- Representan al pueblo, ejercen la **potestad legislativa**, aprueban presupuestos y **controlan la acción del Gobierno**.
- Compuestas por el **Congreso y el Senado**, son **inviolables**.

#### **Art. 67: Incompatibilidades y mandato**

- No se puede ser miembro de ambas Cámaras a la vez ni estar ligado por mandato imperativo.
- Reuniones no reglamentarias no vinculan a las Cámaras.

#### **Art. 68: Congreso de los Diputados**

- **Entre 300 y 400 Diputados**, elegidos por **sufragio universal, directo y secreto**.
- Circunscripción electoral: **provincia**.
- Mandato: **4 años**.

#### **Art. 69: Senado**

- Cámara de representación territorial.
- Composición: **4 senadores por provincia**, más representantes de islas y CCAA según población.

#### **Art. 70: Inelegibilidades e incompatibilidades**

- Afectan a **altos cargos, magistrados, jueces, fiscales, militares en activo**, entre otros.

#### **Art. 71: Protección de parlamentarios**

- **Inviolabilidad por opiniones expresadas en funciones**.
- **Inmunidad salvo flagrante delito**, juzgados por el Tribunal Supremo.

#### **Art. 72: Reglamentos de las Cámaras**

- Cada Cámara elabora su propio reglamento (mayoría absoluta) y elige su Presidencia y Mesa.

#### **Art. 73: Periodos de sesiones**

- **Dos periodos ordinarios:** septiembre-diciembre y febrero-junio.
- Sesiones extraordinarias: solicitadas por Gobierno, Diputación Permanente o mayoría absoluta de miembros.

#### **Art. 74: Sesiones conjuntas de las Cámaras**

- Para competencias no legislativas del Título II. Presididas por el Presidente del Congreso.

#### **Art. 75: Funcionamiento de las Cámaras**

- **En Pleno o Comisiones.**
- En comisiones permanentes pueden aprobar proyectos de ley, salvo reformas constitucionales, leyes orgánicas y presupuestos.

#### **Art. 76: Comisiones de investigación**

- Obligatorias para comparecer, pero sus conclusiones no son vinculantes.

#### **Art. 77: Derecho de petición**

- Ejercido por escrito.

#### **Art. 78: Diputación Permanente**

- Representación proporcional de grupos parlamentarios, presidida por el Presidente de la Cámara.
- Asume competencias en casos de disolución de las Cámaras o estados excepcionales.

#### **Art. 79: Adopción de acuerdos**

- Mayoría requerida, con asistencia reglamentaria de los miembros.
- El voto es **personal e indelegable**.

#### **Art. 80: Sesiones plenarias**

- Son **públicas**, salvo acuerdo por mayoría absoluta de la Cámara o por lo estipulado en su Reglamento.

#### **Art. 81: Leyes orgánicas**

- Regulación de los **derechos fundamentales y libertades públicas**, Estatutos de Autonomía, régimen electoral y otras materias según la Constitución.
- Requieren **mayoría absoluta del Congreso** en una votación final sobre el conjunto del texto.

#### **Art. 82: Delegación legislativa al Gobierno**

- Las Cortes pueden delegar al Gobierno la capacidad de dictar normas con rango de ley.
- Instrumentos: **Leyes de bases** (para textos articulados) y leyes ordinarias (para refundir textos).

#### **Art. 83: Limitaciones a la delegación legislativa**

- No podrá concederse para materias propias de **leyes orgánicas**, ni para regular competencias exclusivas del Congreso o del Senado.

#### **Art. 84: Modificación de normas delegadas**

- Si se tramita un proyecto de ley en las Cortes que contradiga una norma dictada por delegación, esta quedará **sin efecto en lo que contradiga la nueva ley**.

#### **Art. 85: Real Decreto Legislativo**

- Las normas dictadas por delegación legislativa se adoptan bajo la forma de **Decreto Legislativo**.

#### **Art. 86: Decretos-leyes**

- El Gobierno podrá dictarlos en casos de **extraordinaria y urgente necesidad**.
- No podrán afectar a materias de leyes orgánicas.
- Deben ser sometidos al Congreso para **su convalidación o derogación** en un plazo máximo de **30 días**.

#### **Art. 87: Iniciativa legislativa**

- Corresponde al **Gobierno, al Congreso, al Senado, a las Asambleas Legislativas de las CCAA** y mediante **iniciativa popular** con al menos **500,000 firmas** (excepto en materias reservadas a leyes orgánicas).

#### **Art. 88: Proyecto de ley**

- Aprobados por Consejo de Ministros, y presentados ante el Congreso, acompañado de una exposición de motivos.

#### **Art. 89: Proposiciones de ley**

- Regulada por los Reglamentos de las Cámaras

#### **Art. 90: Actuación legislativa del Senado**

- Tras la aprobación de un proyecto de ley en el Congreso, se remite al Senado para **deliberación en un plazo de 2 meses**.
- El Senado puede:
  - **Oponer veto** (mayoría absoluta).
  - **Introducir enmiendas**.
- En caso de veto:
  - El Congreso puede ratificarlo por **mayoría absoluta** o por mayoría simple tras 2 meses.
- Proyectos urgentes: plazo reducido a **20 días naturales**.

#### **Art. 91: Sanción y promulgación de las leyes**

- El Rey sancionará y promulgará las leyes en un plazo de **15 días** desde su aprobación.

#### **Art. 92: Referéndum**

- Convocado por el Rey, a **propuesta del Presidente del Gobierno**, previa autorización del Congreso, para decisiones políticas de **especial trascendencia**.
- Regulación por **Ley Orgánica**.

### **Título IV: Del Gobierno y de la Administración**

#### **Art. 97: Funciones del Gobierno**

- Dirige la **política interior y exterior**, la **defensa del Estado** y la **Administración civil y militar**.
- Ejerce la función **ejecutiva** y la potestad reglamentaria.

#### **Art. 98: Composición del Gobierno**

- Formado por el **Presidente, Vicepresidentes, Ministros** y otros miembros según la ley.
- El Presidente dirige la acción del Gobierno y coordina las funciones de sus miembros.

#### **Art. 99: Elección del Presidente del Gobierno**

- El Rey propone un candidato tras consultar a los grupos políticos.
- El Congreso otorga su confianza al candidato por **mayoría absoluta** o, en segunda votación, por mayoría simple.
- Si en **2 meses** no se consigue la investidura, el Rey disolverá las Cámaras y convocará elecciones.

#### **Art. 100: Nombramiento de Ministros**

- Realizado por el Rey a propuesta del Presidente del Gobierno.

#### **Art. 101: Cese del Gobierno**

- Ocurre tras elecciones, pérdida de confianza, dimisión o fallecimiento del Presidente.
- El Gobierno en funciones limita sus actividades a asuntos ordinarios.

#### **Art. 102: Responsabilidad criminal del Gobierno**

- Enjuiciados por la **Sala de lo Penal del Tribunal Supremo**.
- Para delitos graves, se requiere la aprobación por **mayoría absoluta del Congreso**.

#### **Art. 103: Principios de la Administración Pública**

- Actúa según los principios de **eficacia, jerarquía, descentralización, desconcentración y coordinación**.
- El acceso a la función pública se basa en los principios de **mérito y capacidad**.

#### **Art. 104: Fuerzas y Cuerpos de Seguridad**

- Su misión es garantizar la **seguridad ciudadana** y proteger el libre ejercicio de derechos y libertades.

#### **Art. 105: Participación ciudadana y acceso a información**

- Derecho de los ciudadanos a participar en los procedimientos administrativos que les afecten y a acceder a archivos y registros, salvo en casos de **seguridad o intimidad**.

#### **Art. 106: Control judicial de la Administración**

- Los Tribunales controlan la **legalidad de los actos administrativos**.
- Derecho a indemnización por daños causados por la Administración, salvo fuerza mayor.

#### **Art. 107: Consejo de Estado**

- Es el **supremo órgano consultivo del Gobierno**.
- Su regulación se realiza por **ley orgánica**.

### **Título V: De las relaciones entre el Gobierno y las Cortes Generales**

#### **Art. 108: Responsabilidad del Gobierno**

- El Gobierno responde de su gestión política de forma **solidaria** ante las Cámaras.

#### **Art. 109: Derecho de información**

- Las Cámaras y Comisiones pueden solicitar **información y ayuda** al Gobierno, Departamentos y Administraciones públicas.

#### **Art. 110: Presencia del Gobierno en las Cámaras**

- Las Cámaras pueden reclamar la **presencia de los miembros del Gobierno**.
- Los miembros del Gobierno tienen derecho a asistir y **ser escuchados** en las Cámaras.

#### **Art. 111: Sesión de control**

- El Gobierno responde a **interpelaciones y preguntas** formuladas por las Cámaras.

#### **Art. 112: Cuestión de confianza**

- **El Presidente del Gobierno** puede plantear una cuestión de confianza previa deliberación del Consejo de Ministros.
- Se otorga si obtiene **mayoría simple** del Congreso.

#### **Art. 113: Moción de censura**

- Propuesta por **1/10 de los Diputados**, debe incluir un candidato a la Presidencia.
- Se aprueba con **mayoría absoluta** del Congreso.

#### **Art. 114: Consecuencias de la moción de censura**

- Si es aprobada: **dimisión del Gobierno** y el candidato propuesto será investido.

- Si no prospera: los firmantes no podrán presentar otra durante el mismo período de sesiones.

#### **Art. 115: Disolución de las Cámaras**

- Puede ser propuesta por el **Presidente del Gobierno**, deliberada en Consejo de Ministros y decretada por el Rey.
- No procede durante una **moción de censura** ni antes de un año desde la última disolución.

#### **Art. 116: Estados de alarma, excepción y sitio**

- Declarados según ley orgánica:
  - **Estado de alarma:** Máximo 15 días, prorrogable con autorización del Congreso.
  - **Estado de excepción:** Máximo 30 días, autorizado por el Congreso.
  - **Estado de sitio:** Declarado por **mayoría absoluta del Congreso**, a propuesta del Gobierno.

### **Título VIII: De la Organización Territorial del Estado**

#### **Art. 137: Organización territorial**

- El Estado se organiza en **municipios, provincias y comunidades autónomas**, todos ellos con **autonomía para gestionar sus intereses**.

#### **Art. 138: Solidaridad interterritorial**

- El Estado garantiza el **equilibrio económico y social** entre las distintas zonas del territorio.

#### **Art. 139: Igualdad territorial**

- Todos los españoles tienen **los mismos derechos y obligaciones en todo el territorio**.
- Derecho a la **libre circulación** por todo el territorio nacional.

#### **Art. 140: Municipios**

- Gozan de **personalidad jurídica plena**.
- Su gobierno corresponde a **alcaldes y concejales**, elegidos por los vecinos.

#### **Art. 141: Provincias**

- Son **entidades locales** determinadas por la agrupación de municipios.
- Su gobierno se ejerce a través de **Diputaciones u otras corporaciones representativas**.

#### **Art. 142: Haciendas locales**

- Se financian con **tributos propios, participación en los del Estado y CCAA, y otros recursos**.

#### **Art. 143: Constitución de las CCAA (Vía ordinaria)**

- Provincias con características comunes pueden constituirse en **comunidades autónomas**.
- El proceso debe ser impulsado por las **Diputaciones y 2/3 de los municipios**.

#### **Art. 144: Constitución de CCAA (Vía excepcional)**

- Puede establecerse por **ley orgánica**, por razones de **interés general**.

#### **Art. 145: Prohibición de federación**

- Las **CCAA no pueden federarse** ni establecer convenios que impliquen privilegios.

#### **Art. 146: Proyecto de Estatuto**

- Elaborado por una **asamblea** de Diputaciones y representantes parlamentarios.
- Elevado a las **Cortes Generales** para su tramitación como ley.

#### **Art. 147: Estatutos de autonomía**

- Norma institucional básica de cada **CCAA**.
- Contenido: **Denominación de la Comunidad, delimitación del territorio, instituciones de autogobierno y competencias asumidas**.
- Su **reforma** requiere aprobación por **Ley Orgánica**.

#### **Art. 148: Competencias de las CCAA**

- Ejemplos: **urbanismo, vivienda, agricultura, museos, sanidad, policía local, ordenación del territorio, y obras públicas**.
- Tras **5 años**, las competencias pueden ampliarse mediante reforma del Estatuto.

#### **Art. 149: Competencias exclusivas del Estado**

- Incluyen: **nacionalidad, defensa, relaciones internacionales, legislación básica, transporte, comunicaciones, justicia, estadística, y normativa electoral**.
- En caso de conflicto, prevalecen las normas estatales, salvo competencias exclusivas de las CCAA.

#### **Art. 150: Delegación de competencias**

- **Leyes marco** permiten a las CCAA dictar normas legislativas en competencias estatales.
- Posibilidad de **leyes de armonización** para coordinar disposiciones autonómicas (por **mayoría absoluta**).

#### **Art. 151: Vía especial de acceso a la autonomía**

- Requiere: **Aprobación por Asamblea y referéndum provincial**.
- Aumenta el nivel de competencias sin esperar 5 años.

#### **Art. 152: Organización institucional CCAA**

- Basada en: **Asamblea Legislativa, Consejo de Gobierno y Presidente**.

- Tribunal Superior de Justicia culmina la organización judicial en la CCAA.

#### **Art. 153: Control estatal sobre CCAA**

- Se ejerce a través del: **Tribunal Constitucional, Gobierno, jurisdicción contencioso-administrativa y Tribunal de Cuentas.**

#### **Art. 154: Delegado del Gobierno**

- Representa al Estado en la **CCAA**, dirige la Administración estatal y la coordina con la autonómica.

#### **Art. 155: Control excepcional sobre CCAA**

- El Gobierno puede obligar a una CCAA al cumplimiento forzoso de sus obligaciones.
- Requiere aprobación por **mayoría absoluta del Senado**.

#### **Art. 156: Autonomía financiera de las CCAA**

- Basada en **solidaridad y coordinación** con Hacienda estatal.
- Permite recaudar tributos y gestionar recursos financieros propios.

#### **Art. 157: Recursos económicos de las CCAA**

- Incluyen: **impuestos cedidos parcial o totalmente, impuestos propios, tasas, transferencias del Fondo de Compensación interterritorial y operaciones de crédito.**

#### **Art. 158: Fondo de compensación interterritorial**

- Distribuido por las **Cortes Generales** para corregir desigualdades económicas entre **CCAA y provincias**.

### **Título IX: Del Tribunal Constitucional**

#### **Art. 159: Composición**

- Formado por **12 miembros**:
  - **4 designados por el Congreso** (mayoría 3/5).
  - **4 por el Senado** (mayoría 3/5).
  - **2 por el Gobierno**.
  - **2 por el CGPJ**.
- Mandato de **9 años**, renovados por tercios cada 3 años.
- Requisitos: **Juristas de reconocida competencia y +15 años de ejercicio profesional**.

#### **Art. 160: Presidencia del TC**

- Nombrada por el Rey entre sus miembros, a propuesta del Tribunal.
- Período: **3 años**.

#### **Art. 161: Competencias del TC**

- Incluyen:
  - Declaración de **inconstitucionalidad de normas con rango de ley**.
  - **Recurso de amparo** por violación de derechos y libertades.
  - **Conflictos de competencias** entre Estado y CCAA o entre CCAA.

#### **Art. 162: Recurso de inconstitucionalidad y de amparo**

- **Recurso de inconstitucionalidad:** Puede ser interpuesto por **Presidente del Gobierno, Defensor del Pueblo, 50 Diputados, 50 Senadores, órganos de las CCAA**.
- **Recurso de amparo:** Accesible para **toda persona natural o jurídica**, Defensor del Pueblo y Ministerio Fiscal.

#### **Art. 163: Cuestión de inconstitucionalidad**

- Puede plantearse por **cualquier órgano judicial** si depende de la validez de una norma con rango de ley.

#### **Art. 164: Sentencias del TC**

- Publicadas en el **BOE** con valor de **cosa juzgada**.
- No cabe recurso contra ellas.

#### **Art. 165: Regulación del TC**

- Regulado mediante **Ley Orgánica**: funcionamiento, estatuto y procedimientos.

### **Título X: De la reforma constitucional**

#### **Art. 166: Iniciativa de reforma**

- Puede ser propuesta por: **Gobierno, Congreso, Senado y CCAA**.

#### **Art. 167: Reforma parcial**

- Requiere aprobación por **3/5 de Congreso y Senado**.
- En caso de desacuerdo, puede aprobarse por **2/3 del Congreso y mayoría absoluta del Senado**.
- Referéndum si lo solicitan **1/10 de cualquier Cámara**.

#### **Art. 168: Reforma total o sobre ciertos títulos**

- Requiere:
  - Aprobación inicial por **2/3 de Congreso y Senado**.
  - **Disolución de las Cortes**.
  - Nuevas Cortes deben ratificarlo con **2/3** y someterlo a referéndum.

**Art. 169: Prohibición de reforma**

- No puede realizarse en tiempos de **guerra** o bajo los **estados de alarma, excepción o sitio.**

# Estructura y Datos relevantes de la Constitución

## Fechas claves

Aprobada por las Cortes	<b>31 de Octubre de 1978</b>
Ratificada por el Pueblo Español	6 de Diciembre de 1978
Sancionada por el Rey	27 de Diciembre de 1978
Publicada en el BOE	29 de Diciembre de 1978
Última modificación ( <i>art. 135. Deuda Pública</i> )	27 de Septiembre de 1978

## Estructura

- **PREÁMBULO**
- **TÍTULO PRELIMINAR** [art. 1-9]
- **TÍTULO I** De los derechos y deberes fundamentales [art. 10-55]
  - **CAPÍTULO PRIMERO** De los españoles y extranjeros [art. 11-13]
  - **CAPÍTULO SEGUNDO** Derechos y libertades [art. 14]
    - Sección 1ª De los derechos fundamentales y de las libertades públicas [art. 15-29]
    - Sección 2ª De los derechos y deberes de los ciudadanos [art. 30-38]
  - **CAPÍTULO TERCERO** De los principios rectores de la política social y económica [art. 39-52]
- **CAPÍTULO CUARTO** De las garantías de las libertades y derechos fundamentales [art. 53-54]
- **CAPÍTULO QUINTO** De la suspensión de los derechos y libertades [art. 55]
- **TÍTULO II** De la Corona [art. 56-65]
- **TÍTULO III** De las Cortes Generales [art. 66-96]
  - **CAPÍTULO PRIMERO** De las Cámaras [art. 66-80]
  - **CAPÍTULO SEGUNDO** De la elaboración de las leyes [art. 81-92]
  - **CAPÍTULO TERCERO** De los Tratados Internacionales [art. 93-96]
- **TÍTULO IV** Del Gobierno y de la Administración [art. 97-107]
- **TÍTULO V** De las relaciones entre el Gobierno y las Cortes Generales [art. 108-116]
- **TÍTULO VI** Del Poder Judicial [art. 117-127]
- **TÍTULO VII** Economía y Hacienda [art. 128-136]
- **TÍTULO VIII** De la Organización Territorial del Estado [art. 137-158]
  - **CAPÍTULO PRIMERO** Principios generales [art. 137-139]
  - **CAPÍTULO SEGUNDO** De la Administración Local [art. 140-142]
  - **CAPÍTULO TERCERO** De las Comunidades Autónomas [art. 143-158]
- **TÍTULO IX** Del Tribunal Constitucional [art. 159-165]
- **TÍTULO X** De la reforma constitucional [art. 166-169]
- **DISPOSICIONES ADICIONALES** (1ª a 4ª)
- **DISPOSICIONES TRANSITORIAS** (1ª a 9ª)
- **DISPOSICIONES DEROGATORIA** (única)
- **DISPOSICIÓN FINAL** (única)

**Datos más relevantes de la Constitución Española**

Tema/Acción	Artículo(s)	Datos Importantes	Mayoría Necesaria
<b>Reforma parcial de la Constitución</b>	Artículo 167	<ul style="list-style-type: none"> <li>- Aprobación inicial por ambas Cámaras.</li> <li>- Si no hay acuerdo, se forma una Comisión Mixta para elaborar un texto común.</li> <li>- Posibilidad de referéndum si lo solicita el 10% de cualquiera de las Cámaras.</li> </ul>	3/5 de ambas Cámaras
<b>Reforma total o de partes esenciales (*)</b>	Artículo 168	<ul style="list-style-type: none"> <li>- Aprobación por 2/3 de ambas Cámaras.</li> <li>- Disolución inmediata de las Cortes Generales.</li> <li>- Nuevas Cortes deben ratificar la decisión y aprobar el texto por 2/3.</li> <li>- Referéndum obligatorio.</li> </ul>	2/3 de ambas Cámaras en dos legislaturas
<b>Aprobación de Leyes Orgánicas</b>	Artículo 81	<ul style="list-style-type: none"> <li>- Relativas a derechos fundamentales, Estatutos de Autonomía y régimen electoral general.</li> </ul>	Mayoría absoluta del Congreso
<b>Aprobación de Leyes Ordinarias</b>		<ul style="list-style-type: none"> <li>- No requieren mayoría cualificada.</li> </ul>	Mayoría simple del Congreso
<b>Decretos Legislativos</b>	Artículos 82-85	<ul style="list-style-type: none"> <li>- Delegación de las Cortes Generales al Gobierno para dictar normas con rango de ley.</li> <li>- Mediante Ley de Bases o Ley Ordinaria.</li> </ul>	Según delegación establecida
<b>Decretos-Leyes</b>	Artículo 86	<ul style="list-style-type: none"> <li>- Normas provisionales dictadas por el Gobierno en casos de urgente necesidad.</li> <li>- No pueden afectar a ciertas materias (ej. LO).</li> <li>- Deben ser convalidados por el Congreso en 30 días.</li> </ul>	Aprobación por mayoría simple del Congreso
<b>Estados de Alarma, Excepción y Sitio</b>	Artículo 116	<ul style="list-style-type: none"> <li>- <b>Estado de Alarma:</b> Declarado por el Gobierno por 15 días, prorrogable con autorización del Congreso.</li> <li>- <b>Estado de Excepción:</b> Requiere autorización previa del Congreso, máximo 30 días, prorrogable.</li> <li>- <b>Estado de Sitio:</b> Declarado por mayoría absoluta del Congreso a propuesta del Gobierno.</li> </ul>	Variable según el estado (ver datos)

<b>Cuestión de Confianza</b>	Artículo 112	- Planteada por el Presidente del Gobierno. - Si no obtiene la confianza, debe dimitir.	Mayoría simple del Congreso
<b>Moción de Censura</b>	Artículos 113-114	- Iniciada por al menos 1/10 de los Diputados. - Debe incluir candidato a Presidente. - Si se aprueba, el Gobierno cesa y el candidato es investido.	Mayoría absoluta del Congreso
<b>Elección del Presidente del Gobierno</b>	Artículo 99	- Propuesto por el Rey tras consulta con los partidos. - Debe exponer su programa ante el Congreso.	Primera votación: mayoría absoluta Segunda votación (48h después): mayoría simple
<b>Aprobación de Presupuestos Generales</b>		- Ley anual presentada por el Gobierno.	Mayoría simple del Congreso
<b>Autorización para celebrar Tratados Internacionales</b>	Artículo 94	- Tratados de carácter político, militar o que afecten a la soberanía requieren autorización de las Cortes Generales.	Mayoría simple del Congreso
<b>Designación de miembros del Tribunal Constitucional</b>	Artículo 159	- 4 por el Congreso, 4 por el Senado, 2 por el Gobierno y 2 por el CGPJ.	Congreso y Senado: mayoría de 3/5
<b>Suspensión de Derechos y Libertades</b>	Artículo 55	- Durante estados de excepción y sitio pueden suspenderse ciertos derechos. - Suspensión individual para investigaciones sobre terrorismo, mediante LO.	Según lo establecido en la LO correspondiente
<b>Control excepcional de las CCAA</b>	Artículo 155	- El Gobierno puede obligar a una CCAA al cumplimiento forzoso de sus obligaciones.	Aprobación por mayoría absoluta del Senado
<b>Iniciativa Legislativa Popular</b>	Artículo 87	- Presentación de proposiciones de ley con al menos 500,000 firmas acreditadas.	No aplica (se excluyen ciertas materias)

\* Partes esenciales incluyen el Título Preliminar, Capítulo II Sección 1º del Título I (Derechos Fundamentales y Libertades Públicas) y el Título II (De la Corona).

**Notas Adicionales:**

- **Mayorías en las Cámaras:**
  - **Mayoría Simple:** Más votos a favor que en contra.
  - **Mayoría Absoluta:** Mitad más uno del total de miembros.
  - **Mayoría de 3/5 y 2/3:** Se calcula sobre el total de miembros de cada Cámara.
- **Referéndum:**
  - Puede ser consultivo para decisiones de especial trascendencia política (Artículo 92).
  - Es obligatorio en ciertas reformas constitucionales (Artículo 168).
- **Estados de Excepción:**
  - Durante estos estados, se pueden suspender derechos como la libertad personal, inviolabilidad del domicilio, secreto de las comunicaciones, etc.
- **Funciones del Rey (Artículo 62):**
  - Sancionar y promulgar leyes.
  - Convocar y disolver las Cortes Generales.
  - Nombrar y separar a los miembros del Gobierno.
  - Expedir los decretos acordados en el Consejo de Ministros.

## Estatuto de Autonomía de la Comunidad Valenciana

# Ley Orgánica 5/1982, de 1 de julio, de Estatuto de Autonomía de la Comunidad Valenciana

### Título I: La Comunitat Valenciana

#### Art. 1: Comunitat Valenciana

- El pueblo valenciano, organizado históricamente como Reino de Valencia, se constituye como Comunidad Autónoma en la unidad de la Nación Española. Reconocida como **nacionalidad histórica**, ejerce su derecho de autogobierno bajo la denominación de "Comunitat Valenciana".
- **Voluntad democrática** y derecho de autogobierno.
- **Objetivo:** Refuerzo de la democracia y participación ciudadana.
- Asume los **valores de la Unión Europea**.

#### Art. 2: Territorio

- Incluye los municipios de las provincias de **Alicante, Castellón y Valencia**.

#### Art. 3: Condición política de valencianos

- Aplicable a los españoles con **vecindad administrativa** en la CV.
- Residentes en el extranjero con última vecindad en la CV y sus descendientes españoles (si lo solicitan).
- Derecho civil foral valenciano para quienes posean **vecindad civil valenciana**.

#### Art. 4: Bandera y simbología de la CV

- **Senyera:** Cuatro barras rojas sobre fondo amarillo con franja azul junto al asta.
- **Simbología heráldica:** Regulada por ley de Les Corts.

#### Art. 5: Sede de las instituciones

- **Palacio de la Generalitat:** Valencia.
- Otras instituciones pueden ubicarse en cualquier municipio de la CV.

#### Art. 6: Lengua propia

- **Valenciano y Castellano:** Lenguas oficiales.
- **Derecho a conocer, usar y recibir enseñanza** en ambas lenguas.
- **L'Acadèmia Valenciana de la Llengua** regula el idioma.

#### Art. 7: Recuperación de Fueros

- Recuperación del contenido de los **Fueros históricos del Reino de Valencia**, con eficacia territorial salvo que otras normas sean aplicables.

## Título II: De los derechos de los valencianos y valencianas

### Art. 8: Derechos y obligaciones

- Derechos de la **Constitución Española**, la **UE** y la **Declaración Universal de Derechos Humanos (DUDH)**.

### Art. 9: Igualdad lingüística y participación

- Derecho a dirigirse a la Administración en **cualquiera de las lenguas oficiales** y recibir respuesta en la misma.
- Participación en la vida política, económica, cultural y social de la CV.

### Art. 10: Derechos sociales

- La Generalitat debe defender los derechos sociales.
- **Carta de Derechos Sociales**: Principios para guiar políticas sociales.

### Art. 11: Igualdad de oportunidades

- Garantiza la **no discriminación** y la compatibilidad entre la vida familiar y laboral.

### Art. 12: Protección de la identidad

- **Defensa y promoción** de la identidad, valores e intereses del pueblo valenciano.

### Art. 13: Discapacidad

- Derecho a **prestaciones públicas** que aseguren autonomía personal, integración socioprofesional y participación en la vida social.

### Art. 14: Catástrofes naturales

- Derecho a recibir **asistencia pública** en situaciones de catástrofe.

### Art. 15: Solidaridad y renta de ciudadanía

- Derecho a la **solidaridad** y a una **renta de ciudadanía** para los más necesitados.

### Art. 16: Derecho a la vivienda

- Acceso a una **vivienda digna** como derecho fundamental.

### Art. 17: Entorno sano y agua

- Derecho a un medio ambiente **sano y equilibrado**.
- Derecho a **agua de calidad** y redistribución de recursos sobrantes.

### Art. 18: Protección del sector agrario

- Fomento y protección de la **agricultura** y sectores agrarios esenciales.

### Art. 19: Equilibrio territorial

- Promoción de un modelo de desarrollo **sostenible y equilibrado** entre zonas costeras e interiores.
- Derecho al acceso a **nuevas tecnologías**.

### Título III: La Generalitat

#### Art. 20: La Generalitat

- Es el **conjunto de instituciones de autogobierno de la Comunitat Valenciana**.
- **Se compone de:**
  - **Instituciones principales: Les Corts, el President y el Consell.**
  - También incluye: **Sindicatura de Comptes, Síndic de Greuges, Consell Valencià de Cultura, Acadèmia Valenciana de la Llengua, Consell Jurídic Consultiu y Comité Econòmic i Social.**

### CAPÍTULO II: LES CORTS VALENCIANAS

#### Art. 21: Les Corts

- **Potestad legislativa** y representación del pueblo valenciano.
- Son **inviolables** y gozan de autonomía.
- Sede: **Palacio de los Borja, Valencia**.

#### Art. 22: Funciones de Les Corts

- **Aprobar presupuestos**, emitir deuda pública y controlar la acción del Consell.
- Elegir al **President de la Generalitat** y exigir su responsabilidad política.
- Presentar iniciativas legislativas, recursos de inconstitucionalidad y acuerdos de cooperación.
- Designar senadores y debatir legislación europea relevante

#### Art. 23: Composición de Les Corts

- Diputados: **Mínimo 99**, elegidos por **sufragio universal, libre, igual, directo y secreto**.
- Designados según la **Ley Electoral Valenciana** y criterios de proporcionalidad y comarcalización.
- **Inviolabilidad**: Por opiniones y votos emitidos en el ejercicio de sus funciones, salvo delito flagrante.
- Competencia judicial:
  - **Tribunal Superior de Justicia de la CV**: Delitos en la CV.

- **Tribunal Supremo:** Delitos fuera de la CV.
- Mandato: **4 años**, salvo disolución anticipada.
- Convocatoria: **Decreto del President de la Generalitat**, especificando diputados, duración de campaña, día de votación y constitución.

#### **Art. 24: Ley Electoral Valenciana**

- Aprobación por **2/3 de Les Corts**.
- Garantiza un **mínimo de 20 diputados por circunscripción provincial**.
- Resto de diputados distribuidos proporcionalmente a la población, respetando una **desproporción inferior a 1/3**.

#### **Art. 25: Funcionamiento de Les Corts**

- Organizan su funcionamiento mediante **Reglamento interno** aprobado por **mayoría absoluta**.
- **Funcionamiento:** Pleno y Comisiones.
- **Delegación en Comisiones** para la elaboración de leyes, salvo bases y presupuestos.
- Sesiones:
  - **Ordinarias:** Dos al año, mínimo 8 meses (septiembre y febrero).
  - **Extraordinarias:** Convocadas por el President de Les Corts o a petición del Consell, la Diputación Permanente o 1/5 de los diputados.
- **Adopción de acuerdos:** Por mayoría simple, salvo excepciones.
- Leyes promulgadas por el **President de Les Corts** en nombre del Rey, publicadas en el **DOG y BOE** en un plazo de 15 días, y en ambas lenguas oficiales.

#### **Art. 26: Iniciativa legislativa**

- **Corresponde:** Les Corts y Consell.
- Ejercicio: Por grupos parlamentarios, diputados e iniciativa popular.

### **CAPÍTULO III: EL PRESIDENT DE LA GENERALITAT**

#### **Art. 27: Elección del President**

- **Elegido por Les Corts** de entre sus miembros y nombrado por el Rey.
- Propuesto por el **President de Les Corts**.
- **Mayoría requerida:**
  - Primera votación: **Mayoría absoluta**.
  - Segunda votación (48 horas): **Mayoría simple**.

- Si no se elige en 2 meses: **Disolución de Les Corts** y convocatoria de nuevas elecciones.

#### **Art. 28: Funciones del President**

- Dirige la acción del Consell y coordina sus funciones.
- **Más alta representación** de la CV y ordinaria del Estado.
- Disolución de Les Corts (previo acuerdo del Consell), salvo en caso de moción de censura.
- **Moción de censura:**
  - Propuesta por **1/5 de los diputados**.
  - Debe incluir un candidato alternativo.
  - Aprobación por **mayoría absoluta** tras un plazo de 5 días.

### **CAPÍTULO IV: EL CONSELL**

#### **Art. 29: El Consell**

- Órgano colegiado con **potestad ejecutiva y reglamentaria**.
- Dirige la Administración bajo autoridad de la Generalitat.
- Miembros designados por el **President**.
- Sede del Consell: **Ciudad de Valencia**

#### **Art. 30: Responsabilidad del Consell**

- Responde **solidariamente** ante Les Corts, sin perjuicio de la responsabilidad directa de cada miembro.
- **Cuestión de confianza:** Propuesta por el President, requiere mayoría simple.

#### **Art. 31: Responsabilidad penal y civil**

- Igual régimen que para los diputados: TSJCV (dentro de la CV) y Tribunal Supremo (fuera de la CV).

#### **Art. 32: Recurso de inconstitucionalidad**

- Podrá ser interpuesto por el Consell en las mismas condiciones que el Estado.

#### **Art. 33: Tribunal Superior de Justicia de la CV (TSJCV)**

- **Máximo órgano judicial** en la Comunidad Valenciana.
- Coordina con la Generalitat a través de la **Comisión Mixta**.

#### **Art. 34: Miembros del Tribunal Superior de Justicia de la Comunitat Valenciana (TSJCV)**

- **Presidente:** Nombrado por el Rey a propuesta del Consejo General del Poder Judicial (CGPJ).

- Resto de miembros: Según la **Ley Orgánica del Poder Judicial (LOPJ)**.

#### **Art. 35: Oposiciones**

- A instancia de La Generalitat.

#### **Art. 36: Administración de Justicia**

- La Generalitat asume las competencias que la **LOPJ** le reconozca al Estado en su ámbito territorial.

#### **Art. 37: Competencias judiciales**

- Incluyen litigios, recursos de casación y revisión en el ámbito de la CV.

#### **Art. 36: Administración de Justicia**

- La Generalitat asume las facultades que le otorga la **LO del Poder Judicial**.

#### **Art. 38: Síndic de Greuges**

- **Defensor del Pueblo Valenciano** designado por Les Corts.
- Presenta informe anual.

#### **Art. 39: Sindicatura de Comptes**

- Órgano de **control financiero externo** de la Generalitat y entes locales.

#### **Art. 40: Consell Valencià de Cultura**

- **Institución consultiva y asesora** de las instituciones públicas en materias culturales valencianas.
- **Regulación:** Por Ley de Les Corts.

#### **Art. 41: Acadèmia Valenciana de la Llengua**

- Institución **normativa del valenciano**, cuyas disposiciones son de aplicación obligatoria en todas las AAPP.

#### **Art. 42: Comité Econòmic i Social**

- Órgano consultivo del **Consell** y otras instituciones públicas en materias económicas, sociolaborales y de empleo.
- Regulado por **Ley de Les Corts**.

#### **Art. 43: Consell Jurídic Consultiu**

- **Órgano consultivo supremo** del Consell, la Administración Autonómica y las administraciones locales de la CV en materia jurídica.
- Regulado por **Ley de Les Corts**.

#### **Art. 44: Desarrollo legislativo**

- **Decretos legislativos** y **Decretos-Leyes** regulados de forma análoga a la Constitución, pero sin carácter "Real".

#### **Art. 45: Derecho Valenciano**

- Aplicación preferente dentro del territorio de la CV.

#### **Art. 46: Competencias**

- Incluye las competencias explícitas e implícitas recogidas en el Estatuto.

#### **Art. 47: Leyes de la Generalitat**

- Están excluidas de la jurisdicción contencioso-administrativa y solo sujetas al **control de constitucionalidad** por el Tribunal Constitucional.

#### **Art. 48: Potestades y privilegios de la Generalitat**

- Son equivalentes a los de la Administración del Estado.

#### **Art. 49: Competencias exclusivas**

- Cultura, patrimonio, educación, sanidad, carreteras, turismo, pesca interior, y policía autonómica, entre otras.

#### **Art. 50: Desarrollo legislativo y ejecución**

- La Generalitat tiene competencias de desarrollo legislativo y ejecución en:
  - **Régimen jurídico** de las AAPP.
  - Expropiación forzosa, contratos administrativos, ordenación del crédito, banca y seguros.
  - **Medio ambiente** y pesca en aguas interiores.
  - Consultas populares en el ámbito autonómico.

#### **Art. 51: Ejecución de legislación del Estado**

- Competencias de **ejecución** en materias como:
  - **Legislación laboral.**
  - **Propiedad intelectual.**
  - Pesos, medidas, ferias internacionales y catastro.
  - Salvamento marítimo, playas, puertos y aeropuertos sin interés general.

#### **Art. 52: Ordenación de la actividad económica**

- **Planificación** y regulación de la actividad económica dentro de la CV.
- Competencia en **sectores estratégicos** y reestructuración económica.

#### **Art. 53: Educación**

- Competencia **exclusiva** en la regulación y administración de la enseñanza en todos sus niveles, grados y modalidades.
- **Alta inspección** corresponde al Estado.

#### **Art. 54: Instituciones sanitarias**

- Organización, administración y gestión de todas las instituciones sanitarias en la CV.
- Desarrollo legislativo y ejecución de la legislación básica del Estado.
- Gestión económica de la Seguridad Social, salvo **alta inspección** (Estado).

#### **Art. 55: Policía Autonómica y Policía Judicial**

- **Policía Autónoma:** Creada mediante Ley de Les Corts y LO.
  - **Funciones:** Protección de personas y bienes, **seguridad pública**, vigilancia de edificios de la Generalitat.
  - La Generalitat ejerce el **mando supremo** y coordina la Policía Local.
- **Policía Judicial:** Depende de la Administración de Justicia, conforme a leyes procesales.
- **Junta de Seguridad:** Coordina actuaciones entre la Policía Autónoma y las Fuerzas y Cuerpos de Seguridad del Estado.

#### **Art. 56: Medios de comunicación**

- Desarrollo legislativo y ejecución en la CV.
- Creación del **Consell Audiovisual** mediante Ley de Les Corts (**3/5**).

#### **Art. 57: Real Monasterio de Santa María de la Valldigna**

- Reconocido como **símbolo de la grandeza del Pueblo Valenciano** y del antiguo Reino de Valencia.

#### **Art. 58: Notarios y Registradores**

- Nombrados por el **Consell**.

### **Título V: Relaciones con el Estado y otras Comunidades Autónomas**

#### **Art. 59: Convenios de colaboración**

- **Aprobados por Les Corts** y comunicados a las Cortes Generales.
- Entrada en vigor: **30 días** tras publicación.
- Otros supuestos: Requieren aprobación expresa de las Cortes Generales.

#### **Art. 60: Transferencia o delegación de competencias**

- Mediante Leyes Marco y Leyes de Bases.

### **Título VI: Relaciones con la Unión Europea**

#### **Art. 61: Relaciones con la UE**

- **Delegación en Bruselas:** Representación, defensa y promoción de intereses multisectoriales de la CV.
- Derecho a participar en procesos que afecten a la CV.

## Título VII: Acción exterior

### Art. 62: Participación en la acción exterior del Estado

- Convenios con regiones europeas: Previa autorización de **Les Corts**.
- Acuerdos no normativos: Notificados a **Les Corts**.

## Título VIII: Administración Local

### Art. 63: Administraciones locales

- Regidas por los principios de **coordinación, cooperación y colaboración**.

### Art. 64: Municipios

- Regidos por **Ayuntamientos**, elegidos por sufragio universal, igual, libre, directo y secreto.
- Responsabilidades distribuidas según el principio de **subsidiariedad**.

### Art. 65: Comarcas

- División comarcal regulada por **Ley de Les Corts** (aprobación por **2/3**).
- Agrupación de municipios para servicios comunes y gestión de asuntos locales.
- También aplicable a **áreas metropolitanas y agrupaciones de comarcas**.

### Art. 66: Diputaciones Provinciales

- Expresión de la **autonomía provincial**.
- Fórmulas de coordinación reguladas por **Ley de Les Corts** (mayoría absoluta).
- Les Corts pueden revocar competencias delegadas.

## Título IX: Economía y Hacienda

### Art. 67: Financiación de la Generalitat

- Principios: **Autonomía, suficiencia y solidaridad**.
- Sistema regulado por Ley Orgánica.

### Art. 68: Medidas de compensación

Si el sistema tributario español se modifica, la CV tiene derecho a medidas compensatorias del Estado.

**Art. 69: Servicio Tributario Valenciano**

Órgano encargado de aplicar tributos propios de la Generalitat.

**Art. 70: Compensación a entes locales**

El Estado adoptará medidas similares a las del Art. 68.

**Art. 71: Patrimonio de la Generalitat**

- Conformado por bienes propios, adquiridos, herencias intestadas, donaciones y demás activos.

**Art. 72: Hacienda de la Generalitat**

- Fuentes de ingresos:
  - Impuestos propios, tasas, contribuciones especiales.
  - Rendimientos de impuestos cedidos por el Estado.
  - Recargos, subvenciones, deuda, sanciones, fondos de la UE.
- Regulado por **Fondo de Compensación Interterritorial**.

**Art. 73: Impuestos cedidos**

- IRPF e IVA: 50%.
- Impuestos especiales como hidrocarburos, alcohol y tabaco: **58%-100%** según el caso

**Art. 74: Participación en impuestos del Estado**

- Se fija mediante acuerdo con el Parlamento y el Gobierno de España.

**Art. 75: Materia tributaria**

- Se regula mediante **Ley Orgánica**.

**Art. 76: Presupuestos de la Generalitat**

- Elaborados por el **Consell** con carácter anual.
- Presentación a Les Corts: **2 meses** antes del ejercicio.
- Si no se aprueban: Prórroga automática del presupuesto anterior.

**Art. 77: Emisión de Deuda Pública**

- Autorizada por **Les Corts**.

**Art. 78: Instituciones de crédito**

- La Generalitat está facultada para **crear instituciones de crédito**.

**Art. 79: Empresas públicas**

- Se crean mediante **Ley de Les Corts**.

**Art. 80: Derecho al trabajo**

- Derecho a un **trabajo digno**, acceso a **servicios públicos de empleo y formación profesional**.

## Título X: Reforma del Estatuto

### Art. 81: Procedimiento de reforma

- **Iniciativa:** Consell, 1/3 de Les Corts, 2 Grupos Parlamentarios o Cortes Generales.
- **Aprobación por Les Corts:**
  - **Reforma: Mayoría de 2/3.**
  - **Ampliación competencial: Mayoría simple**
- Si aprobada: Proposición de Ley ante Cortes Generales.
  - Estas pueden no aprobarla, modificarla, o aprobarla mediante LO
  - La aprobación incluirá un **referéndum de ratificación**, salvo ampliaciones competenciales, en el **plazo de 6 meses**

# Estructura y Datos relevantes del Estatuto de la CV

## Fechas claves

Aprobada por el Congreso de los Diputados	<b>28 de abril de 1982</b>
Aprobada por el Senado	7 de mayo de 1982
Disposición	1 de julio de 1982
Publicada en el BOE	10 de julio de 1982
Última modificación ( <i>rel. inversión Estado</i> )	12 de marzo de 2019

## Estructura

- **PREÁMBULO**

- **TÍTULO I** La Comunitat Valenciana [1-7]
- **TÍTULO II** De los derechos de los valencianos y valencianas [8-19]
- **TÍTULO III** La Generalitat [20-48]
  - **CAPÍTULO I** Les Corts Valencianes o Les Corts [art. 21-26]
  - **CAPÍTULO II** El President de la Generalitat [art. 27-28]
  - **CAPÍTULO III** El Consell [art. 29-32]
  - **CAPÍTULO IV** La Administración de Justicia [art. 33-37]
  - **CAPÍTULO V** De las otras Instituciones de la Generalitat [art. 38-43]
  - **CAPÍTULO VI** Régimen Jurídico [art. 44-48]
- **TÍTULO IV** Las Competencias [49-58]
- **TÍTULO V** Relaciones con el Estado y otras Comunidades Autónomas [59-60]
- **TÍTULO VI** Relaciones con la Unión Europea [61]
- **TÍTULO VII** Acción Exterior [62]
- **TÍTULO VIII** Administración Local [63-66]
- **TÍTULO IX** Economía y Hacienda [67-80]
- **TÍTULO X** Reforma del Estatuto [81]
  
- **DISPOSICIONES ADICIONALES** (1<sup>a</sup> a 4<sup>a</sup>)
- **DISPOSICIONES TRANSITORIAS** (1<sup>a</sup> a 9<sup>a</sup>)
- **DISPOSICIONES DEROGATORIA** (única)
- **DISPOSICIONES FINALES** (única)

## Gobierno Valenciano

# Ley 5/1983, de 30 de diciembre, de Gobierno Valenciano

### Título I: Del President de la Generalitat

#### CAPÍTULO I: DE LA ELECCIÓN Y EL ESTATUTO PERSONAL

##### Art. 1: "President de la Generalitat"

- Dirige la acción del Consell y coordina sus funciones.
- Ostenta la más alta representación de la Comunitat Valenciana y la ordinaria del Estado en ella.

##### Art. 2: Elección del President

- Elegido por **Les Corts entre sus miembros**, y nombrado por el Rey.
- El Presidente de Les Corts propondrá un candidato, quien deberá exponer su programa y solicitar la confianza de la Cámara.
- Aprobación:
  - **Mayoría absoluta** en primera votación.
  - Si no se consigue, se somete a mayoría simple tras 48 horas.
  - Si no se logra, se tramitarán otras propuestas.
- Si tras **2 meses** no hay acuerdo, Les Corts se disolverán, y el President en funciones convocará elecciones.

##### Art. 3-7, 9: Nombramiento, publicación, posesión, juramento, incompatibilidades y responsabilidades

- **Nombramiento** comunicado al Rey y publicado en el BOE y DOCV en un plazo de **10 días**.
- El cargo comienza con la publicación en el BOE.
- **Incompatibilidad** con cualquier otra función pública o mercantil, excepto como Diputado de Les Corts.
- Responde políticamente ante Les Corts y ostenta el tratamiento de "**Muy honorable**".

##### Art. 8: Cese y Sustitución

- Causas de cese:
  - Renovación de Les Corts, renuncia, fallecimiento, pérdida de condición de Diputado, o incompatibilidad no subsanada en **10 días**.
- En caso de incapacidad o fallecimiento:
  - Sustitución por el **Presidente de Les Corts**.

- En el Consell, el vicepresidente con más antigüedad o un conseller asumirá el cargo.

## CAPÍTULO II: DE LAS ATRIBUCIONES DEL PRESIDENT

### Art. 10: Funciones del President

- Representa legalmente a la Comunitat Valenciana.
- Firma convenios y acuerdos de cooperación con la AGE o CCAA.
- Solicita competencias legislativas estatales o delegaciones de competencias.
- Designa al representante de la Comunitat Valenciana en el Comité de las Regiones de la UE y otros organismos.

### Art. 11: Promulgación de Leyes

- En nombre del Rey, dentro de un plazo de **15 días**.

### Art. 12: Funciones en el Consell

- Dirige y coordina su acción.
- Puede crear Consellerías, nombrar y separar Consellers, disolver Les Corts y convocar elecciones.

## Título II: Del Consell

## CAPÍTULO I: DEL CONSELL Y SU COMPOSICIÓN

### Art. 13: Naturaleza del Consell

- Órgano colegiado que ostenta la **potestad ejecutiva y reglamentaria** y dirige la Administración de la Generalitat.

### Art. 14: Composición del Consell

- President, Vicepresidentes y Consellers.
- Secretarios Autonómicos pueden asistir a las reuniones si son convocados.

### Art. 15: Vicepresidentes y Consellers

- Los Consellers son titulares de los departamentos de la Administración Autonómica.
- Los Vicepresidentes no necesariamente deben ser Consellers.
- Ausencias del President superiores a **1 mes** deben ser comunicadas a Les Corts.

## CAPÍTULO II: DE LAS ATRIBUCIONES DEL CONSELL

### Art. 16: Competencias del Consell

- Establecer directrices de la acción política y administrativa.

- **Planificar y desarrollar** la política general de la Comunitat Valenciana.
- Ejercer todas las competencias atribuidas por ley.

#### **Art. 17: Funciones ejecutivas y administrativas**

- **Nombrar y cesar altos cargos** de la Administración de la Generalitat (a propuesta del President).
- Reglamentar e inspeccionar Diputaciones Provinciales y Entes Locales.
- Proponer convenios de colaboración con el Estado y las CCAA.
- **Aprobar directrices de coordinación** para garantizar la eficacia de las políticas públicas.

#### **Art. 18: Funciones normativas**

- Proponer la **reforma del Estatuto de Autonomía**.
- Elaborar **proyectos de ley de presupuestos** y ejercer la potestad reglamentaria.
- Dictar **decretos legislativos y decretos-leyes**.
- Emitir deuda pública para gastos de inversión.

#### **Art. 19: Funciones parlamentarias**

- Proponer la celebración de **sesiones extraordinarias** en Les Corts.
- **Deliberar y aprobar proyectos de ley**, cuestiones de confianza y decisiones políticas relevantes.
- Disolver Les Corts cuando proceda.

#### **Art. 20: Relaciones con el Estado y otras CCAA**

- **Interponer recursos de inconstitucionalidad**.
- Plantear conflictos de competencias o cuestiones de inconstitucionalidad.

#### **Art. 21: Competencias residuales**

- Ejercer competencias no atribuidas expresamente a otros órganos de la Generalitat.

### **CAPÍTULO III: DEL FUNCIONAMIENTO DEL CONSELL**

#### **Art. 22: Actas de las reuniones**

- El Secretario del Consell levantará acta de las sesiones.

#### **Art. 23: Carácter reservado de las sesiones**

- Solo se hará público el contenido de los acuerdos adoptados.

#### **Art. 24-26: Comisiones Delegadas e Interdepartamentales**

- Las **Comisiones Delegadas** están formadas por President, Vicepresidentes, Consellers y Secretarios Autonómicos.

- Las **Comisiones Interdepartamentales** incluyen altos cargos y coordinan actividades específicas.
- La **Comisión de Secretarios Autonómicos y Subsecretarios** apoya la acción del Consell.

## CAPÍTULO IV: DE LAS CONSELLERÍAS Y LOS CONSELLERS

### Art. 27: Consellerías

- Son los **departamentos organizativos** de la Generalitat, dirigidos por un Conseller.

### Art. 28: Funciones de los Consellers

- Asistir a las reuniones del Consell.
- Proponer el **nombramiento y cese de altos cargos** de su Departamento.
- Presentar **anteproyectos de ley** y ejercer la potestad reglamentaria en su ámbito.

## CAPÍTULO V: DE LA CONSELLERÍA Y DE LOS CONSELLERS

### Art. 29: Nombramiento y cese de los Consellers

- Por decisión del **President de la Generalitat**.

### Art. 30: Incompatibilidades y tratamiento

- **Incompatibilidad** con funciones públicas o privadas (excepto Diputado de Les Corts).
- Tratamiento de “**Honorable Señor**”.

## CAPÍTULO VI: DE LA POTESTAD LEGISLATIVA Y REGLAMENTARIA DEL CONSELL

### Art. 31: Potestad reglamentaria

- Se ejerce de acuerdo a la CE, EA y leyes.

### Art. 32-38: Jerarquía normativa

1. **Decretos del Consell:** Firmados por el President y refrendados por Consellers.
  2. **Decretos del President:** Ceses, nombramientos y funciones asignadas.
  3. **Órdenes de Comisiones Delegadas:** Firmadas por el Presidente de la Comisión.
  4. **Órdenes de Consellerías:** Firmadas por los Consellers en materias de su Departamento.
  5. **Disposiciones de órganos inferiores:** Instrucciones y órdenes de servicio.
- **Nota:** Decretos publicados en el DOCV para su entrada en vigor.

### Art. 39-41: Límites de la potestad reglamentaria

- No se pueden establecer **penas, sanciones, multas o tasas** ni limitar derechos individuales.
- Son nulas de pleno derecho las disposiciones que contradigan la CE, EA o leyes.

#### **Art. 42: Iniciativa legislativa del Consell**

- Corresponde al Consell **elaborar y remitir proyectos de ley** a Les Corts.
- Requiere informes técnicos, memoria económica, y aprobación previa del Consell.

#### **Art. 43: Elaboración de Reglamentos**

- El proyecto de disposición se remite a la Presidencia y Consellerías para informe en un plazo de **10 días**.
- Audiencia a los interesados: **15 días**, reducibles a **7 días** en casos de urgencia.
- Informe de la Abogacía General de la Generalitat, seguido del dictamen del **Consell Jurídic Consultiu**.
- Aprobación: Por el Conseller o por el **Pleno del Consell**.
- Entrada en vigor: **Al día siguiente de su publicación en el DOCV**, salvo disposición en contra.

### **Título III: De las relaciones entre el Consell y Les Corts**

#### **CAPÍTULO I: DEL IMPULSO Y CONTROL DE LA ACCIÓN DEL CONSELL**

- **Art. 44-45: Comparecencia ante Les Corts**
  - El Consell y sus miembros deben comparecer obligatoriamente ante el Pleno y las Comisiones.
  - Se deben entregar los datos, informes y documentos solicitados en un plazo máximo de **30 días**.
- **Art. 46: Responsabilidad del Consell**
  - Exigible mediante la **moción de censura** o la **cuestión de confianza**.

#### **CAPÍTULO II: DE LA MOCIÓN DE CENSURA**

##### **Art. 47-50: Moción de censura**

- Permite exigir responsabilidad política del **President de la Generalitat**.
- Requisitos:
  - Propuesta por **1/5 de los Diputados**.
  - Incluye un candidato alternativo en un escrito motivado.
  - Presentación de mociones alternativas en **2 días**.

- No se votará hasta pasados **5 días** desde su presentación.
- Aprobación por **mayoría absoluta**.
- Si no prospera:
  - Los firmantes no podrán presentar otra durante el mismo periodo de sesiones.
  - En caso de aprobación, el candidato quedará **investido automáticamente** como President.

### CAPÍTULO III: DE LA CUESTIÓN DE CONFIANZA

- **Art. 51-52: Cuestión de confianza**
  - Propuesta por el President del Consell tras deliberación.
  - Aprobación: **Mayoría simple**.
  - Si no se aprueba: Se procede a la elección de un nuevo President.

### CAPÍTULO IV: DE LA LEGISLACIÓN DELEGADA Y DE URGENCIA

- **Art. 53-57: Decretos Legislativos**
  - Les Corts pueden delegar la potestad legislativa al Consell mediante:
    - **Ley de Bases**: Formación de textos articulados.
    - **Ley Ordinaria**: Refundición de textos legales.
  - **Exclusiones**: Derechos fundamentales, régimen electoral y normas básicas institucionales.
  - La delegación debe ser expresa y con **plazo fijado** para su ejercicio.
- **Art. 58: Decretos-Leyes**
  - Emitidos por el Consell en casos de **extraordinaria y urgente necesidad**.
  - Exclusiones: Derechos fundamentales, régimen electoral, y ordenamiento institucional básico.
  - Debate y votación en Les Corts en un plazo de **30 días**.

### CAPÍTULO V: DE LA EXPIRACIÓN DEL MANDATO

- **Art. 59: Elecciones**
  - Convocadas por el **President de la Generalitat** tras la disolución de Les Corts.
  - El decreto debe especificar:

- Número de diputados a elegir (no inferior a 99, o el superior que establezca la Ley Electoral Valenciana).
- Duración de la campaña electoral.
- Día de votación.
- Fecha y lugar de constitución de Les Corts.

## Título IV: De la Administración Pública de la Generalitat

### CAPÍTULO I: PRINCIPIOS GENERALES

#### Art. 60: Administración Pública de la Generalitat

- Posee **personalidad jurídica única**.
- Actúa bajo **criterios de eficacia, publicidad, jerarquía, descentralización, desconcentración y coordinación**.
- Sometida plenamente a la ley y al derecho.

#### Art. 61: Adaptación normativa

- El Consell adapta normas estatales a la organización de la Generalitat.

#### Art. 62: Creación de órganos administrativos

- Requiere **estudio económico previo** si incrementa el gasto público.

#### Art. 63: Delegación de competencias

- Delegación al **órgano inmediatamente inferior**.
- No delegable: Atribuciones del Estatuto de Autonomía, competencias de los Consellers, y relaciones con Estado, CCAA o Les Corts.
- Delegaciones publicadas en el **DOCV**.

### CAPÍTULO II: ORGANIZACIÓN, COMPETENCIAS Y ESTRUCTURA

#### Art. 64-65: Reglamento orgánico de cada Consellería

- Elaborado a propuesta del Conseller.

#### Art. 66: Organización funcional de las Consellerías

- **Órganos Superiores:** Conseller y Secretarios Autonómicos.
- **Nivel Directivo:** Subsecretarios y Directores Generales.
- **Nivel Administrativo:** Subdirecciones generales, servicios, secciones, unidades y negociados.

#### Art. 67: Subsecretarías

- Inspección de servicios, jefatura del personal, elaboración de proyectos y asistencia técnica.

**Art. 68: Directores Generales**

- Dirigen y gestionan servicios, supervisan dependencias y elaboran informes anuales.

**Art. 69: Unidades Administrativas**

- Dependientes de las Secretarías Autonómicas, Subsecretarías, Direcciones Generales o directamente del Conseller, con carácter excepcional.

**Art. 70: Organización del Nivel Administrativo**

- **Compuesto por:** Subdirecciones generales, servicios, secciones, unidades y negociados.

**Art. 71: Secretaría General Administrativa**

- **Órgano administrativo superior** de cada Consellería, dependiente de la Subsecretaría.
- Apoyo directo al titular y gestión de servicios generales.

**CAPÍTULO III: ORGANIZACIÓN TERRITORIAL**

**Art. 74-76: Servicios centrales y periféricos**

- **Servicios centrales:** Competencia en todo el territorio de la Comunitat Valenciana.
- **Servicios periféricos:** Competencia en el ámbito territorial asignado.

**Título V: De la responsabilidad de los miembros del Consell y de la Administración Pública**

**Art. 77-78: Responsabilidad penal y civil**

- Miembros del Consell: Ante el **TSJCV** o el Tribunal Supremo.
- Autoridades y funcionarios: Ante el **TSJCV**.

**Art. 79: Responsabilidad patrimonial de la Generalitat**

- Exigible por **lesión a ciudadanos**, salvo fuerza mayor.

## Unión Europea

# Características del Ordenamiento Jurídico de la Unión Europea

La Unión Europea (UE) es una **organización supranacional** compuesta por **27 Estados miembros** que ceden parte de sus competencias para formar un sistema jurídico de obligado cumplimiento. Fue establecida mediante el **Tratado de Maastricht** el 1 de noviembre de 1993.

El **ordenamiento jurídico de la UE** se basa en el **principio de atribución de competencias**, según el cual la UE actúa únicamente dentro de los límites de las competencias que le han sido cedidas por los Estados miembros. Este ordenamiento genera **derechos y obligaciones** tanto para los Estados como para los ciudadanos, y se rige por tres tipos de fuentes: **derecho primario, derivado y complementario**.

### Fuentes del Derecho de la Unión Europea

- **Derecho Primario (u originario):** Es la normativa suprema dentro de la jerarquía del derecho de la UE. Constituye la base de todas las actuaciones de la Unión y está compuesto principalmente por:
  - **Tratados constitutivos o fundacionales:**
    - **Tratado de la Unión Europea (TUE):** Contiene los principios constitucionales de la UE.
    - **Tratado de Funcionamiento de la Unión Europea (TFUE):** Define el marco jurídico para las políticas y acciones de la UE.
    - **Tratado constitutivo de la Comunidad Europea de la Energía Atómica (Euratom):** Regula el progreso en el ámbito de la energía nuclear.
    - **Carta de los Derechos Fundamentales de la Unión Europea (CDF):** Asegura los derechos civiles, políticos, económicos y sociales de los ciudadanos.
  - **Otros documentos:** Tratados de modificación, protocolos, tratados de adhesión y la Carta de los Derechos Fundamentales.
  - **Características:**
    - Son normas internacionales con dimensión constitucional.
    - Establecen la **base del poder** de las instituciones de la UE y el reparto de competencias entre la UE y los Estados miembros.
    - Contienen regulaciones esenciales como las libertades comunitarias y las políticas comunes.
- **Derecho Derivado:** Elaborado por las **instituciones de la UE** para alcanzar los objetivos establecidos en los tratados.
  - **Tipos de actos jurídicos:**

- **Reglamentos:** De alcance general, directamente aplicables y de obligado cumplimiento en todos los Estados miembros.
- **Directivas:** Obligan a los Estados miembros a alcanzar un resultado específico, dejando libertad en los medios de implementación.
- **Decisiones:** Obligatorias en todos sus elementos y, si tienen destinatarios concretos, sólo aplicables a ellos.
- **Recomendaciones y Dictámenes:** No vinculantes, pero ofrecen orientación y ayuda interpretativa.
- **Derecho Complementario:** Comprende los principios generales del derecho de la UE, costumbres y jurisprudencia. Hay dos grandes grupos de normas:
  - Normas basadas en el derecho internacional.
  - Normas derivadas de la jurisprudencia, los principios generales y la costumbre.

### **Principios de Interacción entre el Derecho de la UE y los Derechos Nacionales**

- **Eficacia directa:** Permite que los ciudadanos invoquen normas de la UE ante tribunales nacionales.
- **Supremacía:** El derecho de la UE prevalece sobre el nacional en caso de conflicto.
- **Seguridad jurídica:** Los Estados deben integrar el derecho de la UE de forma clara y pública.
- **Responsabilidad estatal:** Los Estados miembros deben reparar los daños causados por la infracción del derecho comunitario.

### **Instituciones de la Unión Europea**

La Unión Europea cuenta con **7 instituciones principales** a las que los Estados miembros han atribuido competencias para ejercer poderes comunitarios. Estas instituciones representan los intereses de los ciudadanos, los Estados miembros y la Unión en su conjunto:

- **Parlamento Europeo:** Representa directamente a los ciudadanos de la Unión Europea y actúa como una especie de "Cortes Generales" de la UE.
  - **Composición:**
    - **Integrantes:** 705 eurodiputados elegidos según reglas de proporcionalidad basadas en la población de cada país, con un mínimo de 6 y un máximo de 96 eurodiputados por Estado miembro.
    - **Elección:** Sufragio universal directo.
    - **Mandato:** 5 años.
  - **Funciones:**

- **Legislativas y presupuestarias:** Participa en la elaboración y aprobación de leyes y presupuestos de la UE.
- **Supervisión:**
  - Otorga y retira la confianza a la Comisión Europea.
  - Supervisa la actividad cotidiana de la Comisión.
  - Recibe información de otras instituciones.
- **Otras:**
  - Aprueba la adhesión de nuevos Estados miembros.
  - Emite opiniones sobre acuerdos internacionales.
  - Garantiza los derechos de los ciudadanos europeos.
  - Aprueba su reglamento interno por mayoría.
- **Sesiones:**
  - **Ordinarias:** Un período de sesiones anual que comienza el segundo martes de marzo.
  - **Extraordinarias:** Convocadas a petición de la mayoría de sus miembros, del Consejo o de la Comisión Europea.
- **Sedes:**
  - **Estrasburgo:** Sede oficial del Parlamento.
  - **Bruselas:** Lugar de reunión de las comisiones parlamentarias.
  - **Luxemburgo:** Ubicación de la Secretaría General.
- **Comisión Europea:** Representa los intereses generales de la Unión Europea y actúa como su **órgano ejecutivo**, encargado de proponer y aplicar leyes.
  - **Composición:**
    - **Integrantes:** 27 comisarios (uno por Estado miembro).
    - **Estructura:**
      - 1 presidente.
      - 3 vicepresidentes ejecutivos.
      - 1 alto representante de Asuntos Exteriores y Política de Seguridad (con rango de vicepresidente).
      - 4 vicepresidentes adicionales.
      - 18 comisarios.
    - **Mandato:** 5 años.
  - **Funciones:**

- Proponer legislación para alcanzar los objetivos de los tratados de la UE.
- Supervisar el cumplimiento de las leyes de la Unión.
- Gestionar y aplicar las políticas y el presupuesto de la UE.

- **Consejo Europeo**

Establece las orientaciones y prioridades políticas de la Unión Europea.

- **Composición:**

- 27 jefes de Estado o de Gobierno de los Estados miembros.
    - El presidente de la Comisión Europea.
    - El presidente del Consejo Europeo, quien dirige las reuniones.

- **Funciones:**

- Definir las estrategias generales de la UE.
    - Nombrar a los altos cargos de la Unión, como el presidente de la Comisión y del BCE.

- **Consejo de la Unión Europea (Consejo de Ministros)**

Está compuesto por los ministros de los gobiernos de los Estados miembros, dependiendo del tema tratado.

- **Composición:**

- No tiene miembros fijos. Cada Estado envía al ministro responsable según el área de discusión (por ejemplo, Agricultura, Educación, etc.).

- **Funciones:**

- Negocia y adopta la legislación de la UE junto con el Parlamento Europeo.
    - Coordina las políticas de los Estados miembros.
    - Desarrolla la política exterior y de seguridad común.
    - Celebra acuerdos internacionales en nombre de la UE.
    - Aprueba el presupuesto de la UE junto con el Parlamento Europeo.

- **Tribunal de Justicia de la Unión Europea (TJUE)**

Garantiza el respeto al derecho comunitario y su correcta interpretación y aplicación.

- **Composición:**

- **Tribunal de Justicia:**

- 1 juez por cada Estado miembro.
      - 11 abogados generales que presentan dictámenes jurídicos imparciales.

- **Tribunal General:**

- 2 jueces por cada Estado miembro.

- No cuenta con abogados generales.
- **Mandato:** 6 años.
- **Funciones:**
  - Controlar la legalidad de los actos de las instituciones de la UE.
  - Velar por el cumplimiento de las obligaciones de los Estados miembros.
  - Interpretar el derecho de la UE a solicitud de los tribunales nacionales.
- **Banco Central Europeo (BCE)**

Gestiona el euro y formula la política monetaria de la zona euro.

  - **Composición:**
    - Consejo de Gobierno.
    - Comité Ejecutivo.
    - Consejo General.
  - **Funciones:**
    - Mantener la estabilidad de precios.
    - Contribuir al crecimiento económico y al empleo en la eurozona.
- **Tribunal de Cuentas Europeo (TCE)**

Es el auditor externo de la UE, encargado de supervisar sus finanzas.

  - **Composición:**
    - 27 miembros, uno por cada Estado miembro.
  - **Funciones:**
    - Mejorar la gestión financiera de la Unión.
    - Contribuir a la rendición pública de cuentas sobre los ingresos y gastos del presupuesto de la UE.
    - Garantizar la fiabilidad de las cuentas y proporcionar asesoramiento técnico.

### **Procedimiento Legislativo Ordinario**

La legislación se adopta conjuntamente por el Parlamento Europeo y el Consejo, a propuesta de la Comisión. Esto incluye reglamentos, directivas y decisiones.

## Leyes de Igualdad

# Ley Orgánica 3/2007, para la igualdad efectiva de mujeres y hombres

### Objeto y Principios Generales

La **Ley Orgánica 3/2007** tiene como objetivo garantizar la **igualdad de trato y oportunidades** entre mujeres y hombres, eliminando cualquier forma de discriminación hacia la mujer en los ámbitos político, civil, laboral, económico, social y cultural. Busca construir una sociedad **más democrática, justa y solidaria**.

- **Ámbito de aplicación:** Aplica a toda persona, física o jurídica, que se encuentre o actúe en territorio español, independientemente de su nacionalidad, domicilio o residencia.
- **Principio de igualdad de trato:** Ausencia de toda discriminación directa o indirecta por razón de sexo. Se consideran especialmente relevantes las discriminaciones relacionadas con la maternidad, las obligaciones familiares y el estado civil.
  - Es un **principio informador del ordenamiento jurídico**, que debe observarse en la interpretación y aplicación de todas las normas jurídicas.

### Discriminación y Acoso

- **Discriminación directa:** Trato menos favorable hacia una persona por razón de su sexo en una situación comparable.
- **Discriminación indirecta:** Disposición, criterio o práctica aparentemente neutra que coloca a personas de un sexo en desventaja frente al otro.
- **Acoso sexual:** Conducta verbal o física de naturaleza sexual que atente contra la dignidad de una persona, creando un entorno **intimidatorio, degradante u ofensivo**.
- **Acoso por razón de sexo:** Comportamiento basado en el sexo de una persona con el mismo propósito y efectos.
- **Discriminación por embarazo o maternidad:** Se considera una forma de **discriminación directa**.
- **Represalias:** Constituyen discriminación.

### Consecuencias Jurídicas y Tutela Judicial

- Los actos y cláusulas discriminatorias son **nulos de pleno derecho** y generan responsabilidad.
- **Acciones positivas:** Los poderes públicos deben adoptar medidas específicas para **corregir desigualdades estructurales** a favor de las mujeres.

- **Carga de la prueba:** Corresponde a la persona demandada demostrar la ausencia de discriminación.
- **Tutela judicial efectiva:** Cualquier persona puede recabarla. La persona acosada es la **única legitimada** en los litigios sobre acoso.

## Actuación de los Poderes Públicos

- **Plan Estratégico de Igualdad de Oportunidades:** Periódicamente aprobado por el Gobierno, incluye medidas para eliminar la discriminación.
- **Informe periódico:** El Gobierno debe informar a las Cortes Generales sobre el impacto de las políticas de igualdad.
- **Proyectos normativos:** Deben incorporar un **informe de impacto de género**.
- **Estadísticas y estudios:** Es obligatorio incluir la variable sexo en estadísticas oficiales.
- **Conferencia Sectorial de la Mujer:** Coordina la colaboración entre Administraciones Públicas.
- **Planificación del tiempo:** Fomento de planes municipales de organización del tiempo para una distribución equitativa.
- **Educación:**
  - Integrar el principio de igualdad en el sistema educativo.
  - Eliminar comportamientos y contenidos sexistas.
  - Fomentar la **presencia equilibrada** en órganos de control.
  - Reconocer el papel histórico de las mujeres.
  - En las universidades: Promoción de estudios específicos, investigaciones especializadas y programas de postgrado en igualdad.
- **Producción artística e intelectual:** Ayudas e incentivos para proyectos que fomenten la igualdad.
- **Deporte:** Promoción del deporte femenino.
- **Sociedad de la información:** Proyectos tecnológicos públicos deberán usar **lenguaje no sexista**.
- **Políticas urbanas:** Fomentar el acceso a la vivienda de mujeres en situación de necesidad o víctimas de violencia de género.
- **Desarrollo rural:** Reconocimiento de derechos y mejora formativa para mujeres en áreas rurales.

## Ámbito Laboral

- **Planes de igualdad:** Obligatorios para empresas con más de 50 trabajadores, deben incluir:
  - Diagnóstico inicial elaborado por una **Comisión Negociadora**.
  - Medidas específicas para eliminar la discriminación.
  - Registro obligatorio en el **Registro de Planes de Igualdad de las Empresas**.
- **Prevención del acoso:** Códigos de buenas prácticas, campañas informativas y acciones formativas.
- **Distintivo empresarial:** Otorgado por el Ministerio de Trabajo y Asuntos Sociales a empresas con políticas destacadas en igualdad.

## Administraciones Públicas

- **Conciliación:** Remover obstáculos que dificulten la conciliación de la vida personal, familiar y laboral.
- **Convocatorias selectivas:** Requieren informes de impacto de género (excepto en casos urgentes).
- **Maternidad y paternidad:** Computarán como tiempo trabajado en concursos de méritos.
- **Formación en igualdad:** Obligatoria en todos los niveles, con reserva del 40% de plazas en cursos directivos para mujeres.
- **Plan de Igualdad:** Aprobado anualmente para la Administración General del Estado.

## Acceso a Bienes y Servicios

- **Principio de igualdad obligatorio** para todas las entidades que suministren bienes o servicios.
- **Seguros:** Prohibidas las diferencias en primas y prestaciones por razón de sexo.
- **Protección del embarazo:** Prohibido indagar sobre el embarazo salvo por razones de protección.

## Medios de Comunicación y Publicidad

- **Medios públicos:**
  - Velarán por una imagen igualitaria y no estereotipada.
  - Utilizarán **lenguaje no sexista**.
  - Promoverán la incorporación de mujeres a puestos de responsabilidad.

- **Medios privados:** Deben evitar cualquier forma de discriminación.
- **Publicidad:** Será ilícita aquella que promueva conductas discriminatorias.

### Órganos de Igualdad

- **Comisión Interministerial de Igualdad:** Coordina políticas de igualdad entre departamentos ministeriales.
- **Unidades de Igualdad:** En todos los ministerios, se encargan de recabar información estadística, elaborar estudios, asesorar y fomentar el cumplimiento de la ley.
- **Consejo de Participación de la Mujer:** Órgano consultivo que facilita la participación de las mujeres en la promoción de la igualdad.

### Otros Aspectos Relevantes

- **Publicidad engañosa en igualdad:** El Instituto de la Mujer puede cesar campañas de publicidad engañosa.
- **Evaluación en empleo público:** Los Departamentos Ministeriales deben reportar anualmente el grado de aplicación de las políticas de igualdad.
- **Reserva del 40% de plazas:** En formación directiva, como medida positiva para fomentar la igualdad.

# Ley 9/2003, de igualdad entre mujeres y hombres (Comunidad Valenciana)

## Objeto y Ámbito de Aplicación

El objeto de la ley es **regular y hacer efectivo el principio de igualdad de mujeres y hombres** en la Comunidad Valenciana, estableciendo los principios generales, las acciones básicas y la organización administrativa necesarias.

- **Ámbito territorial:** La ley se aplica en todo el territorio de la Comunidad Valenciana.

## Principios Generales y Rectores de la Acción Administrativa

- La **discriminación contraria al ordenamiento jurídico** está prohibida, pero no toda desigualdad constituye discriminación. Se considera discriminatoria la desigualdad que carezca de una justificación **objetiva, racional y razonable**.
- **Principios rectores:**
  - Modificar patrones socioculturales asignados por género.
  - **Estrategia dual:** Combina medidas de acción positiva y transversalidad de género.
  - Los proyectos normativos incluirán un **informe de impacto de género**.
  - El Consell informará a Les Corts sobre las actuaciones realizadas.

## Educación y Participación Política

- **Educación:**
  - Implementación de un sistema **coeducativo** que rechace la discriminación y la orientación académica sesgada.
  - Igualdad real en las dimensiones curricular, escolar y otras.
  - **Ampliación del horario de apertura** de centros públicos para fomentar la corresponsabilidad.
  - Financiación de asignaturas y proyectos universitarios con **enfoque de género**.
- **Participación política:**
  - Promoción de una **presencia paritaria** en los órganos políticos.
  - Incremento del 10% en subvenciones electorales por escaños obtenidos por mujeres, siempre que sea compatible con la **Ley Electoral Valenciana**.

## Ámbito Laboral y Conciliación

- **Igualdad en el empleo:**

- Los **Planes de Empleo Valenciano** incluirán medidas específicas de igualdad.
- Creación de la **Red Valenciana de Igualdad** para incorporar la perspectiva de género en las políticas públicas, asesorar y sensibilizar, y ayudar a las empresas a elaborar planes de igualdad.
- **Planes de igualdad:**
  - Documentos que definen estrategias para garantizar la igualdad de oportunidades.
  - **Obligatorios** en empresas con predominancia de capital público.
  - Deberán ser visados por la Generalitat para recibir ayudas. Si no se resuelven en **6 meses**, se entenderán **desestimados**.
- **Conciliación de vida familiar y laboral:**
  - Incentivos, flexibilización de horarios y permisos parentales.
  - **Plan Integral de la Familia e Infancia:** Fomenta la corresponsabilidad en tareas familiares y domésticas.
  - Impulso de la participación femenina en **puestos técnicos y diseño de tecnologías de la información**.

### Asistencia a Víctimas de Violencia de Género

- Las Administraciones Públicas ofrecerán a las víctimas:
  - **Asistencia jurídica y psicológica especializada y gratuita.**
  - Acceso preferente a **viviendas sociales**.
- En los medios públicos se fomentará la **pluralidad de roles** para la mujer.

### Actuación de la Administración Pública

- **Eradicación de la violencia:**
  - Campañas de sensibilización y programas para combatir la violencia de género, el acoso sexual y la explotación sexual.
- **Formación y promoción:**
  - Planes plurianuales de formación basados en los principios de mérito y capacidad.
- **Contrataciones públicas:**
  - En caso de empate, tendrá preferencia la empresa que presente un plan de igualdad, siempre que su oferta sea igual de ventajosa.
- **Acoso sexual:**

- Incorporación obligatoria del **código de conducta** contra el acoso sexual.
- **Lenguaje no sexista:** Obligatorio en los escritos administrativos.
- **Datos estadísticos:** Desagregación por sexos para estudios e investigaciones.

### **Organización Institucional**

- **Consejo Valenciano de las Mujeres:** Órgano de participación y asesoramiento para eliminar discriminaciones y promover la participación de las mujeres en la vida política, económica y social.
- **Defensoría de la Igualdad:** Encargada de vigilar el cumplimiento de la ley, desempeñada por el **Síndic de Greuges**.

## Leyes contra de Violencia de Género

### **Ley Orgánica 1/2004, de medidas de protección integral contra la violencia de género**

#### **Definición**

*“Todo acto de **violencia física y psicológica** que se ejerce sobre las mujeres por parte de quienes estén o hayan estado ligados a ellas por relaciones de afectividad”.*

#### **Título Preliminar**

#### **Objeto**

- Actuar contra la **violencia ejercida sobre las mujeres por parte de quienes sean o hayan sido sus cónyuges o personas ligadas a ellas** por relaciones de afectividad, aun sin convivencia.
- Reconoce la violencia como una manifestación de **discriminación, situación de desigualdad y relaciones de poder** de los hombres sobre las mujeres.
- Establece medidas de protección integral para:
  - **Prevenir, sancionar y erradicar** la violencia de género.
  - **Prestar asistencia** a las mujeres, a sus hijos menores y a los menores bajo su tutela, guarda o custodia.

#### **Principios Rectores**

- **Sensibilización ciudadana y prevención.**
- **Consagración de derechos** para las mujeres víctimas.
- Reforzar servicios sociales: **información, atención, emergencia, apoyo y recuperación.**
- Garantizar derechos **laborales y económicos.**
- Establecer un sistema de **tutela institucional.**
- Fortalecer el marco **penal y procesal.**
- Coordinar recursos e instrumentos de los **poderes públicos.**
- Promover la colaboración con entidades, asociaciones y organizaciones.
- **Fomentar la especialización profesional.**
- **Principio de transversalidad** para atender necesidades específicas de las mujeres.

## Título I: Medidas de sensibilización, prevención y detección

### Planes de Sensibilización

- **Plan Nacional de Sensibilización y Prevención de la Violencia de Género:**
  - Persigue una **nueva escala de valores** basada en derechos fundamentales, igualdad, tolerancia y libertad desde la perspectiva de género.
  - **Dirigido a hombres y mujeres.**
  - Controlado por una comisión **especializada**.
  - Incluye **campañas** de información y sensibilización.

### En el ámbito educativo

- Incorporación de principios y valores en el sistema educativo:
  - Formación en el respeto a los derechos y libertades fundamentales, igualdad entre hombres y mujeres, tolerancia y libertad.
  - **Escalarización inmediata** por cambio de residencia debido a violencia de género.
  - Eliminación de **estereotipos sexistas y discriminatorios**.
  - Formación inicial y permanente del profesorado en igualdad.
  - Promoción de actitudes igualitarias, resolución pacífica de conflictos y detección de violencia familiar.
  - Los **Consejos Escolares** fomentarán la igualdad real.
  - La inspección educativa supervisará la aplicación de estos principios.

### En el ámbito de la publicidad y los medios de comunicación

- **Publicidad ilícita:** Aquella que utilice la imagen de la mujer de manera vejatoria o discriminatoria.
- **Titulares con potestad para cesar o rectificar esta publicidad:**
  - **Delegación Especial del Gobierno contra la Violencia sobre la Mujer.**
  - **Instituto de la Mujer (o equivalente).**
  - **Ministerio Fiscal.**
  - **Asociaciones especializadas.**
- Los medios de comunicación evitarán cualquier forma de discriminación, y las AAPP promoverán acuerdos de autorregulación y velarán por su cumplimiento.

### En el ámbito sanitario

- Las administraciones sanitarias deben:
  - Impulsar la **detección precoz** de la violencia de género.

- Promover programas de **sensibilización y formación continua** para diagnóstico, asistencia y rehabilitación.
- **Planes Nacionales de Salud:** Incluirán prevención e intervención integral.
- **Consejo Interterritorial del Sistema Nacional de Salud:**
  - Creará una Comisión contra la Violencia de Género, encargada de dar apoyo técnico, evaluar y proponer medidas sanitarias.
  - Representación de todas las CCAA.
  - Informe anual remitido al **Observatorio Estatal de la Violencia sobre la Mujer** y al Pleno del Consejo Interterritorial.

## **Título II: Derechos de las mujeres víctimas de violencia de género**

### **Derecho a la información, asistencia social integral y jurídica gratuita**

- **Garantizados** a todas las mujeres víctimas, sin importar origen, religión u otras circunstancias.
- **Asistencia social integral:** Servicios de atención, emergencia, apoyo y recuperación. Incluye a los menores a cargo.
- **Principios de actuación:**
  - **Atención permanente.**
  - **Actuación urgente.**
  - **Especialización y multidisciplinariedad.**
- Asesoramiento jurídico gratuito antes de la denuncia.
- Defensa jurídica gratuita y especializada, ofrecida de forma inmediata.

### **Derechos laborales y prestaciones de la Seguridad Social**

- **Derechos laborales:**
  - Reducción o reordenación de jornada.
  - Movilidad geográfica y cambio de centro.
  - Suspensión de la relación laboral con reserva de puesto.
  - Extinción del contrato justificada.
- **Justificación de ausencias:** Por violencia de género.
- **Programa de acción específico de empleo**, en el marco del Plan de Empleo del Reino de España.
- **Acreditación** de situaciones de violencia **mediante:**
  - **Sentencia condenatoria, orden de protección, resolución judicial, informe del Ministerio Fiscal o servicios sociales.**

### Derechos económicos

- Ayudas sociales para mujeres con ingresos inferiores al **75% del SMI**, que no puedan trabajar por edad o falta de formación.
- **Cuantías:**
  - **6 meses** de subsidio base.
  - Hasta **24 meses** en casos de discapacidad y responsabilidades familiares.
- Acceso prioritario a viviendas protegidas y residencias públicas.

### Título III: Tutela Institucional

#### Delegación Especial del Gobierno contra la Violencia sobre la Mujer

- Formula políticas públicas en materia de violencia de género y coordina acciones gubernamentales.
- Adscrita al Ministerio de Trabajo y Asuntos Sociales.

#### Observatorio Estatal de Violencia sobre la Mujer

- Órgano colegiado encargado de asesorar, evaluar, elaborar informes y proponer medidas.
- **Informe anual sobre la evolución de la violencia de género**, remitido al Gobierno.

#### Fuerzas y Cuerpos de Seguridad

- Contarán con **unidades especializadas** en:
  - Prevención de violencia de género.
  - Control de medidas judiciales adoptadas.

#### Planes de colaboración

- Ordenarán las actuaciones de los poderes públicos en prevención, asistencia y persecución de actos de violencia de género.

#### Atención prioritaria a mujeres con mayor riesgo o dificultades para acceder a servicios:

- Mujeres de minorías, inmigrantes, en exclusión social o con discapacidad.

## Gobierno Abierto, Transparencia, y Buen gobierno

# Ley 19/2013 de Transparencia, Acceso a la Información Pública y Buen Gobierno

### Objeto

- **Ampliar y reforzar la transparencia** de la actividad pública.
- **Regular y garantizar el derecho de acceso a la información pública.**
- Establecer las **obligaciones de buen gobierno** y las **consecuencias de su incumplimiento.**

### Título I: Transparencia de la Actividad Pública

#### Ámbito subjetivo

- **Aplicación total:**
  - **Administraciones públicas:** AGE, administraciones autonómicas, locales, entidades gestoras de la Seguridad Social, mutuas, organismos autónomos, agencias estatales, universidades, y entidades de derecho público.
  - **Organismos constitucionales:** Casa de SM el Rey, Congreso, Senado, TC, CGPJ, Banco de España, Consejo de Estado, Defensor del Pueblo, Tribunal de Cuentas, Consejo Económico y Social.
  - **Sociedades mercantiles:** Con capital social público superior al **50%**.
  - Fundaciones y asociaciones del sector público.
- **Aplicación parcial:**
  - Partidos políticos, sindicatos, organizaciones empresariales y entidades privadas que:
    - Perciban ayudas públicas superiores a **100.000€**.
    - Perciban ayudas que representen al menos el **40%** de sus ingresos anuales, con un mínimo de **5.000€**.

#### Publicidad activa

- **Definición:** Publicar información **antes de ser solicitada**, garantizando transparencia.
- **Obligaciones:**
  - Publicación periódica y actualización de información relevante.
  - Uso de **sedes electrónicas o páginas web**.

- **Formatos reutilizables, accesibles y gratuitos**, respetando el principio de **accesibilidad universal y diseño para todos**.
- **Infracción grave**: El incumplimiento reiterado de la publicidad activa.
- **Tipos de información**:
  - **Institucional, organizativa y de planificación**:
    - Funciones desarrolladas, normativa aplicable, estructura organizativa (organigramas), planes anuales y plurianuales con objetivos concretos.
  - **Información jurídica**:
    - Directrices, instrucciones, acuerdos, circulares, proyectos de ley, decretos legislativos, reglamentos sometidos a dictámenes, memorias e informes.
  - **Económica, presupuestaria y estadística**:
    - Contratos, convenios, subvenciones, ayudas, presupuestos, cuentas anuales, retribuciones de altos cargos, estadísticas.
- **Órganos relevantes**:
  - **Consejo de Transparencia y Buen Gobierno**: Controla el cumplimiento de la Ley en la AGE. Incumplimientos reiterados son **infracciones graves**.
  - **Portal de Transparencia**: Facilita el acceso a información pública, incluyendo datos solicitados con frecuencia. Depende del Ministerio de la Presidencia.
- **Principios técnicos ("AIR")**: **Accesibilidad, Interoperabilidad y Reutilización**.

#### Derecho de acceso a la información pública

- **Definición**: Derecho de toda persona a acceder a documentos en poder de los sujetos obligados, elaborados o adquiridos en el ejercicio de sus funciones.
- **Límites al acceso**:
  - **Justificados y proporcionados**:
    - Defensa y seguridad.
    - Economía.
    - Confidencialidad.
    - Protección del medio ambiente.
  - **Protección de datos personales**: Aplicable salvo disociación de datos.
  - **Datos especialmente protegidos**:
    - **Ideología, religión, afiliación sindical**: Requieren consentimiento expreso y escrito, salvo datos manifiestamente públicos.

- **Origen racial, salud, vida sexual:** Requieren consentimiento expreso, salvo norma con rango de ley.
- **Acceso parcial:** Cuando los límites solo afectan a una parte.

### Procedimiento de acceso

- **Solicitud:**
  - No requiere motivación.
  - **Contenidos obligatorios:** Identidad del solicitante, información requerida, dirección de contacto y modalidad de acceso.
- **Causas de inadmisión:**
  - Información en curso de elaboración.
  - Documentos auxiliares o sujetos a reelaboración.
  - Información desconocida por el órgano.
  - Solicitudes abusivas.
- **Tramitación:**
  - **Subsanación:** 10 días.
  - **Alegación de terceros:** 15 días.
  - **Resolución:** Máximo 1 mes, prorrogable.
  - **Motivación requerida:** Resoluciones denegatorias, accesos parciales o diferentes a la modalidad solicitada, accesos tras oposición de terceros.
- **Formalización:**
  - Electrónica preferentemente, gratuita.
  - Si no es posible en el momento, debe formalizarse en 10 días.

### Régimen de impugnaciones

- **Recurso ante el Consejo de Transparencia y Buen Gobierno:**
  - Sustituye a los recursos administrativos.
  - **Plazos:**
    - Presentación: 1 mes.
    - Resolución: 3 meses. Silencio administrativo: Desestimación.
  - No aplicable frente a órganos constitucionales.
  - Resoluciones: Se comunicarán al **Defensor del Pueblo**
- **Recurso contencioso-administrativo:** Procede tras agotar la vía administrativa.

## Título II: Buen Gobierno

### Ámbito subjetivo

- Se aplica a los **miembros del Gobierno**, Secretarios de Estado, altos cargos de la AGE, entidades del sector público estatal (de derecho público y privado) y otras entidades análogas en las CCAA o EELL.
- Se consideran **"Altos Cargos"** a aquellos con mayor responsabilidad administrativa o política en estas instituciones.

### Principios de buen gobierno

- **Principios generales ("DICTES"):**
  - **Dedicación** al servicio público.
  - **Imparcialidad** en la toma de decisiones.
  - **Conducta digna y ética**.
  - **Transparencia** en la gestión de asuntos públicos, garantizando la eficacia, economía y eficiencia.
  - **Eficiencia** y orientación al interés general.
  - **Satisfacción** del interés colectivo, evitando favoritismos y discriminaciones.
- **Principios de actuación:**
  - Cumplimiento pleno de la normativa vigente.
  - **Denuncia de actividades irregulares**.
  - **Confidencialidad** en asuntos sensibles o reservados.
  - **Plena dedicación** al cargo y abstención en caso de conflicto de intereses.
  - Prohibición de aceptar **regalos o favores** que puedan comprometer la imparcialidad.

### Infracciones y sanciones en materia de buen gobierno

- **Infracciones y sanciones en materia de conflicto de intereses:** Según normativa de la AGE y propia de cada administración.
- **Infracciones en materia de gestión económico-presupuestaria:**
  - **Muy graves:**
    - Uso indebido de fondos públicos.
    - Compromiso de gastos sin crédito suficiente.
    - Incumplimiento de destinar ingresos por encima de lo previsto a la reducción de deuda.
    - No presentar planes económicos-financieros o de reequilibrio.

- Desviación de fondos.
- No rendir cuentas.
- **Infracciones disciplinarias:**
  - **Muy graves:**
    - Incumplir la Constitución o el Estatuto de Autonomía.
    - Discriminación por cualquier causa.
    - Revelar secretos oficiales.
    - Actuar con parcialidad manifiesta.
    - Beneficio indebido derivado del cargo.
    - Acoso laboral.
    - Reiteración de infracciones graves en **1 año**.
  - **Graves:**
    - Abuso de autoridad.
    - Participación indebida en procedimientos donde deba abstenerse.
    - Falta de confidencialidad.
    - Incumplimiento reiterado de plazos legales.
    - Reiteración de infracciones leves en **1 año**.
  - **Leves:**
    - Incorrección, descuido o negligencia en las funciones.

### Sanciones aplicables

- **Por infracciones leves:**
  - Amonestación.
- **Por infracciones graves:**
  - Declaración de incumplimiento.
  - Publicación en el **BOE**.
  - Supresión de indemnizaciones (en caso de cese).
- **Por infracciones muy graves:**
  - Destitución del cargo.
  - Inhabilitación para ocupar altos cargos durante **5-10 años**.

### Procedimiento sancionador

- **Inicio del procedimiento:**

- De oficio: Por iniciativa propia, orden superior, petición razonada o denuncia.
- **Órganos competentes:**
  - **Consejo de Ministros:** Para miembros del Gobierno y Secretarios de Estado.
  - **Ministro de Hacienda y Administraciones Públicas:** Para altos cargos de la AGE.
  - **Órganos competentes en CCAA o EELL** para altos cargos de su ámbito.
- **Comunicación al Fiscal General del Estado:**
  - Si la infracción pudiera constituir delito, la Administración se abstendrá de continuar el procedimiento sancionador y lo remitirá al Ministerio Fiscal.
- **Recursos:** Contencioso-Administrativo
- **Plazos de prescripción:** (Diferente al TREBEP)
  - **Infracciones:**
    - **Muy graves:** 5 años.
    - **Graves:** 3 años.
    - **Leves:** 1 año.
  - **Sanciones:**
    - **Muy graves:** 5 años.
    - **Graves:** 3 años.
    - **Leves:** 1 año.

### Título III: Consejo de Transparencia y Buen Gobierno

- **Definición:** Organismo público con personalidad jurídica propia, plena capacidad de obrar, autonomía y plena independencia.
  - Está adscrito al **Ministerio de Hacienda y Administraciones Públicas**.

#### Fines del Consejo

- **Promover la transparencia** de la actividad pública.
- **Velar por el cumplimiento** de las obligaciones de publicidad activa.
- **Salvaguardar el ejercicio del derecho de acceso** a la información pública.
- **Garantizar el cumplimiento de las disposiciones de buen gobierno**.

#### Composición

- **Presidente del Consejo:**

- **Nombramiento:** Por un período de **5 años no renovable**, entre personas de reconocido prestigio en materias relacionadas con la Ley.
- **Ratificación:** Por mayoría absoluta del Congreso de los Diputados.
- **Funciones:**
  - Establecer **criterios de interpretación uniforme** de la Ley.
  - Velar por el cumplimiento de las **obligaciones de publicidad activa**.
  - Resolver las **reclamaciones** presentadas en el ámbito de la transparencia.
  - Responder **consultas** de las administraciones.
  - Promover el **inicio de procedimientos sancionadores** en caso de infracciones.
  - Aprobar el **anteproyecto de presupuesto** del Consejo.
- **Comisión de Transparencia y Buen Gobierno:**
  - **Composición:**
    - **Presidente del Consejo.**
    - **1 Diputado y 1 Senador.**
    - **5 representantes:** Tribunal de Cuentas, Defensor del Pueblo, Agencia Española de Protección de Datos (AEPD), Secretaría de Estado de Administraciones Públicas y la Autoridad Independiente de Responsabilidad Fiscal (AIReF).
  - **Funciones:**
    - Adoptar **recomendaciones** para mejorar la transparencia y el buen gobierno.
    - Asesorar en la aplicación de la Ley.
    - Evaluar el grado de aplicación de la Ley mediante una **memoria anual**.
    - Promover actividades de **formación y sensibilización**.
    - Elaborar **directrices, normas y recomendaciones** relacionadas con la transparencia y el buen gobierno.
    - Colaborar con otros órganos y entidades en materia de transparencia.

# Ley 1/2022, de Transparencia y Buen Gobierno de la Comunitat Valenciana

## Título Preliminar

### Objeto

- Regular y garantizar la **transparencia de la actividad pública**.
- Promover la **reutilización de la información**.
- Regular el **Consejo Valenciano de Transparencia**.
- Establecer principios básicos de **integridad y buen gobierno** en las administraciones públicas valencianas mediante códigos éticos y marcos de integridad pública.
- Impulsar la **rendición de cuentas** a través de la planificación y evaluación de normativas y políticas públicas.
- Regular el régimen de garantías, responsabilidades y obligaciones.

### Principios

- **Transparencia máxima**
- **Transparencia desde el diseño**
- **Publicidad**
- Comprensibilidad y claridad
- **Veracidad**
- **Reutilización de la información**
- Accesibilidad tecnológica universal
- No discriminación
- **Orientación a la ciudadanía** y continuidad en el tiempo
- Gobierno abierto
- Modernización y neutralidad tecnológica
- **Responsabilidad y rendición de cuentas**
- **Integridad**
- **Buen gobierno**
- **Planificación y evaluación** de políticas y servicios
- Buena regulación
- Protección de datos

## Ámbito subjetivo

- **Aplicación total:**
  - Administración de la Generalitat
  - Sector público instrumental de la Generalitat
  - Instituciones estatutarias (Corts Valencianes, Síndic de Greuges, Sindicatura de Comptes, Consell Valencià de Cultura, Acadèmia Valenciana de la Llengua, Comité Econòmic i Social, Consell Jurídic Consultiu, etc.).
- **Aplicación parcial:**
  - Partidos políticos, organizaciones sindicales y asociaciones empresariales.
  - Entidades privadas que reciben ayudas o subvenciones públicas.

## Definición de alto cargo

- Incluye a los integrantes del Consell, titulares de secretarías autonómicas, subsecretarías, direcciones generales, contratos laborales de alta dirección, y personas con consideración de alto cargo.

## Título I: Transparencia de la actividad pública

### Portal de Transparencia

- Obligatoriedad de publicación para la Administración de la Generalitat y sus organismos autónomos.

### Información sujeta a publicidad

- Institucional, organizativa y de planificación.
- Sobre altos cargos o asimilados.
- De relevancia jurídica.
- Presupuestaria, financiera, contable, endeudamiento y patrimonial.
- Contratación pública, convenios de colaboración, subvenciones.
- Publicidad y promoción institucional.
- Ordenación del territorio, urbanismo y medio ambiente.
- Estudios, estadísticas y cartografía.
- Otras solicitadas por la ciudadanía.

### Acceso a la información pública

- Cualquier ciudadano puede solicitarla.
- No es necesario motivar la solicitud ni invocar la ley.

### Apertura de datos

- Mejora la transparencia, promueve la interoperabilidad administrativa y genera valor social.
- **Publicación en formato digital**, accesible vía web, estandarizado y abierto.

### Título II: Consejo Valenciano de Transparencia

#### Características

- Autoridad de garantía en materia de transparencia en la Comunitat Valenciana.
- Garantiza el derecho de acceso a la información pública y vela por el cumplimiento de la publicidad activa.
- **Autonomía orgánica e independencia funcional**, sin jerarquías.

#### Composición

- Integrado por 3 personas.
- Candidaturas propuestas por los grupos parlamentarios entre expertos con más de **10 años de experiencia**.
- Aprobación por mayoría de **3/5 del parlamento**.
- Mandato de **5 años** con posibilidad de una única reelección.
- Los integrantes eligen a su presidente y tienen dedicación exclusiva.

#### Órganos

- Pleno.
- Presidencia.
- Secretaría (desempeñada por un funcionario).

### Título III: Buen Gobierno e Integridad Pública

#### Principios de actuación

- Actuar con **integridad, ejemplaridad y transparencia**.
- Garantizar una **gestión financiera justa y equitativa**.
- Ejercicio fiel de la función pública y de buena fe.
- Principio de participación y trato igualitario, sin arbitrariedad ni discriminación.
- **Responsabilidad personal** en las actuaciones propias y las de los organismos dirigidos.
- **Rendición de cuentas como principio básico**.
- Cumplir el régimen de incompatibilidades y la política de regalos.

- No uso indebido de tarjetas de crédito o débito con cargo a fondos públicos.
- Garantizar que reconocimientos honoríficos recaigan en personas de relevante compromiso público y sin condenas penales.

#### **Códigos éticos y de conducta**

- Cada institución del ámbito subjetivo debe elaborarlos para fomentar la integridad y el buen gobierno.

#### **Sistema de integridad institucional**

- Incluye códigos éticos, formación, sensibilización y mecanismos para formular y resolver dilemas.
- Garantía del cumplimiento, seguimiento, evaluación y mejora continua.

### **Título IV: Planificación y Evaluación**

#### **Plan de gobierno**

- **Plan estratégico de la legislatura.**
- Define objetivos, líneas de actuación y proyectos de ley clave.
- Incluye indicadores para el seguimiento.

#### **Seguimiento del plan de gobierno**

- **Periodicidad semestral.**

## Régimen Jurídico del Sector Público

# Ley 40/2015 - Régimen Jurídico del Sector Público

### CAPÍTULO I: DISPOSICIONES GENERALES

#### Objeto

La Ley establece las bases del régimen jurídico de las Administraciones Públicas (AAPP), regulando:

- Los principios del sistema de **responsabilidad** de las AAPP.
- El ejercicio de la **potestad sancionadora**.
- La **organización y funcionamiento** de la Administración General del Estado (AGE) y de su **sector público institucional**.

#### Ámbito de aplicación

La ley se aplica al **sector público**, compuesto por:

- **Administración General del Estado (AGE)**.
- **Administraciones de las Comunidades Autónomas (CCAA)**.
- **Entidades que integran la Administración Local (AALL)**.
- **Sector Público Institucional (SPI)**:
  - Organismos públicos y entidades de derecho público vinculados a las AAPP.
  - Entidades de derecho privado vinculadas a las AAPP (*No son AAPP*).
  - Universidades públicas (*No son AAPP*).

#### Principios generales de las AAPP

Las AAPP actúan con **objetividad**, en servicio de los intereses generales, de acuerdo con los principios de:

- **Eficacia, jerarquía, descentralización, desconcentración y coordinación**.
- Servicio efectivo a los ciudadanos.
- **Simplicidad, claridad y proximidad**.
- Participación, objetividad y transparencia.
- **Racionalización y agilidad** de los procedimientos administrativos.
- **Buena fe**, confianza legítima y lealtad institucional.
- **Responsabilidad** por la gestión pública.
- Planificación, dirección por objetivos y evaluación de resultados.
- **Eficiencia** en el uso de recursos públicos.

- Cooperación, colaboración y coordinación entre las AAPP.
- Uso preferente de **medios electrónicos** en relaciones interadministrativas.

### Principios de intervención administrativa

Cuando las actuaciones limiten derechos, deben cumplir:

- **Proporcionalidad.**
- Selección de la medida menos restrictiva.
- **Motivación** en interés público.
- Prohibición de discriminación.
- **Evaluación periódica** de los efectos.

## CAPÍTULO II: DE LOS ÓRGANOS DE LAS ADMINISTRACIONES PÚBLICAS

### Órganos administrativos

Son las unidades administrativas a las que se les atribuyen funciones que tienen efectos jurídicos frente a terceros o carácter preceptivo.

Cada Administración Pública delimitará sus órganos administrativos cumpliendo los siguientes **requisitos**:

- **No duplicidad:** No debe existir otro órgano con la misma función en la misma administración.
- **Determinación clara:** Se debe definir su forma de integración, dependencia jerárquica, funciones, competencias y dotación de créditos necesarios.

### Instrucciones y órdenes de servicio

Son instrumentos que permiten a los órganos jerárquicamente superiores dirigir las actividades de sus dependientes para garantizar el cumplimiento de sus objetivos.

### Órganos consultivos

- No pueden estar sujetos a dependencia jerárquica.
- Son **específicos y dotados de autonomía orgánica y funcional.**
- Prestarán asistencia jurídica a la Administración activa.

### Competencia de los órganos administrativos

- **Irrenunciable:** Las competencias son ejercidas únicamente por los órganos que las tienen atribuidas como propias, salvo delegación o avocación.
- **Titularidad:** La delegación, encomienda de gestión, delegación de firma o suplencia no alteran la titularidad de las competencias.
- **Instrucción y resolución:** Si no se especifica, corresponde a los órganos inferiores, salvo que haya más de uno, en cuyo caso será del superior jerárquico.

### **Delegación de competencias**

- Puede delegarse en:
  - Órganos de la misma administración, incluso si no son jerárquicamente dependientes.
  - Organismos públicos o entidades vinculadas.
- **Requisitos:**
  - La delegación requiere la aprobación del órgano ministerial del que dependa el órgano que delega, o el órgano máximo de dirección en organismos vinculados.
  - Si no están jerárquicamente relacionados:
    - En el mismo ministerio → Aprobación por el superior común.
    - En distintos ministerios → Aprobación por el órgano superior.
- **Competencias indelegables:**
  - Asuntos de Jefatura del Estado, Presidencia del Gobierno, Cortes Generales y presidencias de CCAA.
  - Adopción de disposiciones de carácter general.
  - Resolución de recursos administrativos.
  - Competencias que se ejerzan por delegación.
- **Publicidad:** La delegación y su revocación deberán publicarse en el BOE, BOP o DOA correspondiente.
- Las **resoluciones delegadas** se considerarán dictadas por el órgano delegante.

### **Avocación**

Un órgano administrativo superior puede asumir competencias de uno inferior, ordinarias o delegadas, en los siguientes casos:

- Por motivos técnicos, económicos, sociales, jurídicos o territoriales.
- **Requisitos:**
  - Acuerdo motivado.
  - Notificación a los interesados.
- La avocación no es recurrible.

### **Encomiendas de gestión**

Permiten la realización de actividades materiales o técnicas por razones de eficacia o falta de medios técnicos.

- No implican cesión de titularidad ni alteración de la competencia.
- El órgano encomendado tendrá la condición de **encargado del tratamiento**.

- **Formalización:**
  - En la misma administración → Según normativa o acuerdo expreso.
  - Entre administraciones diferentes → Mediante convenio.
- **Publicidad:** Su formalización y resolución deberán publicarse en el BOE, BOP o DOA correspondiente.

### **Delegación de firma**

Los titulares de órganos administrativos podrán delegar la firma de resoluciones y actos en subordinados. En dichos actos debe constar esta circunstancia.

### **Suplencia**

Los titulares de órganos administrativos podrán ser suplidos temporalmente en caso de:

- Vacante, ausencia, enfermedad, abstención o recusación.
- **Publicación:** No será necesaria su publicación en boletines.
- Las resoluciones y actos deben reflejar la suplencia.

### **Decisiones sobre competencia**

- Cuando un órgano se estime incompetente, remitirá el asunto al órgano que considere competente.
- **Requisitos:**
  - Los órganos deben pertenecer a la misma administración.
  - No deben estar jerárquicamente relacionados.
  - El procedimiento no debe haberse resuelto previamente.
- **Notificación:** La remisión será notificada a los interesados, quienes también podrán solicitarla.

### **Órganos colegiados**

Son aquellos que se crean formalmente con al menos tres integrantes y que tienen funciones administrativas de decisión, propuesta, asesoramiento, seguimiento o control.

### **Creación, modificación y supresión**

- Requieren norma específica y publicación en el BOE o DOA.
- **Forma de la norma:**
  - Real Decreto: Órganos interministeriales con presidente de rango superior a Director General.
  - Orden ministerial conjunta: Resto de órganos interministeriales.
  - Orden ministerial: Órganos ministeriales.

### **Clasificación y composición**

- **Interministeriales:** Miembros de distintos ministerios.

- **Ministeriales:** Miembros de un único ministerio.

### Funcionamiento de los órganos colegiados

- **Convocatorias y sesiones:**
  - Presenciales o a distancia, salvo disposición contraria en su reglamento.
  - Requieren la asistencia del presidente, secretario y al menos la mitad de los miembros.
  - Solo se deliberará sobre asuntos del orden del día, salvo asistencia total y declaración de urgencia por mayoría.
- **Acuerdos:** Aprobados por mayoría.
- **Actas:**
  - Redactadas por el secretario en cada sesión.
  - Incluirán asistentes, orden del día, lugar y tiempo, puntos principales de debate y acuerdos.
  - Podrán aprobarse en la misma sesión o en la siguiente.

### Funciones de los miembros

- **Presidente:** Representación, convocatoria, fijación del orden del día, moderación de debates, voto de calidad en empates, y visado de actas.
  - Sustitución: Vicepresidente o miembro más antiguo o de mayor edad.
- **Miembros:** Participar en debates, votar, formular ruegos y preguntas, y obtener información necesaria para sus funciones.
  - Sustitución: Suplentes.
  - Derecho a: Solicitar transcripciones de intervenciones y emitir voto particular.
- **Secretario:** Convocar sesiones, recibir comunicaciones, preparar el despacho de asuntos, redactar actas y expedir certificaciones. Puede tener voz sin voto o voz con voto si es miembro del órgano.

### Órganos colegiados

Son órganos formalmente creados, integrados por tres o más personas, con funciones administrativas de decisión, propuesta, asesoramiento, seguimiento o control, que actúan en el ámbito de la Administración General del Estado (AGE) o de sus organismos públicos.

### Clasificación y composición

- **Órganos colegiados interministeriales:** Integrados por miembros de diferentes Ministerios.
- **Órganos colegiados ministeriales:** Compuestos por miembros de un único Ministerio.

### Creación, modificación y supresión

- Requieren una norma específica, publicada en el **BOE** o en el **Diario Oficial Autonómico** correspondiente.
- La norma que regule su creación será:
  - **Real Decreto:** Si el presidente tiene rango superior al de Director General.
  - **Orden Ministerial Conjunta:** Para el resto de órganos interministeriales.
  - **Orden Ministerial:** Para los órganos ministeriales.

### **Abstención y recusación**

- **Abstención:**
  - Procederá en caso de interés personal, parentesco hasta el cuarto grado, relación de amistad/enemistad, intervención previa como perito o testigo, relación de servicio o ejercicio profesional en los dos años anteriores.
- **Recusación:**
  - Puede ser solicitada por los interesados en cualquier momento de la tramitación.
  - Si el recusado niega la causa, resolverá su superior en un plazo de **tres días**.

### **Potestad sancionadora**

- **Principio de legalidad:** Solo los órganos administrativos que tengan expresamente atribuida la potestad sancionadora por norma de rango legal o reglamentario pueden ejercerla.
- **Irretroactividad:** Las disposiciones sancionadoras no serán retroactivas, salvo cuando favorezcan al presunto infractor.

### **Infracciones administrativas**

- **Principio de tipicidad:** Las infracciones deben estar expresamente definidas en una norma.
- **Clasificación de infracciones:**
  - **Leves**
  - **Graves**
  - **Muy graves**

### **Responsabilidad administrativa**

- Puede recaer sobre:
  - Personas físicas y jurídicas.
  - Grupos de afectados, uniones, entidades sin personalidad jurídica y patrimonios independientes o autónomos (si tienen reconocida capacidad de obrar por ley).

### **Sanciones administrativas**

- **Prohibiciones:** Las sanciones no pueden implicar privación de libertad.
- **Principio de proporcionalidad:** Se tendrán en cuenta:
  - **Grado de culpabilidad** o existencia de intencionalidad.
  - Continuidad o **persistencia** de la conducta infractora.
  - **Naturaleza** y magnitud de los perjuicios causados.
  - **Reincidencia:** Cuando en menos de un año se cometa una infracción similar con resolución firme.

### Reglas específicas

- Puede imponerse una sanción de grado inferior por razones justificadas.
- Si de una infracción derivan otras, solo se sancionará la infracción más grave.
- **Infracción continuada:** Cuando varias acciones u omisiones se ejecuten bajo un plan preconcebido o aprovechando la misma ocasión.

### Prescripción de infracciones y sanciones

- Plazos para las infracciones:
  - **Muy graves:** 3 años.
  - **Graves:** 2 años.
  - **Leves:** 6 meses.
- Plazos para las sanciones:
  - **Muy graves:** 3 años.
  - **Graves:** 2 años.
  - **Leves:** 1 año.
- **Inicio del cómputo:**
  - Para las **infracciones:** Desde el día en que se cometió la infracción.
  - Para las **sanciones:** Desde el día siguiente a que la resolución sea ejecutable o haya finalizado el plazo de recurso.
- **Interrupción del plazo:** Si los procedimientos sancionadores o administrativos se paralizan por más de un mes por causas no imputables al infractor, el plazo continuará corriendo.

## CAPÍTULO IV: RESPONSABILIDAD PATRIMONIAL DE LAS AAPP

### Principio de responsabilidad

- Los particulares tienen derecho a ser indemnizados por las AAPP por cualquier lesión sufrida en sus bienes y derechos, salvo en casos de fuerza mayor o si el particular tiene la obligación jurídica de soportar el daño.

- **Supuestos adicionales:** Incluye daños derivados de normas declaradas inconstitucionales o contrarias al Derecho de la Unión Europea.

#### **Modalidades de indemnización**

- Puede sustituirse por **compensación en especie** o abonarse mediante **pagos periódicos**, si existe acuerdo con el interesado.

#### **Exigencia de responsabilidad al personal de las AAPP**

- Las indemnizaciones serán solicitadas directamente a la AAPP.
- Una vez indemnizado el particular, la AAPP podrá exigir responsabilidad a las autoridades o empleados públicos mediante un procedimiento interno.

#### **Procedimiento para la responsabilidad patrimonial**

1. **Alegaciones:** Plazo de 15 días.
2. **Pruebas:** Plazo de 15 días.
3. **Audiencia:** Plazo de 10 días.
4. **Propuesta de resolución:** Plazo de 5 días.
5. **Resolución definitiva:** Plazo de 5 días.

## Procedimiento Administrativo Común de las Administraciones Públicas

# Ley 39/2015 - Procedimiento Administrativo Común de las Administraciones Públicas

### Título Preliminar

#### Objeto

- Regular los requisitos de **validez y eficacia** de los actos administrativos.
- Establecer el procedimiento administrativo común aplicable a todas las Administraciones Públicas, incluyendo:
  - Procedimientos sancionadores.
  - Reclamaciones de responsabilidad de las AAPP.
- Definir los principios del ejercicio de la iniciativa legislativa y la potestad reglamentaria.

#### Modificaciones permitidas:

- **Solo por ley** se pueden establecer trámites adicionales o distintos de los previstos.
- **Reglamentariamente** se regulan especialidades en órganos competentes, plazos, formas de iniciación y terminación, publicación e informes.

#### Ámbito de aplicación:

- Aplica a todo el sector público e institucional:
  - AGE, Administraciones de las CCAA, Entidades locales y sector público institucional.
  - Incluye organismos públicos, entidades vinculadas a las AAPP (de derecho público o privado) y universidades públicas.

### Título I: De los interesados en el procedimiento

#### CAPÍTULO I: LA CAPACIDAD DE OBRAR Y EL CONCEPTO DE INTERESADO

##### Capacidad de obrar y concepto de interesado

- Personas físicas, jurídicas y, cuando lo declare la ley:
  - Grupos de afectados, uniones y entidades sin personalidad jurídica, y patrimonios independientes.
- Incluye a menores.
- **Se excluyen discapacitados graves.**

##### Concepto de interesado:

- Titulares de derechos o intereses legítimos y los afectados por el procedimiento.

#### Representación:

- **Acreditada** mediante:
  - **Apoderamiento apud acta**, personal o electrónico.
  - Inscripción en el **registro electrónico de apoderamientos** de la AAPP competente.
- **Tipos de poderes:** generales, para actuar ante un organismo concreto o realizar trámites específicos.
- Validez: **5 años**, prorrogables otros 5.

## CAPÍTULO II. IDENTIFICACIÓN Y FIRMA DE LOS INTERESADOS EN EL PROCEDIMIENTO ADMINISTRATIVO

#### Identificación y firma de los interesados

- Las AAPP verificarán la identidad mediante:
  - Medios ordinarios (nombre, DNI).
  - Medios electrónicos basados en **certificados electrónicos cualificados**.
- Sistemas de firma aceptados:
  - Firma electrónica cualificada y avanzada.
  - Sello electrónico cualificado y avanzado.
- La **identificación se entiende acreditada** con el acto de la firma.

#### Uso obligatorio de la firma electrónica:

- Para formular solicitudes, presentar declaraciones responsables, interponer recursos, desistir de acciones y renunciar a derechos.
- La AAPP debe garantizar medios electrónicos para relacionarse con los interesados.

## Título II: De la actividad de las Administraciones Públicas

### CAPÍTULO I: NORMAS GENERALES DE ACTUACIÓN

#### Derechos de las personas

- Comunicarse electrónicamente con las AAPP a través del **Punto de Acceso General electrónico**.
- Ser asistidos en el uso de medios electrónicos.
- Acceder a la información pública.
- Exigir responsabilidades a la AAPP.

- Obtener y utilizar medios de identificación y firma electrónica.
- Garantizar la protección de datos personales.

#### **Obligaciones de relacionarse electrónicamente con las AAPP:**

- **Personas físicas:** Pueden elegir entre medios electrónicos o no, salvo obligación expresa.
- **Personas jurídicas** y entidades sin personalidad jurídica: **Obligadas** a relacionarse electrónicamente.
- **Obligados adicionales:**
  - Profesionales con colegiación obligatoria.
  - Representantes de interesados obligados a medios electrónicos.
  - Empleados públicos en ejercicio de sus funciones.
  - Otras personas según disposiciones reglamentarias.

#### **Registro Electrónico General**

- Cada AAPP debe disponer de un registro para incluir documentos presentados en cualquier órgano administrativo.
- Los documentos podrán presentarse en:
  - Registros de las AAPP a las que se dirigen.
  - AGE, Administraciones de las CCAA, Administraciones locales, universidades, oficinas de correos, consulados, etc.

#### **Digitalización obligatoria de documentos presentados presencialmente.**

#### **Archivo único de documentos electrónicos**

- Cada AAPP debe mantener un archivo único de los documentos electrónicos de procedimientos finalizados, garantizando:
  - **Autenticidad, integridad y conservación.**

#### **Comparecencia**

- Puede ser presencial o electrónica.
- Será obligatoria únicamente si así lo establece la ley.

#### **Responsabilidad de tramitación**

- Los titulares de las unidades administrativas y el personal a su cargo son responsables de la correcta tramitación de los procedimientos.

#### **Obligación de resolver**

- Las AAPP están **obligadas a dictar resolución expresa** y a notificarla.
- Plazo máximo para notificar la resolución:

- Fijado por norma.
- **Por defecto: 3 meses.**
- **No excederá 6 meses**, salvo disposición en contrario.

#### **Suspensión del plazo máximo para resolver**

- En casos como:
  - Subsanación de deficiencias o aportación de documentos.
  - Pronunciamientos de la UE.
  - Informes preceptivos.
  - Pruebas en el procedimiento.

#### **Ampliación del plazo máximo para resolver**

- Solo en **casos excepcionales y de forma motivada**.

#### **Silencio administrativo**

- **Estimatorio (positivo):** Por defecto, el vencimiento del plazo sin resolución expresa da por estimada la solicitud del interesado.
- **Desestimatorio (negativo):**
  - En procedimientos relacionados con actividades que puedan dañar el medio ambiente.
  - En procedimientos de responsabilidad patrimonial.
  - Derecho de petición.
- **Efectos:** La desestimación permite al interesado recurrir por vía administrativa o contencioso-administrativa.
- **Certificado acreditativo del silencio:**
  - Lo expedirá de oficio el órgano competente en **15 días** desde la expiración del plazo máximo de resolución.
  - El interesado puede solicitarlo en cualquier momento.

#### **Documentos públicos administrativos**

- Emitidos válidamente por las AAPP:
  - Deben realizarse por escrito, preferentemente mediante **medios electrónicos**.
  - Salvo que la naturaleza del procedimiento requiera otra forma.

#### **Requisitos de validez de los documentos administrativos**

- Soporte electrónico.
- Formato identificable y tratable de forma diferenciada.

- Datos de identificación del órgano que lo emite.
- Referencias temporales y metadatos.
- Firma electrónica si procede.

#### **Excepción de firma electrónica**

- No requieren firma los documentos informativos y los que no formen parte de un expediente administrativo, aunque deben permitir identificar su origen.

#### **Régimen de validez y eficacia de las copias**

- **Copias auténticas:**
  - Realizadas por funcionarios habilitados o mediante actuación administrativa automatizada.
  - **Tienen la misma validez y eficacia que los originales.**
  - Las AAPP deben mantener un registro actualizado de funcionarios habilitados para expedir copias auténticas.

#### **Autenticidad garantizada:**

- En documentos electrónicos: Mediante **metadatos visibles** que acrediten la condición de copia.
- En documentos en papel: Mediante digitalización y metadatos.

#### **Documentos aportados por los interesados**

- Las AAPP no pueden requerir documentos que ya hayan sido aportados por el interesado previamente, que ya obren en su poder o que hayan sido elaborados por otra administración.

## **CAPÍTULO II: TÉRMINOS Y PLAZOS**

#### **Cómputo de plazos**

- **Las horas y días serán hábiles (salvo que se exprese otro cómputo)**
  - **Días hábiles:** Excluyen sábados, domingos y festivos.
  - **Horas hábiles:** Dentro de los días hábiles.
- Los plazos empiezan a contarse desde el día siguiente a la notificación o publicación.
- Plazos en meses o años: Finalizan el mismo día que se produjo la notificación o publicación.

#### **Cómputo en registros electrónicos**

- Basado en la fecha y hora oficial de la sede electrónica de acceso.
- Permiten presentación de documentos **24/7**.

- Si se presenta en día inhábil, se considera presentado el primer día hábil siguiente.

#### **Ampliación de plazos**

- Solo aplicable antes del vencimiento.
- Puede ser:
  - De oficio o a solicitud del interesado.
  - No puede exceder la mitad del plazo original.
  - Procede cuando **no afecta derechos de terceros**.

#### **Por incidencia técnica o ciberincidente:**

- Se publicará la incidencia y la ampliación del plazo correspondiente.

#### **Tramitación de urgencia**

- Por interés público, los plazos se reducen a la mitad, salvo en solicitudes y recursos.
- Puede acordarse de oficio o a petición del interesado.

### **Título III: De los actos administrativos**

#### **CAPÍTULO I. REQUISITOS DE LOS ACTOS ADMINISTRATIVOS**

##### **Actos motivados:**

- Requieren motivación aquellos actos que:
  - **Limiten derechos e intereses de los ciudadanos.**
  - Resuelvan procedimientos de **revisión de oficio**.
  - Decidan sobre **recursos administrativos**.
  - Resuelvan procedimientos de arbitraje.
  - Se separen de actuaciones precedentes.
  - Incluyan suspensión de actos, tramitación de urgencia, ampliaciones de plazo, actuaciones complementarias o rechacen pruebas propuestas.
  - Terminen el procedimiento por imposibilidad material.
  - Sean procedimientos de **carácter sancionador**.

##### **Forma de los actos administrativos:**

- Deben dictarse **por escrito** a través de medios electrónicos, salvo que la naturaleza del acto exija otra forma.
- Si la competencia se ejerce verbalmente, el funcionario debe dejar constancia escrita.

## CAPÍTULO II. EFICACIA DE LOS ACTOS

### Inderogabilidad singular:

- Las resoluciones administrativas particulares no pueden vulnerar disposiciones generales, aunque sean dictadas por órganos de igual o superior jerarquía.
- **Infringir esta norma conlleva la nulidad del acto.**

### Ejecutividad de los actos administrativos:

- Los actos administrativos son **ejecutivos** desde la fecha en que se dicten, salvo disposición en contrario.
- Si un acto administrativo se basa en otro considerado ilegal, será necesario declarar su nulidad o proceder a su revisión.

### Notificaciones:

- El órgano que dicte los actos administrativos debe notificarlos en un plazo de **10 días** desde su emisión.
- **Preferencia por medios electrónicos:**
  - En todo caso, los interesados obligados deberán recibir notificación electrónica, salvo excepciones:
    - Comparecencia espontánea del interesado en la oficina.
    - Asegurar la eficacia del acto mediante notificación directa.
    - Cuando el acto contenga elementos no susceptibles de conversión a formato electrónico o incluya medios de pago.
- Los interesados no obligados pueden optar entre notificación en papel o electrónica.
- Se puede señalar un dispositivo o dirección electrónica para recibir avisos de notificación, pero no para realizar notificaciones oficiales.

### Notificaciones en papel:

- Deben ponerse a disposición del interesado en la sede electrónica.
- Si se practica en el domicilio, puede ser recogida por un mayor de **14 años**.

### Notificaciones electrónicas:

- Se practican mediante comparecencia en la sede electrónica, accediendo al contenido de la notificación de forma identificada.
- Si el interesado no accede al contenido en **10 días naturales**, se entenderá como rechazada.
- **Notificación infructuosa:** Si no puede realizarse de otra forma, se publicará un anuncio en el BOE, y opcionalmente en otros boletines o tablones.

## CAPÍTULO III. NULIDAD Y ANULABILIDAD

**Nulidad de pleno derecho:**

- Los actos son nulos cuando:
  - Lesionan derechos y libertades susceptibles de amparo constitucional.
  - Son dictados por órganos manifiestamente incompetentes.
  - Tienen contenido imposible.
  - Son constitutivos de infracción penal.
  - Carecen de elementos esenciales o contravienen normas de rango legal.

**Anulabilidad:**

- Los actos son anulables cuando:
  - Infringen el ordenamiento jurídico.
  - Carecen de los requisitos formales indispensables.
  - Causan indefensión a los interesados.
- La anulabilidad no afecta a los actos sucesivos en la medida en que puedan subsistir por sí mismos.

**Título IV: De las disposiciones sobre el procedimiento administrativo común**

**CAPÍTULO I: GARANTÍAS DEL PROCEDIMIENTO**

**Derechos del interesado**

- Conocer el estado de la tramitación.
- Saber el sentido del silencio administrativo aplicable.
- Identificar al órgano competente para la instrucción y resolución del procedimiento.
- Formular alegaciones y presentar documentos en cualquier fase del procedimiento.
- Actuar asistido por un asesor o representante si lo desea.

**CAPÍTULO II: INICIACIÓN DEL PROCEDIMIENTO**

**Sección 1.ª Disposiciones generales**

- **Clases de iniciación:**
  - **De oficio:** Por iniciativa de la Administración, orden superior, petición razonada de otros órganos o denuncia.
  - **A petición del interesado.**
- **Información y actuaciones previas:**

- Finalidad: Determinar las circunstancias del caso y la conveniencia o no de iniciar el procedimiento.
- **Medidas provisionales:**
  - Aseguran la eficacia del procedimiento.
  - Pueden incluir: Suspensión de actividades, embargo preventivo, retención de bienes, etc.
  - No se adoptarán si pueden causar perjuicio de difícil o imposible reparación.

## Sección 2.<sup>a</sup> Iniciación del procedimiento de oficio

- **Formas de iniciación:**
  - **Iniciativa propia:** Por conocimiento directo o indirecto de circunstancias, hechos o conductas.
  - **Orden superior:** Emitida por un órgano jerárquicamente superior.
  - **Petición razonada de otros órganos:** Si carecen de competencia para iniciar el procedimiento, pero han tenido conocimiento de los hechos.
  - **Por denuncia:** Requiere identificar al denunciante y detallar los hechos denunciados.
    - El denunciante está **exento de pago de multas**.
- **Especialidades:**
  - **Procedimientos sancionadores:**
    - Siempre de oficio, con separación entre la fase instructora y la sancionadora.
  - **Responsabilidad patrimonial:**
    - Requiere que no haya prescrito el derecho del interesado para reclamar.

## Sección 3.<sup>a</sup> Iniciación del procedimiento a solicitud del interesado

- **Requisitos de la solicitud:**
  - Identificación del medio electrónico para notificaciones.
  - Detalle de hechos, razones y petición.
  - Identificación del órgano administrativo destinatario.
  - Uso obligatorio de modelos específicos, cuando existan.
- **Responsabilidad patrimonial:**
  - Derecho a reclamar prescribirá en **1 año**.
- **Subsanación y mejora de la solicitud:**
  - Plazo de **10 días** desde la notificación del requerimiento.

- **Declaración responsable y comunicación:**
  - Permiten el ejercicio de derechos o inicio de actividades desde su presentación.
  - **Declaración responsable:** El interesado declara cumplir requisitos y tener la documentación requerida.
  - **Comunicación:** Informa a la AAPP de datos para iniciar una actividad o ejercer un derecho.

## CAPÍTULO III: ORDENACIÓN DEL PROCEDIMIENTO

### Expediente administrativo

- Conjunto de documentos y actuaciones que fundamentan la resolución administrativa.
- **Formato electrónico obligatorio.**
- Cuando se remita, debe estar completo, foliado, autenticado y acompañado de un índice autenticado.
- No incluirá información auxiliar o de apoyo.

### Impulso del procedimiento

- Siempre por medios electrónicos, respetando los principios de **transparencia y publicidad**.

### Concentración de trámites

- Agrupación en un único trámite cuando sea posible, siguiendo el principio de simplificación administrativa.

### Cumplimiento de trámites:

- Plazo de **10 días** salvo disposición específica.

## CAPÍTULO IV: INSTRUCCIÓN DEL PROCEDIMIENTO

### Sección 1.<sup>a</sup> Disposiciones generales

- **Actos de instrucción:**
  - Realizados de oficio y por medios electrónicos.
  - Deben garantizar:
    - Control de tiempos y plazos.
    - Identificación de los órganos responsables.
    - Simplificación y publicidad del procedimiento.
- **Alegaciones:**

- Pueden presentarse en cualquier momento antes del trámite de audiencia.

## Sección 2.ª Prueba

- **Medios de prueba:**
  - Admitidos en derecho, siguiendo la Ley de Enjuiciamiento Civil.
- **Plazos:**
  - Período ordinario: Entre **10 y 30 días**.
  - Período extraordinario: Máximo de **10 días**.
- **Informes como prueba:**
  - Emitidos por órganos administrativos, son preceptivos.

## Sección 3.ª Informes

- **Tipos de informes:**
  - **Preceptivos:** Obligatorios, pueden suspender plazos.
  - **Facultativos:** No vinculantes.
- **Plazos:**
  - **Preceptivos:** Plazo de 10 días, salvo dictámenes (2 meses).

## Sección 4.ª Participación de los interesados

- **Trámite de audiencia:**
  - Antes de la solicitud de informe del órgano jurídico o del dictamen del Consejo de Estado.
- **Información pública:**
  - Anunciada en Diarios Oficiales cuando el procedimiento lo exija.

# CAPÍTULO V: FINALIZACIÓN DEL PROCEDIMIENTO

## Sección 1.ª Disposiciones generales

- **Formas de terminación del procedimiento:**
  - Resolución.
  - Desistimiento del interesado.
  - Renuncia al derecho en que se funde la solicitud.
  - Declaración de caducidad.
- **Procedimientos sancionadores:**
  - Se podrá resolver con la imposición de una sanción si el infractor reconoce su responsabilidad.
- **Terminación convencional:**

- Cuando el acuerdo sea competencia directa de la Administración.
- **Requerirá aprobación expresa** del Consejo de Ministros u órgano equivalente de las CCAA en determinados casos.

## Sección 2.ª Resolución

- **Actuaciones complementarias:**
  - Podrán ser realizadas antes de dictar resolución por el órgano competente.
  - Notificación a los interesados en el plazo de **7 días** para formular alegaciones.
  - El plazo para practicar actuaciones complementarias es de **15 días**.
- **Contenido de la resolución:**
  - Se realizará por medios electrónicos.
  - Garantizará la **identidad del órgano competente y la autenticidad e integridad del documento**.
- **Resoluciones en procedimientos sancionadores:**
  - Serán ejecutivas si no cabe recurso ordinario en vía administrativa.

## Sección 3.ª Desistimiento y renuncia

- **Derecho del interesado:**
  - Puede desistir de su solicitud o renunciar a sus derechos en cualquier momento y por cualquier medio que permita su constancia.
  - La Administración podrá limitar los efectos de la renuncia si afecta al interés general.

## Sección 4.ª Caducidad

- **Plazos para declarar la caducidad:**
  - **3 meses** para procedimientos iniciados por interesados y paralizados por causas imputables a ellos.
  - **6 meses** para procedimientos de revisión iniciados de oficio.

## CAPÍTULO VI: TRAMITACIÓN SIMPLIFICADA DEL PROCEDIMIENTO ADMINISTRATIVO COMÚN

- **Motivos para aplicar la tramitación simplificada:**
  - Por razones de interés público.
  - Cuando la falta de complejidad del procedimiento lo aconseje.
- **Notificación y oposición de los interesados:**
  - Si se acuerda de oficio, se notificará a los interesados, quienes podrán oponerse y solicitar la tramitación ordinaria.

- Si lo solicita un interesado, la Administración podrá desestimarla en un plazo de **5 días**, sin posibilidad de recurso.
- **Plazo máximo para resolver:**
  - **30 días**, contados desde la notificación del acuerdo de tramitación simplificada.
- **Trámites esenciales:**
  - Iniciación (de oficio o a solicitud del interesado).
  - Subsanación.
  - Alegaciones (plazo de **5 días**).
  - Audiencia (si la resolución es desfavorable).
  - Informes del servicio jurídico o Consejo de Estado (cuando sean preceptivos).
  - Resolución.

## CAPÍTULO VII: EJECUCIÓN

- **Inicio de la ejecución:**
  - Las AAPP no iniciarán la ejecución de un acto sin que haya sido adoptada y notificada la resolución correspondiente.
- **Medios electrónicos de pago:**
  - Incluyen tarjeta, transferencia bancaria, domiciliación y otros.
- **Ejecución forzosa:**
  - Aplicable para garantizar el cumplimiento de resoluciones administrativas, respetando el principio de proporcionalidad.
  - Requiere previo apercibimiento al obligado.
- **Medios de ejecución forzosa:**
  - **Apremio sobre el patrimonio:** Obligación de pagar o embargo de bienes.
  - **Ejecución subsidiaria:** Otro realiza la prestación a cargo del obligado.
  - **Multa coercitiva:** Pueden ser reiteradas hasta el cumplimiento del acto.
  - **Compulsión sobre las personas:** Obliga al cumplimiento de deberes personalísimos.
- **Coerción física:**
  - Solo aplicable en los casos previstos por la ley, para impedir, prohibir o ejecutar.

## Título V: De la revisión de los actos en vía administrativa

### CAPÍTULO I: REVISIÓN DE OFICIO

#### Revisión de disposiciones y actos nulos

- Los actos administrativos y disposiciones que sean **nulos de pleno derecho** podrán ser revisados de oficio.
- El procedimiento para la revisión de oficio caducará si:
  - **Iniciado de oficio:** Caduca si no se resuelve en **6 meses**.
  - **Iniciado por el interesado:** Desestimado por **silencio administrativo**.

#### Declaración de lesividad:

- Para actos anulables que perjudiquen al interés público, es necesaria una **declaración de lesividad** antes de su impugnación ante el orden jurisdiccional contencioso-administrativo.
- Si no se declara en **6 meses**, el procedimiento caducará.

#### Revocación de actos:

- Procede la revocación de actos desfavorables siempre que no hayan prescrito y no contravengan el ordenamiento jurídico ni perjudiquen derechos de terceros.

#### Rectificación de actos:

- Podrán rectificarse errores materiales, de hecho o aritméticos en cualquier momento.

### CAPÍTULO II: RECURSOS ADMINISTRATIVOS

#### Finalidad de los recursos administrativos:

- Pueden interponerse contra resoluciones y actos administrativos que:
  - Decidan sobre el fondo del asunto.
  - Determinen la imposibilidad de continuar el procedimiento.
  - Produczan indefensión o perjuicio irreparable.

#### Tipos de recursos administrativos:

##### 1. Recurso de alzada:

- **Objeto:**
  - Contra resoluciones y actos de trámite que no pongan fin a la vía administrativa.
- **Plazo para interponerlo:**
  - **1 mes** desde la notificación (si el acto es expreso).

- Si el acto no es expreso, puede interponerse en cualquier momento desde el día siguiente a los efectos del silencio administrativo.
- **Órgano competente:**
  - Puede presentarse ante el órgano que dictó el acto o el competente para resolver.
- **Plazo de resolución:**
  - **3 meses** desde la interposición. Si no se resuelve, el recurso se entiende desestimado por silencio administrativo.
- **Recurso adicional:**
  - No cabe otro recurso administrativo salvo el extraordinario de revisión.

## **2. Recurso potestativo de reposición:**

- **Objeto:**
  - Contra actos administrativos que pongan fin a la vía administrativa.
- **Plazo para interponerlo:**
  - **1 mes** desde la notificación (si el acto es expreso).
  - Si el acto no es expreso, puede interponerse en cualquier momento desde el día siguiente a los efectos del silencio administrativo.
- **Órgano competente:**
  - Se interpone ante el mismo órgano que dictó el acto.
- **Plazo de resolución:**
  - **1 mes** desde la interposición. Si no se resuelve, se entiende desestimado por silencio administrativo.

## **3. Recurso extraordinario de revisión:**

- **Objeto:**
  - Contra actos firmes en vía administrativa cuando concurren las siguientes circunstancias:
    - **Error de hecho** que resulte de los propios documentos.
    - Aparición de **documentos de valor esencial** desconocidos al dictar el acto.
    - Acto basado en documentos falsos declarados como tales.
    - Acto dictado como consecuencia de **prevaricación, cohecho, violencia u otra conducta punible**.
- **Plazo para interponerlo:**
  - **4 años:** Si el motivo es un error de hecho.

- **3 meses:** Para el resto de casos desde que se tuvo conocimiento del motivo.
- **Órgano competente:**
  - El mismo que dictó el acto.
- **Plazo de resolución:**
  - **3 meses.** Si no se resuelve, se entiende desestimado.

#### **Fin de la vía administrativa:**

- Finaliza con las siguientes resoluciones y actos:
  - Resoluciones de recursos de alzada.
  - Resoluciones de procedimientos cuya competencia esté atribuida al órgano administrativo.
  - Acuerdos, pactos, convenios y contratos que finalicen el procedimiento.
  - Actos administrativos de los miembros del Gobierno y Ministros.
  - Actos de Secretarios de Estado, Directores Generales (o superior) en materia de personal, y máximos órganos de dirección de organismos públicos.

#### **Causas de inadmisión de recursos:**

- Falta de competencia del órgano administrativo.
- Recurrente no legitimado.
- Acto no recurrible.
- Presentación fuera de plazo.
- Recursos que carezcan de fundamento.

#### **Suspensión de la ejecución de los actos impugnados:**

- **Regla general:**
  - La interposición de un recurso no suspende la ejecución del acto impugnado.
- **Suspensión de oficio:**
  - Procede si la ejecución pudiera causar perjuicios de difícil o imposible reparación.
  - Si hay causas de nulidad de pleno derecho.
- **Solicitud de suspensión por parte del interesado:**
  - Si no se resuelve en **1 mes**, se entiende desestimada.

**Requisitos formales para la interposición de recursos:**

- Identificación del interesado y del acto recurrido.
- Motivación de la impugnación.
- Órgano al que se dirige.
- Si hay varios interesados, se debe dar audiencia para alegaciones (plazo de **10-15 días**).

## Ley 9/2017- Contratos del Sector Público

# Ley 9/2017 - Contratos del Sector Público

### Objeto

- Regular la contratación del sector público.
- Garantizar los principios de **libertad de acceso a las licitaciones, publicidad y transparencia** en los procedimientos, y **no discriminación e igualdad de trato** entre los licitadores.
- Asegurar una **eficiente utilización de los fondos públicos** mediante la exigencia previa de identificar las necesidades a satisfacer.

### Contratos del sector público

Se consideran contratos del sector público aquellos **onerosos** celebrados por las entidades que forman parte del **Sector Público**, que incluye:

- **Administración General del Estado (AGE)**, Comunidades Autónomas (CCAA), Entidades Locales (EELL).
- Entidades gestoras de servicios comunes de la Seguridad Social, Organismos Autónomos, Entidades Públicas Empresariales (EPE).
- Universidades Públicas, Autoridades Administrativas Independientes.
- Sociedades mercantiles con participación superior al **50%**.
- Fundaciones con financiación o aportación superior al **50%**.
- Mutuas colaboradoras de la Seguridad Social.

### Poderes adjudicadores

Incluyen:

- Administraciones Públicas (AAPP).
- Fundaciones públicas.
- Mutuas colaboradoras de la Seguridad Social.
- Otras entidades descritas en la ley.

### Negocios y contratos excluidos

Excluye contratos relacionados con:

- **Defensa y seguridad.**
- Investigación y desarrollo (I+D).
- Servicios prestados al Banco de España.
- Servicios relacionados con estabilidad presupuestaria.
- Abono de tarifas, tasas y campañas políticas, entre otros.

## Régimen jurídico

- Los contratos pueden someterse a un régimen de **derecho administrativo** o **derecho privado**, según lo establecido en la ley.

## Tipos de contratos

- **Contrato de obras:** Ejecución o realización de una obra.
  - **Tipos:** Primer establecimiento, reforma, restauración, gran reparación, reparación simple, conservación y mantenimiento, demolición.
- **Contrato de concesión de obras:** El concesionario realiza las obras.
  - Límite de duración: **40 años**.
- **Contrato de concesión de servicios:** Gestión y explotación de un servicio.
  - Límite de duración:
    - **25 años** (general).
    - **10 años** (servicios sanitarios).
- **Contrato de suministro:** Adquisición, arrendamiento financiero o arrendamiento con opción de compra de bienes muebles.
  - **Incluye:**
    - Entrega de bienes sucesiva.
    - Adquisición y arrendamiento de equipos y sistemas de telecomunicaciones.
    - Adquisición de energía y bienes fabricados.
  - **Excluye:** Programas informáticos desarrollados a medida (considerados servicios).
  - Límite de duración: **5 años** (incluidas prórrogas).
- **Contrato de servicios:** Prestación de una actividad o resultado distinto de una obra o suministro.
  - Límite de duración: **5 años** (incluidas prórrogas).

- **Contratos mixtos:** Combinan varias prestaciones de diferente naturaleza.

### Contratos menores

- **Adjudicación directa** a empresarios con capacidad de obrar y habilitación profesional.
- **Duración máxima: 1 año**, sin prórrogas.
- **Tramitación:** Aprobación del gasto, factura e informe motivando la necesidad del contrato.
- **Cuantías:**
  - Obras: Inferior a **40.000€**.
  - Servicios y suministros: Inferior a **15.000€**.

### Contratos sujetos a regulación armonizada (SARA)

**Aplica** a contratos que superen ciertos importes de **valor estimado** (sin incluir IVA):

- **Obras**, concesión de obras y concesión de servicios: **5.382.000€**.
- **Suministros:**
  - **140.000€** (AGE, etc.).
  - **215.000€** (otros).
- **Servicios:**
  - **140.000€** (AGE).
  - **215.000€** (sector público).
  - **750.000€** (otros).
- **Excluidos:** Contratos relacionados con defensa, comunicación audiovisual, riesgos laborales, suministro de agua, entre otros.

### Contratos privados

**Incluyen** contratos celebrados por:

- **AAPP**, cuando no sean de obra, concesión, suministro o servicios.
- **Entidades del sector público** que no sean AAPP o **poderes adjudicadores**.
- **Casos específicos:**
  - Financieros, seguros, bancarios.
  - Creación artística o literaria.

- Suscripción a publicaciones periódicas.

### Cómputo de plazos

- En días naturales.
  - Si el último día fuera inhábil, se entenderá prorrogado al primer día hábil

### Formalización de contratos

- Obligatoria, salvo en casos de emergencia.
- Contratos perfeccionados con su formalización.

### Competencia para contratar

- La tienen los órganos de contratación, que pueden ser unipersonales o colegiados.
  - Ejemplos:
    - Ministros y Secretarios de Estado, en la AGE
    - Presidentes o Directores de organismos autónomos o EPEs, en su ámbito
- Juntas de contratación: Actuarán como órganos de contratación
- Requiere autorización del Consejo de Ministros en contratos de:
  - +12.000.000€.
  - Arrendamientos superiores a 4 años.

### Responsable del contrato

- Supervisará la ejecución y adopción de decisiones, y dictará las instrucciones necesarias
- Deberá existir uno con independencia de la unidad encargada del seguimiento y ejecución

### Perfil del contratante

- Obligatorio en las páginas web de las AAPP.
- Publica información sobre licitaciones, adjudicaciones, pliegos, etc.

## Aptitud y prohibiciones para contratar

### Aptitud para contratar

- Personas naturales o jurídicas, españolas o extranjeras, que cumplan los siguientes requisitos:
  - **Plena capacidad de obrar.**
  - No estar incursas en una **prohibición para contratar.**
  - Acreditar su **solvencia económica, financiera, técnica o profesional** o estar debidamente clasificadas.

### Tipos de empresas aptas:

- Empresas comunitarias.
- Empresas no comunitarias.
- **Uniones de empresarios (UTEs).**

### Prohibición de contratar

Causas por las que NO se puede contratar:

- **Condenas o sanciones firmes** por delitos relacionados con la contratación pública, corrupción, fraude o blanqueo de capitales.
- Declaración en concurso voluntario o situación de insolvencia en cualquier procedimiento.
- Incumplimiento de obligaciones tributarias o con la Seguridad Social.
- Retirada injustificada de una proposición o imposibilidad de adjudicar el contrato debido a acciones del contratista.
- Empresas de más de **50 trabajadores** sin un **plan de igualdad** obligatorio.

### Duración de la prohibición:

- General: **Máximo 3 años.**
- Por condena o sanción: **Máximo 5 años.**

### Acreditación de la ausencia de prohibición:

- Declaración responsable emitida por el contratista.
- Inscripción en el **Registro Oficial de Licitadores y Empresas Clasificadas del Sector Público.**

## Solvencia

### Requisitos de solvencia

- Las empresas deben acreditar que cumplen las **condiciones mínimas de solvencia económica, financiera y técnica o profesional**, determinadas por el órgano de contratación.
- La solvencia podrá ser sustituida por la **clasificación de empresas** en determinados contratos.

### Publicación de requisitos

- Los requisitos mínimos deben indicarse en:
  - El **anuncio de licitación**.
  - El **pliego de cláusulas administrativas particulares (PCAP)**.

## Clasificación

### Características de la clasificación

- Clasificación basada en la **solvencia** de la empresa.
- Para obtenerla, se debe acreditar:
  - Personalidad jurídica y capacidad de obrar.
  - Habilitación para realizar la actividad.
  - Ausencia de prohibiciones para contratar.

### Aprobación y recursos

- La clasificación es aprobada por las **Comisiones Calificadoras** de la Junta Consultiva de Contratación Pública.
- Recursos por denegación:
  - **Recurso de alzada** ante el Ministro de Hacienda.

### Duración de la clasificación

- **Indefinida**, siempre que se mantengan las condiciones requeridas.

### Inscripción

- Obligatoria en el **Registro Oficial de Licitadores y Empresas Clasificadas del Sector Público**.

## Objeto del contrato

### Determinación del objeto

- El objeto del contrato debe ser claro y **determinado**.
- **Prohibición de fraccionamiento:** No puede dividirse para reducir la cuantía y eludir publicidad o procedimientos de adjudicación.

### Lotes

- Si se permite fraccionar, el contrato se dividirá en **lotes independientes**.

## Presupuesto base de licitación, valor estimado y precio

### Definiciones clave

- **Presupuesto base de licitación:** Límite máximo de gastos que el órgano de contratación puede comprometer (incluye IVA).
- **Valor estimado del contrato:** Importe total del contrato sin incluir IVA.
- **Precio:** Retribución en euros que percibirá el contratista por la ejecución del contrato (incluye IVA).

## Expediente de contratación

### Contenido del expediente

- Conjunto ordenado de documentos y actuaciones que justifican y fundamentan un contrato.
- **Elementos** que incorpora:
  - **Pliego de Cláusulas Administrativas Particulares (PCAP)**.
  - **Pliego de Prescripciones Técnicas (PPT)**.
  - **Existencia de crédito** mediante el documento RC.
  - **Fiscalización previa** de la Intervención.

### Justificación del expediente

- **Deberá incluir:**
  - Elección del procedimiento.
  - Clasificación del contrato.
  - Criterios de solvencia técnica o profesional.
  - Valor estimado del contrato.
  - Necesidad a satisfacer por la administración.

## Tramitación del expediente

- **Ordinaria:** Requiere un contenido mínimo (art. 35).
  - Identificación de las partes, acreditación de suscribir el contrato, definición del objeto y tipo de contrato, precio cierto, duración, condiciones de pago,...
- **Urgente:** Para **necesidades inaplazables**, plazos reducidos a la mitad. La ejecución debe iniciarse en **1 mes** desde la formalización.
- **De emergencia:** Contratos inmediatos por acontecimientos catastróficos, grave peligro o defensa nacional.
  - No requiere formalidades como expediente o crédito.
  - Plazo de inicio de ejecución de **1 mes**. Pasado el plazo se requiere un procedimiento ordinario
  - Se informa al Consejo de Ministros en un máximo de **30 días**.

## Pliegos

### Tipos de pliegos

- **Pliegos de cláusulas administrativas generales (PCAG):** Aprobados por el Consejo de Ministros.
- **Pliegos de cláusulas administrativas particulares (PCAP):** Aprobados por el órgano de contratación.
- **Pliego de prescripciones técnicas generales (PPTG):** Aprobados por el Consejo de Ministros, ajustados a la AGE.
- **Pliego de prescripciones técnicas particulares (PPTP):** Aprobados por el órgano de contratación.

### Contenido de los pliegos

- Describen las prestaciones esperadas y las condiciones técnicas y administrativas.
- Detallan las calidades y ejecución de las prestaciones.

## Procedimiento de adjudicación

### Principios generales

La adjudicación debe garantizar:

- **Igualdad de trato** entre los licitadores.
- **Transparencia** y libre competencia.
- Mejor relación calidad-precio.

### Tipos de procedimientos

- **Ordinarios:**
  - **Abierto:** Todo empresario puede presentar proposiciones, sin negociación.
  - **Abierto simplificado:** Procedimiento más ágil.
  - **Restringido:** Sólo licitadores previamente seleccionados por su solvencia (mínimo 5).
- **Con negociación:** La administración negocia con los candidatos seleccionados (mínimo 3).
  - **Causas:**
    - Dificultad técnica para especificar condiciones.
    - Ofertas irregulares en procedimientos ordinarios.
    - Exclusividad del proveedor.
  - **Modalidades:** Negociado con y sin publicidad
- **Diálogo competitivo:** Se dialoga con candidatos seleccionados para desarrollar soluciones (mínimo 3).
- **Asociación para la innovación:** Desarrollar productos o servicios aún inexistentes en el mercado.
- **Concurso de proyectos:** Desarrollo de una idea para un proyecto (mínimo 3).
- **Subasta electrónica:** Evaluación automática del precio o valores cuantificables.

#### Plazos de presentación

- Contratos **SARA:** 30 días.
- Contratos no **SARA:** 15-25 días.

## Función pública

# RDL 5/2015 - Ley del Estatuto Básico del Empleado Público (TREBEP)

### Objeto

- **Establecer las bases** del régimen estatutario de los funcionarios públicos incluidos en su ámbito de aplicación.
- **Determinar las normas aplicables** al personal laboral al servicio de las Administraciones Públicas (AAPP).

### Fundamentos del Estatuto

- **Servicio a los ciudadanos** y a los intereses generales.
- **Igualdad, mérito y capacidad** en el acceso y en la promoción profesional.
- **Sometimiento pleno a la ley y al Derecho.**
- **Igualdad de trato entre mujeres y hombres.**
- Objetividad, profesionalidad e imparcialidad en el servicio, garantizadas con la **inamovilidad** en la condición de funcionario de carrera.
- Eficacia en la planificación y gestión de los recursos humanos.
- Desarrollo y cualificación profesional permanente de los empleados públicos.
- Transparencia.
- Evaluación y responsabilidad en la gestión.
- Jerarquía en la atribución, ordenación y desempeño de funciones y tareas.
- Negociación colectiva y participación a través de los representantes para las condiciones de empleo.
- **Cooperación entre las AAPP** en la regulación y gestión del empleo público.

### Ámbito de aplicación

- **Incluye:**
  - Personal funcionario y personal laboral de la Administración General del Estado (AGE), Administraciones Públicas de las Comunidades Autónomas (AAPP CCAA), entidades locales, organismos públicos y universidades públicas.
- **Personal docente** y personal estatutario de los Servicios de Salud:
  - Se rigen por **legislación específica** dictada por el Estado y por las CCAA.
- **Personal funcionario de las Entidades Locales:**

- Se aplican **TREBEP** + legislación estatal y autonómica.
- Policías Locales, salvo lo que disponga la Ley Orgánica de las Fuerzas y Cuerpos de Seguridad.
- **Personal con legislación específica propia:**
  - Incluye: Cortes Generales, asambleas legislativas, órganos constitucionales del Estado, jueces, magistrados, fiscales, Administración de Justicia, Fuerzas Armadas, cuerpos de seguridad, personal retribuido por arancel, CNI, Banco de España y Fondo de Garantía de Depósitos.
- **Personal de la Sociedad Estatal Correos y Telégrafos:**
  - Se aplica **TREBEP** + normas específicas.
- **Leyes de Función Pública:**
  - Aprobadas por **Cortes Generales y CCAA**.
- **Personal laboral:**
  - Se rige por la legislación laboral, aplicándose los permisos establecidos por **AAPP y TREBEP**.

## Personal al servicio de las Administraciones Públicas

### Concepto y clases de empleados públicos

- **Definición:**
  - Empleados públicos son quienes desempeñan funciones **retribuidas** en las AAPP al servicio de los intereses generales.
- **Clases:**
  - **Funcionarios de carrera:**
    - Designados por **nombramiento legal**.
    - Vinculados a una AAPP para desempeñar **servicios profesionales retribuidos y permanentes**.
    - Funciones exclusivas: Participación en **potestades públicas o salvaguarda de intereses generales**.
  - **Funcionarios interinos:**
    - Nombrados por razones **justificadas de necesidad y urgencia** para funciones propias de funcionarios de carrera.
    - **Supuestos:**
      - Plazas vacantes sin cobertura inmediata por funcionarios de carrera.
      - Sustituciones transitorias.

- Programas temporales (máximo 3 años, ampliable 12 meses según leyes de función pública).
- Acumulación de tareas (6 meses en 12 meses).
- **Régimen:** Igual que los funcionarios de carrera.
- **Personal laboral:**
  - Vinculados mediante **contrato de trabajo escrito** para servicios retribuidos.
  - Tipos: **Fijo, indefinido o temporal.**
- **Personal eventual:**
  - Designado para funciones de **confianza o asesoramiento especial.**
  - Nombramiento y cese **libres.**
  - No constituye mérito para acceso o promoción interna.

### **Personal Directivo**

- Realizan funciones directivas profesionales en las AAPP
- Designado según **principios de mérito, capacidad e idoneidad**, y por procedimientos que garanticen la **publicidad y concurrencia**
- Funciones: **Dirección profesional en AAPP.**
- Sujetos a evaluación de eficacia, eficiencia y resultados.
- No son materia de **negociación colectiva.**

### Título III: Derechos y deberes. Código de conducta de los empleados públicos

#### Derecho a la jornada de trabajo, permisos y vacaciones

##### Jornada de trabajo

- Puede ser a **tiempo completo o parcial.**

##### Teletrabajo

- Modalidad de prestación de servicios a distancia.
- El contenido competencial del puesto debe ser compatible con su desarrollo fuera de las dependencias de la Administración.
- **Condiciones:**
  - Ha de ser **autorizado expresamente.**
  - Tiene carácter **voluntario y reversible.**
  - Compatible con la modalidad presencial.
  - La Administración proporciona los **medios tecnológicos necesarios.**

##### Permisos de los funcionarios públicos

- **Fallecimiento, accidente o enfermedad graves, hospitalización o intervención quirúrgica de un familiar:**
  - **Primer grado:**
    - 3 días en misma localidad.
    - 5 días en distinta localidad.
  - **Segundo grado:**
    - 2 días en misma localidad.
    - 4 días en distinta localidad.
- **Traslado de domicilio sin cambio de residencia:** 1 día.
- **Otros permisos específicos:**
  - Por el ejercicio de **funciones sindicales.**
  - Para concurrencia a **exámenes finales** o pruebas definitivas de aptitud.
  - **Exámenes prenatales**, técnicas de preparación al parto, o adopción.
  - **Lactancia:**
    - Por hijo menor de 12 meses:
      - 1 hora diaria, divisible en dos fracciones.
      - Posibilidad de reducción de jornada en una hora con la misma finalidad.

- **Nacimiento de hijos prematuros o hospitalización tras el parto:**
  - Derecho a ausentarse del trabajo hasta 2 horas diarias con retribuciones íntegras.
- **Cuidado de familiares hasta el segundo grado de consanguinidad o afinidad:**
  - Reducción de jornada con disminución proporcional de la retribución.
- **Cumplimiento de un deber inexcusable** de carácter público o personal.
- **Permiso por asuntos particulares:** 6 días al año.
- **Permiso por matrimonio:** 15 días.

#### Vacaciones

- **Duración:**
  - **22 días hábiles** al año o la parte proporcional si el tiempo trabajado es inferior al año.
- **Disfrute posterior:**
  - Si no se pudieran iniciar las vacaciones por causas como permisos de maternidad/paternidad, incapacidad temporal u otras circunstancias justificadas, podrán disfrutarse posteriormente, siempre que no hayan transcurrido más de **18 meses** desde el final del año natural correspondiente.
- **Restricción:**
  - No se pueden sustituir las vacaciones por una **compensación económica**.

# Ley 4/2021 - Función Pública Valenciana

## Título I: Objeto, principios y ámbito de aplicación de la ley

### Objeto

Ordenar y regular la función pública valenciana y los instrumentos de gestión y determinación del régimen jurídico del personal.

### Principios informadores

Los principios y fundamentos que ordenan la función pública valenciana (FPV) son:

- Servicio a la ciudadanía y a los intereses generales.
- **Sometimiento pleno a la ley y al derecho.**
- Economía, eficacia y eficiencia.
- Igualdad.
- Objetividad, profesionalidad, transparencia, integridad, imparcialidad y austeridad.
- Desarrollo y cualificación profesional permanente.
- Igualdad, mérito, capacidad, publicidad y transparencia en el acceso y la promoción profesional.
- Eficacia en la planificación y gestión de los recursos humanos.

**La FPV está constituida por** el conjunto de personas que prestan servicios retribuidos en la administración mediante una relación regulada por normativa administrativa o laboral.

### Principios de la actuación del empleado público

Imparcialidad, profesionalidad, diligencia, buena fe, confidencialidad, responsabilidad, ejemplaridad y honradez.

### Ámbito de aplicación

La ley se aplicará a:

- Personal funcionario.
- Personal laboral (cuando se disponga expresamente).
- Personal eventual, en los términos y limitaciones previstas.

Se aplica a quienes presten servicios en:

- La Administración de la Generalitat.
- Organismos públicos de la Generalitat.
- Consorcios adscritos a la Generalitat.
- Administraciones de entidades locales de la Comunidad Valenciana.
- Universidades públicas de la Comunidad Valenciana.

## **Exclusiones**

- **Personal docente no universitario** y personal estatutario de sanidad (régimen específico).

## **Personal con legislación específica**

- Personal al servicio de las Cortes Valencianas e instituciones de la Generalitat reguladas por el Estatuto de Autonomía.
- Administración de Justicia.
- Personal docente investigador de universidades públicas.

## **Título III: Personal al servicio de las administraciones públicas**

### **Concepto y clases de personal empleado público**

El personal empleado público es aquel que desempeña profesionalmente funciones retribuidas al servicio de los intereses generales en:

- La Generalitat.
- Las Entidades Locales.
- Las Universidades públicas.

### **Se clasifica en:**

- **Personal funcionario de carrera.**
- **Personal funcionario interino.**
- **Personal laboral** (fijo, indefinido o temporal).
- **Personal eventual.**

### **Personal funcionario de carrera**

- **Definición:** Persona que, en virtud de un nombramiento legal, se incorpora a la administración pública mediante una relación jurídica regulada por derecho administrativo para realizar servicios profesionales retribuidos de carácter permanente.
- **Acceso:** Por procedimiento selectivo o por vía de transferencia.

### **Personal funcionario interino**

- **Definición:** Persona que, en virtud de un nombramiento legal, presta servicios en una administración pública por razones justificadas de necesidad y urgencia mediante una relación profesional de carácter temporal. Realiza funciones atribuidas al personal funcionario de carrera.
- **Supuestos de nombramiento:**

- Cobertura de plazas vacantes cuando no sea posible hacerlo con personal funcionario de carrera.
- Sustitución transitoria de titulares.
- Programas de carácter temporal, con duración no superior a 3 años, prorrogable por 1 año más.
- Exceso o acumulación de tareas, con una duración máxima de 6 meses dentro de un periodo de 12 meses.
- **Selección:**
  - Basada en los principios de igualdad, mérito, capacidad y publicidad.
  - Puede realizarse mediante bolsas u otras vías, siempre que se exija superar alguna prueba de conocimiento.
- **Cese:**
  - Finalización de la causa que dio lugar al nombramiento.
  - Provisión de la plaza por funcionario de carrera.
  - Transcurso de los plazos máximos establecidos.
  - Amortización de la plaza.
  - Incumplimiento de requisitos.
- **Régimen aplicable:**
  - General de los funcionarios de carrera.
- **Categoría de entrada:** El puesto con el menor nivel de complemento competencial.

## Personal laboral

- **Definición:** Persona que, tras superar un proceso selectivo, formaliza un contrato de trabajo por escrito con la administración pública, estableciendo una relación profesional caracterizada por ajenidad, dependencia, voluntariedad y retribución.
- **Tipos:**
  - Fijo.
  - Por tiempo indefinido.
  - Temporal.
- **Selección:**
  - Basada en los principios de igualdad, mérito, capacidad y publicidad.
  - Puede realizarse mediante bolsas u otras vías, siempre que se exija superar alguna prueba de conocimiento.
- **Puestos de trabajo:**

- Se incluyen en la oferta de empleo público o en la siguiente.
- No podrán ocupar puestos de funcionarios de carrera, salvo excepciones (Salud, Violencia de Género, sentencia judicial, entre otras).
- **Régimen aplicable:**
  - General de los funcionarios de carrera.
- **Categoría de entrada:** El puesto con el menor nivel de complemento competencial.

### Personal eventual

- **Definición:** Persona que, en virtud de nombramiento, ocupa un puesto con carácter no permanente para desempeñar funciones expresamente definidas como de confianza o asesoramiento especial.
- **Características:**
  - Nombramiento y cese libres.
  - Cese automático al cesar la autoridad que lo designó.
  - Nombramiento por:
    - Gabinetes de la Presidencia de la Generalitat, Vicepresidencia del Consell y Consellers.
    - Rector en las Universidades públicas.
    - Instituciones estatutarias o Entidades Locales, según su normativa.
  - No constituye mérito para el acceso a la función pública ni para la promoción interna.
- **Régimen aplicable:**
  - General de los funcionarios de carrera.
- **Funciones de confianza:**
  - Asesoramiento estratégico o difusión de propuestas.
  - Dedicación especial y disponibilidad horaria.

### Personal directivo público profesional

- **Definición:** Persona que desarrolla funciones directivas profesionales en la administración pública.
- **Funciones:**
  - Establecimiento y evaluación de objetivos.
  - Formulación y ejecución de programas y políticas.

- Planificación, coordinación, evaluación, innovación, entre otras.
- **Requisitos:**
  - Titulación universitaria.
  - Acreditación de experiencia y conocimientos.
- **Designación:**
  - Basada en los principios de igualdad, mérito, capacidad, transparencia e idoneidad.
  - Convocatoria pública.
  - Nombramiento realizado por la Presidencia de la Generalitat o la conselleria correspondiente.
- **Puestos reservados a funcionarios de carrera:**
  - En la Administración de la Generalitat: Subgrupo A1, nivel competencial 24 y grado de desarrollo profesional II.
  - En otras administraciones: Subgrupo A1, nivel competencial 24 y 10 años de antigüedad.
- **Régimen aplicable:**
  - Funcionarios: "Servicio activo".
  - No funcionarios: Establecido por decreto del Consell.
- **Evaluación:**
  - Periódica, basada en criterios de eficacia, eficiencia y responsabilidad en la gestión.
  - Cese sin derecho a indemnización.

## Título V: Nacimiento y extinción de la relación de servicio

### CAPÍTULO I: SELECCIÓN DE PERSONAL

#### Principios de selección

La selección del personal empleado público se regirá por los principios de:

- Igualdad, mérito y capacidad.
- Publicidad, transparencia e imparcialidad.
- Profesionalidad, independencia, confidencialidad y discrecionalidad.
- Adecuación entre el contenido de las pruebas y las funciones del puesto.
- Agilidad, eficacia y eficiencia.
- Igualdad de oportunidades y accesibilidad universal.

### **Procedimiento de selección**

El procedimiento tendrá carácter abierto y garantizará la libre concurrencia.

### **Contenido de las bases de la convocatoria**

Deberán incluir:

- Número de vacantes, requisitos de acceso y sistema selectivo.
- Composición del órgano técnico de selección.
- Características del curso selectivo, distribución por sexos, entre otros.  
Se publicarán en el **Diario Oficial de la Generalitat Valenciana (DOGV)** o equivalente.

### **Requisitos de los aspirantes**

- Nacionalidad española o de la UE, en los términos previstos.
- Haber cumplido 16 años.
- Titulación exigida para el puesto.

### **Reserva de plazas para discapacitados**

- Un mínimo del 10% de plazas (con 3% para discapacidad intelectual y 2% para enfermedad mental con grado igual o superior al 33%).

### **Sistemas selectivos**

- **Oposición:** Sistema ordinario.
- **Concurso-oposición:** Máximo 40% del valor del concurso.
- **Concurso:** Sólo en casos excepcionales.

### **Idiomas**

Las pruebas se realizarán en castellano o valenciano, salvo excepciones justificadas.

### **Duración del curso selectivo**

- Grupo A: Máximo 6 meses.
- Otros grupos: Máximo 3 meses.

### **Órganos técnicos de selección**

- Designación a propuesta de la EVAP.
- Compuestos exclusivamente por personal funcionario (o laboral, si la selección es de este tipo).
- Requisitos de los miembros: Titulación igual o superior a la del puesto, mayoría con la titulación requerida en la convocatoria.
- Incompatibilidades: No haber formado a aspirantes en los últimos 5 años.

## **CAPÍTULO II: ADQUISICIÓN Y PERDIDA DE LA CONDICIÓN DE PERSONAL EMPLEADO PÚBLICO**

### **Adquisición y pérdida de la condición de personal funcionario de carrera**

### **Adquisición de la condición de personal funcionario de carrera**

Se adquiere al:

1. Superar el proceso selectivo.
2. Ser nombrado por la administración y publicado en el DOGV (máximo 6 meses desde la resolución).
3. Realizar el juramento o promesa.
4. Tomar posesión del puesto.

### **Causas de pérdida de la condición de personal funcionario de carrera**

#### **1. Renuncia:**

- Debe presentarse por escrito y ser aceptada expresamente.
- No se admitirá si el funcionario está sujeto a expediente disciplinario o procesamiento penal.

#### **2. Pérdida de la nacionalidad:**

- Española, de la UE o de países con tratados internacionales aplicables.

#### **3. Inhabilitación:**

- **Absoluta:** Afecta a todos los empleos o cargos.
- **Especial:** Limita los empleos especificados en la sentencia.

#### **4. Jubilación:**

- **Voluntaria:** Según lo establecido en la normativa.
- **Forzosa:** Con posibilidad de prórroga hasta los 70 años.
- **Incapacidad permanente:** Reconocida oficialmente.

#### **5. Sanción firme de separación del servicio:**

- Impuesta como medida disciplinaria.

#### **6. Fallecimiento.**

### **Rehabilitación de la condición de personal funcionario**

Se podrá solicitar si desaparecen las causas que motivaron la pérdida.

### **Adquisición y pérdida de la condición de personal laboral fijo**

- **Adquisición:** Superación del proceso selectivo, formalización del contrato y juramento o promesa.
- **Pérdida:** Causas similares a las aplicables al personal funcionario, ajustadas a la normativa laboral.

## Título VI: Derechos, deberes e incompatibilidades del personal empleado público

### CAPÍTULO I: DERECHOS DEL PERSONAL EMPLEADO PÚBLICO

#### Derechos individuales

- **Inamovilidad** en la condición de personal funcionario de carrera.
- Desempeño efectivo de funciones.
- Promoción y desarrollo profesional.
- Percepción de retribuciones e indemnizaciones.
- Ser informado sobre tareas a desempeñar.
- Asistencia y defensa jurídica en procedimientos derivados de actos en el ejercicio de sus funciones.
- Formación continua y actualizada.
- Derecho a la intimidad, a la protección de datos y conciliación de la vida personal, familiar y laboral.
- Libertad de expresión.
- Vacaciones, permisos y licencias.
- Derecho a la jubilación.
- Derecho a la libre asociación.

#### Derecho al teletrabajo

- Condicionado a que el contenido competencial del puesto lo permita y no afecte las necesidades del servicio.
- **Voluntario y reversible.**
- La administración proporcionará y mantendrá los medios tecnológicos necesarios.
- Derecho garantizado a la desconexión digital.
- Regulación establecida reglamentariamente.

#### Derechos individuales ejercidos de forma colectiva

- Libertad sindical.
- Derecho a participar y negociar colectivamente.
- Derecho de huelga.
- Participación en conflictos colectivos.
- Derecho de reunión.

#### Derecho a la protección frente a represalias por denuncias

- Régimen de protección específico para quienes denuncien irregularidades.

- Prohibición de medidas desfavorables motivadas por la denuncia.
- Si se adoptan medidas desfavorables, corresponde a la administración justificar que no están vinculadas a la denuncia.
- Posibilidad de eximir de sanciones al denunciante que haya participado en los hechos, siempre que existan otras personas responsables.

## CAPÍTULO II: RÉGIMEN DE JORNADA, PERMISOS, LICENCIAS Y VACACIONES

### Jornada de trabajo

- Determinada según la normativa básica estatal.
- **Tiempo mínimo entre jornadas:** 12 horas.
- Reducción de jornada para quienes estén a menos de 5 años de la jubilación forzosa.

### Permisos

- **Asuntos particulares:** 6 días por año, incrementándose con antigüedad:
  - +2 días a partir del sexto trienio.
  - +1 día más desde el octavo trienio.
- **Permiso retribuido por embarazo:** Desde la semana 37 (o 35 en caso de embarazo múltiple).

### Licencias

- Para cursos externos o estudios.
- Participación en programas de cooperación internacional.
- Por interés particular.
- Para atender enfermedades de familiares o personas bajo guarda y custodia.

### Vacaciones

- 22 días hábiles por año trabajado (o la parte proporcional).
- **Vacaciones no disfrutadas** por incapacidad temporal podrán disfrutarse hasta 18 meses después del final del año.
- Incremento por antigüedad:
  - +1 día adicional cada 5 años (15/20/25/30 años → 23/24/25/26 días).

### Personal laboral

- Jornada, permisos, licencias y vacaciones regulados en el TREBEP.

## CAPÍTULO III: RÉGIMEN RETRIBUTIVO Y SEGURIDAD SOCIAL

### Retribuciones

- **Básicas:** Sueldo y trienios (incluyen las dos pagas extraordinarias).
- **Complementarias:**
  - Complemento de carrera administrativa (progresión profesional).
  - Complemento del puesto de trabajo:
    - **Competencial:** Dificultad técnica y complejidad.
    - **De desempeño:** Condiciones particulares, dedicación y disponibilidad.
  - Complemento de actividad profesional: Basado en interés, iniciativa, esfuerzo y rendimiento. **No será fijo ni periódico.**

### Personal funcionario en prácticas

- Percibirá las retribuciones del grupo al que aspire.
- Si ya ocupaba otro puesto, puede optar por mantener su sueldo anterior.
- Mantendrá los trienios reconocidos.

### Deducción de retribuciones

- Proporcional al tiempo no trabajado sin justificación.

### Régimen de seguridad social

- Aplicable al personal funcionario propio o de nuevo ingreso: **Régimen General de la Seguridad Social.**

## CAPÍTULO IV: DEBERES, CÓDIGO DE CONDUCTA Y RÉGIMEN DE INCOMPATIBILIDADES

### Deberes del personal empleado público

- **Cumplir con diligencia las tareas encomendadas.**
- Velar por los intereses generales.
- Respetar la Constitución, el Estatuto de Autonomía y el resto del ordenamiento jurídico.

### Código de conducta

- Principios de actuación:
  - Satisfacción de los intereses generales.
  - Lealtad, buena fe y respeto.
  - Prohibición de aceptar tratos de favor.
  - Confidencialidad.

- Uso adecuado de recursos públicos.
- Obligaciones específicas:
  - Mantener actualizada su formación.
  - Seguridad laboral y eficiencia.

#### **Incompatibilidades**

- **Prohibición de realizar actividades** que comprometan imparcialidad, menoscaben el cumplimiento de sus deberes o perjudiquen los intereses generales.

#### **Resolución de incompatibilidades**

- **Administración de la Generalitat:** Conseller en materia de función pública.
- **Universidades:** Rector.

### **CAPÍTULO V: FORMACIÓN DEL PERSONAL EMPLEADO PÚBLICO**

#### **Definición**

Formación como aprendizaje planificado para adquirir, retener y transferir conocimientos y destrezas que mejoren el servicio público.

#### **L'Escola Valenciana d'Administració Pública (EVAP)**

- Diseña, organiza, coordina y homologa acciones formativas.
- Asistencia a formaciones consideradas tiempo de trabajo.
- Formación accesible durante permisos (maternidad/paternidad) o incapacidades temporales.

#### **Obligatoriedad de la formación**

- Excepto por causas justificadas.

### **Título VII: Provisión de puestos y movilidad**

### **CAPÍTULO I: DISPOSICIONES GENERALES**

#### **Movilidad**

- **Personal funcionario de carrera:** Derecho a la movilidad voluntaria.
- **Personal laboral:** Regido por convenios colectivos y planes de igualdad.

#### **Clases de movilidad:**

- **Movilidad provisional o definitiva.**
- **De carácter voluntario o forzoso,** en función de las necesidades del servicio.

## CAPÍTULO II: MOVILIDAD VOLUNTARIA DEL PERSONAL FUNCIONARIO DE CARRERA

### Sistemas ordinarios de provisión de puestos

Permiten cubrir puestos vacantes de carácter funcional mediante:

- **1. Concurso de méritos**
  - **Tipos de concurso:**
    - **Concurso ordinario:** Valoración exclusiva de méritos, capacidades y aptitudes.
    - **Concurso específico:** Incluye evaluación de méritos y competencias, pruebas prácticas, memorias, entrevistas, etc.
  - Publicación en DOGV.
  - **Periodicidad máxima:** Cada 2 años, salvo circunstancias excepcionales.
  - Permanencia mínima en el puesto definitivo: **2 años.**
- **2. Libre designación:** Selección discrecional basada en la idoneidad del candidato respecto a los requisitos.
  - Publicación en DOGV.
  - Plazo de solicitud: **10 días.**
  - **Puestos limitados a:**
    - Subdirección general o jefatura de servicio.
    - Secretarías de altos cargos.
    - Coordinadores-asesores de subsecretarías o secretarías autonómicas.
    - Personal conductor.
  - Resuelto por el conseller de la Conselleria a la que esté adscrito

### Remoción y cese de puestos

- **Por libre designación:** Carácter discrecional.
- **Por concurso:** Por evaluación negativa, rendimiento insuficiente o incumplimiento de funciones.
- En caso de cese:
  - **El funcionario queda a disposición** del órgano superior de personal de su adscripción.
  - **Preferencia sobre nuevo ingreso** para elegir puesto.
  - Retribuciones garantizadas durante **1 mes** si el puesto es suprimido.

### Otras formas de provisión de puestos de trabajo

- **Comisión de servicios ordinaria:**

- Temporal y excepcional para casos de necesidad urgente.
- Máximo: **2 años** (6 meses si es por libre designación).
- Los puestos vacantes deben incluirse en la OPE o concursos.
- **Comisión de servicios para la puesta en marcha de proyectos y desempeño de funciones especiales no asignadas específicamente a un puesto de trabajo:**
  - Para tareas de naturaleza especial.
  - Máximo: **1 año, prorrogable otro año más.**
- **Comisión de servicios en misiones o programas de cooperación internacional:**
  - Máximo: **6 meses.**
  - **Si excede**, cambia la situación administrativa:
    - Retribución por la AAPP: **Servicio activo.**
    - Retribución externa: **Servicios especiales.**
- **Adscripción provisional:** Temporal, aplicable por cese, reingreso o rehabilitación.
- **Permuta de puestos:** Intercambio entre titulares de puestos similares.
- **Mejora de empleo provisional:** Permite ocupar temporalmente puestos de cuerpos distintos.
  - Se reserva el puesto original y se perciben retribuciones del nuevo puesto.
- **Cambio por motivos de salud, discapacidad o diversidad funcional:**
  - No implica merma retributiva.
  - Preferencia sobre interinos.
- **Traslado por violencia de género o terrorismo:**
  - Considerado forzoso y no requiere vacante.

### CAPÍTULO III: MOVILIDAD FORZOSA DEL PERSONAL FUNCIONARIO DE CARRERA

#### Comisión de servicios forzosa

- Aplicable por necesidades urgentes del servicio.
- **Orden de asignación:**
  - Misma localidad.
  - Prioridad por conciliación familiar.
  - Menor antigüedad.
  - Menor edad.
- **Máximo: 6 meses, prorrogable otros 6.**

- **Cambio de localidad:** Derecho a indemnización.

#### **Reasignación de efectivos**

- Aplicable por supresión del puesto.
- Puede requerir cursos formativos.
- Carácter definitivo.
- **Indemnización:** Por cambio de residencia.

#### **Adscripción temporal**

- Por acumulación de tareas, programas concretos o necesidades temporales.
- Duración máxima: **1 año, prorrogable otro.**
- No implica cambio de localidad.

### **CAPÍTULO IV: MOVILIDAD INTERADMINISTRATIVA E INTERSECTORIAL**

#### **Movilidad interadministrativa**

- Acceso a puestos en otras administraciones bajo el principio de reciprocidad.
- Situación administrativa: **Servicio en otras AAPP.**

#### **Movilidad intersectorial**

- Regida por la "Comissió Intersectorial de l'Ocupació Pública de la Generalitat".

### **Título VIII: Promoción profesional**

#### **Derecho a la promoción profesional del personal funcionario de carrera**

El personal funcionario de carrera tiene derecho a un conjunto ordenado de oportunidades de ascenso y expectativas de progreso profesional.

#### **Modalidades de promoción profesional del personal funcionario de carrera**

- **Carrera horizontal:**
  - Progresión a través de un sistema de grados, sin necesidad de cambiar de puesto de trabajo.
  - Reconoce individualmente el desarrollo profesional alcanzado.
- **Carrera vertical:**
  - Adquisición de un mayor nivel competencial al obtener puestos con destino definitivo.
  - **Requisito:** Ejercer un puesto con el mismo nivel competencial durante **2 años continuados o 3 años con interrupciones.**

- **Promoción interna vertical:**

- Acceso de un grupo o subgrupo a otro superior (según lo dispuesto en el TREBEP).
- Ejemplo: Pasar de A2 a A1.
- **Requisito:** Haber prestado **2 años de servicios** en el cuerpo o escala de origen.

- **Promoción interna horizontal:**

- Acceso a una plaza de igual clasificación profesional en otra área o sector.
- Ejemplo: Pasar de la Administración General a la Administración Especial.

### **Promoción profesional del personal laboral**

El personal laboral tiene derecho a la promoción profesional conforme a los convenios colectivos aplicables.

### **Evaluación del desempeño**

- Mide y valora la conducta profesional y el rendimiento con el objetivo de individualizar y diferenciar la contribución del personal empleado público.
- La **continuidad en los puestos obtenidos por concurso** dependerá de los resultados de esta evaluación.

## **Título IX: Situaciones administrativas del personal funcionario de carrera (FC)**

### **Servicio activo**

- El personal funcionario de carrera se encuentra en esta situación cuando ocupa un puesto mediante cualquiera de los procedimientos de provisión previstos en la ley.
- **Circunstancias que no alteran esta situación:**
  - Licencias, permisos, incapacidades temporales y vacaciones.
- El personal cesado en su puesto permanece en servicio activo hasta que se le asigne otro.

### **Servicios especiales**

- Aplica cuando el funcionario es nombrado para:
  - Organismos internacionales, Ministro/Conseller, alto cargo, miembro del Tribunal Constitucional, Defensor del Pueblo, diputado, personal eventual, entre otros.
- **Plazo para solicitar el reingreso al servicio activo:** 1 mes.
  - De no hacerlo, será declarado en excedencia voluntaria por interés particular.
- **Derechos:**
  - Retribuciones del puesto que desempeñen (más trienios).

- Se computa el tiempo de permanencia como servicio activo.
- Reserva del puesto si se obtuvo por concurso.

#### Servicio en otras administraciones públicas

- Cuando el personal funcionario de carrera obtiene destino en otra administración por concurso o libre designación.
- Legislación aplicable: La de la administración en la que presta servicios.
- El tiempo computará como **servicio activo**.

#### Excedencia voluntaria

- **Por interés particular:**
  - **Requisitos:** 3 años de servicios efectivos en cualquier administración.
  - No aplica durante expedientes disciplinarios o sanciones.
  - **Retribuciones:** Ninguna.
  - **Cómputo de tiempo:** No.
  - **Reingreso:** Requiere al menos 2 años en excedencia.
- **Por agrupación familiar:**
  - Aplica si el cónyuge reside en otra localidad desempeñando un puesto definitivo.
  - No hay requisito de servicios previos.
  - **Retribuciones:** Ninguna.
  - **Cómputo de tiempo:** No.
- **Automática por prestar servicios en el sector público:**
  - Aplica al acceder a otro puesto en el sector público.
  - **Retribuciones:** Ninguna.
  - **Cómputo de tiempo:** Reconocido posteriormente.
- **Por cuidado de familiares:**
  - **Duración:** Máximo de 3 años.
  - **Supuestos:** Hijo, cónyuge, familiar hasta 2.º grado o persona bajo guarda y custodia.
  - **Restricción:** Puede limitarse a dos funcionarios si es por la misma persona.
  - **Cómputo de tiempo:** Sí, con excepciones.
  - **Reserva del puesto:** Hasta 3 años.
- **Por razón de violencia de género o terrorismo:**

- Sin tiempo mínimo previo ni plazo de permanencia.
- **Reserva del puesto:** Hasta **6 meses** (prorrogable hasta 18 meses en períodos de 3 meses).
- **Retribuciones:** Íntegras durante los 3 primeros meses.
- **Incentivada:**
  - Aplica a quienes están en "expectativa de destino" o "excedencia forzosa".
  - Duración máxima: **5 años**.
  - Retribuciones: Una mensualidad por año, hasta un máximo de **12**.
  - Reingreso: Posible tras **2 años** si ambas partes acuerdan.

### **Excedencia forzosa**

- **Causas:**
  - Suspensión firme del puesto por sanción sin vacantes disponibles al reingresar.
  - Finalización de excedencia voluntaria sin vacantes disponibles.
  - Expectativa de destino agotada sin causas imputables al funcionario.
- **Derechos:**
  - Retribuciones básicas.
  - Cómputo del tiempo como servicio activo.
  - Participación obligatoria en concursos convocados (de no hacerlo, pasa a excedencia voluntaria).

### **Expectativa de destino**

- Aplica cuando el puesto de trabajo es suprimido o no hay dotación presupuestaria.
- **Derechos:**
  - **Retribuciones básicas más el 50%** del complemento del puesto.
- **Obligaciones:**
  - Aceptar destinos, participar en concursos y cursos de formación.
- Duración máxima: **1 año**.
  - Superado este plazo, pasa a excedencia forzosa salvo causas no imputables al interesado.

### **Suspensión de funciones**

- **Suspensión provisional:**
  - Medida cautelar durante un procedimiento judicial o disciplinario.
  - Duración: **Máx. 6 meses** (salvo paralización del proceso judicial).

- Retribuciones básicas percibidas, salvo que la sentencia sea firme, debiendo devolverlas.
- **Suspensión firme:**
  - Excede los **6 meses** y conlleva la pérdida del puesto de trabajo.
  - Privación del ejercicio de funciones y derechos inherentes.

### **Reingreso al servicio activo**

- Mediante convocatoria de concurso o libre designación.
- También puede ser por adscripción provisional, de forma motivada.

### **Situaciones administrativas del personal laboral**

- Se aplican según normativa específica o convenios colectivos, pudiendo adoptar situaciones similares a las del personal funcionario de carrera.

## **Título X: Régimen disciplinario**

### **Responsabilidad disciplinaria**

El personal empleado público es responsable disciplinariamente cuando:

- Realiza actos o conductas tipificadas como falta.
- Induce a otro a realizar faltas.
- Encubre faltas consumadas muy graves o graves que causen daño grave a la administración o la ciudadanía.

Cuando el cumplimiento de la sanción no sea posible debido a una situación que lo impida, se hará efectiva cuando la situación cambie, salvo que haya prescrito.

### **Principios de la potestad disciplinaria**

- **Legalidad y tipicidad:** Solo serán sancionables actos tipificados en la normativa aplicable.
- **Irretroactividad:** No se aplicará una sanción retroactivamente salvo que sea favorable al interesado.
- **Proporcionalidad:** Adecuación entre la infracción cometida y la sanción impuesta.
- **Culpabilidad:** Solo se sancionan actos dolosos o culposos.
- **Presunción de inocencia:** Nadie será sancionado sin pruebas suficientes.
- **Contradicción y audiencia:** Derecho del interesado a ser escuchado y defenderse.

Cuando existan indicios fundados de criminalidad, se suspenderá el procedimiento disciplinario y se remitirá al Ministerio Fiscal.

## Clasificación de las faltas

### 1. Muy graves:

- Las Tipificadas en el TREBEP.
- Perjuicio grave a la administración o ciudadanía.
- Daños graves intencionados al patrimonio.
- Realización reiterada de actividades profesionales incompatibles.
- Agresión grave.
- **Sanciones correspondientes:**

- Separación del servicio.
- Suspensión de funciones (3 a 6 años).
- Traslado forzoso con cambio de localidad (1 a 3 años).
- Demérito (pérdida de dos grados, exclusión de procedimientos 2-4 años, prohibición de ocupar puestos de jefatura durante 2-4 años).

### 2. Graves:

- Falta de obediencia debida.
- Abuso de autoridad.
- Grave desconsideración con empleados públicos o ciudadanía.
- Daños al patrimonio de menor entidad.
- Rendimiento insuficiente sin justificación.
- Incumplimiento de deberes de confidencialidad.
- Incumplimiento de jornada superior a 10 horas al mes.
- Evasión del control horario.
- Simulación de enfermedad para obtener permisos.
- **Sanciones correspondientes:**

- Suspensión de funciones (15 días a 3 años).
- Traslado forzoso (con o sin cambio de localidad).
- Demérito (pérdida de un grado, exclusión de procedimientos 2 años, prohibición de ocupar puestos de jefatura 2 años).

### 3. Leves:

- Incumplimiento ocasional de la jornada laboral.
- Falta injustificada de un día.
- Incorrección o descuido en el cumplimiento de las tareas.

- Negligencia leve.
- **Sanciones correspondientes:**
  - Suspensión de funciones hasta **15 días**.
  - Apercibimiento.

### Prescripción de infracciones y sanciones

- **Infracciones:**\*
  - **Muy graves:** 3 años.
  - **Graves:** 2 años.
  - **Leves:** 6 meses.

\*El plazo comienza desde la comisión del acto o su cese si es continuado.

- **Sanciones:**\*
  - **Muy graves:** 3 años.
  - **Graves:** 2 años.
  - **Leves:** 1 año.

\*El plazo comienza desde la firmeza de la sanción.

### Extinción de la responsabilidad disciplinaria

- Cumplimiento de la sanción.
- Fallecimiento del responsable.
- Prescripción de la falta o sanción.

### Procedimiento disciplinario

- **Duración máxima:** 1 año para resolver y notificar.
- **Fase de información previa:** Duración máxima de 1 mes para determinar si procede la incoación.
- **Separación entre fase instructora y sancionadora.**
- **Sanciones leves:** Procedimiento sumario y simplificado, duración máxima de 1 mes.

### Órganos competentes

- **Iniciación del procedimiento:**
  - La jefatura superior de personal de la Generalitat, conselleria, organismo público o consorcio correspondiente.
- **Resolución:**
  - **Separación del servicio:** Consell.

- **Demérito:** Dirección General de Función Pública.
- **Sanciones graves y muy graves:** President de la Generalitat o conseller.
- **Sanciones leves:** Jefatura superior de personal correspondiente.

# Decreto 42/2019 - Condiciones de trabajo del personal funcionario de la Administración de la Generalitat

## Jornada de trabajo

- **Duración:** Depende del **complemento de desempeño**:
  - **Inferior a E038:** 35 horas semanales.
  - **Igual o superior a E038:** 37 horas y 30 minutos semanales (**Especial dedicación**), sujeto a **incompatibilidades**.
- **Compensación por exceso de horario (urgencias):**
  - Horas trabajadas en **días hábiles**: Se compensan a razón de **2 horas por cada hora trabajada**.
  - Horas trabajadas en **días inhábiles**: Se compensan a razón de **2 horas y 30 minutos por cada hora trabajada**.
  - **Plazo para disfrutar la compensación:** Dentro de los **3 meses siguientes**.

## Horario laboral

- **Descanso mínimo entre jornadas:** **12 horas**.
- **Distribución del horario:**
  - **Parte fija:** De 9:00 a 14:00 (de lunes a viernes).
  - **Parte variable:** El resto del tiempo, distribuido entre:
    - **Mañanas:** De 7:30 a 9:00.
    - **Tardes:** De 14:00 a 19:00 (hasta las 16:00 los viernes).
- **Compensación horaria:** Dentro del mes natural o, como máximo, en los **dos meses siguientes**.
- **Descanso semanal:**
  - Preferentemente **48 horas continuadas**.
  - Si no es posible: mínimo de **36 horas continuadas**.

## Pausa diaria

- Duración: **30 minutos, computable como tiempo de trabajo efectivo**.
- **Horario para el personal burocrático:** Entre las **10:00 y las 12:00**.

## Justificación de ausencias

- **Sin parte médico:** Notificación dentro de la **primera hora** al personal responsable.
- **Con parte médico:** Presentación en un plazo máximo de **3 días desde su expedición**.
- **Ausencias prolongadas o reiteradas:** Podrá exigirse parte médico aunque no excedan de **2 o 3 días**.

## Permisos

- **Generalidades:**
  - No requieren autorización, excepto los permisos por asuntos propios, que **sí necesitan autorización expresa.**
  - **Denegación de permisos:** Deberá estar **motivada.**
- **Permisos específicos:**
  - **Matrimonio:** **15 días.**
  - **Conciliación de la vida personal, familiar y laboral:** **Tiempo indispensable.**
  - **Fallecimiento, accidente o enfermedad grave:**
    - **Familiar de primer grado:**
      - **Misma localidad:** **3 días.**
      - **Distinta localidad:** **5 días.**
    - **Familiar de segundo grado:**
      - **Misma localidad:** **2 días.**
      - **Distinta localidad:** **4 días.**
  - **Exámenes finales o pruebas definitivas de aptitud:** **Día del examen.**
  - **Traslado de domicilio habitual:**
    - **Misma localidad:** **1 día.**
    - **Distinta localidad:** **2 días.**
  - **Por deber inexcusable:** **Tiempo indispensable.**
  - **Asuntos propios:** **6 días al año**, disfrutables hasta el **15 de febrero del año siguiente.**
    - **Personal interino:** **1 día por cada 2 meses trabajados.**
  - **Días compensatorios:**
    - **24 y 31 de diciembre** si coinciden con festivo, sábado o día no laborable.
    - **2 días adicionales** por festividad autonómica.

## Licencias

- **Generalidades:** Requieren **autorización expresa.** Las denegaciones deben estar **motivadas.**
- **Licencias retribuidas:**
  - **Cursos externos:** Hasta **40 horas al año.**

- **Estudios relacionados:** Hasta **12 meses**.
- **Programas de cooperación internacional:** Hasta **6 meses**.
- **Licencias no retribuidas** (periodos continuados e ininterrumpidos):
  - **Por interés particular:** Hasta **6 meses cada 3 años**.
  - **Por enfermedad de familiares o guarda y custodia:** Hasta **1 año**.
  - **Por perfeccionamiento profesional:** Hasta **3 meses cada año**.

## Vacaciones

- **Duración:**
  - **22 días hábiles al año.**
  - **Días adicionales por antigüedad:**
    - **15, 20, 25 y 30 años de servicio → 1 día adicional por cada tramo,** hasta un máximo de **25 días**.
- **Disfrute:**
  - **Plazo general:** Durante el **año natural** y hasta el **31 de enero del año siguiente**.
  - **Condiciones:**
    - La mitad de los días debe disfrutarse entre **junio y septiembre**, en periodos mínimos de **7 días**.
    - Derecho **no condicionado al servicio**.
    - Interrupción en caso de **hospitalización no voluntaria**.
    - **No se sustituyen** por compensaciones económicas.
  - **Solicitud de preferencia:** Antes del **1 de mayo**.
- **Preferencias para disfrutar las vacaciones:**
  - **Personas con hijos menores de 14 años.**
  - **Personas con mayores de 65 años a su cargo.**

# **Decreto 49/2021 - Regulación del teletrabajo como modalidad de prestación de servicios del personal empleado público de la Administración de la Generalitat**

## **Puestos de trabajo susceptibles de ser desempeñados mediante teletrabajo**

Son aquellos puestos que **puedan ser ejercidos de forma autónoma y a distancia**, siempre que se consideren las características específicas del puesto y los medios requeridos para su desarrollo. Algunos ejemplos destacados incluyen:

- **Estudio y análisis de proyectos**
- **Elaboración de informes y asesoramiento técnico**
- **Redacción, corrección y tratamiento de documentos**
- **Gestión de sistemas de información y comunicaciones**
- **Análisis, diseño y programación de sistemas de información y comunicaciones**
- **Traducción**
- **Tramitación de expedientes** mediante aplicaciones informáticas, ofimáticas o redes corporativas

## **Requisitos para acceder al teletrabajo**

Para optar al teletrabajo, el empleado público deberá cumplir los siguientes requisitos:

- Estar en situación de **servicio activo**
- Haber desempeñado el puesto de trabajo durante un **mínimo de 3 meses**
- Que el puesto de trabajo sea de **tipología aceptada** como susceptible de teletrabajo
- Que el lugar donde se realice el teletrabajo cumpla con la **normativa establecida** en materia de seguridad, salud y ergonomía

## **Duración máxima del teletrabajo**

El teletrabajo se autoriza por una duración máxima de **1 año**, aunque podrá ser prorrogado por **periodos sucesivos de igual duración** previa evaluación de su desempeño.

## **Jornada y organización del teletrabajo**

- El teletrabajo estará limitado a un máximo de **3 días a la semana**, siendo el resto de los días de carácter **presencial**.

- Durante los días de teletrabajo, se establecen **periodos mínimos de interconexión** para garantizar el control y seguimiento de la actividad laboral.

### **Medios tecnológicos para el teletrabajo**

La Administración de la Generalitat será responsable de proporcionar y mantener los **medios tecnológicos necesarios** para que el personal empleado público pueda desarrollar su actividad de manera eficiente y segura.

### **Formación obligatoria**

Es imprescindible que el personal que desee acceder al teletrabajo realice un **curso de formación específico**, diseñado para garantizar el conocimiento adecuado de las herramientas y protocolos asociados a esta modalidad de prestación de servicios.

### **Comisión de Control y Seguimiento del Teletrabajo de la Administración de la Generalitat**

Se crea esta comisión como órgano encargado de la **supervisión, seguimiento y evaluación** del teletrabajo. Este organismo velará por el cumplimiento de los objetivos y la correcta implementación de la modalidad de teletrabajo en los distintos servicios.

### **Inspección General de Servicios**

Este organismo será el encargado de **evaluar la repercusión** que tiene el teletrabajo en la prestación de los servicios públicos, asegurando que la calidad y eficiencia no se vean afectadas por esta modalidad.

## Hacienda Pública

# Ley 1/2015 - de Hacienda Pública, del Sector Público Instrumental y de Subvenciones

### Objeto de la Ley

- Regular el **régimen económico-financiero** del sector público de la Generalitat.
- Se centra en aspectos como **hacienda pública, presupuesto, contabilidad, tesorería, endeudamiento y control financiero**.
- Proporciona el **régimen jurídico básico** del sector público instrumental de la Generalitat.
- Define el **régimen jurídico de las subvenciones** otorgadas por la Generalitat.

### Ámbito de Aplicación

- **Sector público de la Generalitat**, que incluye:
  - **Administración de la Generalitat**.
  - **Sector público instrumental**, compuesto por organismos públicos, sociedades mercantiles, fundaciones y consorcios adscritos.
  - **Instituciones de la Generalitat**.

### Estructura del Sector Público de la Generalitat

- **Sector público administrativo:**
  - Incluye la **Administración de la Generalitat**, organismos autónomos, instituciones de la Generalitat, consorcios y entidades de derecho público orientadas al beneficio público.
  - Presupuestos de carácter **limitativo y vinculante**.
- **Sector público empresarial y fundacional:**
  - Compuesto por entidades públicas empresariales, sociedades mercantiles, fundaciones y otras entidades de derecho público diferentes al sector administrativo.
  - Presupuestos de carácter **estimativo y no vinculante**.

### Presupuestos de la Generalitat

- **Definición:** Expresión cifrada, conjunta y sistemática de los derechos y obligaciones a liquidar durante el ejercicio.

- **Componentes:**
  - Presupuestos de los sujetos del sector público administrativo.
  - Presupuestos de explotación y capital del sector empresarial y fundacional.
  - Presupuestos de fondos sin personalidad jurídica financiados mayoritariamente por la Generalitat.
- **Características:**
  - Presupuesto único y anual, aprobado por **Les Corts**.
  - Elaborado por la **Conselleria de Hacienda**.
- **Clasificaciones de los estados de gastos:** Orgánica, por programas, económica y territorial.
- **Clasificaciones de los estados de ingresos:** Orgánica y económica.

### Sector Público Instrumental

- **Organismos públicos:**
  - Con personalidad jurídica pública, patrimonio y tesorería propios.
  - Se crean por ley de **Les Corts**.
  - Clasificación:
    - **Organismos autónomos:** Regidos por el derecho administrativo.
    - **Entidades de derecho público:** Regidas por el derecho privado, aunque pueden ejercer potestades administrativas.
- **Sociedades mercantiles de la Generalitat:**
  - Sociedades bajo control de la Generalitat.
- **Fundaciones del sector público:**
  - Con personalidad jurídica de naturaleza privada.
  - No ejercen potestades administrativas.
  - Regidas principalmente por el derecho privado y legislación específica.
- **Consorcios de la Generalitat:**
  - Adscritos a la Generalitat según normativa básica estatal.

### Subvenciones

- **Definición:** Ayudas otorgadas por la Generalitat a terceros con objetivos específicos.
- **Procedimientos de concesión:**

- **Concurrencia competitiva:** Modelo general basado en criterios objetivos y comparación de solicitudes.
- **Concesión directa:** Excepcional, limitada a casos específicos justificados por ley.



# BLOQUE ESPECÍFICO (Informática)

## Sociedad Digital

# Tecnología y desarrollo en la Sociedad Digital

**Sociedad Digital:** Busca integrar las tecnologías en todos los ámbitos de la sociedad para generar desarrollo y bienestar. En la Comunitat Valenciana, el **Plan COM DIGITAL 2025** lidera esta transformación, con objetivos agrupados en **seis ejes estratégicos**:

- **1, 2:** Incrementar la conectividad en todo el territorio.
- **3:** Transformar digitalmente la economía, el territorio y el tejido productivo.
- **4:** Fomentar una transformación disruptiva mediante la innovación tecnológica.
- **5, 6:** Digitalizar tanto la ciudadanía como la administración pública.

El plan también contempla iniciativas como el **Observatorio de la IA**, encargado de monitorear avances tecnológicos.

## Brecha Digital

Representa la desigualdad en el acceso, uso o impacto de las tecnologías de la información y comunicación (**TIC**). Este fenómeno afecta principalmente a personas o colectivos excluidos por factores **geográficos, económicos o de capacitación tecnológica**, perpetuando desigualdades sociales.

### Elementos clave:

- **Acceso:** Garantizar infraestructura TIC disponible para todos.
- **Adquisición de competencias:** Capacitación para usar las TIC de manera eficaz.
- **Buen uso:** Evitar malentendidos o abusos de las tecnologías.

**Variables principales:** Procedencia, nivel formativo, edad, género, situación económica y contexto.

La **Consellería de Innovación, Universidades, Ciencia y Sociedad Digital** trabaja en estas áreas mediante:

- Análisis continuo a través del **Observatorio de la Brecha Digital**.
- Capacitación con el marco europeo **DIGICOMP**, enfocado en:
  - Información y alfabetización de datos
  - Comunicación y colaboración
  - Creación de contenido digital
  - Seguridad

- Resolución de problemas

### Índices de economía y sociedad digital (DESI)

El **Índice de Economía y Sociedad Digital (DESI)** mide el progreso en la competitividad digital de los países de la UE. Se estructura en varios bloques:

- Conectividad
- Competencias digitales
- Uso de internet por la ciudadanía
- Integración tecnológica en empresas
- Servicios públicos digitales

### Recomendaciones del DESI 2020:

- Ampliar la cobertura de redes de muy alta capacidad.
- Asignar espectro para servicios 5G.
- Mejorar las competencias digitales de los ciudadanos.
- Continuar digitalizando las empresas y el sector público.

### La Década Digital de Europa: metas digitales para 2030

Europa plantea una **visión sostenible y centrada en el ser humano**, estableciendo objetivos claros a través de la “**Brújula Digital**”:

- **Capacidades:** Lograr que al menos el **80% de la población tenga capacidades digitales básicas** y formar **20 millones de especialistas TIC**.
- **Infraestructuras:**
  - Conectividad gigabit para todos y **5G universal**.
  - Duplicar la cuota de producción global de semiconductores.
  - Crear **10,000 nodos de proximidad climáticamente neutros**.
  - Desarrollar el primer ordenador con aceleración cuántica.
- **Empresas digitales:**
  - El **75% de las empresas usarán nube, IA y macrodatos**.
  - Duplicar los unicornios y fomentar la digitalización de las pymes.
- **Servicios públicos digitales:**
  - Digitalización completa de servicios clave.
  - Acceso universal a historiales médicos electrónicos.

- Identidad digital utilizada por el **80% de los ciudadanos**.

### Ciudadanía Digital: derechos y principios

La **Declaración de derechos y principios digitales** pone a las personas en el centro de la transformación digital. Incluye:

- Prioridad a las personas
- Libertad de elección
- Seguridad y protección
- Solidaridad e inclusión
- Participación
- Sostenibilidad

### Propone derechos como:

1. Poner a las personas en el centro del cambio digital.
2. Promover la solidaridad e inclusión.
3. Garantizar la libertad de elección en línea.
4. Fomentar la participación en el espacio digital.
5. Incrementar la seguridad y el empoderamiento.
6. Apostar por la sostenibilidad digital.

### Itinerario hacia la Década Digital

El **Itinerario hacia la Década Digital** establece un marco para monitorizar avances y promover proyectos multinacionales en áreas como **blockchain, 5G, computación de alto rendimiento, hubs de innovación**, y más. Esto fomenta la cooperación internacional y alinea los esfuerzos con los estándares de la UE.

## Agenda Digital

# Agenda Digital de la Comunitat Valenciana (ADCV)

La Agenda Digital de la Comunitat Valenciana (ADCV) es una estrategia promovida por el Consell de la Generalitat Valenciana, orientada a fomentar una sociedad digital avanzada, con una administración ágil, eficiente e innovadora. Su propósito es utilizar el potencial transformador de las tecnologías de la información y la comunicación (TIC) para contribuir a un modelo económico sostenible, basado en la innovación y el conocimiento, así como a un modelo social inclusivo que se apoya en una ciudadanía activa y capacitada.

### Objeto de la Agenda Digital

La ADCV tiene como objetivo fundamental catalizar un cambio estructural hacia un modelo económico y social más sostenible. Esta transformación se estructura en tres pilares:

- La **innovación y el conocimiento** como base del modelo productivo.
- La **ciudadanía participativa y capacitada** como núcleo de la sociedad digital.
- Una **administración pública eficiente y ágil** que lidere la innovación tecnológica.

### Estructura de la ADCV

La Agenda se articula en **17 líneas estratégicas y 73 actuaciones**, distribuidas en torno a tres ejes principales: **Ciudadanía, Economía y Administración Pública**. Cada eje responde a metas específicas que buscan integrar plenamente a la Comunitat Valenciana en la era digital.

### Ejes estratégicos de la ADCV

#### 1. Ciudadanía Digital:

- Este eje busca fomentar una ciudadanía tecnológicamente avanzada, capaz de utilizar las TIC para mejorar su calidad de vida y participar activamente en una sociedad digital inclusiva.
- **Objetivo:** Promover la plena integración de los ciudadanos en la sociedad digital, facilitando el acceso a tecnologías avanzadas y mejorando su capacitación tecnológica.
- **Líneas de actuación:**

- TIC para la Salud, Educación y Justicia
- Gobierno abierto, transparencia y acceso a la información pública
- Ciudades inteligentes
- Seguridad y confianza en la red
- Inclusión digital

## 2. Administración Digital:

- El propósito de este eje es avanzar hacia una administración pública digitalizada, que no solo incremente su eficiencia y eficacia, sino que también dinamice la innovación tecnológica en la gestión pública.
- **Objetivo:** Completar el proceso de digitalización mediante la implantación de la tramitación electrónica en todos los procedimientos administrativos, eliminando así el papel y optimizando los recursos TIC.
- **Líneas de actuación:**
  - Servicios públicos digitales
  - Administración sin papel
  - Cooperación interadministrativa e interoperabilidad
  - Gestión racional de los recursos TIC
  - Impulso a la innovación tecnológica en la gestión pública

## 3. Economía Digital:

- Este eje se centra en potenciar una economía impulsada por la tecnología, orientada a la competitividad y al empleo de calidad.
- **Objetivo:** Fomentar la innovación tecnológica en las empresas y su especialización en mercados concretos para aumentar su productividad y sostenibilidad.
- **Líneas de actuación:**
  - TIC para la competitividad
  - Impulso y especialización del Hipersetor TIC
  - TIC para el empleo
  - Sistema valenciano de I+D+i en TIC
  - Despliegue de redes y servicios de banda ancha

### Objetivos Generales de la ADCV

La ADCV expresa el compromiso de la Generalitat Valenciana con los principios de la estrategia Europa 2020 y la Agenda Digital para España, enmarcando su acción en una planificación regional. Este plan, impulsado en base a prioridades comunitarias, tiene como objetivo general fomentar el uso de las TIC en beneficio del desarrollo social y económico de la región.

## Gestión de los servicios TIC

### Guías ITIL

**Definición:** La Biblioteca de Infraestructura de Tecnologías de la Información (ITIL, por sus siglas en inglés) es un conjunto de prácticas que recoge las mejores prácticas en la gestión de servicios, desarrolladas a lo largo de los años mediante la observación de organizaciones diversas.

**Objetivo:** La meta principal de ITIL es alinear el negocio con las tecnologías de la información (TI) mediante una gestión basada en procesos, aportando valor tanto a clientes externos como internos.

1. **Alineación de los servicios con el negocio:** Busca asegurar que los servicios TI apoyen directamente los objetivos empresariales.
2. **Mejora continua:** La revisión y optimización constante de procesos para asegurar eficacia, eficiencia y calidad en los servicios TI.
3. **Reducción de costes:** Minimizar gastos en la entrega de servicios, mejorando la rentabilidad y la sostenibilidad de las TI en la organización.

### Principios de ITIL

- **Alineación negocio-TI:** Proporciona una estructura de procesos adaptable a toda la organización y sus tecnologías.
- **Servicios basados en procesos:** Asegura que los servicios TI se desarrollos con calidad, utilizando buenas prácticas y gestionando adecuadamente los recursos humanos.
- **Dimensiones de la gestión de servicios (4 P's):**
  - **Personas:** También denominado “Organización y Personas”.
  - **Procesos:** Incluye la estructura de “Procesos y Flujos de Valor”.
  - **Productos:** Enfocado en “Información y Tecnología”.
  - **Partners:** Se refiere a “Socios y Proveedores”.

### Características de ITIL

- **Evolución cultural:** Facilita el paso de una cultura puramente tecnológica a una cultura orientada al servicio y enfocada en los objetivos empresariales.
- **Certificación de personas:** ITIL permite la certificación de profesionales, garantizando un conocimiento estandarizado.
- **Carácter prescriptivo:** Proporciona directrices claras sobre “cómo” llevar a cabo la gestión de servicios TI.

- **Valor para el negocio:** La búsqueda del valor en cada servicio es un principio fundamental.
- **Procedimientos detallados:** ITIL ofrece una descripción detallada de procedimientos independientes del proveedor, que sirven como guía integral para toda la infraestructura, el desarrollo y las operaciones de TI.
- **División en procesos y fases:** Se organiza en diez procesos, cinco operativos (Libro Azul) y cinco tácticos (Libro Rojo).

## Ciclo de Vida del Servicio

ITIL estructura la gestión del servicio en cinco fases principales, con sus respectivos procesos:

1. **Fase de Estrategia:** Define cómo generar valor para el cliente y alinea los objetivos de TI con los del negocio.
  - **Procesos:** Generación de estrategia, gestión financiera, gestión de la demanda, gestión de la relación comercial y gestión del portafolio de servicios.
2. **Fase de Diseño:** Crea y modifica los servicios, garantizando un equilibrio entre las 4 P's.
  - **Procesos:** Gestión del diseño, catálogo de servicios, niveles de servicio, capacidad, disponibilidad, continuidad, seguridad de la información y gestión de suministradores.
3. **Fase de Transición:** Asegura que cualquier cambio en el servicio, nuevo o modificado, se implemente correctamente.
  - **Procesos:** Gestión de la transición, planificación y soporte, configuración y activos, cambios, versiones, validación y pruebas, evaluación del servicio y gestión del conocimiento.
4. **Fase de Operación:** Coordina y ejecuta las actividades necesarias para gestionar y entregar los servicios.
  - **Procesos:** Gestión de eventos, incidencias, peticiones, problemas y accesos.
  - **Funciones:** Incluye el Centro de Atención al Usuario, gestión técnica, gestión de operaciones y gestión de aplicaciones.
5. **Fase de Mejora Continua:** Apoya a todas las fases para asegurar un desarrollo y optimización constantes de los servicios.

## Procesos clave

1. **Gestión de Cambios:** Controla la implementación de cambios, maximizando su valor y minimizando incidentes.
  - **Aspectos a considerar:** Riesgos, impacto en los servicios, requisitos, beneficios empresariales, viabilidad técnica y financiera.

- **Ciclo de vida del cambio:** Registro, evaluación, autorización, priorización, planificación, prueba, implementación, documentación y revisión.
  - **Tipos de solicitudes:**
    - **Estándares:** Cambios preautorizados de bajo riesgo.
    - **Normales:** Requieren seguir el ciclo completo y autorización por el gestor de cambio.
    - **Urgentes:** Circunstancias extremas; implementación rápida sin olvidar controles básicos.
2. **Gestión de Incidencias:** Interrupciones no planificadas en el servicio que impactan en las operaciones.
- **Objetivo:** Minimizar el impacto, restableciendo rápidamente el servicio.
  - **Proceso:** Identificación, registro, categorización, priorización y gestión de la incidencia.
  - **Prioridad:** Se basa en impacto y urgencia, definiendo tiempos de resolución.
3. **Gestión de Problemas:** Identifica y soluciona las causas desconocidas de incidentes, a través de una gestión proactiva y preventiva.
- **Resultados:** Documentación de errores conocidos o creación de solicitudes de cambio.
  - **Gestión proactiva vs. preventiva:** La primera responde a problemas actuales, mientras la segunda intenta prevenir futuros.

### Introducción a la Gestión de Proyectos

Un proyecto es una estructura organizacional temporal creada para desarrollar un producto o servicio único (entregable) dentro de limitaciones como tiempo, coste y calidad. La gestión de proyectos consiste en planificar, organizar, obtener, supervisar y gestionar los recursos y actividades necesarias para cumplir eficaz y eficientemente con los objetivos específicos de cada proyecto. Es fundamental adaptar el enfoque de gestión a las características de cada proyecto.

## Gestión y Dirección de Proyectos

### Metodología PM2

PM2 es una metodología de gestión de proyectos desarrollada por la Comisión Europea. Su objetivo es facilitar a los Directores de Proyecto (DP) la entrega de soluciones y beneficios a sus organizaciones mediante una gestión eficaz durante el ciclo de vida del proyecto. PM2 proporciona:

- Una estructura de gobernanza del proyecto.
- Directrices de procesos y plantillas de artefactos.
- Pautas para el uso de estos artefactos.
- Un enfoque orientado a los resultados.

#### Pilares de PM2

La metodología se estructura en torno a los siguientes elementos:

- **Modelo de gobernanza del proyecto:** Define los roles y responsabilidades.
- **Ciclo de vida del proyecto:** Organiza las fases del proyecto.
- **Conjunto de procesos:** Describe las actividades de gestión del proyecto.
- **Conjunto de artefactos del proyecto:** Proporciona plantillas y guías para la documentación.

#### Ciclo de Vida del Proyecto

El ciclo de vida del proyecto en PM2 se divide en cuatro fases principales, cada una con actividades y objetivos específicos:

- **Fase de Inicio:** Define los resultados deseados, elabora un Caso de Negocio y establece el alcance del proyecto. Las actividades incluyen:
  - Reunión de inicio.
  - Solicitud de Inicio del Proyecto.
  - Creación del Caso de Negocio.
  - Acta de constitución del proyecto.
- **Fase de Planificación:** Asigna el Equipo Central del Proyecto (ECP), desarrolla el alcance y planifica el trabajo. Las actividades principales son:
  - Reunión de inicio de planificación.
  - Creación del Manual del proyecto.
  - Definición de la Matriz de partes interesadas.

- Elaboración de planes específicos (de trabajo del proyecto, de aceptación de entregables, de implementación en el negocio, etc.).
- **Fase de Ejecución:** Coordina la ejecución de los planes y produce los entregables. Es la etapa que requiere mayor cantidad de recursos y supervisión. Las actividades son:
  - Reunión de inicio de ejecución.
  - Coordinación del proyecto.
  - Aseguramiento de la calidad.
  - Elaboración de informes y distribución de la información.
- **Fase de Cierre:** Implica la aceptación formal del proyecto, la elaboración de un Informe final y el cierre administrativo. Se capturan las lecciones aprendidas y recomendaciones para futuros proyectos. Las actividades incluyen:
  - Reunión de revisión de fin de proyecto.
  - Informe de fin de proyecto.
  - Cierre administrativo.

### **Seguimiento y Control (Transversal)**

Este proceso supervisa todas las actividades de gestión y ejecución del proyecto, abarcando el seguimiento del progreso, la medición del avance, la gestión de cambios, la identificación de riesgos y la toma de acciones correctivas. Las actividades incluyen:

- Seguimiento del progreso del proyecto.
- Control del cronograma y de los costes.
- Gestión de requisitos, cambios, riesgos, calidad, partes interesadas, aceptación de entregables, y transición.
- Puertas de fase: Cada fase del proyecto culmina con una revisión y aprobación, conocidas como “puertas de fase”.

### **Roles y Organización del Proyecto**

PM2 estructura los roles del proyecto en varias capas de responsabilidad:

- **Capa de gobernanza:** Establece la visión y la estrategia.
- **Capa rectora:** Ofrece la dirección y orientación general.
- **Capa de dirección:** Asegura la propiedad del Caso de Negocio.
- **Capa de gestión:** Supervisa el día a día del proyecto.
- **Capa de ejecución:** Realiza el trabajo del proyecto.

**Matriz de Asignación de Responsabilidades** (RAM o RASCI): Clarifica las funciones de cada participante, asignando roles de Responsable, Aprobador, Soporte, Consultado e Informado para las distintas tareas y decisiones del proyecto.

## GvLOGOS

GvLOGOS es la metodología desarrollada por la Dirección General de Tecnologías de la Información y las Comunicaciones (DGTIC) para la gestión y desarrollo de proyectos y servicios TIC en la Generalitat Valenciana. Se enfoca en definir procesos y métodos de trabajo necesarios para la gestión de proyectos, servicios, incidencias y cambios, cubriendo desde la recepción de la demanda hasta la entrega final. La metodología toma como base ITIL e ISO 20000 para gestión de servicios y PMI para la gestión de proyectos.

### Modelo Integral de Gestión de Calidad TIC de la DGTIC

GvLOGOS forma parte del modelo integral de calidad TIC de la DGTIC, que promueve una gestión unificada de la demanda de productos y servicios TIC, así como una gestión estructurada de los proyectos, mejorando la eficiencia en la administración de recursos.

#### Subsistemas y Procesos de GvLOGOS

La metodología se estructura en tres subsistemas principales, con dos procesos transversales:

1. **Subsistema de Gestión de la Demanda:** Incluye la gestión de diversas solicitudes y servicios:
  - **gvLOGOS-ent:** Gestión de Entradas.
  - **gvLOGOS-inc:** Gestión de Incidencias.
  - **gvLOGOS-ser:** Gestión de Peticiones de Servicio.
  - **gvLOGOS-cam:** Gestión de Cambios.
  - **gvLOGOS-pro:** Gestión de Proyectos.
2. **Subsistema de Gestión de la Calidad:**
  - **gvLOGOS-qua:** Asegura la calidad en todas las fases del proyecto y servicio.
3. **Subsistema de Gestión de la Seguridad:**
  - **gvLOGOS-seg:** Gestión de la seguridad aplicada a productos y servicios TIC.
4. **Procesos transversales:**
  - **gvLOGOS-gedes:** Gestión de Despliegues.
  - **gvLOGOS-plan:** Gestión del Plan de Proyectos.

## Ciclo de Gestión de Proyectos en GvLOGOS

El ciclo de gestión de proyectos en GvLOGOS se divide en cuatro fases:

1. **Fase de Verificación de la Solicitud:** Revisión de la solicitud entrante a través de gVLOGOS-ent. Participan roles como el supervisor de la solicitud y el solicitante.
2. **Fase de Propuesta:** Incluye los siguientes pasos críticos:
  - o **TOMREQ:** Toma de requisitos por el gestor de proyecto.
  - o **VAREQ:** Validación de requisitos por la oficina de calidad.
  - o **IMPAEV:** Evaluación de impacto de la solución.
  - o **ANCOBE y VACOBE:** Análisis de coste-beneficio y su validación.
3. **Fase de Proyecto:** Desarrollo y gestión del proyecto, donde se crean documentos como el **PLAPRO** (Plan del Proyecto) y se realizan validaciones (VAPRO).
4. **Fase de Cierre:** Cierre formal de la petición, en la que participan el gestor de facturación, oficina de calidad, y el gestor del proyecto.

## Herramientas de GvLOGOS

Para una ejecución efectiva, GvLOGOS utiliza varias herramientas:

- **JIRA:** Gestión de incidencias y solicitudes.
- **gvEstima:** Estimación de esfuerzos en desarrollo.
- **HP-PPM:** Herramienta de gestión de proyectos.
- **Confluence:** Espacio colaborativo para compartir conocimientos.

## Roles en la Metodología GvLOGOS

- **Responsable funcional/Usuario experto:** Define la funcionalidad de la aplicación.
- **Grupo de asignación:** Atiende, diagnostica y resuelve incidencias.
- **Gestor de proyecto:** Supervisa el desarrollo del proyecto.
- **Comité de decisión:** Aprueba recursos y propuestas.
- **Oficina de calidad:** Realiza validaciones.
- **Gestor de entregas:** Monitorea la implementación.

## Otros elementos de control y documentación

GvLOGOS utiliza documentos y actas para asegurar la trazabilidad y control en todas las fases del proyecto, tales como el **ACTACO** (Acta de seguimiento del contrato) y el **ACTAAR** (Acta de Arranque).

## Planificación Estratégica y Metodologías Ágiles

### Metodologías Ágiles

Las metodologías ágiles de desarrollo se centran en la entrega incremental y colaborativa de software, promoviendo la adaptabilidad y la satisfacción del cliente. Su clasificación responde a tres conceptos: desarrollo, trabajo y conocimiento. Estas se distinguen por el modo de abordar los requerimientos (completo o incremental), el flujo de trabajo (secuencial o concurrente) y el tipo de conocimiento requerido (basado en procesos o personas).

#### Metodologías Ágiles de Desarrollo

En 2001, la Agile Alliance estableció el **Manifiesto Ágil**, fundamentado en **4 valores**:

1. Personas e interacciones sobre procesos y herramientas.
2. Software funcional sobre documentación exhaustiva.
3. Colaboración con el cliente sobre negociación contractual.
4. Respuesta ante el cambio sobre seguimiento de un plan.

Y **12 principios**, entre ellos: priorizar la satisfacción del cliente, dar la bienvenida a cambios en cualquier fase, trabajar en entregas frecuentes de software funcional, y promover la colaboración diaria entre desarrolladores y personal de negocios.

#### Buenas Prácticas Ágiles

##### SCRUM

**SCRUM** es una metodología ágil propuesta en 1986 por Nonaka y Takeuchi, caracterizada por sus roles, artefactos y eventos específicos:

- **Roles:** Incluyen el *Scrum Master* (facilitador), el *Product Owner* (gestor de la visión del producto) y el *Equipo Scrum* (responsable del desarrollo).
- **Artefactos:** *Product Backlog* (requerimientos), *Sprint Backlog* (tareas del sprint) e *Incremento* (resultado).
- **Eventos:** *Sprints* (iteraciones de 1-2 semanas), reuniones diarias, de planificación, revisión y retrospectiva.

##### XP (Extreme Programming)

**Extreme Programming** lleva al extremo prácticas como la programación en parejas, pruebas continuas y propiedad compartida del código. Promueve valores de comunicación, simplicidad, retroalimentación, coraje y respeto, y enfatiza la refactorización continua y la entrega frecuente.

## Lean

El **Lean Software Development**, basado en el *Lean Manufacturing*, busca eliminar desperdicios y mejorar la eficiencia en el desarrollo. Sus **7 principios** incluyen:

1. Eliminación de desperdicios.
2. Orientación a la calidad.
3. Conocimiento compartido.
4. Diferir el compromiso.
5. Entregas rápidas.
6. Respeto.
7. Visión holística.

## Kanban

**Kanban** es una técnica visual de gestión de proyectos que emplea tableros divididos en columnas (Backlog, To Do, Doing, Done) para representar el flujo de trabajo. Facilita la comunicación y la transparencia dentro del equipo.

## Escalado Ágil

En grandes organizaciones, el escalado ágil busca aplicar principios ágiles a niveles organizativos más amplios mediante marcos como **SAFe**, **LeSS** y **SoS**:

- **SAFe** (Scaled Agile Framework): Orientado a grandes empresas, requiere liderazgo ágil, agilidad técnica y DevOps. Implica un costo elevado y una reestructuración significativa.
- **LeSS** (Large Scale Scrum): Amplía Scrum para equipos medianos, permitiendo un costo bajo y comunicación centrada en equipos y gestión.
- **SoS** (Scrum of Scrums): Facilita la coordinación entre múltiples equipos Scrum, es de bajo coste y adecuado para empresas con varios equipos de Scrum.

## Calidad del Software

# Análisis de Requisitos

El análisis de requisitos es un proceso fundamental en el desarrollo de software que tiene como objetivo definir y comprender las necesidades y expectativas de los clientes y usuarios finales. Este proceso incluye técnicas específicas para la captura, especificación, análisis y validación de los requisitos necesarios para construir un sistema eficaz y ajustado a las necesidades del cliente.

### Requerimientos

Los requerimientos especifican lo que el sistema debe hacer (requisitos funcionales) y cómo debe comportarse en términos de atributos no funcionales como rendimiento, seguridad o portabilidad. Existen dos tipos principales de requisitos:

- **Funcionales:** Definen las funciones y comportamientos específicos del sistema, como los casos de uso.
- **No funcionales:** Definen atributos del sistema, como rendimiento y seguridad.

### Captura de Requerimientos

El proceso de captura de requerimientos tiene como objetivo comprender las expectativas de los clientes y usuarios. A través de entrevistas, reuniones y otros métodos de toma de datos, se busca construir una visión clara de lo que el sistema debe lograr.

### Procesos en la Ingeniería de Requisitos

El proceso de ingeniería de requisitos abarca varias etapas:

- **Estudio de viabilidad:** Evalúa si el proyecto es factible en términos de tecnología, costo y recursos.
- **Obtención y análisis de requerimientos:** Recolecta los requisitos y evalúa su viabilidad y claridad.
- **Especificación de requerimientos:** Documenta los requisitos de forma precisa y verificable.
- **Validación:** Confirma que los requisitos cumplen las expectativas del cliente.

### Especificación de Requerimientos (ERS)

La especificación de requisitos (ERS) es un documento detallado que describe el comportamiento completo del sistema. Contiene:

- **Casos de uso:** Detallan las interacciones entre el usuario y el sistema.
- **Descripción verificable:** El ERS debe ser completo, preciso y verificable, separando funcionalidad de implementación.

### Características de los Requisitos

Los requisitos deben cumplir ciertas características según el estándar IEEE 830-1998:

- **Correctos:** El software debe cumplir con los requisitos.
- **Consistentes:** No debe haber contradicciones entre los requisitos.
- **Completos:** Todos los requisitos necesarios están documentados.
- **Inequívocos:** Deben estar redactados de forma clara.
- **Trazables:** Deben poder seguirse y verificarse a lo largo del proceso de desarrollo.
- **Priorizables:** Los requisitos se ordenan por su importancia.
- **Modificables:** Pueden actualizarse fácilmente.
- **Verificables:** Debe existir un método de prueba para cada requisito.

### Tipos de Requisitos

- **Ambientales:** Aspectos como el entorno de ejecución.
- **Interfaces:** Definen las interacciones del sistema.
- **Factores Humanos:** Consideraciones relacionadas con la usabilidad.
- **Funcionalidad:** Acciones específicas que el sistema debe realizar.
- **Seguridad:** Requisitos para proteger la información.

### Casos de Uso

Los casos de uso capturan los requisitos funcionales y especifican las interacciones entre el usuario y el sistema. Cada caso de uso representa una acción del sistema y sigue un flujo de eventos que define cómo los usuarios y otros sistemas interactúan con él.

- **Estructura de un Caso de Uso:**
  - **Caso de uso:** Describe una función que realiza el sistema.
  - **Actor:** Usuario o sistema que interactúa con el caso de uso.
  - **Subsistemas:** Unidades independientes en el sistema.
  - **Relaciones:** Asociación entre casos de uso y actores.
- **Diagrama de casos de uso:** Representa el contexto del sistema y sus interacciones.

### **Documentación de Requisitos**

La documentación de requisitos debe incluir una descripción clara de lo que el cliente espera y una especificación técnica para los desarrolladores. Esta documentación sirve de base para el diseño y desarrollo del sistema, y debe actualizarse a medida que evolucionan los requisitos.

### **Gestión de Requisitos**

La gestión de requisitos asegura que estos se mantengan actualizados a lo largo del desarrollo, permitiendo modificaciones sin perder el control del alcance del proyecto.

## Aseguramiento de la Calidad

El aseguramiento de la calidad del software es un conjunto de procedimientos y normas que garantizan que el desarrollo y los productos de software cumplan con los niveles de calidad establecidos. Este proceso busca minimizar errores y asegurar que el software entregado se ajuste a las especificaciones y necesidades del cliente, garantizando su correcto funcionamiento y fiabilidad.

### Marco de Trabajo y Normativa

El aseguramiento de calidad se apoya en estándares y normativas, como ISO 9000, que define principios para la gestión y control de calidad en proyectos de software. Estos estándares ayudan a establecer un marco de trabajo que guía la evaluación de calidad, la auditoría, la seguridad y la eficiencia del software.

### Departamentos de Calidad

Los departamentos de calidad incluyen oficinas técnicas, oficinas de proyectos y oficinas de gestión de proyectos (PMO), además de los equipos de aseguramiento de calidad (QA). Cada uno tiene roles específicos en el control y supervisión de calidad a lo largo del ciclo de vida del desarrollo del software.

### Evaluación del Proyecto

En la evaluación del proyecto, se consideran múltiples factores para asegurar un desarrollo de calidad:

- **Facilidad de auditoría:** Que permita una revisión clara y precisa.
- **Consistencia y Completitud:** Todos los elementos deben estar bien definidos y ser coherentes.
- **Estandarización y Exactitud:** Cumplir con las normas establecidas para facilitar el control y la precisión.
- **Tolerancia a errores y Seguridad:** Proveer de mecanismos que minimicen errores y riesgos de seguridad.

### Plan de Calidad: Principios

El plan de calidad se estructura en torno a tres principios:

- **Gestión de la Calidad:** Involucra políticas de calidad y asignación de responsabilidades.
- **Aseguramiento de la Calidad:** Conjunto de actividades planificadas para garantizar que el software cumple con los requisitos.

- **Control de la Calidad:** Actividades para verificar el cumplimiento de los requisitos de calidad mediante la evaluación de procesos y productos.

### Actividades y Métodos de Aseguramiento de la Calidad

- **Revisiones Técnicas y de Gestión:** Evaluaciones para detectar errores en las fases tempranas.
- **Inspección (Verificación):** Revisión detallada de los productos de trabajo para asegurar que cumplan los requisitos.
- **Pruebas (Validación):** Validación mediante pruebas funcionales y no funcionales.
- **Auditorías (Cumplimiento):** Evaluación independiente para asegurar que se sigan los procesos y estándares de calidad.

### Principios de los Sistemas de Calidad

Los sistemas de calidad en software se basan en los siguientes principios:

- **Enfoque en el cliente:** La calidad se define en función de las necesidades del cliente.
- **Compromiso organizacional:** Todos los miembros de la organización son responsables de la calidad.
- **Medición y Mejora Continua:** Seguimiento y análisis continuo para mejorar los procesos de desarrollo.
- **Comunicación y Reconocimiento:** Transparencia en la comunicación de políticas de calidad y reconocimiento de logros.

### Tipos de Mantenimiento de Software

Existen diferentes tipos de mantenimiento, cada uno con un objetivo específico:

- **Correctivo:** Corregir defectos y errores encontrados en el software.
- **Evolutivo:** Implementar cambios para añadir nuevas funcionalidades.
- **Adaptativo:** Modificar el software para adaptarse a nuevos entornos o plataformas.
- **Perfectivo:** Optimizar el rendimiento o mejorar la usabilidad del software.

### Métricas de Calidad

Las métricas de calidad permiten evaluar aspectos clave del software:

- **Medidas:** Indicadores cuantitativos de atributos como tamaño y capacidad.
- **Métricas:** Indicadores específicos de la calidad del proceso, producto o proyecto.
- **Indicadores:** Combinaciones de métricas que ofrecen una visión general del estado de calidad.

### Tipos de métricas:

- **Orientadas al tamaño:** Como líneas de código (LoC) o personas-mes.
- **Orientadas a la función:** Basadas en la complejidad del problema.
- **Orientadas a la productividad:** Enfocadas en el proceso de desarrollo.

### Tipos de Pruebas de Software

El aseguramiento de calidad incluye pruebas para validar y verificar el funcionamiento del software:

- **Pruebas Funcionales:** Aseguran que el software cumpla con los requisitos especificados, como pruebas unitarias, de integración, de regresión y de aceptación.
- **Pruebas No Funcionales:** Evalúan atributos no relacionados directamente con la funcionalidad, como rendimiento, carga y estrés.

### Ejemplos de pruebas específicas:

- **Pruebas de carga y rendimiento:** Verifican la capacidad del sistema bajo alta carga.
- **Pruebas de regresión:** Validan que el software siga funcionando correctamente tras cambios o actualizaciones.

### Deuda Técnica y Métricas de Complejidad

La deuda técnica es el esfuerzo futuro necesario para solucionar problemas introducidos durante el desarrollo por urgencias u otras limitaciones. Existen métricas específicas para evaluar la complejidad del software, como:

- **Complejidad ciclomática:** Mide la cantidad de caminos independientes en el código.
- **Índice de mantenibilidad:** Evalúa la facilidad de mantenimiento del software.
- **Cobertura de código:** Proporción de código ejecutado durante las pruebas.

### Notas Relevantes sobre la Calidad

Es importante recordar que la calidad del software es difícil de medir de forma absoluta debido a su naturaleza. La certificación de calidad se otorga a los procesos de desarrollo, no al software en sí. En última instancia, el usuario final percibe la calidad del software según su experiencia y sus necesidades.

## DevOps

DevOps es un conjunto de prácticas que busca integrar los equipos de desarrollo de software (Dev) y de operaciones de TI (Ops) para acelerar el ciclo de vida del desarrollo y mejorar la calidad de la entrega. El objetivo principal de DevOps es fomentar una comunicación fluida, colaboración y automatización a lo largo del ciclo de desarrollo y operación del software, promoviendo una cultura de cambio constante y mejora continua.

### Principios Fundamentales de DevOps

Los principios de DevOps incluyen:

- **Automatización:** Uso extensivo de herramientas que facilitan la gestión, integración, pruebas y despliegue.
- **Colaboración:** Facilitar el trabajo conjunto y la comunicación entre los equipos de desarrollo y operaciones.
- **Integración Continua:** Integrar cambios en el código de manera frecuente para detectar errores pronto.
- **Entrega Continua:** Automatización del flujo de trabajo para lanzar nuevas versiones de software de manera regular y confiable.

DevOps se basa en metodologías ágiles y se centra en el cambio cultural dentro de la organización.

### Cadena de Herramientas DevOps

La cadena de herramientas DevOps abarca cada fase del ciclo de vida del software, apoyando la automatización y facilitando la colaboración:

- **Planificación:** Define requisitos y valores empresariales (Herramientas: JIRA, Git).
- **Codificación:** Diseño y desarrollo del código (Herramientas: GitHub, GitLab, Bitbucket).
- **Compilación:** Gestión de versiones y compilación (Herramientas: Docker, Maven, Puppet).
- **Prueba:** Pruebas continuas para asegurar calidad (Herramientas: JUnit, Selenium).
- **Puesta en marcha:** Automatización de tareas de despliegue (Herramientas: Jenkins, Kubernetes).
- **Funcionamiento:** Gestión del software en producción (Herramientas: Ansible, Chef).
- **Supervisión:** Detección y solución de problemas (Herramientas: Grafana, Splunk).

### Ciclo de Vida de DevOps: Prácticas Clave

El ciclo de vida de DevOps incluye varias prácticas continuas que ayudan a mejorar la agilidad y la calidad:

- **Desarrollo Continuo:** Incluye planificación y codificación.
- **Integración Continua (CI):** Integración frecuente de código, verificada automáticamente con pruebas.
- **Testing Continuo:** Ejecución constante de pruebas para detectar errores de manera temprana.
- **Despliegue Continuo (CD):** Automatiza el lanzamiento de código en producción.
- **Monitorización Continua:** Supervisión constante del software en producción.
- **Feedback Continuo:** Retroalimentación inmediata sobre problemas en producción.

### Integración Continua (Continuous Integration, CI)

La integración continua es una práctica en la que los desarrolladores integran su trabajo frecuentemente en un repositorio central (por ejemplo, rama “develop”). Cada integración se verifica automáticamente a través de pruebas unitarias y de integración, permitiendo identificar errores cuanto antes.

#### Componentes de CI:

- **Compilación automática** del código.
- **Pruebas automatizadas** de cada integración.
- **Notificaciones** sobre el estado de las pruebas.

### Entrega Continua (Continuous Delivery, CD)

La entrega continua asegura que el software esté listo para ser lanzado en producción en cualquier momento. En esta práctica, el código pasa por una serie de pruebas y empaquetado de forma automatizada, aunque la decisión de desplegar puede requerir intervención humana.

### Despliegue Continuo (Continuous Deployment, CD)

El despliegue continuo lleva la automatización un paso más allá, permitiendo que el código se despliegue automáticamente en producción tras cada integración sin intervención humana. El proceso solo se interrumpe si fallan las pruebas automáticas.

### CI/CD: Integración y Entrega/Despliegue Continuo

El término CI/CD hace referencia a la combinación de prácticas de integración continua, entrega continua y despliegue continuo, dependiendo del nivel de automatización deseado por

el equipo o la organización. Implementar CI/CD optimiza el flujo de trabajo y asegura una entrega de software confiable y rápida.

### Ciclo de Despliegue de Aplicaciones

El ciclo de despliegue puede variar según el autor, pero generalmente sigue una de estas dos estructuras:

- **Modelo A:** Requerimientos → Diseño → Implementación → Verificación → Mantenimiento.
- **Modelo B:** Planificación → Requisitos → Diseño y Prototipado → Desarrollo → Pruebas → Despliegue → Operaciones y Mantenimiento.

### Herramienta Destacada en CI/CD: Jenkins

Jenkins es un servidor de integración continua de código abierto escrito en Java, ampliamente utilizado para automatizar el desarrollo, las pruebas y el despliegue. Sus características clave incluyen:

- **Instalación multiplataforma:** Compatible con Windows, MacOS y Linux.
- **Configuración:** Realizada a través de una interfaz web.
- **Integración:** Soporta una gran variedad de plugins (JIRA, Slack, Maven, etc.).
- **Arquitectura Master-Slave:** Escalable para distribuir el procesamiento en múltiples máquinas.

## Fundamentos del Testeo (ISTQB)

El testeo de software es una disciplina crítica dentro del desarrollo de software que permite identificar defectos y verificar que el software cumple con los requisitos establecidos. Según los fundamentos de ISTQB (International Software Testing Qualifications Board), el testeo de software ayuda a validar la funcionalidad del sistema y a mejorar la calidad general del producto antes de su implementación en entornos productivos.

### Errores, Defectos y Fallos

En el proceso de testeo, se distingue entre errores, defectos y fallos:

- **Error (equivocación):** Es la acción humana que conduce a un problema en el código o diseño.
- **Defecto:** Es el resultado de un error en el código, una imperfección que puede causar un fallo.
- **Fallo:** Es el comportamiento incorrecto del sistema al ejecutar el defecto, evidenciando la presencia de un problema en el software.

### Los Siete Principios de la Prueba

1. **La prueba muestra la presencia de defectos, no su ausencia.**
2. **La prueba exhaustiva es imposible:** No se pueden cubrir todos los casos posibles.
3. **La prueba temprana ahorra tiempo y dinero:** Detectar defectos en etapas tempranas reduce los costos.
4. **Los defectos se agrupan:** La mayoría de los defectos suelen concentrarse en ciertas áreas del software.
5. **Paradoja del pesticida:** Repetir siempre las mismas pruebas reduce su efectividad; es necesario actualizar las pruebas para detectar nuevos defectos.
6. **La prueba depende del contexto:** Las pruebas varían según el tipo de software.
7. **La ausencia de errores es una falacia:** Un sistema sin defectos puede ser inutilizable si no cumple con los requisitos.

### Roles en el Proceso de Revisión

El proceso de revisión, que busca detectar defectos sin ejecutar el software, involucra diferentes roles:

- **Autor:** Persona que ha creado el código o documento revisado.
- **Dirección:** Supervisa la efectividad del proceso.
- **Facilitador:** Coordina el proceso de revisión.

- **Líder de revisión:** Responsable de la planificación y ejecución de la revisión.

### Niveles de Prueba

Los niveles de prueba son conjuntos de actividades de testeo organizadas de manera estructurada:

- **Prueba de Componente:** Evalúa unidades individuales del sistema, como funciones o métodos, de forma aislada.
- **Prueba de Integración:** Verifica la interacción entre componentes, asegurando que funcionen correctamente juntos.
- **Prueba de Sistema:** Prueba el sistema completo para validar su comportamiento general y las tareas de usuario.
- **Prueba de Aceptación:** Valida que el sistema cumple con los requisitos del cliente y se espera que funcione correctamente.

### Pruebas específicas:

- **Prueba Alfa:** Realizada por clientes en las instalaciones del desarrollador, con este último como observador.
- **Prueba Beta:** Realizada por clientes en sus propias instalaciones para obtener una retroalimentación del uso real.

### Tipos de Pruebas de Software

- **Pruebas Funcionales:** Validan que el sistema realice las funciones para las que fue diseñado.
- **Pruebas No Funcionales:** Evalúan características como rendimiento, usabilidad, eficiencia y seguridad.
- **Pruebas de Caja Blanca:** Basadas en el conocimiento de la estructura interna del software; permiten verificar la funcionalidad mediante pruebas directas del código.
- **Pruebas de Caja Negra:** Se realizan sin conocer la estructura interna, evaluando la respuesta del software a diferentes entradas.
- **Pruebas Asociadas al Cambio:**
  - **Pruebas de Confirmación:** Confirman que un defecto ha sido solucionado.
  - **Pruebas de Regresión:** Verifican que nuevas funcionalidades o cambios no introduzcan defectos en áreas previamente correctas.

### Pruebas Dinámicas y Estáticas

- **Pruebas Dinámicas:** Evalúan el comportamiento del software ejecutándolo; incluyen pruebas de caja blanca, caja negra, etc.

- **Pruebas Estáticas:** Analizan el código o documentos sin ejecutarlos, como revisiones manuales o análisis estáticos automatizados.

## Técnicas de Pruebas

Las técnicas de pruebas buscan definir las condiciones y los casos de prueba para garantizar una cobertura exhaustiva:

### Pruebas de Caja Negra:

- **Partición de Equivalencia:** Divide el conjunto de datos en clases que deben dar el mismo resultado.
- **Análisis de Valores Frontera (AVF):** Evaluación de los valores límites de cada partición.
- **Prueba de Tabla de Decisión:** Ayuda a documentar reglas complejas de negocio.
- **Prueba de Transición de Estado:** Verifica secuencias de estados en el sistema, como los diferentes niveles de un menú.
- **Prueba de Caso de Uso:** Basada en los requisitos funcionales, enfocada en las interacciones esperadas.

### Pruebas de Caja Blanca:

- **Cobertura de Sentencia:** Evalúa cada sentencia en el código para garantizar que ha sido ejecutada al menos una vez.
- **Cobertura de Decisión:** Verifica que todas las decisiones (condiciones) posibles en el código se evalúen.

### Pruebas Basadas en la Experiencia:

- **Predicción de Errores:** Basada en la experiencia previa de los evaluadores.
- **Prueba Exploratoria:** Los evaluadores exploran el software sin un caso de prueba predefinido.
- **Prueba Basada en Listas de Comprobación:** Usa listas para verificar que se cumplen ciertos criterios.

## Familia de Normas ISO/IEC 25000 (SQuaRE)

La familia de normas ISO/IEC 25000, también conocida como SQuaRE (System and Software Quality Requirements and Evaluation), tiene como objetivo proporcionar un marco de trabajo común para evaluar la calidad de los productos de software. Estas normas abarcan desde la especificación de requisitos de calidad hasta la evaluación de dicha calidad, facilitando su aplicación en diversas áreas del desarrollo de software.

### Objetivos de ISO/IEC 25000

Las normas ISO/IEC 25000 están diseñadas para:

- **Especificación de requisitos de calidad:** Determinar los atributos de calidad necesarios para el software.
- **Evaluación de la calidad del software:** Proveer herramientas para medir y analizar la calidad del producto de software.

### Divisiones de las Normas ISO/IEC 25000

Las normas se dividen en varias categorías, cada una enfocada en un aspecto específico de la calidad del software:

- **División de Gestión de Calidad (ISO/IEC 2500n):** Define los modelos, términos y definiciones comunes utilizados en la familia 25000.
- **División de Modelo de Calidad (ISO/IEC 2501n):** Contiene modelos detallados para evaluar la calidad interna, externa y en uso del software.
  - **ISO/IEC 25010:** Proporciona un modelo de calidad para productos de software y su calidad en uso.
  - **ISO/IEC 25012:** Modelo de calidad de datos para evaluar datos estructurados en sistemas de información.
- **División de Medición de Calidad (ISO/IEC 2502n):** Proporciona un modelo de referencia y definiciones de métricas para la calidad.
- **División de Requisitos de Calidad (ISO/IEC 2503n):** Ayuda en la especificación de requisitos de calidad.
  - **ISO/IEC 25030:** Contiene recomendaciones para la especificación de requisitos de calidad.
- **División de Evaluación de Calidad (ISO/IEC 2504n):** Proporciona guías y modelos para la evaluación del software.
  - **ISO/IEC 25040:** Modelo de referencia para la evaluación, que incluye las entradas, restricciones y recursos necesarios para el proceso.

## ISO/IEC 25010: Modelo de Calidad del Software

La norma ISO/IEC 25010 define un modelo de calidad que identifica las características a evaluar en un producto de software. Estas características son:

- **Adecuación Funcional:** Capacidad para cumplir con la funcionalidad acordada.
  - Completitud funcional, Corrección funcional y Pertinencia funcional.
- **Eficiencia de desempeño:** Uso de recursos de manera óptima.
  - Comportamiento temporal, Utilización de recursos y Capacidad.
- **Compatibilidad:** Capacidad para funcionar en conjunto con otros sistemas.
  - Coexistencia e Interoperabilidad.
- **Usabilidad:** Facilidad de uso y comprensión del software.
  - Reconocibilidad, Aprendizabilidad, Operabilidad, Estética de la interfaz de usuario, Accesibilidad.
- **Fiabilidad:** Capacidad para mantener un funcionamiento correcto.
  - Madurez, Disponibilidad, Tolerancia a fallos y Capacidad de recuperación.
- **Seguridad:** Protección contra accesos no autorizados.
  - Confidencialidad, Integridad, No repudio, Responsabilidad, Autenticidad.
- **Mantenibilidad:** Facilidad para realizar cambios y adaptaciones.
  - Modularidad, Reusabilidad, Analizabilidad, Modificabilidad, Capacidad para ser probado.
- **Portabilidad:** Capacidad para ser transferido y usado en otros entornos.
  - Adaptabilidad, Capacidad para ser instalado, Capacidad para ser reemplazado.

Además, la **ISO/IEC 25059** extiende este modelo para considerar aspectos específicos de la Inteligencia Artificial, como la Adaptabilidad Funcional y la Intervenibilidad.

## ISO/IEC 25012: Modelo de Calidad de Datos

La norma ISO/IEC 25012 define las características de calidad que deben tener los datos en un sistema de información. Estas características se agrupan en dos categorías:

- **Calidad de Datos Inherente:** Grado en que los datos poseen cualidades intrínsecas.
  - Exactitud, Completitud, Consistencia, Credibilidad, Actualidad.
- **Calidad de Datos Dependiente del Sistema:** Grado en que el sistema mantiene la calidad de los datos.
  - Disponibilidad, Portabilidad, Recuperabilidad.

### **ISO/IEC 25040: Proceso de Evaluación del Software**

La norma ISO/IEC 25040 describe el proceso de evaluación de software, que consta de cinco actividades:

1. **Establecer los requisitos de la evaluación:** Definir qué aspectos del software se evaluarán.
2. **Especificar la evaluación:** Detallar los criterios y métodos de evaluación.
3. **Diseñar la evaluación:** Preparar el plan de evaluación.
4. **Ejecutar la evaluación:** Realizar las pruebas y análisis correspondientes.
5. **Concluir la evaluación:** Documentar los resultados y conclusiones.

## Esquema Nacional de Seguridad (ENS)

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

### Objeto

El objeto de este Real Decreto es regular el Esquema Nacional de Seguridad, el cual establece los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información, a fin de asegurar el acceso, confidencialidad, integridad, trazabilidad, autenticidad, disponibilidad y conservación de los datos, información y servicios.

### Ámbito de aplicación

El ENS aplica a todo el sector público y a las entidades del sector privado cuando presten servicios a las entidades del sector público. Para los sistemas de información clasificada, se podrán adoptar medidas complementarias.

### Principios básicos

1. **Seguridad como proceso integral:** Involucra elementos técnicos, humanos, materiales y organizativos.
2. **Gestión de la seguridad basada en los riesgos:** La seguridad debe gestionarse mediante un sistema actualizado que evalúe riesgos.
3. **Prevención, detección, respuesta y conservación:** Se requiere un enfoque preventivo y reactivo.
4. **Existencia de líneas de defensa:** Deben implementarse medidas organizativas, físicas y lógicas.
5. **Vigilancia continua:** Monitoreo constante de la seguridad.
6. **Reevaluación periódica:** Revisión y actualización constantes.
7. **Diferenciación de responsabilidades:**
  - **Responsable de Información:** Determina los requisitos de la información tratada.
  - **Responsable del Servicio:** Define los requisitos de los servicios prestados.
  - **Responsable de Seguridad:** Establece los requisitos de seguridad de la información y los servicios.
  - **Responsable del Sistema:** Implementa y supervisa la seguridad del sistema, pudiendo delegar en administradores u operadores.

### Requisitos mínimos de la política de seguridad

Permiten una protección adecuada de la información y los servicios, incluyendo:

- **Organización e implantación del proceso de seguridad.**
- **Ánalysis y gestión de riesgos específicos de cada organización.**

- **Gestión de personal:** Formación, información y supervisión.
- **Profesionalidad:** Personal cualificado y dedicado.
- **Autorización y control de accesos:** Control y limitación de accesos.
- **Protección de instalaciones:** Control de acceso y áreas diferenciadas.
- **Adquisición de productos y servicios de seguridad acorde a la categoría y nivel de seguridad.**
- **Mínimo privilegio y seguridad por defecto.**
- **Integridad y actualización del sistema con autorización formal previa.**
- **Protección de la información almacenada y en tránsito.**
- **Prevención ante interconexiones de redes públicas.**
- **Registro de actividad y detección de código dañino.**
- **Gestión de incidentes de seguridad y continuidad de la actividad.**
- **Mejora continua del proceso de seguridad.**

#### **Perfiles de cumplimiento específicos**

El Centro Criptológico Nacional (CCN) valida y publica perfiles de cumplimiento específicos aplicables a entidades o sectores de actividad concretos.

#### **Esquemas de acreditación y validación**

Garantizan que las implementaciones y configuraciones de soluciones de seguridad cumplan con el ENS y las guías de seguridad CCN-STIC.

#### **Auditoría de la seguridad**

Es obligatoria una auditoría ordinaria cada dos años o cuando se realicen modificaciones sustanciales en el sistema. Los niveles de auditoría dependen de la categoría del sistema:

- **Básica:** Autoevaluación y análisis del responsable de seguridad.
- **Media/Alta:** Auditoría completa con informe de cumplimiento.

#### **Estado de seguridad de los sistemas**

El Comité Sectorial de Administración Electrónica debe conocer el estado de la seguridad en los sistemas de información. El CCN facilita la recogida y consolidación de información de seguridad.

#### **Centro Criptológico Nacional (CCN)**

El CCN, a través del CCN-CERT, gestiona la respuesta ante incidentes de seguridad. Sus funciones incluyen:

- Respuesta a incidentes, formación, concienciación y sensibilización.
- Divulgación de buenas prácticas, guías CCN-STIC y avisos de ciberseguridad.
- Validación de perfiles de cumplimiento específicos y esquemas de acreditación.

#### **CCN-CERT**

Es el coordinador estatal de la respuesta técnica ante incidentes de seguridad en el sector

público. Actúa en coordinación con INCIBE-CERT para el sector privado, brindando soporte y supervisando la reconexión de sistemas tras incidentes.

**Normas de conformidad**

El ENS rige la seguridad en sedes y registros electrónicos, así como el acceso de los ciudadanos a servicios públicos. Cada organismo debe establecer su propio mecanismo de control.

**Actualización**

El ENS requiere una actualización constante para adaptarse a los cambios tecnológicos.

**Plazos de adecuación**

Las entidades tienen un plazo de 24 meses para adaptarse a los nuevos requisitos del ENS.

**Categorización de los sistemas de información**

Los sistemas se clasifican en función del impacto de un incidente en las dimensiones de seguridad (Disponibilidad, Autenticidad, Integridad, Confidencialidad, Trazabilidad) y pueden tener una categoría de seguridad Básica, Media o Alta.

### Anexo I: Categorías de los sistemas

Determina la categoría del sistema en función del nivel de seguridad en cada dimensión. Los niveles de seguridad son:

- **Bajo:** Perjuicio limitado.
- **Medio:** Perjuicio grave.
- **Alto:** Perjuicio muy grave.

### Anexo II: Medidas de seguridad

Las medidas de seguridad se estructuran en el Marco Organizativo, el Marco Operacional y las Medidas de Protección:

- **Marco Organizativo:** Define normativa, política y procedimientos de seguridad.
- **Marco Operacional:** Protege la operación del sistema, incluye control de acceso, gestión de recursos externos, servicios en nube y continuidad del servicio.
- **Medidas de Protección:** Protección de instalaciones, gestión del personal, seguridad de equipos y comunicaciones, protección de soportes de información y aplicaciones.

### Proceso de Adecuación al ENS

Para la certificación o conformidad con el ENS, se debe elaborar un Plan de Adecuación que incluya:

1. Identificación del alcance del sistema.
2. Categorización del sistema.
3. Declaración de Aplicabilidad.
4. Análisis de riesgos.
5. Validación de la Declaración de Aplicabilidad definitiva.
6. Política de seguridad.
7. Hoja de ruta para la implementación de medidas de seguridad.
8. Elaboración del marco normativo e implementación.
9. Aprobación del sistema de gestión de seguridad.

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			BÁSICA	MEDIA	ALTA
<b>org</b>	<b>Marco organizativo</b>				
org.1	Política de seguridad	Categoría	aplica	aplica	aplica
org.2	Normativa de seguridad	Categoría	aplica	aplica	aplica
org.3	Procedimientos de seguridad	Categoría	aplica	aplica	aplica
org.4	Proceso de autorización	Categoría	aplica	aplica	aplica
<b>op</b>	<b>Marco operacional</b>				
op.pl	Planificación				
op.pl.1	Análisis de riesgos	Categoría	aplica	+ R1	+ R2
op.pl.2	Arquitectura de Seguridad	Categoría	aplica	+ R1	+ R1 + R2 + R3
op.pl.3	Adquisición de nuevos componentes	Categoría	aplica	aplica	aplica
op.pl.4	Dimensionamiento/gestión de la capacidad	D	aplica	+ R1	+ R1
op.pl.5	Componentes certificados	Categoría	n.a.	aplica	aplica
op.acc	Control de acceso				
op.acc.1	Identificación	T A	aplica	+ R1	+ R1
op.acc.2	Requisitos de acceso	C I T A	aplica	aplica	+ R1
op.acc.3	Segregación de funciones y tareas	C I T A	n.a.	aplica	+ R1
op.acc.4	Proceso de gestión de derechos de acceso	C I T A	aplica	aplica	aplica
op.acc.5	Mecanismo de autenticación (usuarios externos)	C I T A	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5
op.acc.6	Mecanismo de autenticación (usuarios de la organización)	C I T A	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9
<b>op.exp</b>	<b>Explotación</b>				
op.exp.1	Inventario de activos	Categoría	aplica	aplica	aplica
op.exp.2	Configuración de seguridad	Categoría	aplica	aplica	aplica
op.exp.3	Gestión de la configuración de seguridad	Categoría	aplica	+ R1	+ R1 + R2 + R3
op.exp.4	Mantenimiento y actualizaciones de seguridad	Categoría	aplica	+ R1	+ R1 + R2
op.exp.5	Gestión de cambios	Categoría	n.a.	aplica	+ R1
op.exp.6	Protección frente a código dañino	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
op.exp.7	Gestión de incidentes	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3
op.exp.8	Registro de la actividad	T	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5
op.exp.9	Registro de la gestión de incidentes	Categoría	aplica	aplica	aplica
op.exp.10	Protección de claves criptográficas	Categoría	aplica	+ R1	+ R1
<b>op.ext</b>	<b>Recursos externos</b>				
op.ext.1	Contratación y acuerdos de nivel de servicio	Categoría	n.a.	aplica	aplica
op.ext.2	Gestión diaria	Categoría	n.a.	aplica	aplica
op.ext.3	Protección de la cadena de suministro	Categoría	n.a.	n.a.	aplica
op.ext.4	Interconexión de sistemas	Categoría	n.a.	aplica	+ R1
op.nub	Servicios en la nube				
op.nub.1	Protección de servicios en la nube	Categoría	aplica	+ R1	+ R1 + R2
<b>op.cont</b>	<b>Continuidad del servicio</b>				
op.cont.1	Ánálisis de impacto	D	n.a.	aplica	aplica
op.cont.2	Plan de continuidad	D	n.a.	n.a.	aplica
op.cont.3	Pruebas periódicas	D	n.a.	n.a.	aplica
op.cont.4	Medios alternativos	D	n.a.	n.a.	aplica
op.mon	Monitorización del sistema				
op.mon.1	Detección de intrusión	Categoría	aplica	+ R1	+ R1 + R2
op.mon.2	Sistema de métricas	Categoría	aplica	+ R1 + R2	+ R1 + R2
op.mon.3	Vigilancia	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 + R6
<b>mp</b>	<b>Medidas de protección</b>				
<b>mp.if</b>	<b>Protección de las instalaciones e infraestructuras</b>				
mp.if.1	Áreas separadas y con control de acceso	Categoría	aplica	aplica	aplica
mp.if.2	Identificación de las personas	Categoría	aplica	aplica	aplica
mp.if.3	Acondicionamiento de los locales	Categoría	aplica	aplica	aplica
mp.if.4	Energía eléctrica	D	aplica	+ R1	+ R1
mp.if.5	Protección frente a incendios	D	aplica	aplica	aplica
mp.if.6	Protección frente a inundaciones	D	n.a.	aplica	aplica
mp.if.7	Registro de entrada y salida de equipamiento	Categoría	aplica	aplica	aplica
<b>mp.per</b>	<b>Gestión del personal</b>				
mp.per.1	Caracterización del puesto de trabajo	Categoría	n.a.	aplica	aplica
mp.per.2	Deberes y obligaciones	Categoría	aplica	+ R1	+ R1
mp.per.3	Concienciación	Categoría	aplica	aplica	aplica
mp.per.4	Formación	Categoría	aplica	aplica	aplica
<b>mp.eq</b>	<b>Protección de los equipos</b>				
mp.eq.1	Puesto de trabajo despejado	Categoría	aplica	+ R1	+ R1
mp.eq.2	Bloqueo de puesto de trabajo	A	n.a.	aplica	+ R1
mp.eq.3	Protección de dispositivos portátiles	Categoría	aplica	aplica	+ R1 + R2
mp.eq.4	Otros dispositivos conectados a la red	C	aplica	+ R1	+ R1
<b>mp.com</b>	<b>Protección de las comunicaciones</b>				
mp.com.1	Perímetro seguro	Categoría	aplica	aplica	aplica
mp.com.2	Protección de la confidencialidad	C	aplica	+ R1	+ R1 + R2 + R3
mp.com.3	Protección de la integridad y de la autenticidad	I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
mp.com.4	Separación de flujos de información en la red	Categoría	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4
<b>mp.si</b>	<b>Protección de los soportes de información</b>				
mp.si.1	Marcado de soportes	C	n.a.	aplica	aplica
mp.si.2	Criptografía	C I	n.a.	aplica	+ R1 + R2
mp.si.3	Custodia	Categoría	aplica	aplica	aplica
mp.si.4	Transporte	Categoría	aplica	aplica	aplica
mp.si.5	Borrado y destrucción	C	aplica	+ R1	+ R1
<b>mp.sw</b>	<b>Protección de las aplicaciones informáticas</b>				
mp.sw.1	Desarrollo de aplicaciones	Categoría	n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4
mp.sw.2	Aceptación y puesta en servicio	Categoría	aplica	+ R1	+ R1
<b>mp.info</b>	<b>Protección de la información</b>				
mp.info.1	Datos personales	Categoría	aplica	aplica	aplica
mp.info.2	Calificación de la información	C	n.a.	aplica	aplica
mp.info.3	Firma electrónica	I A	aplica	+ R1 + R2 + R3	+ R1 + R2 + R3 + R4
mp.info.4	Sellos de tiempo	T	n.a.	n.a.	aplica
mp.info.5	Limpieza de documentos	C	aplica	aplica	aplica
mp.info.6	Copias de seguridad	D	aplica	+ R1	+ R1 + R2
<b>mp.s</b>	<b>Protección de los servicios</b>				
mp.s.1	Protección del correo electrónico	Categoría	aplica	aplica	aplica
mp.s.2	Protección de servicios y aplicaciones web	Categoría	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3
mp.s.3	Protección de la navegación web	Categoría	aplica	aplica	+ R1
mp.s.4	Protección frente a denegación de servicio	D	n.a.	aplica	+ R1

## Gestión de Riesgos

# Análisis de riesgos en la gestión de proyectos

El análisis de riesgos consiste en estudiar posibles amenazas y eventos no deseados, así como los daños que éstos pueden causar en los activos de una organización. La gestión de riesgos se refiere al conjunto de actividades que una organización realiza para evaluar y reducir tales efectos, utilizando para ello metodologías como MAGERIT, una de las más empleadas en la Administración.

### Definiciones

- **Riesgo:** Combinación de la probabilidad de que ocurra un evento y sus consecuencias. En un sentido más específico, se refiere a la posibilidad de pérdida de un activo digital debido a la explotación de una vulnerabilidad por parte de una amenaza.

### Tipos de riesgo

- **Riesgo inherente:** Nivel de riesgo existente antes de implementar medidas de seguridad y salvaguarda.
- **Riesgo residual:** Riesgo remanente tras la aplicación de las medidas de seguridad.
- **Riesgo de terceros:** Riesgo asociado a los componentes y sistemas de terceros con los que interactúa el sistema en evaluación.

### Atributos del riesgo

Los atributos del riesgo incluyen activos, amenazas y vulnerabilidades:

- **Activos:** Elementos tangibles o intangibles con valor, que requieren protección (ej., personas, sistemas informáticos, infraestructuras, información). Es importante estimar su valor y criticidad.
- **Amenazas:** Causas potenciales de incidentes no deseados. Es esencial conocer sus características, probabilidad de ocurrencia e impacto potencial. Las amenazas incluyen:
  - **Fuente de la amenaza:** Proceso o agente que intenta causar el daño.
  - **Evento de la amenaza:** Resultado de la actividad maliciosa.
- **Vulnerabilidades:** Debilidades en el diseño, implementación, operación o control interno que pueden exponer los sistemas a amenazas. Es necesario identificar posibles puntos de acceso y las contramedidas implementadas.

### Probabilidad de impacto de la amenaza

La probabilidad de impacto permite establecer la prioridad de las amenazas que deben abordarse. Se suele utilizar una matriz de "Probabilidad vs. Impacto" para realizar una evaluación cuantitativa y cualitativa de los riesgos.

### Estrategias de gestión de riesgos

- **Reducción del riesgo:** Implementación de medidas de control.
- **Evitación del riesgo:** No participar en la actividad que lo provoca.
- **Transferencia a un tercero:** Ejemplo típico, la contratación de seguros.
- **Aceptación del riesgo:** Se da cuando el riesgo es tolerable o las pérdidas resultantes son asumibles.

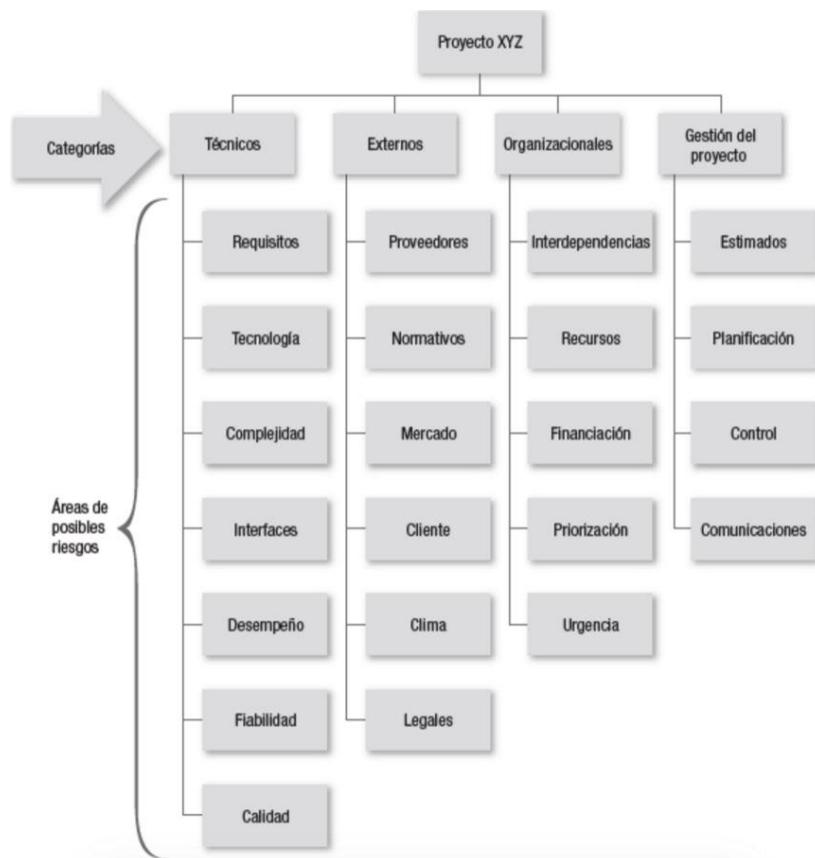
### Principios de gestión de riesgos

De acuerdo con la norma ISO 31000:2009, los principios de la gestión de riesgos son:

- Crear y proteger el valor
- Integrarse en los procesos organizativos
- Formar parte de la toma de decisiones
- Manejar explícitamente la incertidumbre
- Ser sistemática, estructurada y en tiempo
- Basarse en la mejor información disponible
- Adaptarse a los recursos disponibles
- Tener en cuenta factores humanos y culturales
- Ser transparente e inclusiva
- Ser dinámica, interactiva y sensible al cambio
- Facilitar la mejora continua en la organización

### Estructura de desglose de riesgos (RBS, Risk Breakdown Structure)

La Estructura de Desglose de Riesgos (RBS) es una representación jerárquica de los riesgos, organizada por categorías y subcategorías, que identifica las distintas áreas y causas de posibles riesgos dentro de un proyecto. Según el PMBOK, la RBS facilita la identificación y clasificación de riesgos según sus características.



# Metodología MAGERIT

La metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es la principal referencia en la administración para el análisis y gestión de riesgos en sistemas de información. Esta metodología, desarrollada por el Consejo Superior de Administración Electrónica, provee un enfoque formal para identificar, analizar y gestionar los riesgos que amenazan a los sistemas de información, recomendando medidas para su control.

## Objetivos

Los objetivos de MAGERIT incluyen concienciar sobre la existencia de riesgos y la necesidad de gestionarlos, ofrecer una metodología clara para su identificación y análisis, y contribuir a mantener los riesgos bajo control. Esta metodología se enmarca en el Esquema Nacional de Seguridad, que regula la gestión de riesgos en la administración.

## Modelo de MAGERIT

MAGERIT se organiza en tres submodelos interrelacionados: el submodelo de elementos, el submodelo de eventos y el submodelo de procesos.

### Submodelo de Elementos

Este submodelo incluye los siguientes elementos clave:

- **Activos:** Componentes o funcionalidades de un sistema susceptibles de ser atacados, cuya afectación impacta a la organización.
  - **Valoración cuantitativa:** Mide el incremento de gasto por la materialización de una amenaza.
  - **Valoración cualitativa:** Ordena el valor de los activos de forma relativa mediante criterios homogéneos.
- **Amenazas:** Causas potenciales de incidentes que pueden causar daño. Se clasifican según su origen (natural, industrial, defectos, errores o ataques intencionados) y se identifican en términos de probabilidad e impacto.
- **Vulnerabilidades:** Posibilidades de que ocurra una amenaza específica sobre un activo concreto, clasificadas como intrínsecas o efectivas.
- **Impacto:** Medida del daño producido al materializarse una amenaza sobre un activo. Puede clasificarse en pérdidas cuantitativas o cualitativas (con pérdida orgánica o funcional).
  - **Impacto complementario:** Valor del activo más el de los activos dependientes.
  - **Impacto repercutido:** Valor del activo más las amenazas a los activos dependientes.

- **Riesgos:** Probabilidad de que se produzca un impacto determinado en el sistema.
  - **Clasificación en cuatro zonas:** desde riesgos muy probables con alto impacto hasta riesgos poco probables con bajo impacto.
- **Salvaguardas:** Medidas que combaten las amenazas y se pueden evaluar por dominio o activo.
  - **Según el efecto:** Preventivo (disuasorias/eliminatorias), Acotador (minimizadoras/correctivas/repercutivas), o Consolidador (monitorización/detección/concienciación/administrativa).

### Submodelo de Eventos

Este submodelo se divide en tres sub-submodelos:

- **Submodelo estático de eventos:** Relaciona las entidades del submodelo de elementos.
- **Submodelo organizativo dinámico:** Aporta una dimensión temporal al submodelo estático.
- **Submodelo físico dinámico:** Añade una dimensión temporal al submodelo físico.

### Submodelo de Procesos

Describe el desarrollo de un proyecto de seguridad en cuatro fases: planificación, análisis de riesgos, gestión de riesgos y selección de salvaguardas.

### Documentación de MAGERIT

MAGERIT incluye tres documentos esenciales disponibles en la página de administración electrónica:

- **Libro I - Método:** Describe la gestión del riesgo como un proceso que combina análisis y tratamiento. Los componentes de gestión del riesgo incluyen:
  - **Análisis de riesgo:** Valoración de activos, amenazas, salvaguardas e impacto.
  - **Tratamiento de riesgo:** Medidas de protección y reacción.
  - **Proceso de gestión:** Incluye definir el contexto, identificar, analizar, evaluar y tratar riesgos; además de comunicar y revisar continuamente.
- **Libro II - Catálogo de elementos:** Contiene una clasificación detallada:
  - **Activos** (información, datos, servicios, aplicaciones, etc.)
  - **Amenazas** (de origen natural, industrial, defectos, etc.)
  - **Salvaguardas** (protección de datos, claves, seguridad de personal, etc.)

- **Libro III - Guía de técnicas:** Contiene técnicas específicas y generales para el análisis y gestión de riesgos, como el análisis mediante tablas, análisis algorítmico, técnicas gráficas, sesiones de trabajo y valoración Delphi.

### Proceso de Análisis de Riesgos en MAGERIT

El proceso de análisis de riesgos incluye varias etapas clave:

- **Caracterización de los activos:** Identificación y análisis de las dependencias entre los activos de la organización.
- **Caracterización de las amenazas:** Evaluación de la probabilidad de cada amenaza (vulnerabilidad), el impacto que podría generar y el riesgo asociado.
- **Caracterización de las salvaguardas:** Catalogación y evaluación de salvaguardas para reducir el riesgo de vulnerabilidades e impacto.
- **Riesgo residual:** Evaluación del riesgo que permanece después de aplicar las salvaguardas.
- **Estimación del estado de riesgo:** Caracterización de los activos basada en el riesgo residual.

### Implementación de la Metodología

La implementación de MAGERIT incluye las siguientes actividades:

- **Identificación de Activos:** Clasificación de los activos según su función.
- **Valoración de Activos:** Asignación de un valor en función de su criticidad y las cinco dimensiones de seguridad.
- **Identificación de Amenazas:** Identificación de eventos que podrían degradar los activos.
- **Frecuencia y Degradación:** Evaluación de la periodicidad de los eventos y el grado de perjuicio al activo.
- **Impacto y Cálculo de Riesgo:** Evaluación de posibles consecuencias de las amenazas y su probabilidad.
- **Identificación y Valoración de Salvaguardas:** Medidas a tomar para mitigar el riesgo.
- **Cálculo del Riesgo Residual:** Cálculo del riesgo restante tras la implementación de las salvaguardas.

**Caso practico: (Rápido)**

Activo	Amenaza	Vulnerabilidad	Impacto	Riesgo	Dimensión
<b>Nueva app</b>  <b>Información</b>	• Código dañino	• Medio	• Alto	• Baja	• ACID
	• Corrupción de datos • Acceso no autorizado a datos	• Media • Baja	• Media • Alto	• Media • Alto	• I • C
<b>Comunicaciones</b>	• Caída redes	• Baja	• Baja	• Baja	• D

**Caso practico: (Detallado)**

<b>Riesgos del proyecto</b>	<b>Salvaguardas</b>
• Desvíos presupuestarios, Enfermedades o bajas,...	• Control de desvíos, cumplir con la normativa de prevención de riesgos laborales,...
<b>Riesgos técnicos</b>	<b>Salvaguardas</b>
• Errores de diseño, Incumplimiento del servicio,...	• Procedimiento de aseguramiento de la calidad, causas de penalización,...
<b>Riesgos del negocio</b>	<b>Salvaguardas</b>
• A, B, C,...	• A, B, C,...
<b>Riesgos de cumplimiento</b>	<b>Salvaguardas</b>
• A, B, C,...	• A, B, C,...

## Desarrollo Seguro de Aplicaciones

# OWASP 4.0 (Open Web Application Security Project)

OWASP es una iniciativa libre y sin ánimo de lucro que busca promover la seguridad en el software, enfocándose principalmente en aplicaciones web. Este proyecto se organiza en función del estado de madurez del desarrollo, y sus etapas incluyen:

- **Definición:** Revisión de requerimientos.
- **Diseño:** Revisión de arquitectura, diseño, y modelos UML.
- **Desarrollo:** Revisión de código, pruebas unitarias y de sistema.
- **Despliegue:** Pruebas de penetración, revisiones de configuración y pruebas adicionales.
- **Mantenimiento:** Realización de “health checks”, revisiones operacionales y pruebas de regresión.

### Pruebas de seguridad

Las pruebas de seguridad en OWASP se dividen en dos fases principales:

- **Pasiva:** Se examina el funcionamiento de la aplicación para comprender su lógica operativa e identificar posibles vulnerabilidades.
- **Activa:** Se realizan pruebas específicas en base a los vectores de ataque identificados en la fase pasiva.

Estas pruebas están organizadas en **11 categorías**, con un total de **91 puntos de control**. Las categorías incluyen:

Recopilación de información, gestión de configuración y despliegue, gestión de identidades, autenticación, autorización, gestión de sesiones, validación de entrada, tratamiento de errores, criptografía, lógica empresarial y pruebas en el lado del cliente. Ejemplos de puntos de control son pruebas de métodos HTTP, pruebas de inyección SQL y chequeos de integridad.

### Informe de resultados de la auditoría

El informe de auditoría en OWASP se estructura en tres secciones:

- **Informe ejecutivo:** Proporciona una visión clara y no técnica de los resultados.
- **Informe de pruebas:** Describe en detalle las pruebas, el alcance y limitaciones de cada test.
- **Informe de hallazgos:** Presenta los problemas encontrados junto con recomendaciones para mitigarlos.

## Top riesgos de seguridad en OWASP

Algunos de los principales riesgos de seguridad en aplicaciones web son: inyección (SQL, LDAP), ruptura de autenticación y secuestro de sesión, cross-site scripting (XSS), referencias a objetos no seguras, configuración de seguridad insuficiente, exposición de datos sensibles, falta de control en el nivel de acceso, cross-site request forgery (CSRF), componentes con vulnerabilidades conocidas y redirecciones no validadas.

## Seguridad de los servicios en nube

Para asegurar servicios en la nube, se recomienda un decálogo de medidas:

Determinar la categoría del sistema según el ENS, elaborar una declaración de aplicabilidad, realizar un análisis de riesgos, acogerse a un perfil de cumplimiento específico, establecer condiciones contractuales antes de la contratación, detallar aspectos específicos en las condiciones contractuales, supervisar el cumplimiento de requisitos legales por el CSP, realizar un seguimiento de los acuerdos de nivel de servicio (SLA), planificar revisiones periódicas de la información del CSP y desarrollar normativa de seguridad específica para usuarios de la nube.

## Herramientas de seguridad

Las herramientas de seguridad se clasifican en:

- **Herramientas de auditoría**
- **Herramientas de protección** (ej., IDS, IPS, IDS/IPS como Tripwire, OSSEC)
- **Herramientas de detección**
- **Herramientas de reacción**

## Sistema de detección de intrusos (IDS)

Un IDS analiza la actividad en sistemas y redes en busca de entradas no autorizadas o actividades maliciosas. Los IDS se dividen en:

- **NIDS** (Network-Based Intrusion Detection System): Analizan el tráfico de red en tiempo real, buscando ataques DoS, escaneo de puertos e intentos de intrusión, entre otros.
- **HIDS** (Host-Based Intrusion Detection System): Analizan actividades de un host en busca de anomalías que sugieran posibles amenazas.

## Sistemas de Prevención de Intrusiones (IPS)

Los IPS detectan y bloquean intentos de intrusión y amenazas sin afectar el rendimiento. Las características de un IPS incluyen:

- **Detección basada en anomalías:** Identificación, registro y bloqueo de actividad maliciosa.

- **Actualización automática** de bases de firmas.
- **Detección basada en políticas:** Los administradores pueden declarar detalladamente qué actividades son aceptables. Los IPS protegen contra gusanos, spyware, DoS/DDoS, inyección SQL y otros ataques.

Los IPS incluyen diferentes tipos:

- **NIPS:** Basado en la red, buscan tráfico sospechoso en la red.
- **WIPS:** Basado en redes inalámbricas, buscan tráfico sospechoso en la red inalámbrica.
- **NBA:** Analizan comportamientos anómalos en la red, como ciertos tipos de malware y ataques de denegación de servicio.
- **HIPS:** Detectan actividades sospechosas en hosts individuales.

### **AntiDDoS**

Los sistemas AntiDDoS están diseñados para proteger servidores y redes contra ataques de denegación de servicio (DoS).

# Seguridad y protección de redes de comunicaciones

**Seguridad de redes:** Consiste en las políticas y prácticas adoptadas para prevenir y supervisar el acceso no autorizado, el uso indebido, la modificación o la denegación de una red informática y sus recursos accesibles.

**Autenticación:** Puede llevarse a cabo mediante:

- **1-factor:** Basada en lo que el usuario sabe (contraseña).
- **2-factores:** Basada en lo que el usuario tiene (SMS).
- **3-factores:** Basada en lo que el usuario es (huella dactilar).

**Cortafuegos:** Se encargan de aplicar las políticas de acceso.

**Dimensiones de seguridad:** Incluyen confidencialidad, disponibilidad e integridad.

**Honeypot:** Es una herramienta de seguridad informática dispuesta en una red o sistema para atraer posibles ataques informáticos. Facilita la detección de ataques y la obtención de información sobre el mismo y el atacante.

**Honeynet:** Tipo especial de honeypot de alta interacción que actúa sobre una red completa. Está diseñado para ser atacado y recabar información detallada sobre los atacantes.

**Sistema de detección de intrusos (IDS, Intrusion Detection System):** Proceso o dispositivo activo que analiza la actividad del sistema y de la red para identificar accesos no autorizados y actividades maliciosas.

**Tipos de IDS:**

- **NIDS (Network-Based Intrusion Detection System):** Supervisan la actividad de la red, analizando tanto el tráfico entrante como el saliente.
- **HIDS (Host-Based Intrusion Detection System):** Supervisan la actividad de un sistema específico. Realizan chequeo de la integridad de ficheros, detección de rootkits y monitorización de logs.

**Sistemas de Prevención de Intrusiones (IPS):** Detectan y bloquean intentos de intrusión, transmisiones de código malicioso o amenazas en la red, sin afectar el rendimiento del sistema. Detectan anomalías a nivel del sistema operativo.

**Tipos de IPS:**

- **NIPS (Network-based Intrusion Prevention System).**
- **WIPS (Wireless Intrusion Prevention System).**
- **NBA (Network Behavior Analysis).**
- **HIPS (Host-based Intrusion Prevention System).**

## Vulnerabilidades

- **Personal interno.**
- **Entidades externas.**
- **Fast Growth and Overuse.**
- **Fallback attacks / Downgrade attacks:** Ataque criptográfico que degrada el modo de operación seguro (por ejemplo, una conexión encriptada) a un modo menos seguro (texto sin cifrar) para mantener la retrocompatibilidad.
- **Eavesdropping:** Escucha no autorizada de conversaciones o comunicaciones sin el consentimiento de las partes.
- **Replay Attacks:** Repetición malintencionada de una transmisión de datos válida.
- **Insertion attacks:** Cuando el IDS es menos estricto que el sistema final.
- **Fragmentation attacks:** Ataque que utiliza la fragmentación de datagramas para producir un Denegación de Servicio (DoS).
- **Buffer overflows:** Error de software que permite la escritura de datos fuera del buffer, con la posibilidad de alterar el flujo del programa y ejecutar código malicioso.
  - **Shellcode:** Código ejecutable preparado para obtener privilegios sobre un programa vulnerable.
- **XSS attacks (Cross-Site Scripting):** Permite a un atacante injectar código en páginas web visitadas por el usuario (JavaScript, VBScript).
- **Man-in-the-middle:** El atacante adquiere la capacidad de leer, insertar y modificar datos en la comunicación entre dos partes.
- **Session hijacking:** Obtención de acceso no autorizado a información o servicios mediante el secuestro de una sesión.
  - **Session fixation:** El atacante fija una sesión específica en el navegador de la víctima.
  - **Replay session:** Reutilización de una sesión.
- **Spoofing attacks:** Falsificación de datos para suplantar la identidad de otra entidad.
- **Convert channels (Canal encubierto):** Canal usado para transferir información de manera no prevista por los desarrolladores del sistema.
- **Smurf attack (ataque pitufo):** Ataque de denegación de servicio mediante mensajes de ping broadcast con spoofing para inundar el sistema objetivo.
- **Denial of Service (DoS):** Causar la inaccesibilidad de un servicio o recurso para usuarios legítimos, mediante el consumo de ancho de banda o sobrecarga de los recursos del sistema.
  - **Distributed Denial of Service (DDoS)**

- **Malware:** Software malicioso diseñado para realizar acciones dañinas en el sistema de manera intencionada y sin el conocimiento del usuario.

### **Redes privadas virtuales (VPN)**

**Virtual Private Network (VPN):** Tecnología que extiende de forma segura una red local (LAN) sobre una red pública o no controlada, como Internet. Permite que los dispositivos en la red envíen y reciban datos de redes compartidas o públicas como si fueran redes privadas, manteniendo la seguridad y las políticas de gestión de una red privada.

#### **Características básicas de una VPN:**

- Autenticación y autorización.
- Integridad.
- Confidencialidad/Privacidad.
- No repudio.
- Control de acceso.
- Auditoría y registro de actividades.
- Calidad del servicio.

#### **Requisitos básicos de una VPN:**

- **Identificación de usuario:** Usuario y contraseña.
- **Cifrado de datos:** Con cifrado simétrico (DES, 3DES o AES). Se destaca el algoritmo SEAL, más rápido.
- **Administración de claves.**

#### **Tipos de VPN:**

- **VPN de acceso remoto:** Conexión de usuarios desde ubicaciones remotas a la red de la empresa mediante Internet.
- **VPN punto a punto:** Conexión de oficinas remotas con la sede de la organización.
- **Tunneling:** Encapsulación de un protocolo de red sobre otro, creando un "túnel" en la red.
- **VPN over WAN:** Variante del tipo "acceso remoto" que utiliza la red WAN de la empresa en lugar de Internet.

#### **Tipos de conexión en VPN:**

- **Conexión de acceso remoto.**
- **Conexión VPN router a router.**
- **Conexión VPN firewall a firewall.**
- **VPN en entornos móviles.**

### Dispositivos VPN:

- **Enrutador VPN:** Enrutador con software de cliente VPN.
- **Concentrador VPN:** Dispositivo que permite a múltiples usuarios acceder remotamente a la red a través de túneles VPN cifrados. Puede gestionar miles de conexiones simultáneas.

### Control de accesos

**Network Access Control (NAC):** Enfoque de seguridad en redes que unifica las tecnologías de seguridad en equipos finales, usuarios y refuerza la seguridad de acceso a la red.

**Control de acceso informático:** Consiste en la autenticación, autorización de acceso y auditoría.

- **Autenticación/Identificación:** "¿Quién puede entrar al sistema?"
- **Autorización:** "¿Qué puede hacer el sujeto?"
- **Aprobación del acceso:** Definición de políticas de autorizaciones.
- **Auditoría/Rendición de cuentas:** "¿Qué ha hecho el sujeto?"

### Sistemas cortafuegos

Parte de un sistema o red diseñado para bloquear el acceso no autorizado y permitir las comunicaciones autorizadas.

#### Tipos de cortafuegos:

- **Nivel de aplicación de pasarela:** Seguridad para aplicaciones específicas (FTP, Telnet, P2P).
- **Círculo a nivel de pasarela:** Seguridad cuando se establece una conexión TCP o UDP.
- **Cortafuegos de capa de red o de filtrado de paquetes:** Funciona a nivel de red, inspeccionando direcciones IP y paquetes IP.
- **Cortafuegos de capa de aplicación (Application Firewall):** Filtra comunicaciones adaptadas a protocolos de aplicación (ej.: URL).
- **Cortafuegos personal:** Filtra las comunicaciones entre el ordenador y la red.

#### Capa de trabajo de los cortafuegos:

- **Cortafuegos a nivel de red:** Examina los paquetes IP para decidir si deben pasar o no.
- **Cortafuegos a nivel de circuito:** Examina la información TCP para verificar que la sesión es legítima.
- **Cortafuegos a nivel de aplicación:** Utiliza software de servidor Proxy.

### Topologías de cortafuegos:

- **Bastion Host:** Firewall en una instalación específica.
- **Screening Router:** Encaminador con filtrado.
- **Dual-Homed Host:** Host con doble conexión.
- **Screened Host:** Filtrado a nivel de host.
- **Screened Subnet:** Filtrado a nivel de subred.

**Traducción de direcciones de red (NAT):** Oculta la verdadera dirección de la computadora conectada a la red.

### Políticas del cortafuegos:

- **Política restrictiva:** Deniega todo el tráfico, excepto el explícitamente permitido.
- **Política permisiva:** Permite todo el tráfico, excepto el explícitamente denegado.

### Proyecto OWASP

El **Open Web Application Security Project (OWASP)** es un proyecto libre y sin ánimo de lucro orientado a promover la seguridad del software y, en especial, de las aplicaciones web.

### Principales riesgos de seguridad en OWASP:

- **Inyección:** Inyección de código SQL, LDAP, etc.
- **Ruptura de la autenticación y secuestro de sesión:** Robo de credenciales y suplantación de identidad.
- **Cross-Site Scripting (XSS):** Envío de datos no verificados al navegador (ej.: JavaScript en comentarios).
- **Referencias a objetos no seguras:** Acceso a referencias de objetos internos.
- **Configuración errónea o insuficiente de la seguridad.**
- **Exposición de datos sensibles:** Falta de encriptación de información confidencial.
- **Inexistencia de funciones de control del nivel de acceso:** Distinción entre permisos de usuario y administrador.
- **Cross-Site Request Forgery (CSRF):** Ejecución de peticiones malintencionadas.
- **Componentes con vulnerabilidades conocidas:** Utilización de componentes explotables.
- **Redirección no validada:** Exposición a redirecciones no controladas.

# Gestión de Ciberincidentes

**Fases: Preparación, Identificación, Contención, Mitigación, Recuperación y Actuaciones Post-Incidente**

La gestión de ciberincidentes implica un ciclo de vida estructurado en varias fases esenciales:

## 1. Preparación

Después de realizar un análisis de riesgos, se identifican y despliegan medidas de seguridad específicas. En esta fase, se forma un Equipo de Respuesta a Ciberincidentes (ERC), dotado de herramientas y recursos necesarios para actuar. La preparación incluye también el desarrollo de políticas de seguridad y la formación continua del personal para que todos conozcan los protocolos de respuesta.

## 2. Identificación

La fase de identificación engloba la detección, análisis y notificación de brechas de seguridad. Este proceso implica monitorear constantemente el entorno para detectar signos de posibles incidentes. Los elementos clave en esta fase son:

- **Precursos:** Indicios de que un incidente podría ocurrir en el futuro, tales como escaneos de puertos, anuncios de nuevos exploits o amenazas inminentes.
- **Indicadores:** Señales de que un incidente ya ha ocurrido o está en curso, incluyendo alertas de antivirus, desbordamientos de memoria (overflows) o tráfico inusual.

## 3,4,5. Contención, Mitigación y Recuperación

Estas fases consisten en:

- **Contención:** Limitar la propagación del incidente para evitar mayores daños. Se aislan los sistemas comprometidos y se aplican medidas temporales para contener el daño.
- **Mitigación:** Eliminar o neutralizar el incidente. Puede implicar la eliminación de malware, parches de seguridad y restauración de configuraciones.
- **Recuperación:** Restaurar el funcionamiento normal de los sistemas afectados, asegurando que no existan vulnerabilidades residuales que permitan recurrencias del incidente.

## 6. Actuaciones Post-Incidente

Tras resolver el ciberincidente, se realiza un análisis detallado para comprender su causa raíz y los costos asociados. Se redacta un informe exhaustivo que incluye las medidas preventivas recomendadas para evitar incidentes similares en el futuro. La recolección y custodia de evidencias durante esta fase es fundamental para posibles acciones legales y para apoyar el análisis posterior.

## Amenazas y Vectores de Ataque

Las amenazas a la seguridad pueden provenir de diversas fuentes y tomar múltiples formas. La "Guía Nacional de Notificación y Gestión de Ciberincidentes" ofrece un glosario detallado que clasifica los diferentes tipos de amenazas y vectores de ataque, incluidos malware, ataques de denegación de servicio (DDoS), ingeniería social y explotación de vulnerabilidades.

## Clasificación de Ciberincidentes

Los ciberincidentes se clasifican según el tipo y la naturaleza del ataque:

- **Categorías:** Contenido abusivo, dañino, obtención de información, intento de intrusión, disponibilidad, compromiso de información, fraude, vulnerabilidad y otros.
- **Tipos específicos:** Spam, delitos de odio, contenido sexual explícito, escaneo de redes, ingeniería social, explotación de vulnerabilidades, ataques DDoS, mala configuración, sabotaje, entre otros.

## Factores a Valorar en la Clasificación de Incidentes

- **Tipo de amenaza:** Código dañino, intrusiones, fraude, etc.
- **Origen de la amenaza:** Puede ser interna o externa.
- **Categoría de seguridad** de los sistemas afectados, basada en su criticidad y confidencialidad.
- **Perfil de los usuarios afectados:** Según su posición en la estructura organizativa y sus privilegios de acceso a información sensible o confidencial.
- **Número y tipología de sistemas afectados:** Es decir, la extensión y naturaleza de los sistemas comprometidos.
- **Impacto del ciberincidente** sobre la operativa de la organización.
- **Requerimientos legales y regulatorios** que podrían implicar responsabilidades específicas o acciones obligatorias.

## Peligrosidad de los Ciberincidentes

La peligrosidad se clasifica en cinco niveles: BAJO, MEDIO, ALTO, MUY ALTO y CRÍTICO, y su nivel de impacto se evalúa según el Esquema Nacional de Seguridad (ENS).

## Seguimiento por parte del CCN-CERT

El seguimiento de incidentes de seguridad en España se realiza mediante la herramienta LUCIA, que permite coordinar y monitorizar los ciberincidentes. La notificación al CCN-CERT es obligatoria en casos de incidentes de peligrosidad ALTA, MUY ALTA o CRÍTICA.

## Métricas para la Gestión de Incidentes

Existen varias métricas para evaluar la efectividad en la resolución de ciberincidentes:

- **Métricas de implantación, resolución y recursos.**
- **Métricas específicas de gestión de incidentes, como la M5 y M6:**
  - **M5:** Estado de cierre de incidentes. Método: Número de incidentes cerrados sin respuesta / Total notificados.
  - **M6:** Estado de cierre de incidentes con peligrosidad MUY ALTA/CRÍTICA. Método: Número de incidentes cerrados sin respuesta / Total notificados.

## Recolección y Custodia de Evidencias

Es esencial para la resolución de incidentes y su validez legal. La recolección cuidadosa de evidencias permite apoyar tanto las acciones de respuesta como la posible persecución judicial del responsable del incidente.

## LUCIA: Herramienta de Coordinación de Incidentes y Amenazas

LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas) es una herramienta de gestión de tickets que permite a los organismos del ámbito del ENS gestionar sus ciberincidentes. Facilita la integración y sincronización de los incidentes registrados con el CCN-CERT, permitiendo una consolidación y coordinación en el Nodo de Coordinación del CCN-CERT.

**Nota:** Estudiar las “novias” del ENS (ej.: CARMEN, CLARA, CLAUDIA, IRIS, LUCIA,...)

## Funciones de un CERT/CSIRT

Los equipos de respuesta ante emergencias informáticas (CERT, por sus siglas en inglés, o CSIRT) son responsables de dar soporte en la gestión de ciberincidentes:

- **CCN-CERT:** Es el CERT del Centro Criptológico Nacional, parte del Centro Nacional de Inteligencia (CNI).
- **INCIBE-CERT:** Está gestionado por el Instituto Nacional de Ciberseguridad de España.
- **CNPIC:** Forma parte del Centro Nacional de Protección de Infraestructuras y Ciberseguridad.
- **ESP-DEF-CERT:** Pertenece al Mando Conjunto de Ciberdefensa.

## Metodología de Reporte

El sistema de reporte se organiza mediante una **ventanilla única** que sigue los siguientes pasos:

1. **Notificación inicial** al CERT/CSIRT de referencia.
2. **Sincronización** con el organismo receptor o la autoridad competente.
3. **Inicio de la investigación** interna.
4. **Notificación completa** mediante el formulario específico.

5. **Investigación policial o judicial** si se considera necesario.

**Tipos de Seguridad: Activa y Pasiva**

- **Seguridad Activa:** Medidas que buscan evitar la ocurrencia de un ataque, tales como contraseñas seguras, encriptación de datos, antivirus actualizados, auditorías de seguridad y formación continua del personal.
- **Seguridad Pasiva:** Acciones que mitigan los efectos de un ataque una vez que ha ocurrido, como copias de seguridad, uso de servicios en la nube, hardware resistente a fallos y particiones lógicas del disco duro.

## Seguridad de la Información en la Generalitat Valenciana

# Decreto 130/2012 - Organización de la seguridad de la información de la Generalitat

### Objeto

Establecer el reparto de funciones y responsabilidades en materia de seguridad de la información.

### Ámbito

Aplica a Presidencia, Consellerias de la Generalitat y a sus entidades autónomas dependientes, exceptuando a la Conselleria con competencias en sanidad y a la Agencia Valenciana de Salut.

### Principio general de actuación

La seguridad de la información es responsabilidad de todas las personas involucradas en su tratamiento y afecta a todas las personas que forman parte de la organización.

### Agentes de la organización de la seguridad

Definen la estrategia corporativa en materia de seguridad, diseñan, dirigen y monitorizan los planes para su implementación, además de prestar servicios y asesoramiento.

### Estructura de la organización

#### Responsable de la Información (RI)

Es la autoridad máxima sobre el uso y protección de la información. Este cargo recae en la “Comisión Interdepartamental para la Modernización Tecnológica, la Calidad y la Sociedad del Conocimiento en la Comunitat Valenciana”.

- **Funciones:** Aprobar los niveles de seguridad, evaluar riesgos, gestionar códigos tipo y proponer mejoras.
- Tiene la responsabilidad última ante cualquier error o negligencia que derive en incidentes de confidencialidad o integridad.

#### Comité de Seguridad de la Información (CSI)

Coordina la seguridad de la información en toda la Administración de la Generalitat para racionalizar el gasto y evitar disfunciones que generen incidentes de seguridad.

- **Composición:** Presidencia, Vicepresidencia, Vocales y Secretaría.
- **Funciones:** Desarrollar la política y la organización de seguridad de la información, monitorizar riesgos, coordinar esfuerzos y presentar informes de seguridad al Consell.
- **Reuniones:** Ordinarias una vez al año, y extraordinarias según las decida el Presidente.

### **Responsable de los Ficheros de Datos de Carácter Personal (R-FDCP)**

Vigila el cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD).

- **Funciones:** Designar a los Administradores de Seguridad de los Ficheros de Datos de Carácter Personal y gestionar aspectos relacionados con el código tipo en esta materia.

### **Administradores de la Seguridad de los Ficheros de Datos de Carácter Personal**

Ejecutan las tareas delegadas por el R-FDCP.

- **Funciones:** Mantener actualizado el documento de seguridad, ejercer funciones de control y autorización, gestionar los derechos de acceso, rectificación, cancelación y oposición, y registrar incidencias.

### **Responsable del Servicio (RSer)**

Encargado del uso y protección del servicio.

- **Funciones:** Determinar los niveles de seguridad del servicio y asegurarse de que este cumpla con los requisitos de seguridad.
- Es responsable último ante cualquier error o negligencia que afecte la disponibilidad del servicio.

### **Responsable de Seguridad de la Información (RSI)**

Supervisa la seguridad de la información y de los servicios prestados por los sistemas de información conforme a la Política de Seguridad de la Información.

- **Funciones:** Proponer niveles de seguridad, realizar análisis de riesgos, elaborar la declaración de aplicabilidad, gestionar y evaluar el código tipo, elaborar un informe anual sobre el estado de la seguridad, analizar y proponer salvaguardas.
- Es responsable de supervisar la eficacia de las medidas de seguridad implementadas y de asesorar en la determinación de medidas necesarias.

### **Responsable de Seguridad de los Ficheros de Datos de Carácter Personal (RS-FDCP)**

Coordina y controla las medidas de seguridad aplicables a los ficheros de datos personales.

- **Funciones:** Supervisar y coordinar las medidas definidas en el documento de seguridad (para documentos automatizados o no) e informar al R-FDCP.

### **Responsable del Sistema (RSis)**

Encargado de desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, garantizando sus especificaciones, instalación y correcto funcionamiento.

- **Funciones:** Definir y mantener la infraestructura, implementar medidas de seguridad, suspender el servicio en caso de deficiencias graves, desarrollar planes de continuidad, y designar a los administradores de la seguridad del sistema.

### **Administradores de la Seguridad del Sistema**

Implementan, gestionan y mantienen las medidas de seguridad del sistema de información.

- **Funciones:** Implementar las medidas de seguridad, aprobar cambios de configuración, gestionar y actualizar equipos y aplicaciones, y tomar decisiones operativas a corto plazo.

# Decreto 66/2012 - Política de Seguridad de la Información de la Generalitat

El Decreto 66/2012 establece y regula la política de seguridad de la información que se aplica al tratamiento de la información bajo la responsabilidad de los distintos órganos de la Administración de la Generalitat y sus entidades autónomas.

## Objeto y Ámbito de Aplicación

- **Objeto:** Definir y regular la política de seguridad de la información en el tratamiento de la información gestionada por la Administración de la Generalitat y sus entidades autónomas.
- **Ámbito:** Información bajo la responsabilidad de la Administración de la Generalitat y sus entidades autónomas.

## Seguridad como Proceso Integral

La seguridad es un proceso integral que depende de todos los elementos humanos, técnicos, materiales y organizativos que intervienen en el tratamiento de la información. Todos los participantes en el tratamiento son responsables de la seguridad y buen uso de la información. La Generalitat mantendrá a todos informados sobre esta política, y la gestión de la seguridad de la información incluirá monitorización, control y mejora continua.

## Gestión de Riesgos

- La gobernanza y gestión de la seguridad de la información se guiará por los resultados de los procesos de análisis y gestión de riesgos.
- Los **Responsables de Seguridad (RS)** elaborarán un informe anual sobre el estado de la seguridad, los riesgos previsibles y los planes de actuación recomendados.
- Los **Responsables de Información (RI)** y **Responsables de Tratamiento (RT)** fijarán los niveles de riesgo aceptables.
- La reducción de los niveles de riesgo se realizará mediante controles, considerando el nivel de riesgo y el valor de los activos.
- El análisis y gestión de riesgos se aplicará en todas las fases del ciclo de vida de las aplicaciones y servicios.

## Clasificación de la Información

Los activos de información serán inventariados y clasificados en función del riesgo, lo que permitirá una gestión adecuada de la seguridad según la importancia y sensibilidad de la información.

## **Separación de Funciones**

Según el Esquema Nacional de Seguridad (ENS), se establece una separación de funciones entre los responsables de la información, del servicio y de seguridad.

## **Planificación y Coordinación**

Se desarrollarán **planes estratégicos** que incluirán objetivos, líneas de actuación previstas, proyectos a realizar, indicadores de cumplimiento y de progreso, y métricas para evaluar la efectividad. Estos planes serán revisados anualmente, junto con auditorías y evaluaciones, y serán aprobados por los Responsables de Información (RI) y Responsables de Tratamiento (RT).

## **Acceso a la Información No Pública**

El acceso a la información no pública requerirá identificación y privilegios de acceso específicos. Todos los accesos quedarán registrados. Los RI nombrarán un **Responsable de Acceso (RA)** para cada activo de información, quien revisará e informará sobre estos registros.

## **Registro de Actividad**

Las actuaciones podrán ser registradas por exigencias legales, de trazabilidad o para monitorizar el cumplimiento de la política de seguridad, siempre preservando los derechos de los afectados y respetando la normativa laboral.

## **Reserva, Confidencialidad y Sigilo**

Las personas que accedan a datos no públicos en el ejercicio de sus funciones deberán mantener la reserva, confidencialidad y sigilo, incluso tras el cese o finalización contractual.

## **Uso de Instalaciones y Equipamiento**

Las instalaciones y equipamientos no están destinados al uso personal. La instalación o utilización de hardware o software requerirá autorización del órgano competente. Las infraestructuras informáticas y de comunicaciones que no formen parte de los puestos de trabajo deberán ubicarse en áreas separadas, de acceso restringido y suficientemente protegidas.

## **Características de los Sistemas de Información**

Los sistemas de información proporcionarán únicamente la funcionalidad estrictamente necesaria. Deben ser de uso sencillo y seguro; la utilización insegura se considerará un acto consciente. Las funciones de operación, administración, mantenimiento y registro serán las mínimas necesarias y estarán descritas, documentadas y controladas.

## Desarrollo de la Política de Seguridad

La política de seguridad debe abordar:

- Condiciones de acceso a la información.
- Uso de equipos.
- Gestión de incidentes y problemas.
- Continuidad de las operaciones.
- Seguridad, clasificación y tratamiento de la información.
- Análisis y gestión de riesgos.
- Seguridad física y del personal.
- Prevención de malware.
- Ciclo de vida de los sistemas de información.
- Mejora continua y nivel de madurez.

Estos aspectos se agruparán en **Normas** (primer nivel de concreción), **Procedimientos** (pasos para completar una tarea) y **Guías de Buenas Prácticas** (recomendaciones). Las Normas y Procedimientos tendrán carácter obligatorio.

## Publicidad, Monitorización y Revisión de la Política de Seguridad

La Generalitat es responsable de la publicidad, monitorización y revisión de la política de seguridad. Esta política es de carácter obligatorio para todo el personal al servicio de la Administración de la Generalitat y sus entidades autónomas, especialmente para quienes participen en el tratamiento de información o tengan acceso a los locales. El incumplimiento de la política podrá tener consecuencias disciplinarias.

# Orden 19/2013 - Uso Seguro de Medios Tecnológicos en la Administración de la Generalitat

Esta orden establece normas de uso seguro de los medios tecnológicos en los sistemas de información de la Administración de la Generalitat, con el objetivo de minimizar las amenazas que ponen en riesgo la seguridad de dichos sistemas. Desarrolla las directrices generales de la política de seguridad de la información.

## Objeto y Ámbito de Aplicación

- **Objeto:** Regular el uso seguro de los medios tecnológicos de la Administración para minimizar riesgos.
- **Ámbito:** Aplica a todos los usuarios, definidos como cualquier persona con acceso a los medios tecnológicos proporcionados por la Administración de la Generalitat.

## Tratamiento de la Información

La Generalitat es responsable del tratamiento de la información en sus sistemas y redes de comunicación, adoptando medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos. Está prohibido alojar o transmitir información de la Generalitat en sistemas externos sin autorización y contrato expreso, y solo tras un análisis de riesgos asociado.

## Propiedad y Uso de los Medios Tecnológicos

Todos los medios tecnológicos son propiedad de la Administración y no están destinados a uso personal. Está prohibido modificar componentes físicos o lógicos sin autorización. Cualquier medio tecnológico ajeno requiere autorización para conectarse a la red corporativa. No se permite la ejecución de programas sin licencia ni autorización, ni la distribución de material obsceno, difamatorio o atentatorio contra la dignidad.

## Identificación de Acceso

El acceso es personal e intransferible, permitiendo la identificación individual del usuario, quien será responsable de toda actividad relacionada. Las contraseñas deben cumplir con la política de seguridad definida. Cualquier sospecha de uso indebido debe reportarse de inmediato.

## Notificación de Incidencias

Toda incidencia de seguridad que comprometa la confidencialidad, integridad, disponibilidad o autenticidad de la información debe ser notificada de inmediato por los usuarios.

### **Implantación de Medidas Técnicas**

El personal responsable de TI adoptará las medidas técnicas adecuadas al nivel de seguridad exigido.

### **Borrado y Destrucción de Soportes de Información**

Los soportes desechados se destruirán de forma segura, mientras que los reutilizados o liberados deberán ser objeto de borrado seguro.

### **Inspección de los Medios Tecnológicos**

El órgano competente puede realizar revisiones de los medios tecnológicos para verificar su uso adecuado, siempre respetando el derecho a la intimidad del usuario y la seguridad de las comunicaciones.

### **Cese de Actividad**

Cualquier cese de actividad debe comunicarse de inmediato al organismo competente en TI.

### **Copias de Seguridad**

- **Datos en servidores corporativos:** Responsabilidad del órgano competente.
- **Datos en equipo propio:** Responsabilidad del usuario.

### **Acceso desde el Exterior**

El acceso a la Red Corporativa de la Generalitat Valenciana (RCGVA) desde el exterior solo se permite siguiendo el procedimiento autorizado.

### **Incumplimientos**

El incumplimiento de estas normas puede dar lugar a consecuencias disciplinarias.

### **Ordenadores Personales de Sobremesa**

No se permite modificar configuración, instalar programas ni cambiar la ubicación del equipo. Los usuarios deben bloquear su sesión al ausentarse y apagar el equipo al finalizar la jornada. Los ficheros generados en el trabajo deben almacenarse en la carpeta habilitada en la red, y los ficheros temporales deben eliminarse cuando ya no sean necesarios.

### **Equipos Portátiles**

Además de las normas aplicables a los ordenadores de sobremesa, no se debe almacenar información sensible en estos equipos, salvo si se protege con cifrado. Los usuarios deben notificar cualquier pérdida o robo y deben evitar conexiones a redes ajenas, manteniendo desactivada la búsqueda de redes inalámbricas.

### **Impresoras, Fotocopiadoras, Escáneres, Faxes y Equipos Multifunción**

El uso de estos dispositivos debe realizarse mediante buzones de impresión con clave cuando estén disponibles. La documentación impresa debe retirarse de inmediato.

### **Dispositivos Móviles**

Además de las normas aplicables a los portátiles, los dispositivos móviles deben configurarse para que se bloqueen tras un periodo de inactividad.

### **Dispositivos de Almacenamiento Removibles Autorizados**

Solo se utilizarán los proporcionados por la Administración, y toda información sensible debe ser protegida con cifrado.

### **Correo Electrónico Corporativo**

El correo electrónico corporativo se destina exclusivamente a fines profesionales. Queda prohibido su uso para fines comerciales, personales o financieros. No se permite enviar mensajes masivos ni utilizar cuentas externas dentro de la RCGVA sin autorización. La transmisión de información sensible solo puede realizarse con cifrado y firma electrónica. Se deben eliminar mensajes de remitentes desconocidos, y los mensajes con anexos ejecutables serán eliminados automáticamente.

### **Acceso a Internet desde la RCGVA**

El acceso a internet debe realizarse exclusivamente a través de la salida oficial establecida, y el contenido será filtrado según el perfil asignado a cada usuario. El uso de internet debe limitarse a fines laborales, y está prohibido el acceso a páginas con contenido ofensivo o inapropiado. La descarga de programas y archivos solo se permitirá desde sitios oficiales relacionados con el trabajo.

## Inteligencia Artificial

# Inteligencia Artificial: Conceptos Básicos, Tecnologías Fundamentales y Aplicaciones Prácticas

La inteligencia artificial (IA) es una rama de la informática que busca crear sistemas capaces de realizar tareas que normalmente requieren inteligencia humana. Esto incluye actividades como el aprendizaje, el razonamiento, la percepción, la comprensión del lenguaje natural y la toma de decisiones. La IA ha revolucionado múltiples industrias, desde la medicina hasta las finanzas y la logística.

### Inteligencia Artificial Distribuida

La inteligencia artificial distribuida se refiere a sistemas donde múltiples agentes inteligentes colaboran para resolver problemas complejos. Estos agentes pueden estar geográficamente dispersos y comunicarse a través de redes. Este enfoque es esencial en sistemas multiagente, redes neuronales distribuidas y robótica en enjambre.

### Aprendizaje Automático (Machine Learning)

El aprendizaje automático es una subdisciplina de la IA que permite a las máquinas aprender de datos y mejorar con la experiencia sin ser explícitamente programadas.

- **Aprendizaje Supervisado (Supervised):** Los algoritmos se entrena n con datos etiquetados. Por ejemplo, un modelo que clasifica correos electrónicos como "spam" o "no spam" basándose en ejemplos preclasi ficados.
  - **Aprendizaje Semisupervisado (Semi-supervised):** Combina una pequeña cantidad de datos etiquetados con una gran cantidad de datos no etiquetados. Por ejemplo, en reconocimiento de voz, donde solo algunas grabaciones están transcritas.
  - **Aprendizaje Autosupervisado (Self-supervised):** Los modelos generan sus propias etiquetas a partir de los datos. Por ejemplo, los modelos de lenguaje, en donde se trata de predecir la palabra siguiente dada las anteriores.
- **Aprendizaje No Supervisado (Unsupervised):** Trabaja con datos no etiquetados para encontrar estructuras ocultas. Un ejemplo es el agrupamiento de clientes en segmentos de mercado basándose en comportamientos de compra.
- **Aprendizaje por Refuerzo (RL):** Los agentes aprenden mediante ensayo y error, recibiendo recompensas o penalizaciones. Un caso famoso es AlphaGo de DeepMind, que aprendió a jugar Go a nivel superhumano.
- **Aprendizaje en contexto (In-context Learning):** Técnica en la que un modelo (generalmente LLM) puede "aprender" a realizar tareas específicas a partir de los ejemplos proporcionados y sin necesitar reentrenamiento. Esto se realiza en tiempo de inferencia, por lo que **en ningún se modifican sus parámetros**.

- **Aprendizaje de Transferencia (Transfer Learning / Fine-tuning):** Consiste en reutilizar un modelo entrenado en una tarea diferente (pero similar), para ajustarlo a una nueva tarea usando menos datos aunque más específicos. Reduce significativamente el tiempo de aprendizaje
  - **Destilado de conocimiento (Knowledge distillation):** Técnica para transferir el conocimiento de un modelo grande (**teacher model**) a uno más pequeño (**student model**), reduciendo su tamaño y complejidad sin comprometer significativamente la precisión

## Deep Learning y Tipos de Redes Neuronales

El aprendizaje profundo utiliza redes neuronales con múltiples capas para modelar y entender patrones complejos en datos.

- **Perceptrón Multicapa (MLP):** Consiste en capas completamente conectadas. Se utiliza en tareas de clasificación y regresión simples.
- **Redes Neuronales Convolucionales (CNN):** Especializadas en procesar datos con estructura de cuadrícula, como imágenes. Son fundamentales en reconocimiento facial y análisis de imágenes médicas.
- **Redes Neuronales Recurrentes (RNN):** Adecuadas para datos secuenciales, como texto y audio. Por ejemplo, en la generación de subtítulos automáticos.
  - **GRU (Gated Recurrent Unit) y LSTM (Long Short-Term Memory):** Variantes que superan limitaciones de las RNN estándar, permitiendo recordar información a largo plazo.
- **Transformers:** Introducidos para manejar dependencias a largo plazo sin recurrencia. Utilizan mecanismos de atención y son la base de modelos de lenguaje avanzados como GPT-3 y GPT-4.

## Modelo de Atención

El mecanismo de atención permite a los modelos enfocarse en partes específicas de la entrada, asignando pesos a diferentes elementos.

## Procesamiento de Lenguaje Natural (PLN)

El PLN se centra en la interacción entre computadoras y lenguaje humano.

- **Aplicaciones del PLN:**
  - **Traducción Automática:** Google Translate y DeepL ofrecen traducciones en tiempo real entre múltiples idiomas.
  - **Análisis de Sentimiento:** Empresas analizan opiniones en redes sociales para evaluar la percepción de su marca.

- **Reconocimiento de Voz:** Asistentes como Siri y Alexa transcriben y responden a comandos de voz.
- **Chatbots y Asistentes Virtuales:** Soporte al cliente automatizado que entiende y responde en lenguaje natural.

## Procesamiento Inteligente de Documentos

Utiliza IA para automatizar la extracción y procesamiento de información de documentos. Combina PLN, visión por computador y aprendizaje automático para manejar documentos como facturas, contratos y formularios.

## Inteligencia Artificial General (AGI)

La AGI se refiere a sistemas de IA con capacidad para entender, aprender y aplicar inteligencia de manera general, similar a la humana. A diferencia de la IA estrecha (narrow), que se especializa en tareas específicas, la AGI aspira a manejar cualquier tarea intelectual.

El camino hacia la AGI implica avances significativos en modelos y arquitecturas.

- **Modelos Fundacionales (Foundational models):** Grandes modelos pre-entrenados en enormes conjuntos de datos, adaptables a múltiples tareas sin necesidad de re-entrenamiento. Eliminan la necesidad de hacer fine-tuning.
- **Modelos Generativos (Generative AI):** Modelos capaces de generar contenido nuevo (texto, imágenes, audio) a partir de los datos aprendidos.
  - **Riesgo de seguridad:** Puede generar conceptos que no existen en los datos de entrenamiento al poder interpolar entre conceptos conocidos.
- **IA Física (Physical AI):** Permite a las máquinas percibir, entender y realizar acciones complejas en el mundo real (físico).

**Tipos de modelos generativos:** texto-a-texto, texto-a-imagen, texto-a-audio, texto-a-video, texto-a-3d, imagen-a-video, imagen-a-audio, video-a-3d,... (X-a-X)

- **LLMs (Large Language Models):** Son modelos entrenados para predecir la siguiente palabra en una oración. La innovación se da en la observación de que cuando se entrena con suficientes datos y complejidad, se convierten en un “autocompletar con asteroides”, capaces de memorizar una gran cantidad de información y de generalizar e interpolar entre conceptos. No generan conocimiento nuevo, solo interpolan entre puntos conocidos.
  - **Ejemplos:** GPT-3 (175B de parámetros – 175GB de VRAM en 32bits), GPT-4 (~1.8T de parámetros – 1.8TB VRAM en 32bits)
- **Asistentes:** Modelos de lenguaje (LLM) con los que se interactúa de forma conversacional.
  - **Prompt:** “Eres un asistente virtual. Human: {Hola que tal?}. Response:”

- **MLLMs (Multimodal Large Language Models)**: Modelos de lenguaje que procesan múltiples tipos de datos, como texto, imágenes y audio. Ejemplo: GPT4o
- **LRLMs (Large Reasoning Models)**: Modelos de lenguaje enfocados en mejorar las capacidades de razonamiento y resolución de problemas complejos.
- **Otros**: GANs (Generative Adversarial Networks), GANs (Generative Adversarial Networks), Diffusion Models

### **Costes de Entrenamiento e Inferencia**

El entrenamiento de modelos grandes es costoso y requiere recursos significativos.

- **Entrenamiento**: Suelen costar cientos de millones (\$/€). Por ejemplo, entrenar GPT-4 se estima que costó unos 100 millones de dólares (solo en costes computacionales).
- **Hardware necesario**: Granjas con cientos de miles de GPUs y TPUs de última generación.
  - **Coste de H200 (single GPU)**: ~30,000-40,000\$
  - **Coste de DGX H200 (Workstation)**: ~500,000\$
- **Captura de Datos**: Implica el esfuerzo de miles de empleados para etiquetar datos y mejorar la calidad de las respuestas.

### **Problema de las alucinaciones en modelos de lenguaje (LLMs)**

Las alucinaciones en los modelos de lenguaje son respuestas generadas que, aunque puedan parecer coherentes y plausibles, no se basan en datos reales o precisos. Este fenómeno ocurre porque los LLMs están diseñados para predecir la siguiente palabra en una secuencia, basándose en patrones aprendidos durante su entrenamiento, sin una comprensión real del mundo o verificación de hechos.

#### **Causas de las alucinaciones:**

- **Limitaciones en los datos de entrenamiento**: Si el modelo no ha sido expuesto a cierta información durante su entrenamiento, puede generar respuestas incorrectas o inventadas.
- **Sesgos y errores en los datos**: Datos de entrenamiento con información errónea o sesgada pueden llevar al modelo a generar respuestas inexactas.
- **Falta de mecanismos de verificación**: Los LLMs no tienen la capacidad intrínseca de verificar la veracidad de sus respuestas en tiempo real.

### **Tamaño de las Ventanas Contextuales**

La ventana contextual se refiere a la cantidad de información que un modelo puede procesar simultáneamente. Modelos como GPT-4 tienen ventanas contextuales de hasta 32,000 tokens, permitiendo mantener coherencia en textos largos.

## Arquitecturas RAG (Retrieval Augmented Generation)

Las arquitecturas RAG (Generación Aumentada por Recuperación) combinan modelos de lenguaje con sistemas de recuperación de información para mejorar la precisión y relevancia de las respuestas generadas. Este enfoque ayuda a mitigar el problema de las alucinaciones al proporcionar al modelo acceso a información actualizada y verificada durante el proceso de generación.

### Cómo funcionan las arquitecturas RAG:

1. **Consulta del usuario:** El usuario proporciona una entrada o pregunta.
2. **Recuperación de información:** El sistema busca en una base de datos o corpus relevante documentos o fragmentos que puedan contener la respuesta.
3. **Generación de respuesta:** El modelo de lenguaje utiliza tanto la consulta del usuario como la información recuperada para generar una respuesta más precisa y fundamentada.

## Paradigmas: Computación en Tiempo de Entrenamiento vs. Inferencia

- **Computación en Tiempo de Entrenamiento (train-time compute):** Computación utilizada durante la fase de entrenamiento del modelo.
  - Se enfoca en optimizar los parámetros del modelo para que generalice bien en distintas tareas (“one-shot”).
  - **Ejemplo:** “Ver la disposición de un tablero de ajedrez y decidir qué pieza mover”
- **Computación en Tiempo de Inferencia (test-time compute):** Computación utilizada durante la fase de inferencia, cuando el modelo responde.
  - Nuevo paradigma que permite al modelo “razonar” usando más tiempo en tareas complejas (similar a un Chain-of-Thought), mejorando su precisión y eficiencia en problemas difíciles mediante un procesamiento adicional
  - **Ejemplo:** “Ver la disposición de un tablero de ajedrez, hacer varias jugadas mentales con las diferentes piezas (de forma no exhaustiva), y luego decidir qué pieza mover”

## Leyes de Escalado (Scaling Laws)

Describen cómo el rendimiento de los modelos mejora al aumentar:

- **Computación:** Mayor poder computacional permite entrenar modelos más complejos.
- **Datos:** Más datos, y de mayor calidad, proporcionan mejor generalización.
- **Parámetros:** Más parámetros permiten capturar patrones más detallados y complejos.

**\*Nota personal sobre las Scaling Laws:** Las leyes de escalado parecen estar alcanzando un “punto muerto” o un “muro”, en el que las mejoras de rendimiento se vuelven marginales pese

al aumento de computación, la calidad de los datos y/o el tamaño de los modelos. Esto intuitivamente tiene sentido, ya que si nos limitamos a resolver una tarea centrándonos exclusivamente en predecir la siguiente palabra, sin descomponerla en sus componentes principales, acabaremos con una visión local y superficial (limitada a un único nivel de profundidad), lo que dificultará significativamente la resolución de tareas más complejas. En cambio, al incorporar estrategias de computación en tiempo de inferencia, análogo a los algoritmos de búsqueda DFS, podremos explorar estas tareas a diferentes niveles de profundidad, lo que facilitará la resolución y el análisis de problemas más complejos.

### **The Bitter Lesson (Rich Sutton)**

Un ensayo que argumenta que los mayores avances en IA provienen de métodos que aprovechan el aumento del poder computacional y el aprendizaje automático general, en lugar de incorporar conocimiento específico del dominio.

### **Dificultad de Evaluación**

- **Benchmarks limitados:** Las pruebas estándar pueden no reflejar las capacidades reales en situaciones del mundo real. Además, muchos modelos se entranan usando ciertos benchmarks como referencia (overfit), lo que falsea su rendimiento real.
- **Evaluaciones Colaborativas (LMArena):** Plataformas donde la comunidad contribuye a evaluar y mejorar modelos al usarlos, promoviendo transparencia y colaboración.

### **Ejemplos de Modelos Actuales**

- **BERT:** Modelo de Google para tareas de comprensión del lenguaje, utilizado en su motor de búsqueda.
- **GPT-3:** Modelo de OpenAI, con 175 mil millones de parámetros, capaz de generar texto coherente y realizar tareas como traducción y resumen.
- **GPT-4o:** Modelo de OpenAI, que puede procesar y generar texto, imágenes y audio de manera nativa.
- **o1:** Modelo de última generación de OpenAI, que estrena nuevo paradigma (test-time), y que dedica más tiempo al razonamiento antes de responder, lo que le permite abordar tareas complejas y resolver problemas más difíciles que modelos anteriores.
- **DALL·E 2:** Genera imágenes a partir de descripciones textuales, combinando procesamiento de lenguaje y visión por computadora.

## 5 Etapas de la AGI

- **Nivel 1 (IA Conversacional / Chatbots):** Mantienen conversaciones avanzadas y responden preguntas en lenguaje natural. ("Autocompletar++")
  - **Ejemplo:** GPT-4, Claude 3.5
  - **Fecha:** 2020-2022
- **Nivel 2 (Razonadores / Reasoners):** Realizan razonamientos complejos y desglosan problemas paso a paso. ("LLM + DFS")
  - **Ejemplo:** o1
  - **Fecha:** 2024-2025
- **Nivel 3 (Agentes Autónomos / Agents):** Actúan de manera autónoma en entornos controlados, realizando tareas específicas. ("LLM robusto y confiable")
  - **Ejemplo:** Claude 3.5/oct24 (experimental)
  - **Fecha:** 2025-2027
- **Nivel 4 (Innovadores / Innovators):** Ayudan en la generación de ideas y soluciones innovadoras para nuevos problemas. ("Generan nuevo conocimiento, derivado composicionalmente a partir del existente")
  - **Ejemplo:** -
  - **Fecha:** 2028-2032
- **Nivel 5 (Organización Autónoma / Organizations):** IA que puede gestionar y operar una organización de forma autónoma. ("Modelos confiables y altamente integrados en el ecosistema de la organización")
  - **Ejemplo:** -
  - **Fecha:** 2035-2040

## Principios Matemáticos y Evolución de la IA

Los fundamentos matemáticos de las redes neuronales y el aprendizaje automático datan de 1957, con el perceptrón de Frank Rosenblatt. Sin embargo, varias limitaciones técnicas llevaron a períodos conocidos como "invierno de la IA", donde el interés y la inversión disminuyeron.

### Factores que han impulsado la IA Moderna:

- **Almacenamiento Masivo de Datos:** La disponibilidad de grandes conjuntos de datos como ImageNet (con más de 14 millones de imágenes) permitió entrenar modelos más precisos.
- **Computación de Alto Rendimiento:** El avance en hardware, especialmente GPUs, hizo posible entrenar redes neuronales profundas de manera eficiente.

- **Redescubrimiento y Mejora de las Redes Neuronales:** Innovaciones como las funciones de activación ReLU, técnicas de regularización y optimizadores avanzados renovaron la confianza en las redes neuronales.

### Referencias Históricas Clave

- **1805-1809:** Legendre y Gauss utilizaron la regresión lineal por mínimos cuadrados para encontrar un buen ajuste lineal aproximado a un conjunto de puntos para predecir el movimiento planetario.
- **1957:** Introducción del perceptrón por Frank Rosenblatt, marcando el inicio de las redes neuronales.
- **Años 70 y 80:** Primer "invierno de la IA" debido a limitaciones técnicas y sobreexpectativas.
- **2012:** AlexNet gana la competición ImageNet, demostrando el poder de las redes neuronales profundas y reavivando el interés en el aprendizaje profundo.
- **Actualidad:** Proliferación de modelos avanzados, aumento exponencial en parámetros y capacidades, IA generativa, y debates éticos sobre el futuro de la IA.

## Gestión de datos corporativos

### Gestión de Datos Corporativos

La gestión de datos corporativos es fundamental en cualquier organización. Los sistemas de información están compuestos por **hardware** (subsistema físico), **software** (subsistema lógico), **datos, métodos o procedimientos, y personas**. Estos elementos apoyan tres niveles de decisión organizacional:

- **Alta dirección:** Enfocada en decisiones estratégicas.
- **Dirección táctica:** Implementa y supervisa las estrategias.
- **Nivel operativo:** Alinea las operaciones diarias con los objetivos tácticos.

#### Fuentes de Información

Las organizaciones utilizan diversas fuentes de información para la toma de decisiones:

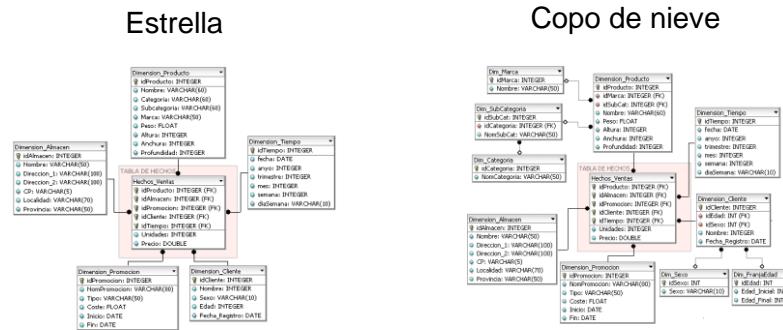
- **Bases de datos corporativas:** Pueden ser relacionales, espaciales, temporales, documentales o multimedia.
- **Webs y redes sociales:** Análisis de opiniones y preferencias de usuarios.
- **Fuentes OSINT (Open Source Intelligence):** Datos de fuentes abiertas.
- **Internet de las Cosas (IoT):** Dispositivos autónomos que recopilan y transmiten datos a través de internet.

#### Almacén de Datos (Data Warehouse)

Un **data warehouse** es una colección integrada y no volátil de datos orientada a un ámbito específico. Su estructura facilita la toma de decisiones a través del almacenamiento de **datamarts**, los cuales modelan hechos, atributos y dimensiones.

- **Modelo Multidimensional (Hipercubo):**
  - **Hechos:** Datos o conceptos de interés (ej.: ventas, personal).
  - **Atributos:** Aspectos medibles de los hechos (ej.: importe, cantidad).
  - **Dimensiones:** Detalles vinculados a los hechos (ej.: tiempo, lugar).
- **Tipos de Modelos:**
  - **Estrella:** Un hecho central rodeado por dimensiones.
  - **Estrella Simple:** Permite un único camino de agregación.

- **Copo de Nieve:** Permite múltiples caminos de agregación.



## Datamart

Un **datamart** es un almacén de datos específico, centrado en un área de negocio. Estructurado en forma de estrella, facilita la consulta y el análisis de datos para un departamento específico.

### Características:

- Usuarios limitados.
- Enfoque en un área específica.
- Función de apoyo.

## Data Lake

Un **data lake** es un almacén no estructurado de información en bruto, accesible y centralizado. Puede contener datos estructurados, semiestructurados (JSON, CSV), no estructurados (emails, tweets) y binarios (fotos, videos). Herramientas como **Apache Hadoop** son esenciales para la gestión de data lakes.

## Arquitecturas OLTP y OLAP

- **OLTP (On-Line Transaction Processing):** Procesamiento transaccional en tiempo real, optimizado para **transacciones** con bases de datos relacionales, con datos detallados y normalizados.
- **OLAP (On-Line Analytical Processing):** Procesamiento analítico orientado a consultas complejas para apoyar la toma de decisiones mediante cubos OLAP.

### Operadores OLAP:

- **Drill:** Desglosa datos por dimensiones.
- **Roll:** Agrega datos por dimensiones.
- **Slice & Dice:** Selecciona y proyecta datos en nuevas vistas.
- **Pivot:** Reorienta dimensiones para recalcular celdas.

### Implementaciones OLAP:

- **ROLAP (Relational OLAP)**: Construido sobre bases de datos relacionales.
- **MOLAP (Multidimensional OLAP)**: Basado en estructuras multidimensionales.
- **HOLAP (Hybrid OLAP)**: Combina ROLAP y MOLAP.

### Esquemas ROLAP

- **Estrella**: Contiene una tabla de hechos central rodeada de tablas de dimensiones, diseñada para simplicidad y eficiencia.
- **Copo de Nieve**: Implementa dimensiones con múltiples tablas, optimizando espacio pero reduciendo rendimiento.

### Elementos de un Almacén de Datos

- **Metadatos**: Documentan tablas, columnas y tipos de datos.
- **Middleware**: Permite la interoperabilidad en plataformas heterogéneas.
- **ETL (Extraction, Transformation & Load)**:
  - **Extracción**: Obtención de datos en bruto.
  - **Transformación**: Limpieza y estructuración de datos.
  - **Carga**: Creación y llenado de datamarts con información depurada.

### Herramientas de Explotación de Datos

- **Sistemas de Información Ejecutiva (EIS)**: Monitoreo de variables clave.
- **Dashboard o Cuadro de Mando Integral (CMI)**: Reportes y análisis interactivos.
- **Minería de Datos**: Descubrimiento de patrones en grandes volúmenes de datos.

# Big Data

Big Data es un término que describe conjuntos de datos demasiado grandes y complejos para ser procesados por métodos tradicionales. Su gestión se centra en las **5 V's**:

- **Volumen:** Cantidades masivas de datos.
- **Velocidad:** Procesamiento y análisis en tiempo real.
- **Variedad:** Diversidad de formatos y fuentes.
- **Veracidad:** Fiabilidad de los datos.
- **Valor:** Conocimiento obtenido de los datos.

## Infraestructura de Almacenamiento

### Bases de Datos NoSQL:

- No requieren estructuras fijas.
- No soportan operaciones JOIN.
- No garantizan completamente ACID.
- Escalan horizontalmente.

### Tipos de NoSQL:

- **Orientadas a Documentos:** Almacenan datos en JSON o XML (ejemplo: MongoDB).
- **Almacenes Clave/Valor:** Pares clave-valor (ejemplo: Redis).
- **Organizadas por Columnas:** Datos en columnas (ejemplo: Cassandra).
- **Basadas en Grafos:** Estructuradas en nodos y relaciones (ejemplo: Neo4j).

## Infraestructura de Procesamiento

Dependiendo de la necesidad de procesamiento:

- **Procesamiento Batch:** Ideal para grandes volúmenes de datos con herramientas como HDFS y MapReduce.
- **Procesamiento Streaming:** Para flujos continuos de datos en tiempo real, usando Apache Kafka y Storm.
- **Procesamiento Híbrido:** Combina batch y streaming, con arquitecturas como Lambda y Kappa.

## Ecosistema Apache Hadoop

Hadoop es un marco de trabajo de código abierto para aplicaciones distribuidas que gestionan grandes volúmenes de datos.

### Componentes Principales:

- **HDFS:** Sistema de archivos distribuido.
- **MapReduce:** Modelo de programación para computación paralela.
- **YARN:** Gestor de recursos.
- **Spark:** Procesamiento de datos en memoria.
- **Pig y Hive:** Procesamiento basado en consultas.
- **HBase:** Base de datos NoSQL.
- **Mahout y Spark MLlib:** Algoritmos de machine learning.
- **Zookeeper:** Gestión de clústeres.
- **Oozie:** Planificación de trabajos.

# Minería de Datos

La **Minería de Datos** es el proceso de extraer conocimiento útil, comprensible y previamente desconocido a partir de grandes volúmenes de datos almacenados en diversos formatos. Este conocimiento permite identificar patrones, tendencias y relaciones ocultas que pueden ser cruciales para la toma de decisiones estratégicas en una organización.

## Modelo CRISP-DM

El **CRISP-DM** (CRoss Industry Standard Process for Data Mining): Es el modelo estándar más utilizado para estructurar proyectos de minería de datos. Este modelo abierto y flexible consta de seis fases interrelacionadas:

- **Fase 1 - Comprensión del negocio:** Se profundiza en los objetivos y requisitos desde una perspectiva empresarial, identificando problemas y oportunidades donde la minería de datos puede aportar valor.
- **Fase 2 - Comprensión de los datos:** Se exploran y analizan los datos disponibles para evaluar su calidad, relevancia y adecuación a los objetivos planteados, afinando así los objetivos iniciales.
- **Fase 3 - Preparación de los datos:** Implica la recopilación, limpieza, integración y transformación de los datos para construir el conjunto de datos final que se utilizará en la fase de modelado.
- **Fase 4 - Modelado:** Se seleccionan y aplican algoritmos y técnicas de modelado adecuados, ajustando sus parámetros para optimizar el rendimiento de los modelos.
- **Fase 5 - Evaluación:** Se evalúan los modelos construidos no solo desde una perspectiva técnica (precisión, error, etc.), sino también en términos de su aportación al negocio y cumplimiento de los objetivos iniciales.
- **Fase 6 - Distribución:** El conocimiento obtenido se presenta y distribuye en la organización, integrándolo en los procesos de toma de decisiones y asegurando su adopción efectiva.

## Tareas y Tipología de Problemas

- **Predictivas:** Buscan predecir valores o categorías futuras basándose en datos históricos etiquetados. Incluyen:
  - **Clasificación (multiclase / multi-class):** Asignar una etiqueta de clase a instancias basándose en características predictoras.
  - **Categorización (multietiqueta / multi-label):** Asignar múltiples etiquetas a cada instancia.
  - **Priorización (ordenación):** Ordenar instancias según una métrica o criterio específico.
  - **Regresión:** Predecir valores numéricos continuos.

- **Descriptivas:** Pretenden descubrir patrones y relaciones en datos no etiquetados, proporcionando una comprensión más profunda del conjunto de datos. Incluyen:
  - **Agrupamiento (clustering):** Agrupar instancias similares sin predefinir categorías.
  - **Correlación:** Identificar relaciones significativas entre variables.
  - **Reglas de asociación:** Descubrir relaciones frecuentes entre variables en grandes bases de datos.
  - **Detección de anomalías:** Identificar instancias que se desvían significativamente del comportamiento normal.

## Modelos de Representación y Preparación de Datos

- **Extracción de características:** Cada objeto o instancia se representa como un vector de características (atributos) que capturan información relevante para el análisis.
- **Técnicas de preparación:**
  - **Discretización:** Convertir atributos numéricos continuos en categorías discretas (por ejemplo, mediante binning).
  - **Numerización:** Transformar atributos categóricos nominales en representaciones numéricas (como codificación one-hot).
  - **Gestión de valores faltantes:** Imputación de datos o eliminación de instancias incompletas para manejar la ausencia de valores.
  - **Reducción de dimensionalidad:** Simplificar el conjunto de datos reduciendo el número de variables, manteniendo la mayor cantidad posible de información relevante. Técnicas como Análisis de Componentes Principales (PCA), autoencoders o selección basada en ganancia de información.

## Técnicas de Modelado

- **Aprendizaje Perezoso (Lazy Learning):** Los algoritmos retrasan la generalización hasta el momento de la predicción. No construyen un modelo explícito durante el entrenamiento. Ejemplo:
  - **K-NN (K-Nearest Neighbors):** Clasifica una instancia basándose en las clases de sus vecinos más cercanos en el espacio de características.
- **Aprendizaje Anticipativo (Eager Learning):** Los algoritmos construyen un modelo generalizado durante el entrenamiento, que se utiliza para realizar predicciones futuras. Incluye:
  - **Métodos bayesianos:** Utilizan probabilidades para predecir la clase más probable.

- **Árboles de decisión:** Modelos en forma de árbol que representan decisiones y sus posibles consecuencias.
- **Redes neuronales:** Modelos inspirados en la estructura del cerebro humano, capaces de capturar relaciones complejas.
- **Máquinas de vectores de soporte (SVM):** Algoritmos que buscan el hiperplano que mejor separa las clases en el espacio de características.
- **Algoritmos evolutivos:** Utilizan principios de evolución biológica para optimizar soluciones.
- **Ensembles o Meta-Clasificadores:** Combinan múltiples modelos para mejorar la precisión y robustez de las predicciones. Estrategias comunes:
  - **Bagging:** Entrenar múltiples modelos en subconjuntos aleatorios del conjunto de datos y promediar sus predicciones.
  - **Boosting:** Construir secuencialmente modelos donde cada uno corrige los errores del anterior.
  - **Stacking:** Combinar las predicciones de varios modelos utilizando un modelo de nivel superior que aprende cómo combinar mejor estas predicciones.

## Evaluación de Modelos

- **Modos de evaluación:**
  - **Split (División simple):** Separar los datos en conjuntos de entrenamiento y prueba (por ejemplo, 70% y 30%).
  - **Validación Cruzada (k-fold):** Dividir los datos en k subconjuntos; entrenar y probar el modelo k veces, cada vez con un subconjunto diferente como prueba.
  - **Leave-One-Out (LOOCV):** Caso especial de validación cruzada donde k es igual al número de instancias; cada instancia se usa una vez como prueba.
  - **Bootstrap:** Muestreo con reemplazo para crear múltiples conjuntos de entrenamiento y evaluar la variabilidad del modelo.
- **Matriz de confusión:** Es una tabla que resume el rendimiento del modelo en términos de verdaderos positivos (TP), verdaderos negativos (TN), falsos positivos (FP) y falsos negativos (FN).

	<b>Predictión Positiva</b>	<b>Predictión Negativa</b>
<b>Real Positiva</b>	Verdadero Positivo (TP)	Falso Negativo (FN)
<b>Real Negativa</b>	Falso Positivo (FP)	Verdadero Negativo (TN)

- **Medidas clave: (Principales)**

- **Accuracy (Precisión general):** Proporción de predicciones correctas en relación con el total de predicciones.
  - **Fórmula:**  $(TP + TN) / (TP + TN + FP + FN)$
- **Precision (Precisión o Valor Predictivo Positivo [PV+]):** Indica la proporción de predicciones positivas que son correctas.
  - **Fórmula:**  $TP / (TP + FP)$
- **Recall (Exhaustividad, Sensibilidad o True Positive Rate [TPR]):** Mide la capacidad del modelo para identificar correctamente los casos positivos.
  - **Fórmula:**  $TP / (TP + FN)$
- **F-Score (F1):** Media armónica de la precisión y la exhaustividad, equilibrando estas dos métricas.
  - **Fórmula:**  $2 * (\text{Precision} * \text{Recall}) / (\text{Precision} + \text{Recall})$

- **Medidas clave: (Principales 2)**

- **True Positive Rate (TPR) o Sensibilidad:** Proporción de casos positivos correctamente identificados por el modelo, también conocida como Recall.
  - **Fórmula:**  $TP / (TP + FN)$
- **False Positive Rate (FPR) o Tasa de Falsos Positivos:** Proporción de casos negativos que el modelo clasifica incorrectamente como positivos.
  - **Fórmula:**  $FP / (FP + TN)$
- **False Negative Rate (FNR) o Tasa de Falsos Negativos:** Proporción de casos positivos que el modelo no detecta (clasifica como negativos).
  - **Fórmula:**  $FN / (TP + FN)$
- **True Negative Rate (TNR) o Especificidad:** Proporción de casos negativos que el modelo clasifica correctamente como negativos.
  - **Fórmula:**  $TN / (TN + FP)$
- **Otras métricas:** Hay más métricas de estas pero con el mareo de nombres que hay, suficiente. (Nota: Ojo con las traducciones!)
  - **Ver tabla:** [https://es.wikipedia.org/wiki/Curva\\_ROC](https://es.wikipedia.org/wiki/Curva_ROC)
- **Curva ROC (Receiver Operating Characteristic):** Muestra el rendimiento de un clasificador binario comparando la Tasa de Verdaderos Positivos (Recall) y la Tasa de Falsos Positivos para distintos umbrales.
  - Permite visualizar cómo el modelo equilibra estos dos aspectos al variar el umbral de decisión.
  - Una curva que se acerca al vértice superior izquierdo indica un mejor rendimiento.

- **Área Bajo la Curva (AUC - Area Under the Curve):** Métrica que cuantifica el rendimiento general del modelo en la Curva ROC.
  - Un AUC de 1 representa un modelo perfecto, mientras que un AUC de 0.5 indica un modelo sin capacidad de clasificación (aleatorio).
  - Cuanto mayor sea el AUC, mejor será la capacidad del modelo para separar las clases correctamente.
- **Evaluación de modelos de regresión:** Se utilizan métricas como:
  - **MSE (Mean Squared Error):** Promedio de los cuadrados de los errores.
  - **RMSE (Root Mean Squared Error):** Raíz cuadrada del MSE, proporciona una medida en las mismas unidades que la variable objetivo.
  - **MAE (Mean Absolute Error):** Promedio de los valores absolutos de los errores.
  - **RSE (Residual Standard Error):** Medida de la calidad de un modelo de regresión.
  - **Coeficiente de correlación de Pearson (r):** Indica la fuerza y dirección de la relación lineal entre dos variables.
- **Evaluación de modelos de agrupamiento:** Se pueden utilizar medidas como:
  - **Verosimilitud (Likelihood):** Evalúa qué tan probable es que los datos se generen a partir del modelo propuesto.
  - **Índice de Silueta (Silhouette):** Mide qué tan similar es una instancia a su propio cluster en comparación con otros clusters.
  - **Coeficiente de Dunn:** Evalúa la compactidad y separación de los clusters.
- **Evaluación de modelos de reglas de asociación:**
  - **Soporte (Cobertura):** Proporción de instancias donde la regla es aplicable.
  - **Confianza:** Probabilidad de que la consecuencia de la regla sea cierta cuando la antecedente es cierta.
  - **Lift:** Medida de la importancia de una regla, calculada como la razón entre la confianza de la regla y la probabilidad de la consecuencia.

#### Diferencias entre Verosimilitud y Probabilidad:

- **Probabilidad:** Mide la posibilidad de que ocurra un evento dado un modelo o distribución conocida.
- **Verosimilitud (Likelihood):** Mide qué tan bien un modelo explica un conjunto de datos observado. En modelado estadístico, se utiliza para estimar parámetros que maximizan la verosimilitud de observar los datos dados.

### Difusión y Estándares

La **explicabilidad** de los modelos es crucial para su adopción en entornos empresariales. Modelos interpretables facilitan la confianza y comprensión por parte de los usuarios finales y stakeholders.

El **PMML (Predictive Model Markup Language)** es un estándar basado en XML que permite definir y compartir modelos de minería de datos entre diferentes herramientas y plataformas. Al proporcionar un formato común, facilita la integración de modelos en sistemas de producción sin necesidad de reimplementarlos, acelerando su despliegue y uso efectivo en la organización.

# Casos prácticos sobre clasificación

## Caso práctico 1: Clasificador para Detección de Cáncer

Supón un clasificador que detecta cáncer (sí/no) con un **accuracy del 99%**. Si la tasa de personas con cáncer es muy baja, un clasificador que siempre predice "no" puede obtener este alto accuracy al fallar en identificar los casos positivos.

Por otro lado, un clasificador con un **recall del 99%** detecta casi todos los casos de cáncer, pero puede tener falsos positivos altos, lo que implica realizar pruebas innecesarias.

Un clasificador con **precisión del 99%** se enfoca en minimizar falsos positivos, asegurando que la mayoría de diagnósticos positivos son correctos. Este ejemplo ilustra cómo las métricas deben seleccionarse en función de la importancia de identificar verdaderos positivos o reducir falsos positivos.

## Caso práctico 2: Clasificador para Detección de Cáncer (con cálculo)

Imaginemos un clasificador para detectar cáncer en un conjunto de datos con 1,000 pacientes, donde solo 10 realmente tienen cáncer. Esto significa que hay **10 casos positivos y 990 casos negativos**.

Supongamos que evaluamos dos clasificadores en este conjunto de datos:

### 1. Clasificador con alto “Accuracy” pero bajo “Precision” y “Recall”

Este clasificador ciego predice que TODOS los pacientes NO tienen cáncer. Así, tendría una precisión general (accuracy) alta debido al bajo número de casos positivos:

- **TP (Verdaderos Positivos)**: 0 (no identificó ningún caso positivo correctamente)
- **TN (Verdaderos Negativos)**: 990
- **FP (Falsos Positivos)**: 0
- **FN (Falsos Negativos)**: 10 (falló en detectar todos los casos de cáncer)

### Cálculo de métricas:

- $$\begin{aligned} \text{Accuracy} &= (TP + TN) / (TP + TN + FP + FN) \\ &= (0 + 990) / (0 + 990 + 0 + 10) \\ &= 990 / 1000 \\ &= 0.99 \text{ o } 99\% \end{aligned}$$

Aunque el **accuracy es del 99%**, este modelo es poco útil para detectar cáncer, ya que **no identifica ningún caso positivo** (0% recall y precisión).

### 2. Clasificador con alto “Recall” pero menor “Precision”

Otro clasificador se centra en identificar todos los casos de cáncer, aunque genere algunos falsos positivos. Este clasificador detecta 9 de los 10 pacientes con cáncer, pero también clasifica erróneamente a 20 pacientes sanos como positivos.

- **TP (Verdaderos Positivos)**: 9

- **TN (Verdaderos Negativos):** 970
- **FP (Falsos Positivos):** 20
- **FN (Falsos Negativos):** 1

**Cálculo de métricas:**

- **Accuracy** =  $(TP + TN) / (TP + TN + FP + FN)$   
 $= (9 + 970) / (9 + 970 + 20 + 1)$   
 $= 979 / 1000$   
 $= 0.979$  o **97.9%**
- **Precision** =  $TP / (TP + FP)$   
 $= 9 / (9 + 20)$   
 $= 9 / 29$   
 $= 0.31$  o **31%**
- **Recall** =  $TP / (TP + FN)$   
 $= 9 / (9 + 1)$   
 $= 9 / 10$   
 $= 0.9$  o **90%**

Aunque el **accuracy** es del 97.9%, similar al primer clasificador, este modelo es más efectivo en la detección de casos positivos gracias a un **recall del 90%**, capturando casi todos los casos de cáncer. Sin embargo, su **precisión es baja** (31%), lo que significa que solo el 31% de los diagnósticos positivos son realmente correctos.

## Tabla de nomenclaturas comunes

Término en Inglés	Término en Español	Definición
<b>Accuracy</b>	Precisión	Proporción de predicciones correctas.
<b>Precision</b>	Valor Predictivo Positivo	Proporción de verdaderos positivos entre todos los positivos predichos.
<b>Recall</b>	Sensibilidad o Exhaustividad	Proporción de verdaderos positivos detectados sobre el total de positivos reales.
<b>Specificity</b>	Especificidad	Proporción de verdaderos negativos detectados sobre el total de negativos reales.
<b>F-Score</b>	Puntaje F	Media armónica de la precisión y la exhaustividad.
<b>True Positive (TP)</b>	Verdadero Positivo	Instancias correctamente predichas como positivas.
<b>True Negative (TN)</b>	Verdadero Negativo	Instancias correctamente predichas como negativas.
<b>False Positive (FP)</b>	Falso Positivo	Instancias incorrectamente predichas como positivas.
<b>False Negative (FN)</b>	Falso Negativo	Instancias incorrectamente predichas como negativas.

Fuentes:

[https://es.wikipedia.org/wiki/Curva\\_ROC](https://es.wikipedia.org/wiki/Curva_ROC)

## Gobernanza del dato

# Gobernanza del dato y metodologías

La gobernanza del dato es un enfoque estratégico para convertir los datos en un activo fundamental de la organización. Implica el ejercicio de autoridad, control y toma de decisiones compartida sobre la gestión de los activos de datos. Esto abarca la definición de políticas y procedimientos para la recopilación, almacenamiento, protección y uso de los datos, asignando responsables e implementando sistemas de control. Las responsabilidades incluyen establecer la infraestructura, configurar y mantener procesos y políticas, e identificar a quienes gestionarán y protegerán los datos. Sus componentes principales son **Personas, Procesos, Tecnología y Mejora continua**, y se rige por principios como ser accesible y seguro, sostenible, y orientado a la mejora continua.

### Marco de gobernanza del dato

El marco de gobernanza establece las bases para la estrategia de gestión de datos. Define reglas, actividades, responsabilidades, procedimientos y procesos para gestionar los datos. Los aspectos clave incluyen el alcance de los datos, estructura organizativa, estándares y políticas de datos, supervisión y métricas de éxito. Entre los marcos de referencia destacan **DMBOK, TOGAF, COBIT y DGI**.

### Metodología DAMA

La **Data Management Association** (DAMA) ofrece un marco de mejores prácticas, recogido en el **DMBOK**, para gestionar los datos como recurso empresarial y asegurar su uso eficaz en la toma de decisiones. DAMA organiza la gestión de datos en torno al gobierno del dato, proporcionando herramientas para el control de la información.

### Áreas de conocimiento de DAMA

La metodología DAMA identifica **11 áreas de conocimiento** clave:

- **Gobierno de datos**
- **Arquitectura de datos:** Define y diseña las vistas maestras para satisfacer las necesidades de datos.
- **Modelado y diseño de datos:** Implementa y mantiene soluciones para cumplir con los requerimientos.
- **Almacenamiento y operaciones de datos:** Gestiona la infraestructura, licencias y copias de seguridad.
- **Seguridad de datos:** Autenticación, autorización y auditoría de acceso.
- **Calidad de datos:** Mide, evalúa y asegura la calidad.

- **Integración e interoperabilidad de datos:** Adquisición y transformación de datos.
- **Gestión de documentos y contenido:** Facilita el acceso e integración de datos estructurados y no estructurados.
- **Datos maestros y de referencia:** Controla valores de datos maestros para consistencia.
- **Data Warehousing y Business Intelligence:** Soporte de decisiones y análisis.
- **Gestión de metadatos:** Administración de información derivada de los datos.

### **Principios de DAMA**

Los principios del gobierno del dato según DAMA son **Accesibilidad, Consistencia, Exactitud, Seguridad y Auditabilidad** para garantizar un uso correcto de los datos.

### **Oficina del dato**

La Oficina del Dato coordina y mejora la gobernanza en una organización, define políticas, estrategias de datos, procesos de gestión y supervisa su cumplimiento. También brinda apoyo en temas de datos y establece roles y modelos de relación.

### **Gestión de datos abiertos**

Para gestionar datos abiertos, se asegura la disponibilidad en el portal, interoperabilidad de catálogos, y se usan metadatos para describir los datos. La seguridad implica anonimización y control de accesos, y la calidad se evalúa mediante indicadores técnicos y funcionales. La **ética del dato** es fundamental en este ámbito.

### **Datos maestros y catálogo de datos**

Los **datos maestros** son esenciales para las operaciones de un negocio, siendo los más complejos y valiosos.

Un **catálogo de datos** permite inventariar y localizar activos de datos, optimizando su uso comercial o analítico.

# Modelo estratégico, operativo y organizativo del dato

## Gobierno del dato

El gobierno del dato se define como un enfoque de trabajo diseñado para establecer los cimientos que permitan convertir los datos en un activo estratégico para la organización. Su propósito es implementar un programa que gestione los datos empresariales y fomente la mejora continua dentro de la compañía, abordando los aspectos de personas, procesos, tecnologías y mecanismos de mejora. Los principios fundamentales del gobierno del dato son: **esponsorizado y alineado, sostenible y escalable, accesible y seguro, ágil y tangible y orientado a la evolución y mejora continua.**

## Bases del gobierno del dato

- **Mapa de entidades de datos (Modelo Operativo):** Define qué datos posee la organización.
- **Catálogo de servicios (Modelo Operativo):** Establece cómo se gestionarán los datos.
- **Roles y responsabilidades (Modelo Organizativo):** Determina quiénes serán los participantes en el gobierno de datos.
- **Estructura organizativa (Modelo Organizativo):** Define la organización interna.
- **Comités de gobierno (Servicios y Tecnología):** Establece cómo se tomarán las decisiones.
- **Arquitectura del dato (Servicios y Tecnología):** Describe las herramientas de gobierno utilizadas.

## Modelo estratégico del dato

Este modelo establece la **estrategia organizacional** en torno a la gestión y el uso de los datos, permitiendo a la organización orientarse hacia una cultura basada en el dato. Facilita la transformación empresarial y ayuda a construir las capacidades y herramientas necesarias para afrontar grandes retos de negocio. Esto se logra mediante la identificación de las necesidades de datos, la definición de objetivos y metas en torno a su uso, y la implementación de planes y políticas para alcanzar estos objetivos.

## Modelo operativo

El modelo operativo del dato define los procesos y políticas de gestión para asegurar la **disponibilidad, integridad, usabilidad y seguridad** de los datos. Este modelo ayuda a establecer estándares y mitigar riesgos, proporcionando un marco documentado que garantice el uso y gestión adecuado de la información.

- **Inventario y mapa de datos:** Permite identificar y describir los datos disponibles en la organización.

- **Procesos y políticas:** Garantizan la seguridad, privacidad e integridad de los datos mediante políticas claras.
  - **Políticas:** Establecen las reglas para todos los involucrados en el gobierno del dato, abarcando aspectos como **calidad, privacidad, seguridad, reglas de negocio y gestión de riesgos.**
  - **Estándares:** Especifican requisitos para mejorar la toma de decisiones y la comunicación interfuncional.
  - **Procedimientos:** Definen el modo de alcanzar los estándares y políticas, detallando tareas, responsables y momentos específicos.
  - **Guías:** Proporcionan instrucciones paso a paso para aplicar los procedimientos.

### **Modelo organizativo**

Este modelo define la estructura organizativa para asegurar la implementación de la estrategia del dato. Puede adoptar distintas formas:

- **Centralizada:** El gobierno del dato (GB) asume toda la carga de trabajo.
- **Descentralizada:** Basada en comités sin un único responsable de GB.
- **Híbrida:** Combina un GB centralizado con grupos de trabajo descentralizados en áreas clave.
- **Federada:** Similar al modelo híbrido, con capas adicionales de centralización y descentralización.

**Comités de gobierno:** Estos organismos promueven y aplican la estrategia, procesos y políticas de gobierno del dato, incluyendo instancias como el **Governance Board** y el **Data Steward Council**.

**Roles y responsabilidades:** Diversos roles aseguran la gestión efectiva del dato, adaptándose a la cultura de la organización. Entre los roles principales se encuentran el **Chief Data Officer (CDO)**, **Data Protection Officer (DPO)**, **Chief Information Officer (CIO)**, **Data Owner (DO)**, **Oficina de Gobierno del Dato** y **Data Steward (DS)**.

### **Oficina de Gobierno del Dato**

Esta unidad es responsable de la gestión y el uso de los datos en la organización, con la misión de dinamizar la compartición, gestión y uso de los datos en todos los sectores de la economía y la sociedad.

- **Identificación e inventario de datos:** La oficina cataloga y documenta los datos existentes en la organización.
- **Definición de políticas y estándares:** Se encargan de la creación de directrices para la gestión de datos y el fomento de una cultura basada en el dato.

### **Cultura del dato**

La cultura del dato se refiere a la actitud organizativa frente a la gestión y uso de datos, promoviendo la toma de decisiones fundamentadas en información, la colaboración entre departamentos y el intercambio de datos. Además, se incentiva la adopción de prácticas éticas y responsables en relación con el dato, consolidando así un entorno de confianza y efectividad en el uso de este activo.

## APIs (Application Programming Interface)

### Apificación

La **apificación** es la generalización del uso de APIs en la estrategia de negocio, permitiendo exponer partes de una aplicación o sistema como APIs. Esto facilita que otras aplicaciones puedan interactuar y acceder a datos o funcionalidades del sistema original. Es un proceso clave en la digitalización y en la conexión de servicios tecnológicos.

#### Qué es una API y para qué sirve?

Una **API** (Application Programming Interface) es un conjunto de **protocolos, herramientas y definiciones** que permite a dos aplicaciones comunicarse entre sí, compartiendo datos y funcionalidades.

- **Interacción de módulos:** Actúan como interfaces que permiten la interacción entre módulos de software diferentes.
- **Usos y aplicaciones:**
  - Integración de sistemas y aplicaciones.
  - Facilitan a empresas y administraciones una gestión más eficiente y flexible de sus datos y servicios.
  - Son fundamentales para habilitar servicios modernos y escalables en entornos digitales.

#### Gestión y gobierno de APIs

El correcto funcionamiento y uso de las APIs en una organización requiere **gestión y gobierno**:

- **Gestión de APIs:**
  - Abarca las actividades necesarias para el mantenimiento y funcionamiento de las APIs.
  - **Incluye:**
    - **Documentación:** Registro claro y accesible de la funcionalidad y uso de la API.
    - **Autenticación y autorización:** Control de acceso para garantizar la seguridad.
    - **Monitorización:** Seguimiento del rendimiento y uso.
    - **Resolución de problemas:** Solución de errores para garantizar la continuidad del servicio.
- **Gobierno de APIs:**

- Se centra en la estrategia y las políticas de uso de las APIs.
- Incluye:
  - **Definición de políticas:** Establecimiento de reglas de uso.
  - **Protección de datos:** Garantía de privacidad y seguridad.
  - **Límites y monetización:** Regulación del uso y posibles modelos de ingresos.

### **Uso de las APIs en la transformación de empresas y de las Administraciones**

Las APIs son herramientas clave para impulsar la transformación digital en diversos contextos:

- **Empresas:**
  - Fomentan la **innovación** y la **colaboración** con terceros.
  - Permiten la integración y conexión de sistemas, optimizando recursos.
- **Administraciones públicas:**
  - Incrementan la **transparencia** y mejoran la **eficiencia** en la prestación de servicios.
  - Facilitan procesos internos más ágiles y servicios más personalizados para los ciudadanos.

## Automatización Robótica de Procesos (RPA)

# Automatización Robótica de Procesos (RPA)

La **Automatización Robótica de Procesos (RPA)** consiste en una tecnología emergente que permite automatizar procesos de negocio replicando las acciones de un ser humano al interactuar con la interfaz de usuario de un sistema informático. A diferencia de otras formas de automatización, RPA prescinde de las dependencias de APIs de programación y utiliza robots de software que interpretan la interfaz de aplicaciones de terceros para ejecutar tareas siguiendo los mismos pasos que un usuario humano. Estos robots son configurados o "entrenados" mediante la demostración de pasos, eliminando la necesidad de programación mediante código.

Existen dos **tipos principales** de robots RPA:

- **Robots atendidos:** Operan bajo supervisión humana directa.
- **Robots desatendidos:** Funcionan de manera autónoma, sin necesidad de intervención humana.

### Procesos susceptibles de automatización en la administración

Los procesos que pueden ser automatizados mediante RPA comparten ciertas características clave:

- **Definición basada en reglas:** Son procesos con pasos estructurados y predefinidos.
- **Volumen de trabajo elevado:** Involucran tareas repetitivas y masivas.
- **Activación mediante disparadores digitales:** Se inician como respuesta a eventos específicos en sistemas digitales.
- **Requieren datos digitalizados:** Solo son viables en procesos donde los datos están previamente digitalizados.

Entre los ejemplos más comunes de procesos susceptibles de automatización en la administración se encuentran:

- Procesamiento de facturas.
- Validación de documentos.
- Actualización de bases de datos.
- Seguimiento de pedidos.
- Gestión de correspondencia.
- Procesamiento de declaraciones y solicitudes.

## Integración en una administración

La integración de RPA en una administración pública permite optimizar el rendimiento operativo y reducir errores humanos. Los robots RPA son altamente flexibles y pueden adaptarse a diferentes flujos de trabajo, mejorando la eficiencia en la ejecución de tareas repetitivas y de alto volumen. La implementación también ahorra tiempo y recursos, permitiendo al personal enfocarse en tareas más estratégicas o de mayor valor añadido.

## Beneficios

La RPA ofrece una amplia gama de beneficios, entre los cuales destacan:

- **Reducción de costes:** Los procesos automatizados disminuyen los costos operativos asociados al trabajo manual.
- **Mejora de la calidad:** Al eliminar el factor humano, se reduce la probabilidad de errores en los procesos.
- **Rapidez:** Los robots ejecutan tareas significativamente más rápido que los humanos.
- **Aumento de la productividad:** Permite a las organizaciones procesar mayores volúmenes de trabajo en menos tiempo.
- **Flexibilidad:** Los robots RPA pueden ajustarse rápidamente a cambios en los procesos.
- **Satisfacción del cliente:** Al mejorar la calidad y rapidez de los servicios, la experiencia del usuario final también se optimiza.

## Plataformas existentes

Entre las principales plataformas de RPA que lideran el mercado se encuentran:

- **Automation Anywhere:** Especializada en la creación de robots flexibles y escalables.
- **UiPath:** Destacada por su enfoque intuitivo y accesibilidad para usuarios no técnicos.
- **Blue Prism:** Reconocida por su robustez y enfoque en entornos corporativos de gran escala.

## Componentes a incorporar

La implementación de RPA en una organización requiere la consideración de diversos componentes esenciales:

- **Selección de procesos candidatos:** Identificar qué procesos son los más adecuados para la automatización.
- **Definición de requisitos y objetivos:** Especificar los objetivos de negocio que se desean alcanzar con la RPA.
- **Selección de la plataforma:** Elegir la herramienta de RPA más adecuada según las necesidades de la organización.

- **Formación del personal:** Asegurar que el personal involucrado comprenda el uso y las capacidades de los robots.
- **Estrategia de gestión y monitoreo:** Implementar un sistema para supervisar la actividad de los robots, garantizar su correcta operación y ajustar procesos cuando sea necesario.

## Tecnología Blockchain

### Tecnología blockchain, funcionamiento, tipos, estructura y aplicaciones

**Tecnología que permite la creación de una base de datos distribuida y descentralizada** de forma segura. Su funcionamiento se basa en bloques de información que están encadenados entre sí, proporcionando una mayor **seguridad, transparencia y confiabilidad** en las transacciones que se realizan.

De manera más técnica, **blockchain** se define como un **libro mayor compartido e inalterable** que facilita el registro y seguimiento de transacciones, así como de activos dentro de una red de negocio. Este sistema es crucial para garantizar la confianza en redes distribuidas.

#### Elementos principales de Blockchain

- **Tecnología de libro mayor distribuido:** Todos los participantes de la red tienen acceso a una copia del libro mayor, que contiene un registro inalterable de todas las transacciones. Este enfoque asegura que todos los nodos de la red posean la misma información y evita manipulaciones.
- **Registros inalterables:** Una vez que una transacción se graba en el libro mayor, no puede ser alterada ni eliminada. Si se comete un error en una transacción, en lugar de modificarla, se añade una nueva transacción para corregir el error. Ambas transacciones permanecen visibles, lo que incrementa la **transparencia**.
- **Contratos inteligentes:** Son conjuntos de reglas almacenadas dentro de la blockchain que se ejecutan automáticamente cuando se cumplen ciertas condiciones. Los contratos inteligentes aceleran las transacciones al eliminar intermediarios y permitir procesos más eficientes.

#### Funcionamiento de Blockchain

El proceso de blockchain puede describirse como una serie de pasos encadenados:

- Cada transacción que se realiza se registra como un **bloque de datos**.
- Cada bloque está enlazado al bloque anterior y al posterior, formando una cadena continua de datos.
- Esta cadena es **irreversible**, lo que refuerza la confianza y la seguridad de la red. A medida que se añaden bloques, la información almacenada se vuelve más robusta contra alteraciones.

## Beneficios de Blockchain

Blockchain ofrece tres beneficios fundamentales:

- **Mayor confianza:** Los participantes de la red pueden estar seguros de que la información es precisa y no ha sido manipulada.
- **Mayor seguridad:** Gracias a los registros inalterables y la criptografía, las transacciones están protegidas frente a accesos no autorizados.
- **Mayor eficiencia:** Al eliminar intermediarios y optimizar procesos mediante contratos inteligentes, se reducen tiempos y costos.

## Tipos de redes blockchain

- **Redes públicas:** Estas redes están abiertas a cualquier persona que quiera participar. En este tipo de redes, la validación de transacciones es realizada por cualquier nodo de la red, lo que fomenta la descentralización.
  - **Desventajas:**
    - Requieren una **gran potencia computacional** debido al proceso de consenso distribuido, como el mecanismo de prueba de trabajo (PoW).
    - Las transacciones tienen **poca privacidad**, ya que toda la información es visible para los nodos participantes.
    - La seguridad puede ser débil si no hay suficiente participación o si un atacante controla una gran parte de la red.
- **Redes privadas:** Están restringidas a un grupo reducido de participantes, quienes tienen permiso para acceder y validar las transacciones. Funcionan como una red **P2P descentralizada**, pero con acceso limitado.
  - **Desventajas:**
    - Una sola organización administra la red, lo que significa que la descentralización está limitada.
    - Existe un **riesgo de centralización del poder**, lo que puede generar problemas de confianza si los administradores no son imparciales.
- **Redes híbridas:** Combinan las características de las redes públicas y privadas. Permiten una **validación flexible** que puede ser tanto abierta como restringida según las necesidades de la red.
  - Este enfoque híbrido es especialmente útil para organizaciones que necesitan mantener ciertos datos privados mientras comparten otros de forma pública para incrementar la transparencia.

## Estructura de datos en Blockchain

- **Árboles de Merkle:** Son estructuras de datos jerárquicas que permiten organizar y verificar grandes cantidades de información de manera eficiente. Los árboles de Merkle funcionan de la siguiente manera:
  - Las transacciones individuales se representan como **nodos hoja** en el árbol.
  - Cada nodo hoja se codifica con un hash único (una función criptográfica que comprime los datos de la transacción en una secuencia fija de caracteres).
  - Los hashes de los nodos hoja se agrupan en pares y se combinan en un nuevo hash, formando los **nodos intermedios**.
  - Este proceso de combinación continúa hasta que se llega a un único hash final en la raíz, llamado **raíz de Merkle**.
    - Permite verificar la integridad de las transacciones de forma rápida, ya que solo es necesario comparar los hashes relacionados, sin tener que revisar cada transacción individual. Esta eficiencia es especialmente valiosa en redes con gran volumen de datos.
- **Cadena de bloques:** Cada bloque en la blockchain contiene tres componentes principales:
  - **Datos de las transacciones:** Información específica de las transacciones que se registran en ese bloque.
  - **Hash del bloque actual:** Un identificador único que representa todo el contenido del bloque, generado mediante funciones criptográficas.
  - **Hash del bloque anterior:** Vincula el bloque actual con el anterior, creando la continuidad de la cadena. Este enlace garantiza que cualquier cambio en un bloque afectará a todos los bloques posteriores, reforzando la inmutabilidad de la cadena.
- **Funciones hash criptográficas:** Son esenciales en blockchain, ya que permiten:
  - Resumir grandes cantidades de datos en un hash único y fijo.
  - Detectar cualquier alteración en los datos, ya que incluso un pequeño cambio genera un hash completamente diferente.
  - Garantizar la integridad de los datos y la confianza entre participantes.

## Aplicabilidad del Blockchain

La **tecnología blockchain** es una herramienta innovadora que permite gestionar y registrar información de manera segura, inmutable y descentralizada, eliminando la necesidad de intermediarios y fortaleciendo la confianza en los sistemas. Se aplica en una amplia gama de áreas, entre las que destacan:

- **Validación de transacciones financieras:** Blockchain garantiza la integridad, trazabilidad y transparencia en las operaciones financieras, reduciendo riesgos de fraude.

- **Registro de propiedad:** Facilita la inscripción segura de bienes y derechos, evitando conflictos y aumentando la transparencia.
- **Identificación digital:** Proporciona sistemas más seguros para verificar identidades, mejorando la protección contra el robo de datos y el fraude de identidad.
- **Gestión de contratos inteligentes:** Automatiza el cumplimiento de acuerdos mediante **smart contracts**, que se ejecutan automáticamente al cumplirse las condiciones establecidas.
- **Trazabilidad en cadenas de suministro:** Permite rastrear el origen y movimiento de bienes, asegurando calidad, autenticidad y cumplimiento normativo.

# Organizaciones descentralizadas (OD)

Las **organizaciones descentralizadas (OD)** constituyen un modelo de gobernanza donde no existe una autoridad central. Las decisiones son tomadas de forma colectiva mediante **procesos de consenso**, lo que fomenta una participación democrática y la transparencia en todas las operaciones. Estas organizaciones se estructuran en torno a principios como la igualdad, la descentralización y la autogestión, siendo ideales para comunidades con intereses compartidos.

## DAO (Decentralized Autonomous Organization)

Una **DAO (Organización Autónoma Descentralizada)** es una forma avanzada de organización descentralizada basada en reglas codificadas en **contratos inteligentes** que operan sobre blockchain. Las DAOs destacan por:

- **Autonomía:** Funcionan automáticamente según las reglas preestablecidas, sin intervención humana directa.
- **Transparencia:** Toda la actividad es visible y verifiable en el blockchain.
- **Toma de decisiones colectiva:** Los miembros participan mediante votaciones digitales, asegurando que las decisiones reflejen los intereses del grupo.
- **Inmutabilidad:** Una vez establecidas, las reglas son difíciles de alterar, aumentando la confianza en el sistema.

## Gobernanza

La **gobernanza** en el contexto de las OD y DAOs se refiere a los procesos y normas que definen cómo se toman las decisiones dentro de estas estructuras descentralizadas. Existen dos principales enfoques:

- **Descentralizado:** Las decisiones son discutidas y acordadas colectivamente por los miembros, sin intermediarios.
- **Descentralizado y autónomo:** La gobernanza está totalmente automatizada mediante contratos inteligentes, lo que garantiza eficiencia y evita manipulaciones externas. Este modelo plantea ventajas significativas en términos de transparencia, pero también desafíos al integrar los intereses de todos los participantes de forma justa.

## Aspectos legales y fiscales sobre Blockchain

El uso de blockchain y la descentralización en OD y DAOs presentan retos complejos en el ámbito legal y fiscal:

- **Responsabilidad:** En estructuras descentralizadas, determinar quién es responsable de las acciones o transacciones puede ser complicado, lo que dificulta la aplicación de regulaciones tradicionales.

- **Jurisdicción:** Al operar en redes globales, es difícil identificar bajo qué leyes se rigen las actividades.
- **Implicaciones fiscales:** Las transacciones en blockchain, especialmente aquellas que usan criptomonedas, presentan desafíos para la fiscalización debido a su anonimato y la falta de intermediarios. Esto requiere nuevos enfoques legislativos.

### Blue (Blockchain Universidades Españolas)

La red **Blue**, impulsada por universidades españolas, tiene como objetivo principal promover la innovación y la formación en blockchain. Esta colaboración entre universidades y empresas busca:

- Potenciar la **colaboración en proyectos innovadores** relacionados con blockchain.
- Formar profesionales especializados en tecnología blockchain, adaptados a las demandas del mercado laboral.
- Desarrollar aplicaciones prácticas como la **verificación de identidad, gestión de diplomas académicos** y la **trazabilidad de documentos**.

### EBSI (European Blockchain Services Infrastructure)

La **EBSI**, promovida por la Comisión Europea, es una iniciativa clave para integrar la tecnología blockchain en sectores públicos y privados en la Unión Europea. Sus áreas de aplicación incluyen:

- **Verificación de identidad digital:** Ofrece soluciones seguras y confiables para la identificación y autenticación de ciudadanos.
- **Gestión de diplomas:** Facilita el intercambio transfronterizo de títulos académicos, garantizando su validez y autenticidad.
- **Seguridad social:** Mejora la eficiencia y transparencia en la gestión de servicios sociales mediante registros inmutables y trazables.
- **Trazabilidad documental:** Simplifica la gestión administrativa asegurando que los documentos sean auténticos y verificables.
- **Sostenibilidad:** Promueve el uso de blockchain para rastrear y garantizar prácticas sostenibles en distintos sectores.

## Centros de Procesamiento de Datos (CPD)

### Diseño de un Centro de Procesamiento de Datos (CPD)

El Centro de Procesamiento de Datos (CPD) o Centro de Datos Corporativo (CDC) es el lugar donde se concentran todos los recursos necesarios para el almacenamiento, procesamiento y transmisión de la información de una organización. Su principal objetivo es garantizar la continuidad y disponibilidad de los servicios, asegurando que los sistemas críticos estén siempre operativos.

Las **características básicas** que debe tener un centro de datos son:

- **Robustez:** Capacidad para resistir fallos y mantener la operatividad bajo condiciones adversas.
- **Modularidad:** Diseño que permite añadir o retirar componentes sin afectar al funcionamiento general.
- **Flexibilidad:** Adaptabilidad a cambios tecnológicos y a las necesidades del negocio.
- **Estandarización:** Uso de estándares para facilitar la interoperabilidad y el mantenimiento.

La **evolución** de los centros de datos ha seguido varias etapas:

- **Mainframes:** Sistemas centralizados de gran capacidad.
- **Grid Computing:** Computación distribuida en múltiples nodos interconectados.
- **Clusters:** Conjuntos de servidores que trabajan como una sola unidad lógica.
- **Cloud Computing:** Servicios en la nube que ofrecen Infraestructura (IaaS), Plataforma (PaaS) y Software (SaaS) como servicio.

### Arquitectura: Diseño Físico y Lógico

El diseño de un centro de datos se basa en dos aspectos fundamentales:

#### Diseño Físico:

- **Ubicación:** Selección del emplazamiento considerando factores como riesgo de catástrofes (incendios, inundaciones, terremotos, sabotajes), disponibilidad de la red eléctrica, redes de telecomunicaciones y facilidad de acceso.
- **Infraestructura y Equipamiento:** Construcción que cumple con normativas como el Código Técnico de la Edificación (CTE), reglamentos electrotécnicos y ordenanzas municipales. Se deben definir las medidas de protección frente a fuego, agua, polvo e intrusiones.
- **Exterior del CPD:** Es recomendable que el edificio no sea fácilmente identifiable como un centro de datos para evitar riesgos de robos o sabotajes. Colocar todo en una sola planta puede reducir costes y facilitar el mantenimiento.

- **Interior del CPD:** Implementación de suelos técnicos o falsos suelos para alojar cableado, facilitar el acceso y mejorar la refrigeración. Se puede considerar un edificio inteligente que incluya domótica, control de accesos y automatización.

#### Diseño Lógico:

- **Conexión y Organización de Sistemas:** Planificación de cómo se conectan y organizan los sistemas y servicios dentro del centro de datos, incluyendo servidores, almacenamiento y dispositivos de red.
- **Topologías de Cableado:** Modelos de jerarquía de cableado como "Top of the Rack" (ToR), donde los switches se colocan en la parte superior de cada rack, y "End of the Row" (EoR), donde los switches se ubican al final de una fila de racks.

#### La Red del Core del Centro y la Seguridad

La red del núcleo o "core" es el corazón del centro de datos, responsable de la interconexión eficiente y segura de todos los sistemas.

#### Características de la Red del Core:

- **Seguridad:** Implementación de medidas de protección para garantizar la confidencialidad, integridad y disponibilidad de la información.
- **Rendimiento:** Alta capacidad de procesamiento y transmisión de datos para satisfacer las necesidades operativas.
- **Disponibilidad:** Redundancia de componentes y enlaces para evitar puntos únicos de fallo.
- **Eficiencia Energética:** Optimización del consumo de energía para reducir costes y minimizar el impacto ambiental.

#### Seguridad en el Centro de Datos:

- **Medidas de Seguridad Física:** Control de accesos mediante cerraduras, sistemas automatizados que registran y permiten el acceso solo a personal autorizado, videovigilancia (CCTV) y racks con cerraduras de llave o sistemas de lector de tarjetas.
- **Esquema Nacional de Seguridad (ENS):** Marco normativo que establece los principios básicos y requisitos mínimos para garantizar la protección adecuada de la información.

#### Principios Básicos del ENS:

- **Seguridad Integral**
- **Gestión de Riesgos**
- **Prevención, Detección, Respuesta y Conservación**
- **Líneas de Defensa**
- **Vigilancia Continua**

- **Reevaluación Periódica**
- **Función Diferenciada**

#### **Dimensiones de Seguridad (DICTA):**

- **Disponibilidad:** Asegurar que los sistemas y datos estén accesibles cuando se necesiten.
- **Integridad:** Garantizar la exactitud y completitud de la información.
- **Confidencialidad:** Proteger la información contra accesos no autorizados.
- **Trazabilidad:** Registrar las acciones realizadas para permitir auditorías y seguimiento.
- **Autenticidad:** Verificar la identidad de usuarios y sistemas.

Cada dimensión de seguridad se evalúa en niveles: Bajo, Medio y Alto, lo que permite determinar el impacto de un incidente y la categoría de los sistemas.

#### **Medidas de Protección:**

- **Áreas Separadas y Control de Acceso:** Separación física de zonas y control estricto de acceso.
- **Identificación de Personas:** Registro y verificación de identidad de todos los individuos que acceden a las instalaciones.
- **Acondicionamiento de Locales:** Control de temperatura, humedad, protección frente a amenazas identificadas en el análisis de riesgos.
- **Energía Eléctrica:** Garantizar el suministro eléctrico continuo mediante sistemas de alimentación ininterrumpida (SAI) y generadores.
- **Protección contra Incendios e Inundaciones:** Instalación de sistemas de detección y extinción de incendios, y medidas para prevenir daños por agua.
- **Registro de Entrada y Salida de Equipamiento:** Control detallado del movimiento de equipos y materiales.
- **Instalaciones Alternativas:** Planes de contingencia que incluyan ubicaciones secundarias con las mismas garantías de seguridad.

## Instalaciones y Equipamiento del CPD

### Sistemas de Alimentación Ininterrumpida (SAI):

Protegen frente a:

- **Cortes de Electricidad:** Proporcionan energía temporal durante interrupciones.
- **Fluctuaciones de Tensión:** Protegen contra sobretensiones (picos) e infratensiones.
- **Ruidos y Transientes:** Filtran interferencias eléctricas.

### Tipos de SAI:

- **Standby:** Protección básica para pequeñas cargas.
- **De Línea Interactiva:** Protección intermedia, corrigen fluctuaciones menores.
- **On-line de Doble Conversión:** Protección total, aíslan completamente la carga de la red eléctrica.

### Generadores:

- **Extensión de Autonomía:** Permiten prolongar el suministro eléctrico durante cortes prolongados.
- **Tipos:** Funcionan con gasóleo, gas natural, entre otros combustibles.

## Protección contra Incendios:

### Detección de Incendios:

- **Detectores:** Iónicos, ópticos, termovelocimétricos y de detección precoz por aspiración.
- **Sistema de Alarma:** Central de señalización y pulsadores manuales.
- **Sistemas Auxiliares:** Acciones automáticas como cierre de compuertas y desconexión de sistemas.

### Extinción de Incendios:

- **Agentes Extintores:**
  - **Gases:** Recomendados para centros de datos.
    - **Tipos:**
      - **Halón:** Prohibido por dañar la capa de ozono.
      - **Novec 1230:** Poco eficiente.
      - **CO<sub>2</sub>:** Asfixiante para humanos.
      - **Halocarburos:** Sustitutos del Halón.
      - **Inertes:** Combinaciones de gases nobles.

- **Agua Nebulizada:** Utiliza agua pulverizada para reducir el calor.

#### **Componentes para Generar Fuego:**

- **Combustible**
- **Oxígeno**
- **Calor**
- **Reacción en Cadena**

#### **Racks y Cableado:**

- **Racks:** Estructuras modulares que alojan equipos TIC. Constan de estructura, puertas, paneles laterales, regletas, techo, suelo, cerraduras, pasahilos, bandejas y guías.
- **Dimensiones Estandarizadas:**
  - **Ancho Interior:** 19 pulgadas (482.6 mm).
  - **Unidad Rack (U):** Altura de 1,75 pulgadas (4,445 cm).

#### **Modelos de Jerarquía de Cableado:**

- **Top of the Rack (ToR):** Switches colocados en la parte superior de cada rack, reduciendo la longitud de cables.
- **End of the Row (EoR):** Switches ubicados al final de una fila de racks, centralizando la gestión.

#### **Sistemas Informáticos del CPD:**

- **Servidores:**
  - **Formato Torre:** Similar a un PC convencional, buena refrigeración pero ocupan más espacio.
  - **Formato Rack:** Diseñados para ser montados en racks, ahorran espacio pero tienen ventilación limitada.
  - **Blade:** Servidores modulares que optimizan el espacio y la eficiencia energética, aunque son más costosos.
- **Almacenamiento:**
  - **NAS (Network Attached Storage):** Dispositivos de almacenamiento conectados a la red que proporcionan acceso a datos a nivel de archivo.
  - **SAN (Storage Area Network):** Redes de alta velocidad que conectan servidores y dispositivos de almacenamiento a nivel de bloque.
- **Dispositivos de Red:**

- **Hubs:** Dispositivos básicos que conectan múltiples ordenadores en una red local, replicando los datos a todos los puertos.
- **Switches:** Conmutadores que envían datos directamente al dispositivo de destino, mejorando la eficiencia y seguridad.
- **Routers:** Encaminadores que reenvían paquetes entre diferentes redes, incluyendo funciones de hub y switch, además de servicios adicionales como firewall, NAT y DNS.

## **Disponibilidad del CPD y Niveles TIER**

El **Uptime Institute** establece clasificaciones de disponibilidad conocidas como **TIERS**, según los estándares **TIA-942**. Estos niveles definen la infraestructura necesaria y la tolerancia a fallos del centro de datos.

### **Resumen de Niveles TIER:**

- **TIER I (Básico):**
  - **Redundancia:** No tiene redundancia en componentes críticos.
  - **Disponibilidad Máxima:** 99.671% (máximo 28.8 horas de inactividad al año).
  - **Características:** Puede tener interrupciones planificadas o no planificadas. No suele tener suelo técnico, SAI ni generador eléctrico.
- **TIER II (Componentes Redundantes):**
  - **Redundancia:** N+1 en componentes críticos.
  - **Disponibilidad Máxima:** 99.741% (máximo 22.7 horas de inactividad al año).
  - **Características:** Dispone de suelo técnico, SAI y generadores eléctricos, pero con una sola línea de distribución eléctrica.
- **TIER III (Mantenimiento Concurrente):**
  - **Redundancia:** N+1 con doble línea de distribución (una activa y otra inactiva).
  - **Disponibilidad Máxima:** 99.982% (máximo 1.6 horas de inactividad al año).
  - **Características:** Permite realizar mantenimiento sin interrumpir el servicio. La carga máxima en situaciones críticas es del 90%.
- **TIER IV (Tolerante a Fallos):**
  - **Redundancia:** 2N+1 con dos líneas de distribución activas simultáneamente.
  - **Disponibilidad Máxima:** 99.995% (máximo 26.3 minutos de inactividad al año).
  - **Características:** Tolerante a fallos y permite cualquier tipo de actividad (planificada o no) sin interrupciones.

**Tabla Resumen:**

Parámetros	TIER I	TIER II	TIER III	TIER IV
<b>Nombre</b>	Básico	Componentes Redundantes	Mantenimiento Concurrente	Tolerante a Fallos
<b>Redundancia</b>	N	N+1	N+1	2N+1
<b>Líneas de Distribución</b>	1	1	1 activa + 1 inactiva	2 activas (simultáneas)
<b>Disponibilidad</b>	99.671%	99.741%	99.982%	99.995%
<b>Downtime</b>	28.8 h/año	22.7 h/año	1.6 h/año	26.3 min/año

**Requisitos y Evaluación del CPD**

Los requisitos del centro de datos se determinan en función de la criticidad de los servicios que soporta, mediante evaluaciones cuantitativas y cualitativas.

**Aspectos Clave:**

- **Disponibilidad 24/7x365:** Operatividad continua.
- **Fiabilidad:** Objetivo de alcanzar una disponibilidad de "cinco nueves" (99.999%).
- **Seguridad:** Protección integral de datos y sistemas.
- **Redundancia y Diversificación:** Evitar puntos únicos de fallo.
- **Control Ambiental y Prevención de Incendios:** Sistemas de climatización y detección/extinción de incendios.
- **Conectividad:** Acceso a Internet y redes WAN.
- **Flexibilidad:** Rápido despliegue y reconfiguración.
- **Gestión Continua del Negocio:** Planes de contingencia y recuperación.
- **Cableado:** Infraestructura robusta y de altas prestaciones.

Es esencial realizar **auditorías periódicas** para evaluar el estado del centro de datos y garantizar el cumplimiento de los requisitos establecidos.

**Climatización del CPD**

La climatización es fundamental para mantener las condiciones ambientales óptimas que aseguren el correcto funcionamiento de los equipos.

**Variables a Controlar:**

- **Humedad:** Mantener un nivel de 45% ±5%. Humedad excesiva puede causar condensación; niveles bajos pueden generar electricidad estática.

- **Polvo:** Uso de filtros y mantenimiento de presión positiva para evitar la entrada de polvo, que dificulta la disipación de calor.

#### Tecnologías de Refrigeración:

- **Expansión Directa:** Con condensación por aire o agua/glicol.
- **Condensación por Torre de Refrigeración:** Utiliza agua para disipar el calor.
- **Unidad Enfriadora de Agua:** Enfriamiento mediante circulación de agua fría.
- **Free-Cooling:** Aprovecha las bajas temperaturas del exterior para refrigerar.

#### Distribución del Aire:

- **Insuflación por el Suelo:** El aire frío se suministra desde el suelo hacia los equipos.
- **Insuflación Superior:** El aire frío se suministra desde arriba de los equipos.
- **Sistema Displacement:** Aprovecha la convección natural de abajo hacia arriba.
- **Rejillas Frontales:** Aire frío suministrado directamente al frontal de los racks.

#### Notas sobre Climatización:

- El sistema de aire acondicionado del CPD debe ser independiente del resto del edificio.
- Es crucial crear una barrera física entre el pasillo frío y el pasillo caliente para optimizar la eficiencia.
- **Técnica de Pasillo Frío/Caliente:** Los racks se disponen de manera que las entradas de aire frío y las salidas de aire caliente estén alineadas en pasillos separados.

## Centro de Datos Definido por Software (SDDC)

El SDDC es una arquitectura de centro de datos donde todos los elementos de infraestructura (redes, almacenamiento, CPU y seguridad) están virtualizados y entregados como un servicio. La gestión del centro de datos está totalmente automatizada por software, permitiendo una mayor eficiencia y agilidad.

### Características del SDDC

- **Virtualización Completa:** Todos los recursos están abstraídos del hardware físico.
- **Automatización y Orquestación:** Procesos automatizados para aprovisionamiento y gestión de recursos.
- **Infraestructura como Código:** La configuración y gestión se realizan mediante scripts y herramientas de automatización.
- **Seguridad Integrada:** Políticas de seguridad aplicadas de forma consistente en todo el entorno virtualizado.

### Ventajas y Desafíos del SDDC

- **Ventajas:**
  - Agilidad en la provisión de recursos.
  - Reducción de costos operativos.
  - Escalabilidad y flexibilidad mejoradas.
- **Desafíos:**
  - Complejidad en la implementación inicial.
  - Necesidad de personal con habilidades especializadas.
  - Consideraciones de seguridad y cumplimiento normativo.

## Infraestructura Convergente e Hipervconvergente

### Infraestructura Convergente (CI):

- Combina servidores, almacenamiento y redes en una solución integrada.
- Gestionada como una unidad única, simplificando la administración.

### Infraestructura Hipervconvergente (HCI):

- Evolución de la CI, definida por software.
- Virtualiza todos los componentes, incluyendo computación, almacenamiento y redes.
- **Ventajas:**
  - Simplificación y unificación de la gestión.
  - Mejora la eficiencia y reduce costes.
  - Mayor escalabilidad y flexibilidad.
- **Desventajas:**
  - Dependencia de soluciones específicas de hardware y software.
  - Posibles desafíos en la integración y migración de aplicaciones.

# Tendencias en Infraestructuras y Operaciones (I&O)

## **Infrastructure and Operations (I&O):**

Se refiere a la **gestión y mantenimiento de la infraestructura tecnológica** de una organización, abarcando hardware, software y servicios de red. La evolución en esta área busca garantizar que las organizaciones sean más ágiles, eficientes y resilientes frente a los cambios tecnológicos.

## **Serverless computing:**

Este modelo elimina la necesidad de que los usuarios gestionen directamente la infraestructura subyacente. **El proveedor de servicios asume la asignación y gestión de los recursos informáticos**, permitiendo que las aplicaciones y servicios se ejecuten sin preocuparse por detalles como el aprovisionamiento de servidores. Esto simplifica el desarrollo y reduce los costes operativos.

## **FaaS (Function Platform as a Service):**

Se trata de un modelo que permite ejecutar código encapsulado en funciones individuales. Los usuarios no necesitan aprovisionar ni gestionar explícitamente la infraestructura, lo que **facilita la escalabilidad automática y la ejecución eficiente de funciones en respuesta a eventos específicos**.

## **Network agility:**

Es la capacidad de una red para adaptarse de manera rápida y eficiente a los **cambios en el entorno o a las necesidades del usuario**. Una red ágil es clave para soportar cargas de trabajo dinámicas, optimizar el rendimiento y mejorar la experiencia del usuario final.

## **Death of the data center:**

La tendencia hacia la **descentralización de la informática** y el uso de la computación en la nube está transformando la manera en que las organizaciones gestionan sus datos. Esto podría conducir a una reducción significativa en el uso de centros de datos físicos tradicionales, favoreciendo entornos híbridos o completamente basados en la nube.

## **Edge computing (Computación frontera):**

Este paradigma lleva el **procesamiento y almacenamiento de datos cerca de donde se generan** o necesitan, en lugar de depender exclusivamente de centros de datos centralizados. Esto mejora los tiempos de respuesta, **reduce la latencia** y optimiza el uso del ancho de banda, siendo especialmente útil en aplicaciones de IoT y análisis en tiempo real.

## **Digital diversity management:**

La **gestión de la diversidad tecnológica** es esencial para integrar múltiples plataformas, dispositivos y tecnologías en una organización. Este enfoque maximiza el potencial de las herramientas disponibles y asegura la interoperabilidad entre los diferentes sistemas.

## **Nuevos roles dentro de I&O:**

La evolución tecnológica está generando nuevos desafíos y oportunidades en el área de infraestructura y operaciones. Esto se traduce en la aparición de **nuevos roles y responsabilidades** que se centran en áreas como la automatización, la inteligencia artificial, la ciberseguridad y la integración de tecnologías emergentes.

## **Negación SaaS:**

Algunas organizaciones optan por rechazar el uso de **software como servicio (SaaS)** debido a

preocupaciones relacionadas con la seguridad, la privacidad o una preferencia por modelos de implementación más controlados. Esta postura puede estar influenciada por la sensibilidad de los datos o por políticas corporativas específicas.

# Tendencias: Impacto Ambiental, Escalabilidad, Automatización y Gestión Remota

Los centros de datos modernos se enfrentan a desafíos y tendencias que influyen en su diseño y operación.

## Impacto Ambiental:

- **Eficiencia Energética:** Implementación de sistemas de climatización eficientes, uso de iluminación LED y equipos de bajo consumo.
- **Energías Renovables:** Integración de fuentes de energía limpias como solar o eólica.
- **Gestión de Residuos:** Políticas de reciclaje y disposición adecuada de equipos obsoletos.

## Escalabilidad:

- **Infraestructura Convergente (CI):** Combina servidores, almacenamiento y redes en soluciones integradas gestionadas como un todo. Facilita la expansión y mejora la eficiencia.
- **Infraestructura Hipervconvergente (HCI):** Virtualiza todos los elementos de los sistemas convencionales definidos por hardware. Incluye computación virtualizada, almacenamiento y redes definidos por software.

## Características de la HCI:

- **Simplificación de la Gestión:** Administración unificada de recursos.
- **Escalabilidad Flexible:** Capacidad para crecer según las necesidades.
- **Ventajas:** Reduce costes, mejora la eficiencia, aumenta la agilidad y la seguridad.
- **Desventajas:** Dependencia de hardware y software específicos, posible dificultad para integrar aplicaciones o migrar a otros sistemas.

## Automatización y Gestión Remota:

- **Centro de Datos Definido por Software (SDDC):** Arquitectura en la que todos los componentes se gestionan y controlan mediante software. Permite una mayor flexibilidad y agilidad en la gestión de recursos.
- **Orquestación y Automatización:** Uso de herramientas que permiten automatizar despliegues, configuraciones y operaciones de mantenimiento.
- **Gestión Remota Segura:** Implementación de protocolos seguros para acceder y administrar el centro de datos desde ubicaciones remotas.

## Casos Prácticos

### Caso Práctico 1: Medidas de Seguridad Física

- **Control de Accesos:**
  - Las puertas deben contar con cerraduras y sistemas automatizados que registren y permitan el acceso solo a personal autorizado.
  - El sistema de seguridad debe mantener una lista de autorizaciones y registrar entradas y salidas, incluyendo fechas y horas.
- **Prevención de Atrapamientos:**
  - Instalación de mecanismos de seguridad que eviten que alguien quede atrapado en las instalaciones.
- **Protección de Equipos:**
  - Los servidores deben estar protegidos con rejas o en zonas restringidas (zonificación).
  - Los racks deben contar con cerraduras, ya sea de llave o con sistemas de lector de tarjetas.
- **Videovigilancia:**
  - Implementación de un sistema de circuito cerrado de televisión (CCTV) para monitorear las instalaciones en tiempo real.
- **Normativas y Protocolos:**
  - Establecimiento de un conjunto de normas y estándares de operación que guíen a los usuarios y personal en las mejores prácticas de seguridad.

## Caso Práctico 2: Medidas de Protección según el ENS

- **Áreas Separadas y Control de Acceso:**
  - El equipamiento debe instalarse en áreas separadas con control de acceso estricto.
  - Se debe identificar a todas las personas que acceden a locales con equipamiento, registrando sus entradas y salidas.
- **Acondicionamiento de Locales:**
  - Los locales deben estar acondicionados con sistemas de control de temperatura y humedad.
  - Protección frente a amenazas identificadas en el análisis de riesgos, incluyendo protección de cableado.
- **Suministro Eléctrico:**
  - Garantizar el suministro de energía eléctrica y el correcto funcionamiento de luces de emergencia.
  - **Nivel Medio:** En caso de fallo del suministro, se debe garantizar energía suficiente para la terminación ordenada de procesos mediante SAIs.
- **Protección contra Incendios e Inundaciones:**
  - Aplicar la normativa industrial pertinente para proteger los locales frente a incendios.
  - Implementar medidas para proteger los locales frente a incidentes causados por el agua.
- **Registro de Equipamiento:**
  - Realizar un registro detallado de toda entrada y salida de equipamiento, incluyendo la identificación de la persona que autoriza el movimiento.
- **Instalaciones Alternativas:**
  - Garantizar la existencia y disponibilidad de instalaciones alternativas en caso de que las habituales no estén disponibles, manteniendo las mismas garantías de seguridad.

## Virtualización de recursos

### Virtualización

La virtualización es una técnica que permite abstraer un recurso físico en uno virtual mediante software. Entre sus ventajas destacan la independencia, escalabilidad, alta disponibilidad, flexibilidad, seguridad, agilidad, protección del medio ambiente y ahorro de costes. Como desventaja, puede presentar un mayor consumo de recursos y un rendimiento ligeramente inferior, aunque en la actualidad este impacto es mínimo.

#### Funciones comunes:

- **Operaciones en caliente:** Realizar operaciones sin necesidad de apagar la máquina.
- **Migración de máquinas virtuales entre servidores físicos.**
- **Distribución de carga en tiempo real:** Permite optimizar el uso de recursos.

#### Tipos de virtualización:

- **Virtualización de servidores:** Permite ejecutar varias máquinas virtuales en un solo host físico.
  - **Virtualización completa, de hardware o nativa:** Utiliza un software llamado **hipervisor** capaz de crear y gestionar máquinas virtuales que emulan varios hosts aislados en un único servidor físico.
    - **Host/Anfitrión:** Máquina física donde está el hipervisor.
    - **Invitado/Guest:** Máquinas virtuales.
    - Consiste en un fichero de configuración y un fichero de datastore que simula el disco duro virtual.
  - **Virtualización parcial o paravirtualización:** Ofrece mayor rendimiento pero requiere sistemas operativos adaptados para realizar llamadas directas al hardware físico.
    - Las llamadas, conocidas como **hypercalls**, se realizan mediante el API del hipervisor.
    - Las operaciones se envían directamente al hardware físico en lugar de ejecutarse en la capa de virtualización.
    - **Ejemplos:** VMware ESXi, Citrix XenServer, Microsoft Hyper-V.
- **Virtualización de sistema operativo:** Permite ejecutar un sistema operativo dentro de otro, tomando parte de los recursos del sistema operativo anfitrión.
  - **Ejemplos:** VMware Workstation, Oracle VirtualBox, Parallels Desktop, Microsoft Virtual PC.

- **Virtualización de escritorio o puesto de trabajo (Virtual Desktop Infrastructure - VDI):** Permite ejecutar un escritorio virtual en un servidor y acceder a él desde cualquier dispositivo.
  - **Características:**
    - Independiza el escritorio que utiliza el usuario del hardware que usa para su acceso.
    - El escritorio se ejecuta remotamente en un servidor, incluyendo el disco duro.
    - Requiere conexión de red.
    - Permite gran flexibilidad y ahorro de costes.
  - **Tipos de escritorios:**
    - **Estático:** Cada usuario se conecta siempre a la misma máquina virtual.
    - **Dinámico:** Se crea una nueva máquina virtual para cada usuario que se conecta.
    - **Persistente:** Los cambios se conservan al reiniciar la máquina.
    - **No persistente:** Los cambios no se conservan al reiniciar la máquina.
- **Virtualización de aplicaciones:** Permite ejecutar aplicaciones en diferentes sistemas operativos o plataformas sin tener que instalarlas de manera nativa.
  - Independiza las aplicaciones del entorno donde se ejecutan, eliminando problemas de incompatibilidad de librerías con otras aplicaciones o el propio sistema operativo.
  - **Ejemplos:** Citrix XenApp, Microsoft App-V, VMware Horizon.
- **Virtualización del almacenamiento:** Permite crear múltiples volúmenes lógicos a partir de un espacio de almacenamiento físico.
  - **Mecanismos de implementación:** SAN (*Storage Area Network*) y NAS (*Network Attached Storage*).
- **Virtualización de red:** Permite crear múltiples redes lógicas a partir de una red física.
- **Virtualización de centros de datos:** Permite virtualizar servidores junto con dispositivos de almacenamiento, redes y otros equipos de infraestructura.
  - Incluye virtualización de cómputo, de red, de almacenamiento y orquestación.

#### Otras formas de virtualización:

- **Emulación:** Permite ejecutar programas en una plataforma diferente de aquella para la cual fueron escritos originalmente, imitando o suplantando vía software la arquitectura y recursos completos (procesador, memoria, conjunto de instrucciones, comunicaciones).

- Es muy lenta.
- **Ejemplos:** Bochs, MAME, QEMU, Microsoft Virtual PC y Wine.
- **Simulación:** Reproduce el comportamiento del programa.

## Hypervisor

El **hypervisor** (o monitor de máquina virtual) es el software encargado de crear y gestionar máquinas virtuales. Actúa como una capa de virtualización de hardware que permite utilizar, al mismo tiempo, diferentes sistemas operativos en una misma computadora.

### Tipos de hipervisores:

- **Hipervisor Tipo 1 (Native, Unhosted o Bare Metal):** Se ejecutan directamente en el hardware del host físico y tienen acceso directo a los recursos de la máquina.
  - Son muy rápidos y eficientes en el uso de recursos, pero requieren hardware especialmente diseñado para soportarlos.
  - **Ejemplos:** Kernel-based Virtual Machine (**KVM**), Microsoft Hyper-V, VMware ESXi, Oracle VM Server.
- **Hipervisor Tipo 2 (Hosted):** Se ejecutan en un sistema operativo existente y comparten los recursos del host físico con el sistema operativo anfitrión.
  - Son más fáciles de instalar y usar, pero menos eficientes en el uso de recursos y menos seguros que los hipervisores de tipo 1.
  - **Ejemplos:** VMware Workstation, Parallels Desktop, VirtualBox, VMware Player, QEMU, Bhyve.
- **Hipervisor Tipo Híbrido:** Combinan características de los hipervisores de tipo 1 y tipo 2. Se ejecutan en el hardware del host físico pero requieren un sistema operativo anfitrión para funcionar.
  - El hipervisor interactúa directamente con el hardware en algunas ocasiones y utiliza servicios del sistema operativo anfitrión en otras.
  - **Ejemplos:** Microsoft Virtual PC y Microsoft Virtual Server 2005 R2.

# Contenedores Docker

Herramientas de virtualización a nivel de sistema operativo que permiten ejecutar aplicaciones de manera aislada y portátil en cualquier entorno. Gracias a su diseño, los contenedores aseguran que las aplicaciones sean consistentes en diferentes entornos, desde el desarrollo hasta la producción.

## Componentes

- **Imágenes Docker:** Son plantillas que contienen todo lo necesario para ejecutar una aplicación, incluyendo el código fuente, librerías, configuraciones, entre otros elementos necesarios.
  - Se generan a partir de un archivo **Dockerfile**, que especifica paso a paso las instrucciones para construir la imagen.
- **Contenedores Docker:** Representan instancias ejecutables de una imagen.
  - Un contenedor puede contener una única aplicación o varias aplicaciones que operen conjuntamente.
  - Los contenedores están **aislados** entre sí, lo que significa que no tienen acceso ni a los recursos del sistema anfitrión ni a otros contenedores. Esto garantiza un alto nivel de seguridad y portabilidad.
- **Docker Engine:** Es el motor que gestiona y ejecuta tanto contenedores como imágenes. Actúa como el núcleo operativo de Docker.
- **Docker Registry:** Es un repositorio utilizado para almacenar y distribuir imágenes Docker.
  - Ejemplo: **Docker Hub**, que es el registro más utilizado y permite a los usuarios subir, descargar y compartir imágenes con facilidad.
- **Docker Machine:** Herramienta para instalar Docker Engine en máquinas virtuales o físicas y gestionarlas desde una única interfaz.
- **Docker Compose:** Permite definir y ejecutar aplicaciones multicontenedor. Los servicios se describen en un archivo YAML, facilitando su configuración y despliegue.
- **Docker Swarm:** Es una herramienta de **orquestación de contenedores** que permite implementar y gestionar aplicaciones en contenedores a escala.
  - Aunque es más sencilla que Kubernetes, su funcionalidad es menos avanzada y su uso es menos extendido.

# Plataforma de Kubernetes

Plataforma open-source diseñada para la **orquestación de contenedores**. Se utiliza para **automatizar** la implementación, escalado y administración de aplicaciones en contenedores, siendo una de las herramientas más robustas y populares en este ámbito.

## Componentes de Kubernetes

- **Nodos:** Son los servidores que ejecutan los contenedores. Cada nodo cuenta con un agente llamado **kubelet**, que se encarga de gestionar los contenedores en el nodo.
- **Clúster:** Agrupación de nodos que trabajan de manera conjunta para ejecutar aplicaciones.
- **Master:** Es el conjunto de componentes encargados de controlar y administrar el clúster.
  - Incluye el **controlador**, que supervisa el estado del clúster y toma decisiones sobre su gestión.
  - Otros componentes clave son el **API Server**, que actúa como intermediario para la comunicación, y el **Scheduler** (Planificador), responsable de asignar las tareas a los nodos.
- **Pods (Cápsulas):** Son las unidades básicas de ejecución en Kubernetes. Pueden contener uno o más contenedores junto con los recursos compartidos que necesitan.
- **Deployments:** Permiten desplegar y gestionar aplicaciones dentro del clúster. Ofrecen mecanismos para el escalado y actualizaciones de las aplicaciones.
- **Services:** Proveen un punto de acceso a las aplicaciones a través de una dirección IP y un puerto específico, facilitando la conectividad entre los componentes.

## Funcionamiento de Kubernetes

El funcionamiento de Kubernetes se centra en la creación y gestión de **pods** y **deployments** para ejecutar aplicaciones en el clúster.

- El usuario define un **deployment**, especificando el número de réplicas necesarias y los nodos donde deben ejecutarse.
- El **Scheduler** asigna las réplicas a los nodos disponibles, mientras que el **Controlador** asegura que se mantenga el número deseado de réplicas activas.
- En caso de fallo de un nodo o de un pod, Kubernetes crea automáticamente nuevos pods para cumplir con el estado deseado.
- Los **Services** permiten la conexión a las aplicaciones mediante direcciones IP y puertos definidos, ofreciendo un acceso consistente incluso en escenarios de escalado o fallos.

## Sistemas de almacenamiento

### Sistemas de almacenamiento: DAS, NAS, y SAN

Los **sistemas de almacenamiento** son fundamentales en entornos empresariales y departamentales de gran envergadura. Se optimizan mediante la **virtualización del almacenamiento**, lo que permite gestionar los recursos de manera más eficiente y flexible.

#### DAS (Direct Attached Storage)

El **DAS** es el método tradicional de almacenamiento que conecta directamente el dispositivo de almacenamiento al computador.

- **Ventajas:**
  - **Económicos:** Coste reducido en comparación con otras soluciones.
- **Desventajas:**
  - **Incapacidad para compartir datos:** No permite compartir recursos no utilizados con otros servidores.
- **Tipo de almacenamiento:** A nivel de archivo.
- **Acceso a dispositivos:** Directo, sin intermediarios.
- **Protocolos:**
  - **SCSI (Small Computer System Interface):** Estándar para la transferencia de datos entre dispositivos en el bus de la computadora.
  - **SAS (Serial Attached SCSI):** Interfaz de transferencia de datos en serie que mejora el rendimiento de SCSI.
  - **FC (Fibre Channel):** Tecnología de red utilizada principalmente para redes de almacenamiento, con velocidades de 1 a 128 Gbit/s.

#### NAS (Network Attached Storage)

El **NAS** es una tecnología que permite compartir la capacidad de almacenamiento de un computador con otros a través de una red.

- **Ventajas:**
  - **Económicos:** Menor coste en comparación con soluciones más complejas.
- **Desventajas:**
  - **Rendimiento inferior a las SAN:** Menos eficiente en operaciones de alta demanda.
- **Tipo de almacenamiento:** A nivel de archivo.

- **Acceso a dispositivos:** A través de la **red local (LAN)**, mediante peticiones **TCP/IP** usando protocolos como **CIFS** o **NFS**.
- **Protocolos de compartición de archivos:**
  - **SMB (Server Message Block) / CIFS (Common Internet File System):** Protocolo de red de Windows para compartir archivos.
  - **Samba:** Versión de código abierto de SMB, común en sistemas Linux y Mac.
  - **NFS (Network File System):** Protocolo de nivel de aplicación para sistemas Unix.

## **SAN (Storage Area Network)**

La **SAN** es una red dedicada al almacenamiento que se integra con las redes de comunicación de una organización.

- **Ventajas:**
  - **Ampliación casi ilimitada:** Escalabilidad para adaptarse a las necesidades crecientes.
  - **Alta disponibilidad de datos:** Redundancia y tolerancia a fallos.
  - **Eficiencia en compartir datos:** Permite compartir información entre servidores de forma muy eficiente.
- **Desventajas:**
  - **Coste de implementación:** Inversión inicial elevada debido a la infraestructura especializada.
- **Tipo de almacenamiento:** A nivel de bloque.
- **Acceso a dispositivos:** Mediante el **sistema operativo** con protocolos de bajo nivel, similar al acceso a discos locales.
- **Protocolos:**
  - **FC (Fibre Channel):** Tecnología de red de alta velocidad específica para SAN.
  - **iSCSI (Internet Small Computer System Interface):** Estándar para la transferencia de datos sobre redes TCP/IP, común en SAN.
- **Elementos de la arquitectura:**
  - **Dispositivos de almacenamiento:** Discos duros, SSD, etc.
  - **Medios de transmisión de alta velocidad:** Fibra óptica, iSCSI.
  - **Equipos de interconexión dedicados:** Routers, switches especializados.

# RAID (Redundant Array of Independent Disks)

El **RAID** es un sistema que utiliza múltiples unidades de almacenamiento para distribuir o replicar datos, presentándolos como una sola unidad lógica.

- **Ventajas:**
  - **Mayor integridad y tolerancia a fallos:** Protección frente a pérdidas de datos.
  - **Aumento de la tasa de transferencia:** Mejor rendimiento en lectura y escritura.
  - **Mayor capacidad:** Combinación de múltiples discos en un volumen único.
- **Soporte:**
  - **Hardware:** Implementación habitual, más eficiente.
  - **Software:** A través del sistema operativo, más lento.

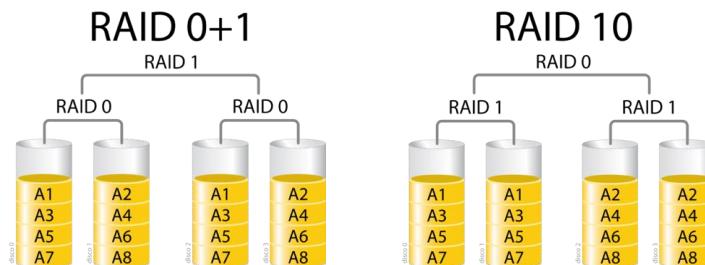
## Niveles RAID estándar

- **RAID 0 (Striping):**
  - **Características:**
    - Distribuye los datos entre dos o más discos sin redundancia.
    - Permite operaciones de lectura/escritura simultáneas.
    - Capacidad total es la suma de las unidades (e.g., 1TB + 1TB = 2TB).
  - **Desventajas:**
    - Sin tolerancia a fallos; la pérdida de un disco implica la pérdida de todos los datos.
- **RAID 1 (Mirroring):**
  - **Características:**
    - Crea copias exactas de los datos en múltiples discos.
    - Incrementa la velocidad de lectura; la escritura permanece constante.
    - Capacidad limitada al tamaño del disco más pequeño (e.g., 1TB + 0.5TB = 0.5TB).
  - **Ventajas:**
    - Alta tolerancia a fallos; los datos permanecen accesibles si falla un disco.
- **RAID 5 (Striping con paridad distribuida):**
  - **Características:**
    - Requiere un mínimo de 3 discos.

- Distribuye la información de paridad entre todos los discos.
- Capacidad equivalente a N-1 discos (e.g., 3 x 1TB = 2TB útiles).
- **Ventajas:**
  - Equilibrio entre rendimiento y tolerancia a fallos.
  - Soporta la falla de un disco sin pérdida de datos.
- **Otros niveles RAID:**
  - **RAID 2 y 3:** Poco utilizados en la práctica.
  - **RAID 4:**
    - Similar al RAID 5, pero con paridad almacenada en un disco dedicado.
    - Puede ser un cuello de botella en operaciones intensivas.
  - **RAID 6:**
    - Como RAID 5, pero con doble paridad.
    - Soporta la falla de hasta dos discos simultáneamente.

### Niveles RAID anidados

Las configuraciones RAID pueden anidarse para combinar ventajas de diferentes niveles.



- **RAID 0+1 (Espejo de divisiones):**
  - Combina **striping y mirroring**.
  - Los datos se dividen entre discos y se duplican en otro conjunto de discos.
  - Ofrece alto rendimiento y redundancia, pero menor tolerancia a fallos que RAID 1+0.
- **RAID 1+0 (División de espejos):**
  - Inversión de RAID 0+1; primero se crean espejos y luego se realiza striping.
  - Mayor tolerancia a fallos; puede soportar la pérdida de varios discos si no afectan al mismo espejo.
- **Otros niveles anidados:**
  - **RAID 30 (RAID 3+0), RAID 50 (RAID 5+0), RAID 100 (RAID 10+0)**, etc.

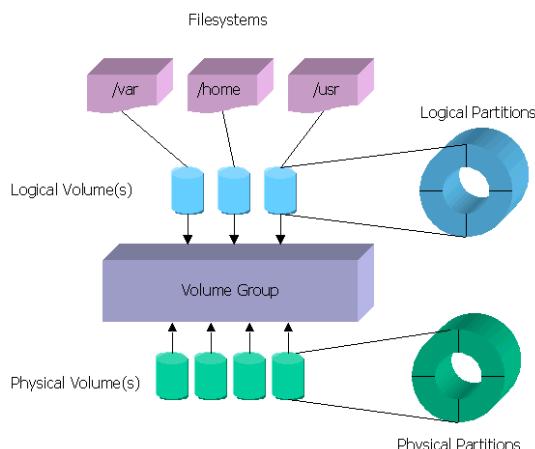
- Utilizados en sistemas que requieren alto rendimiento y alta disponibilidad.

## Volúmenes físicos y lógicos

En el contexto de sistemas de almacenamiento, es crucial diferenciar entre **volúmenes físicos** y **volúmenes lógicos**.

- **Volúmenes físicos:** Corresponden a las unidades de almacenamiento reales, como discos duros o SSDs.
- **Volúmenes lógicos:** Son abstracciones creadas por el sistema operativo o sistemas de gestión de almacenamiento, permitiendo una gestión más flexible y eficiente del espacio disponible.

Al utilizar volúmenes lógicos, es posible redimensionar, mover y gestionar el almacenamiento sin depender directamente del hardware físico, lo que aporta una gran flexibilidad en entornos dinámicos.



## Computación en la Nube (Cloud Computing)

### Computación en la Nube

La computación en la nube (Cloud Computing) es un paradigma que permite acceder a recursos informáticos bajo demanda a través de internet, sin necesidad de una gestión activa directa por parte del usuario. Este modelo facilita el uso de servicios e infraestructuras de manera flexible y escalable, adaptándose a las necesidades cambiantes de las organizaciones.

#### Clúster

Un clúster es un grupo de ordenadores interconectados mediante una red de alta velocidad que funciona como un único sistema. Cada nodo, o equipo individual, realiza la misma tarea, controlada y planificada por software especializado. Este enfoque potencia la **parallelización de tareas**, optimizando el rendimiento y la eficiencia en el procesamiento de datos.

#### Grid Computing

La **computación en malla** o grid computing conecta múltiples clústeres entre sí, donde los recursos no están sujetos a un control centralizado. Cada nodo puede realizar tareas diferentes, lo que promueve la **distribución de tareas** y garantiza la **escalabilidad**. Este modelo permite un comportamiento dinámico y un dimensionamiento en tiempo real, siendo ideal para atender productividades sostenidas.

#### Virtualización

La virtualización es una tecnología que permite la creación de recursos virtuales, facilitando la distribución de la carga de trabajo de manera más sencilla que en la computación grid. Al combinar grid computing con virtualización, se obtiene el **cloud computing**, que ofrece mayores niveles de eficiencia y flexibilidad en la gestión de recursos.

#### Cloud Computing

El cloud computing, o computación en la nube, es un paradigma y modelo de negocio que se basa en la exposición, gestión y uso de recursos, servicios e infraestructuras a través de internet. La nube se define como un conjunto de servicios e infraestructuras accesibles por internet, ofreciendo características como **pago por uso, abstracción, escalabilidad, autoservicio bajo demanda, acceso sin restricciones y elasticidad**.

#### Ventajas del Cloud Computing

- **Económicas:** Reducción de costes de mantenimiento y flexibilidad en la inversión.

- **Tecnológicas:** Facilita el despliegue e implantación, mejora la seguridad y elasticidad, delegación de responsabilidades y mayor respeto al medio ambiente.
- **Organizativas:** Disminuye la dimensión y orientación del departamento de TI, requiere de personal menos cualificado, ofrece oportunidades de cambio y promueve la estandarización.

### Desventajas del Cloud Computing

- **Económicas:** Los costes pueden incrementarse si no se gestionan adecuadamente.
- **Tecnológicas:** Mayores riesgos y vulnerabilidades al trasladar información a una red pública, falta de privacidad y cobertura legal, ausencia de control ante incidentes informáticos, falta de estandarización y problemas de interoperabilidad. Acuerdos de nivel de servicio (SLA) mal definidos y reticencia al cambio.
- **Organizativas:** Centralización excesiva y dependencia del proveedor, lo que puede limitar la libertad y creatividad.

	Cluster Computing	Grid Computing	Cloud Computing
<b>Basic Idea</b>	Aggregation of resources.	Segregation of Resources.	Consolidation of Resources.
<b>Running Processes</b>	Same processes run on all computers over the cluster at the same time.	Job is divided into sub-jobs each is assigned to an idle CPU so they all run concurrently.	Depends on service provisioning. Which computer offers a service and provisions it to the requesting clients.
<b>Operating System</b>	All nodes must run the same operating system.	No restriction is made on the operating system.	No restriction is made on the operating system.
<b>Job Execution</b>	Execution depends on job scheduling. So, jobs wait until it's assigned a runtime.	Execution is scalable in a way that moves the execution of a job to an idle processor (node).	Self-Managed.
<b>Suitable for Apps</b>	Cascading tasks. If one task depends on another one.	Not suitable for cascading tasks.	On-demand service provisioning.
<b>Location of nodes</b>	Physically in the same location	Distributed geographically all over the globe.	Location doesn't matter
<b>Homo/Heterogeneity</b>	Homogenous	Heterogeneous	Heterogeneous
<b>Virtualization</b>	None	None	Virtualization is a key
<b>Transparency</b>	Yes	Yes	Yes
<b>Security</b>	High	High, but doesn't reach the level of cluster computing.	Lower than both types.
<b>Interoperability</b>	Yes	Yes	No
<b>Application Domains</b>	industrial sector, research centers, health care, and centers that offer services on the nation-wide level	industrial sector, research centers, health care, and centers that offer services on the nation-wide level	Banking, Insurance, Weather Forecasting, Space Exploration, Business, IaaS, PaaS, SaaS
<b>Implementation</b>	Easy	Difficult	Difficult – need to be done by the host.
<b>Management</b>	Easy	Difficult	Difficult
<b>Resource Management</b>	Centralized (locally)	Distributed	Both centralized and distributed.
<b>Internet</b>	No internet access is required	Required	Required

## Tipos de Nubes

### Nube Pública

Los servicios ofrecidos están en entornos públicos no propietarios, abiertos al público y gestionados por proveedores externos.

- **Características:** Abiertas al público y gestionadas por los proveedores.
- **Ventajas:** Evita grandes inversiones en equipos y mantenimiento, proporciona flexibilidad y garantías de privacidad, seguridad y disponibilidad.
- **Desventajas:** Dependencia de los servicios en línea y del acceso a través de internet.

### Nube Privada

Los servicios y datos son propiedad de una organización específica, ofreciendo privacidad de datos y gestión personalizada.

- **Características:** Privacidad de datos y gestión localizada.
- **Ventajas:** Mayor seguridad y privacidad de los datos, gestión personalizada.
- **Desventajas:** Mayor inversión en personal, equipos y mantenimiento, menor escalabilidad y posible disminución de la seguridad por gestión no especializada.

### Nube Híbrida

Combina servicios de nubes públicas y privadas, permitiendo aprovechar las ventajas de ambas.

- **Características:** Privacidad de datos y menor coste.
- **Ventajas:** Menor inversión inicial, mantenimiento del control y privacidad de los datos, y beneficios de las nubes públicas.
- **Desventajas:** Requiere el mantenimiento de dos nubes diferentes.

### Nube de Comunidad

Servicios compartidos en una comunidad cerrada de entidades con objetivos comunes, como organizaciones gubernamentales.

- **Características:** Infraestructura compartida por varias organizaciones.
- **Ventajas:** Permite crear una nube especializada según los requisitos de las organizaciones.
- **Desventajas:** Variables según las necesidades y acuerdos entre las entidades.

# Infraestructuras, Plataformas y Software como Servicio (IaaS, PaaS, SaaS)

## Tipos de Servicio en el Cloud Computing

### Software as a Service (SaaS)

Modelo donde el proveedor ofrece aplicaciones a través de internet. El usuario accede a estas aplicaciones mediante una conexión web, sin necesidad de instalar nada localmente. El proveedor se encarga de toda la gestión y mantenimiento del software.

- **Características:** No requiere conocimientos técnicos, pero implica pérdida de control sobre seguridad y privacidad. Se accede mediante un "thin-client" como un navegador web.
- **Ejemplos:** Correo electrónico, CRM, plataformas colaborativas como Slack, GitHub, Google Drive, Dropbox o Salesforce.

### Platform as a Service (PaaS)

El proveedor ofrece una plataforma para desarrollar, probar, ejecutar y mantener aplicaciones. El usuario no se preocupa por la infraestructura necesaria, enfocándose únicamente en el desarrollo de la aplicación. El proveedor gestiona y actualiza la infraestructura.

- **Ejemplos:** Microsoft Azure, Google App Engine, Amazon Web Services (AWS).

### Infrastructure as a Service (IaaS)

Permite a las organizaciones adaptar sus recursos de procesamiento y almacenamiento de manera elástica y eficiente, pagando solo por lo que utilizan. El proveedor ofrece servicios de infraestructura como almacenamiento, procesamiento y redes, encargándose de su gestión y mantenimiento.

- **Ejemplos:** GoGrid, Amazon EC2 (Elastic Compute Cloud), Google Compute Engine.

## Comparación entre IaaS, PaaS y SaaS

- **Nivel de Control:** IaaS ofrece el mayor control sobre los recursos de TI, seguido por PaaS y luego SaaS.
- **Responsabilidades de Gestión:** En IaaS, el cliente gestiona sistemas operativos y aplicaciones; en PaaS, se enfoca en las aplicaciones; en SaaS, el proveedor gestiona todo.
- **Flexibilidad:** IaaS proporciona la máxima flexibilidad para personalizar entornos; PaaS equilibra flexibilidad y facilidad de uso; SaaS ofrece soluciones estándar listas para usar.

# Aspectos varios de la computación en la Nube

## Almacenamiento en la Nube

Modelo de servicio donde los datos generados se almacenan, administran y respaldan de forma remota en servidores gestionados por un proveedor. Los tipos de almacenamiento en la nube incluyen:

- **Público**
- **Privado**
- **Híbrido**

## Software On-Premise vs Off-Premise

- **Software On-Premise:** Software instalado localmente en los servidores de la organización.
- **Software Off-Premise:** Software alojado en la nube (SaaS), gestionado por un proveedor externo.

## Serverless Computing

El **serverless computing** es un modelo donde las empresas pagan solo por el uso efectivo de los recursos informáticos, permitiendo reducir costes y mejorar la eficiencia. El proveedor asume la responsabilidad de ejecutar, escalar y administrar los servidores necesarios para ejecutar el código de las aplicaciones, sin que el usuario tenga que preocuparse por la infraestructura subyacente ni por la demanda de carga de trabajo.

- **Características:** Pago por tiempo de ejecución del código y recursos utilizados.

## Edge Computing

La **computación en el borde** o edge computing busca llevar el procesamiento de datos lo más cerca posible del usuario o del lugar donde se generan los datos, reduciendo la latencia y mejorando la velocidad de procesamiento.

- **Beneficios:** Reducción de latencia y ancho de banda necesarios, ideal para aplicaciones que requieren respuestas rápidas o en tiempo real.

## Contenedores, Orquestación y Microservicios

- **Contenedores:** Permiten empaquetar y distribuir aplicaciones de manera rápida y sencilla, aislando el software en entornos independientes.
- **Orquestación:** Gestión automatizada de contenedores en la nube, facilitando su implementación y escalado.

- **Microservicios:** Enfoque de desarrollo de aplicaciones basado en crear pequeños servicios independientes que pueden integrarse y escalarse de manera eficiente.

## Puesto de trabajo TIC

### **El puesto de trabajo TIC en una organización**

El puesto de trabajo TIC es fundamental para asegurar el correcto funcionamiento y gestión de la infraestructura tecnológica en una organización. Su objetivo principal es garantizar que todos los sistemas y aplicaciones operen de manera eficiente y segura, facilitando así las actividades cotidianas de la empresa.

#### **Normalización**

La normalización implica establecer estándares, políticas y procedimientos para el uso de la tecnología dentro de la organización. Esto garantiza la eficiencia y consistencia en el trabajo, al proporcionar directrices claras sobre cómo deben utilizarse los recursos TIC. Una adecuada normalización facilita la interoperabilidad entre sistemas y simplifica la resolución de problemas.

#### **Seguridad**

La seguridad es esencial para proteger los datos e información de la empresa. Se debe garantizar la integridad y disponibilidad de los sistemas y aplicaciones mediante la implementación de medidas como firewalls, contraseñas seguras y protocolos de encriptación. Además, es crucial formar al personal en el uso seguro de los recursos TIC para prevenir vulnerabilidades humanas.

#### **Actualización**

Mantener los sistemas y aplicaciones actualizados es vital para asegurar su eficiencia y seguridad. Las actualizaciones frecuentes corregir errores, mejoran el rendimiento y protegen contra nuevas amenazas de seguridad. Una política de actualización regular ayuda a prevenir fallos y a mantener la competitividad tecnológica.

#### **Gestión**

La gestión de los recursos TIC implica planificar, organizar y controlar su uso dentro de la organización. Esto incluye la asignación de tareas y responsabilidades, la planificación de proyectos y la toma de decisiones estratégicas sobre la implementación y uso de tecnologías. Una gestión eficaz maximiza el retorno de inversión y alinea la tecnología con los objetivos empresariales.

## Infraestructura del puesto de trabajo virtual (VDI)

La virtualización de escritorio o VDI permite ejecutar un escritorio virtual en un servidor central y acceder a él desde cualquier dispositivo. Esto independiza el sistema operativo y las aplicaciones del hardware utilizado para acceder, proporcionando flexibilidad y ahorro de costes.

### Componentes del VDI

- **Servidor central:** Aloja los escritorios virtuales y gestiona los recursos compartidos.
- **Cliente de escritorio virtual:** Software que permite a los usuarios acceder a los escritorios virtuales desde sus dispositivos.

### Características del VDI

- **Independencia del hardware:** El escritorio virtual no depende del dispositivo de acceso.
- **Ejecución remota:** El escritorio y las aplicaciones se ejecutan en el servidor, no en el dispositivo local.
- **Conexión de red necesaria:** Requiere una conexión estable para acceder al servidor.
- **Flexibilidad y ahorro:** Reduce costes en hardware y facilita la administración centralizada.

### Ventajas del VDI

- **Aprovechamiento del hardware:** Optimiza el uso de recursos del servidor.
- **Eficiencia energética:** Disminuye el consumo eléctrico al utilizar dispositivos menos potentes.
- **Ahorro de espacio:** Reduce la necesidad de equipos físicos en el puesto de trabajo.
- **Administración simplificada:** Facilita la gestión y actualización de sistemas desde un punto central.
- **Alta disponibilidad y recuperación ante desastres:** Mejora la resiliencia ante fallos del sistema.
- **Alto rendimiento y redundancia:** Proporciona un rendimiento consistente y respaldo en caso de fallos.
- **Seguridad mejorada:** Centraliza los datos, reduciendo el riesgo de pérdida o robo.
- **Reducción de costes:** Disminuye gastos en hardware, mantenimiento y soporte.
- **Escalabilidad:** Permite añadir o reducir recursos según las necesidades.
- **Retrocompatibilidad:** Soporta aplicaciones antiguas en entornos modernos.
- **Clústers virtuales:** Facilita la creación de entornos de prueba y desarrollo.

- **Personalización y flexibilidad:** Adapta los escritorios a las necesidades específicas de cada usuario.

#### Otros beneficios del VDI

- **Movilidad y colaboración:** Los trabajadores pueden acceder a su escritorio desde cualquier lugar.
- **Gestión y protección de datos:** Almacena y controla la información de forma centralizada, mejorando la seguridad y cumplimiento normativo.

#### Desventajas del VDI

- **Disminución del rendimiento:** Puede haber latencia o retardos si la infraestructura no es adecuada.
- **Punto único de fallo:** Si el servidor central falla, todos los escritorios pueden verse afectados.
- **Dependencia de la solución elegida:** Limitaciones según el proveedor y el sistema operativo anfitrión.
- **Requisitos de hardware y vídeo:** La aceleración 3D y aplicaciones gráficas intensivas pueden ser problemáticas.
- **Limitaciones en el número de máquinas virtuales:** Depende de la capacidad del servidor.
- **Complejidad añadida:** Requiere personal especializado para su implementación y mantenimiento.
- **Dependencia de una conexión a internet de alta velocidad:** Sin una conexión adecuada, el acceso puede ser deficiente.
- **Coste de mantenimiento y actualización:** La infraestructura de VDI puede ser costosa de mantener y actualizar.

#### Planificación de la virtualización

- **Análisis de roles y requisitos de usuario:** Identificar las necesidades específicas de cada perfil.
- **Evaluación de requisitos de aplicaciones:** Determinar qué software es esencial y sus demandas.
- **Evaluación de la topología de datos:** Comprender cómo se gestionan y almacenan los datos.
- **Servicios de directorio funcionando correctamente:** Asegurar que la autenticación y autorizaciones están operativas.

- **Evaluación de la infraestructura actual:** Identificar limitaciones y áreas de mejora.
- **Verificación de necesidades de seguridad:** Establecer medidas para proteger la información.
- **Establecimiento de expectativas con los usuarios:** Comunicar los cambios y beneficios esperados.
- **Medición del tamaño de almacenamiento:** Planificar el espacio necesario para los datos y sistemas.
- **Requisitos de soporte técnico:** Asegurar recursos para mantenimiento y resolución de problemas.
- **Evaluación del TCO y el ROI:** Analizar los costes totales y el retorno de la inversión.

### Tipos de escritorios virtuales

- **Estático / Dinámico:**
  - **Estático:** Cada usuario accede siempre a la misma máquina virtual, permitiendo personalización persistente.
  - **Dinámico:** Se crea una nueva máquina virtual para cada sesión, ideal para tareas genéricas.
- **Persistente / No-Persistente:**
  - **Persistente:** Los cambios realizados por el usuario se conservan después de reiniciar.
  - **No persistente:** Los cambios no se guardan, manteniendo un entorno limpio en cada inicio.

### Soluciones comerciales de VDI

- **Oracle Secure Global Desktop:** Acceso seguro desde cualquier ubicación, virtualización de escritorio y aplicaciones, compatible con cualquier cliente.
- **Oracle VM VirtualBox:** Virtualización local con capacidad de teletransportar máquinas virtuales entre hosts sin interrupción.
- **Microsoft Hyper-V:** Hipervisor para sistemas de 64 bits con soporte para AMD-V o Intel VT.
- **Citrix XenDesktop y XenApp:** Soluciones comerciales líderes en virtualización de escritorio y aplicaciones.
- **QVD:** Herramienta de código abierto para Linux con hypervisor KVM, compatible con cualquier cliente.
- **Red Hat Enterprise Virtualization:** Virtualización basada en servidores Red Hat Enterprise Linux con hypervisor KVM (no soporta clientes MacOS).

- **VMware**
  - **VMware vSphere**: Virtualización de servidores.
  - **VMware NSX**: Virtualización de redes.
  - **VMware Horizon**: Virtualización de escritorios.
    - **Horizon 7**: Distribución segura de escritorios y aplicaciones en cualquier dispositivo y ubicación.
    - **Horizon Apps**: Acceso a aplicaciones publicadas, SaaS y móviles.
    - **Horizon FLEX**: Trabajo en escritorios virtuales en PC o Mac sin conexión de red, con control centralizado y alta seguridad.
    - **Horizon Cloud**
      - **On-Premises Infrastructure**: Implementación en local o nube privada.
      - **Hosted Infrastructure**: Implementación en la nube pública de VMware.

### Conceptos adicionales

- **SGD Gateway**: Servidor proxy diseñado para ubicarse en una zona desmilitarizada (DMZ), permitiendo que Oracle Secure Global Desktop resida en la red interna. Todas las conexiones se autentican en la DMZ, mejorando la seguridad.
- **Prevención de ejecución de datos (DEP)**: Tecnologías de hardware y software que realizan comprobaciones adicionales en la memoria para proteger contra código malicioso y vulnerabilidades.
- **DMZ (Demilitarized Zone)**: Red local ubicada entre la red interna de una organización y una red externa (Internet). Protege la red interna de ataques al aislar los servidores expuestos al público. Las conexiones desde la red externa a la DMZ están permitidas, mientras que desde la DMZ a la red interna no lo están. Esto evita que un ataque comprometido en la DMZ afecte a la red interna.

## Protección de datos personales

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

La protección de datos personales es un derecho fundamental destinado a salvaguardar la intimidad, privacidad e integridad de los individuos. En España, este ámbito se regula principalmente a través de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPD-GDD), que adapta el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, conocido como Reglamento General de Protección de Datos (RGPD).

### Datos Personales y Objeto de la Ley

Los **datos personales** se definen como cualquier información en texto, imagen o audio que permita la identificación de una persona física. La LOPD-GDD tiene por objeto:

- Adaptar el ordenamiento jurídico español al RGPD.
- Garantizar los derechos digitales de la ciudadanía.
- Proteger la intimidad, privacidad e integridad del individuo.
- Regular los deberes en los procesos de transferencia de datos para garantizar la seguridad del intercambio.

### Ámbito de Aplicación

La LOPD-GDD **se aplica** a:

- Cualquier tratamiento de datos total o parcialmente automatizado.
- Tratamientos no automatizados de datos personales contenidos o destinados a ser incluidos en un fichero.

### Se excluyen:

- Los tratamientos excluidos en el RGPD: actividades personales o domésticas, y aquellos realizados por autoridades con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales.
- Datos de personas fallecidas.
- Materias clasificadas.
- Casos regidos por legislaciones específicas (régimen electoral, instituciones penitenciarias, Registro Civil, Registro de la Propiedad y Mercantiles).

## Acceso a Datos de Personas Fallecidas

Las personas vinculadas por razones familiares o de hecho pueden solicitar el acceso, rectificación y supresión de los datos personales de personas fallecidas, salvo que el fallecido lo hubiera prohibido expresamente o así lo establezca la ley. También pueden ejercer estos derechos:

- Instituciones o personas designadas expresamente por el fallecido.
- Representantes legales de menores y el Ministerio Fiscal.
- Representantes legales de personas con discapacidad, el Ministerio Fiscal y el personal de apoyo.

## Principios de Protección de Datos

Los principios fundamentales son:

- **Exactitud de los datos:** Los datos deben ser exactos y, si es necesario, actualizados. El responsable del tratamiento no será imputable si ha adoptado todas las medidas razonables y los datos fueron obtenidos del afectado, de un mediador, de otro responsable o de un registro público.
- **Deber de confidencialidad:** Responsables, encargados y cualquier persona que intervenga en el tratamiento deben mantener la confidencialidad, complementaria al secreto profesional, incluso después de finalizar su relación con el responsable o encargado.

## Tratamiento Basado en el Consentimiento del Afectado

El consentimiento es una manifestación de voluntad **libre, específica, informada e inequívoca** por la que el afectado acepta el tratamiento de sus datos personales. En el caso de menores de edad:

- **Mayores de 14 años:** Pueden otorgar su consentimiento, salvo que la ley exija la asistencia de los titulares de la patria potestad o tutela.
- **Menores de 14 años:** Se requiere el consentimiento del titular de la patria potestad o tutela.

No será suficiente el consentimiento para levantar la prohibición del tratamiento de **categorías especiales de datos** (ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico), salvo excepciones legales, como en el ámbito sanitario.

El tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos debe estar fundado en el cumplimiento de una obligación legal exigible al responsable.

## Derechos de las Personas

Los afectados tienen los siguientes derechos:

- **Transparencia e información:** Se debe facilitar información básica sobre el tratamiento, incluyendo:

1. La identidad del responsable y su representante.
2. La finalidad del tratamiento.
3. La posibilidad de ejercer sus derechos.

Si los datos no proceden del afectado, también:

4. Las categorías de datos tratados.
  5. Las fuentes de procedencia de los datos.
- **Ejercicio de los derechos:** Puede realizarse directamente o mediante representante legal o voluntario. El responsable está obligado a informar sobre los medios para ejercerlos y no puede negarse por optar por otro medio. La actuación es gratuita.
  - **Derecho de acceso:** El responsable puede pedir que el afectado especifique los datos a los que se refiere la solicitud. Se considera otorgado si se provee un sistema de acceso remoto, directo y seguro. Se puede considerar "repetitivo" si se accede más de una vez en seis meses sin causa legítima.
  - **Derecho de rectificación:** Permite corregir datos personales inexactos o incompletos.
  - **Derecho de supresión ("derecho al olvido"):** El afectado puede solicitar la eliminación de sus datos cuando, entre otros motivos, ya no sean necesarios para los fines para los que fueron recogidos.
  - **Derecho a la limitación del tratamiento:** Implica el marcado de los datos personales conservados con el fin de limitar su tratamiento en el futuro.
  - **Derecho a la portabilidad:** Posibilita recibir los datos personales facilitados en un formato estructurado y transmitirlos a otro responsable.
  - **Derecho de oposición:** El afectado puede oponerse al tratamiento de sus datos por motivos relacionados con su situación particular.

## Responsables y Encargados del Tratamiento

- **Responsable del tratamiento:** Persona física o jurídica que, solo o junto con otros, determina los fines y medios del tratamiento. Establece relaciones con los afectados y controla y se responsabiliza de los datos. Debe determinar si, al finalizar la prestación de servicios del encargado, los datos deben ser destruidos, devueltos o entregados a un nuevo encargado.
- **Encargado del tratamiento:** Persona física o jurídica que trata datos por cuenta del responsable. No decide sobre los fines y medios del tratamiento. Puede conservar los datos bloqueados mientras puedan derivarse responsabilidades de su relación con el responsable.

### Obligaciones de Responsables y Encargados

- **Medidas técnicas y organizativas:** Deben aplicar medidas apropiadas y realizar valoraciones de impacto para garantizar y demostrar el cumplimiento de la normativa.
- **Registro de actividades de tratamiento:** Responsables y encargados deben llevar un registro de las actividades de tratamiento. Deben comunicar los cambios al Delegado de Protección de Datos, si lo hubiera.
- **Bloqueo de datos:** Están obligados a bloquear los datos cuando proceda su rectificación o supresión, conservándolos únicamente a disposición de jueces, tribunales y autoridades competentes. Transcurrido el plazo legal, deben destruirse.
- **Notificación de brechas de seguridad:** Deben notificar cualquier violación de seguridad a la Agencia Española de Protección de Datos en un plazo máximo de 72 horas.

### Delegado de Protección de Datos (DPO)

El Delegado de Protección de Datos actúa como interlocutor entre el responsable o encargado y las autoridades de protección de datos. Sus características son:

- **Designación:** Obligatoria en ciertas entidades como colegios profesionales, centros docentes, entidades financieras, empresas de suministro de energía, centros sanitarios, entre otros.
- **Notificación:** El nombramiento se notifica a la Agencia Española de Protección de Datos o a las autoridades autonómicas en un plazo de 10 días.
- **Cualificación:** Persona física o jurídica cualificada, preferentemente con titulación universitaria y especializada en derecho.
- **Independencia:** No puede ser removido ni sancionado por el responsable o encargado, salvo por dolo o negligencia grave.
- **Acceso a datos:** Tiene acceso a los datos personales, incluso los protegidos por secreto profesional.
- **Funciones:**
  - Documentar y comunicar vulneraciones al órgano de administración o dirección.
  - Responder a reclamaciones de los afectados en un plazo de dos meses.
  - Cooperar con la autoridad de control y ser su punto de contacto.
- **Reclamaciones:** En caso de reclamación ante las autoridades, el afectado puede dirigirse al DPO. Las agencias deben remitir la reclamación al delegado en un plazo de un mes.

## Agencia Española de Protección de Datos (AEPD)

La **AEPD** es la autoridad administrativa independiente que supervisa la aplicación de la normativa de protección de datos en España. Características principales:

- **Personalidad jurídica:** Tiene plena capacidad pública y privada, actuando con independencia de los poderes públicos.
- **Denominación oficial:** "Agencia Española de Protección de Datos, Autoridad Administrativa Independiente".
- **Funciones:** Supervisar y garantizar el cumplimiento de la LOPD-GDD y del RGPD, y representar a España en el Comité Europeo de Protección de Datos.
- **Relación con el Gobierno:** Se relaciona a través del Ministerio de Justicia.
- **Régimen jurídico:** Cuenta con un estatuto propio, aprobado por el Gobierno.
- **Régimen económico y de personal:**
  - Elabora y aprueba sus propios presupuestos, independientes de los Presupuestos Generales del Estado.
  - Su personal puede ser funcionario o laboral.
- **Composición:**
  - **Presidencia:** Dirige y representa a la AEPD, dictando resoluciones, circulares y directrices. Sus actos agotan la vía administrativa. Nombrada por el Gobierno a propuesta del Ministerio de Justicia, por un mandato de cinco años prorrogable.
  - **Adjunto:** Asiste a la Presidencia.
  - **Consejo Consultivo:** Órgano de asesoramiento, compuesto por representantes de diversos sectores y expertos.
- **Investigaciones:** Realizadas por funcionarios de la AEPD o funcionarios ajenos habilitados.
- **Acción exterior:** La AEPD es responsable de las relaciones internacionales en materia de protección de datos.

## Régimen Sancionador

Las **infracciones** se clasifican en:

- **Muy graves** (prescriben a los 3 años):
  - Uso de datos para una finalidad diferente a la comunicada.
  - Omisión del deber de informar al afectado.
  - Exigir pago para acceder a los propios datos.
  - Transferencias internacionales sin garantías adecuadas.

- **Graves** (prescriben a los 2 años):
  - Tratamiento de datos de menores sin consentimiento.
  - No adoptar medidas técnicas y organizativas adecuadas.
  - Incumplir el deber de nombrar responsable o encargado.
- **Leves** (prescriben al año):
  - Falta de transparencia en la información.
  - No atender solicitudes de información del afectado.
  - Incumplimiento por parte del encargado del tratamiento.

### Conceptos Clave Adicionales

- **Responsabilidad Proactiva:** Los responsables deben aplicar medidas técnicas y organizativas para cumplir la ley y demostrar dicho cumplimiento ante las autoridades, adoptando un enfoque preventivo.
- **Registro de Actividades de Tratamiento:** Obligatorio para responsables y encargados, especialmente si la empresa tiene más de 250 empleados o trata datos sensibles (especiales, penales o que impliquen riesgos para derechos y libertades).
- **Nuevos Derechos de los Ciudadanos:** Además de los derechos tradicionales, se incluyen el derecho al olvido y a la desconexión digital. Los derechos se resumen en el acrónimo **ARSULIPO:** Acceso, Rectificación, Supresión, Limitación del tratamiento, Portabilidad y Oposición.
- **Obligación de Informar:** Los responsables deben informar sobre su identidad, tipo de datos recabados, finalidad del tratamiento, cesiones a terceros, plazo de conservación y vías para ejercer los derechos ARSULIPO.
- **Notificación de Brechas de Seguridad:** Se debe notificar cualquier brecha a la AEPD en un plazo máximo de 72 horas.

### Notas sobre la Nueva LOPD-GDD

- **Ampliación de la Información:** Se incrementa la información que se debe proporcionar a los usuarios sobre el tratamiento de sus datos y sus derechos.
- **Privacidad desde el Diseño:** Se promueve la incorporación de medidas de protección de datos desde el inicio de cualquier proyecto o sistema que implique tratamiento de datos personales.
- **Consentimiento Expreso:** El consentimiento debe ser libre, informado, específico e inequívoco, requiriendo una clara acción afirmativa.
- **Figura del Delegado de Protección de Datos:** Se define y regula la figura del DPO, especificando sus funciones, cualificaciones y entidades obligadas a designarlo.

## Reglamento (UE) 2016/679 (RGPD)

El Reglamento General de Protección de Datos (RGPD) es la normativa europea que regula la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y las normas relativas a la libre circulación de dichos datos. Su objetivo principal es proteger los derechos y libertades fundamentales de las personas físicas, especialmente su derecho a la protección de datos personales. Además, establece que la libre circulación de datos personales dentro de la Unión Europea no puede ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

### Ámbito de Aplicación

El RGPD se aplica a:

- Tratamientos total o parcialmente automatizados de datos personales.
- Tratamientos no automatizados de datos personales que formen parte de un fichero o estén destinados a ser incluidos en uno.

Se excluyen de su ámbito:

- Actividades que no estén comprendidas en el Derecho de la Unión.
- Tratamientos realizados por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
- Tratamientos efectuados por autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales.

### Definiciones Clave

- **Datos personales:** Cualquier información sobre una persona física identificada o identifiable.
- **Tratamiento:** Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos automatizados o no.
- **Seudonimización:** Tratamiento de datos personales de manera que no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional se mantenga separada.
- **Fichero:** Cualquier conjunto estructurado de datos personales accesibles según criterios específicos, ya sea centralizado, descentralizado o distribuido de forma funcional o geográfica.
- **Responsable del tratamiento:** Persona física o jurídica que determina los fines y medios del tratamiento.
- **Encargado del tratamiento:** Persona física o jurídica que trata datos personales por cuenta del responsable del tratamiento.

- **Consentimiento del interesado:** Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta el tratamiento de sus datos personales.

### Principios del Tratamiento de Datos

- **Licitud, lealtad y transparencia:** Los datos deben tratarse de manera legal, justa y transparente.
- **Limitación de la finalidad:** Recogidos con fines determinados, explícitos y legítimos, y no tratados ulteriormente de manera incompatible con dichos fines.
- **Minimización de datos:** Adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- **Exactitud:** Datos exactos y, si fuera necesario, actualizados.
- **Limitación del plazo de conservación:** Mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario.
- **Integridad y confidencialidad:** Tratados de manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito.
- **Responsabilidad proactiva:** El responsable del tratamiento es responsable del cumplimiento de estos principios y capaz de demostrarlo.

### Licitud del Tratamiento

El tratamiento es lícito si se cumple al menos una de las siguientes condiciones:

- Consentimiento del interesado.
- Necesario para la ejecución de un contrato.
- Necesario para el cumplimiento de una obligación legal.
- Necesario para proteger intereses vitales del interesado o de otra persona física.
- Necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos.
- Necesario para la satisfacción de intereses legítimos perseguidos por el responsable o por un tercero.

### Condiciones para el Consentimiento

El responsable del tratamiento debe ser capaz de demostrar que el interesado ha dado su consentimiento al tratamiento de sus datos personales. El interesado tiene derecho a retirar su consentimiento en cualquier momento. En el caso de servicios de la sociedad de la información dirigidos a niños, el consentimiento es válido a partir de los 16 años, aunque los Estados

miembros pueden establecer una edad inferior, con un mínimo absoluto de 13 años (en España, 14 años).

### **Tratamiento de Categorías Especiales de Datos Personales**

Está prohibido el tratamiento de datos que revelen:

- Origen étnico o racial.
- Opiniones políticas.
- Convicciones religiosas o filosóficas.
- Afiliación sindical.
- Datos genéticos.
- Datos biométricos dirigidos a identificar de manera unívoca a una persona física.
- Datos relativos a la salud.
- Datos relativos a la vida sexual u orientación sexual.

#### **Excepciones:**

- Consentimiento explícito del interesado (salvo que el Derecho de la Unión o de los Estados miembros lo prohíba).
- Cumplimiento de obligaciones y ejercicio de derechos específicos del responsable o del interesado en el ámbito laboral y de la seguridad y protección social.
- Protección de intereses vitales del interesado o de otra persona física.
- Tratamiento efectuado en el ámbito de sus actividades legítimas y con las garantías adecuadas por parte de fundaciones, asociaciones u otros organismos sin ánimo de lucro.
- Datos que el interesado haya hecho manifiestamente públicos.
- Necesario por razones de interés público esencial.
- Fines de medicina preventiva o laboral, evaluación de la capacidad laboral, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social.
- Fines de archivo en interés público, investigación científica o histórica o fines estadísticos.

### **Tratamiento de Datos Personales Relativos a Condenas e Infracciones Penales**

Sólo puede llevarse a cabo bajo la supervisión de autoridades públicas o si está autorizado por el Derecho de la Unión o de los Estados miembros que prevea garantías adecuadas para los derechos y libertades de los interesados.

## Derechos del Interesado

- **Derecho de Información:** El responsable debe proporcionar al interesado información clara y transparente sobre el tratamiento de sus datos en el plazo de un mes, prorrogable hasta dos meses más en casos necesarios, informando del motivo de la prórroga.
  - **Información a facilitar:**
    - Identidad y datos de contacto del responsable y, en su caso, de su representante.
    - Datos de contacto del delegado de protección de datos.
    - Fines del tratamiento.
    - Base jurídica del tratamiento.
    - Destinatarios o categorías de destinatarios de los datos personales.
    - Intención de transferir datos personales a un tercer país u organización internacional.
    - Plazo de conservación de los datos.
    - Existencia de derechos de acceso, rectificación, supresión, limitación, oposición y portabilidad.
    - Derecho a retirar el consentimiento en cualquier momento.
    - Derecho a presentar una reclamación ante una autoridad de control.
- **Derecho de Rectificación:** El interesado tiene derecho a obtener sin dilación indebida la rectificación de los datos personales inexactos que le conciernan.
- **Derecho de Supresión ("Derecho al Olvido"):** El interesado tiene derecho a obtener sin dilación indebida la supresión de los datos personales que le conciernan cuando:
  - Ya no sean necesarios en relación con los fines para los que fueron recogidos.
  - Retire el consentimiento en que se basaba el tratamiento.
  - Se oponga al tratamiento y no prevalezcan otros motivos legítimos.
  - Los datos hayan sido tratados ilícitamente.
  - Deban suprimirse para el cumplimiento de una obligación legal.
- **Excepciones:**
  - Ejercicio del derecho a la libertad de expresión e información.
  - Cumplimiento de una obligación legal.
  - Razones de interés público en el ámbito de la salud pública.
  - Fines de archivo en interés público, investigación científica o histórica o fines estadísticos.

- Formulación, ejercicio o defensa de reclamaciones.
- **Derecho a la Limitación del Tratamiento:** El interesado tiene derecho a obtener la limitación del tratamiento cuando:
  - Impugne la exactitud de los datos personales.
  - El tratamiento sea ilícito y se oponga a la supresión de los datos.
  - El responsable ya no necesite los datos, pero el interesado los necesite para reclamaciones.
  - Se haya opuesto al tratamiento y esté pendiente la verificación de motivos legítimos.
- **Obligación de Notificación:** El responsable debe comunicar cualquier rectificación, supresión o limitación del tratamiento a cada uno de los destinatarios a quienes se hayan comunicado los datos personales.
- **Derecho a la Portabilidad de los Datos:** El interesado tiene derecho a recibir los datos personales que le incumban en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable sin impedimentos.
- **Derecho de Oposición:** El interesado puede oponerse en cualquier momento al tratamiento de sus datos personales por motivos relacionados con su situación particular.
  - **Excepciones:**
    - Cuando existan motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, derechos y libertades del interesado.
    - Para el reconocimiento, ejercicio o defensa de reclamaciones.
    - Fines de investigación científica o histórica o fines estadísticos por razones de interés público.
- **Limitaciones:** El Derecho de la Unión o de los Estados miembros puede limitar el alcance de los derechos y obligaciones para salvaguardar:
  - Seguridad del Estado.
  - Defensa.
  - Seguridad pública.
  - Prevención, investigación, detección o enjuiciamiento de infracciones penales.
  - Otros intereses públicos importantes.
  - Protección judicial e independencia de los jueces.
  - Protección del interesado o de los derechos y libertades de otras personas.

## Delegado de Protección de Datos (DPD)

El Delegado de Protección de Datos es el profesional encargado de garantizar el cumplimiento de la normativa de protección de datos dentro de una organización.

- **Designación Obligatoria:**
  - Cuando el tratamiento lo lleva a cabo una autoridad u organismo público.
  - Cuando las actividades principales del responsable o encargado consistan en operaciones que requieran una observación habitual y sistemática de interesados a gran escala.
  - Cuando las actividades principales consistan en el tratamiento a gran escala de categorías especiales de datos o datos relativos a condenas e infracciones penales.
- **Designación Conjunta:** Una entidad puede designar un único DPD para varias autoridades u organismos públicos, teniendo en cuenta su estructura y tamaño.
- **Cualificaciones:** El DPD debe ser designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y las prácticas en materia de protección de datos.
- **Posición en la Organización:**
  - El responsable o encargado debe publicar sus datos de contacto y comunicarlos a la autoridad de control.
  - Debe garantizar que el DPD no reciba instrucciones en cuanto al desempeño de sus funciones.
  - No puede ser destituido ni sancionado por el desempeño de sus funciones.
  - Rinde cuentas directamente al más alto nivel jerárquico.
- **Funciones:**
  - Informar y asesorar al responsable o encargado y a los empleados sobre sus obligaciones en protección de datos.
  - Supervisar el cumplimiento del RGPD, incluyendo la asignación de responsabilidades, formación y auditorías.
  - Asesorar en la evaluación de impacto relativa a la protección de datos.
  - Cooperar y actuar como punto de contacto con la autoridad de control.
- **Confidencialidad:** Está obligado a mantener el secreto o confidencialidad en el desempeño de sus funciones.
- **Compatibilidad de Funciones:** Puede desempeñar otras funciones y cometidos, siempre que no den lugar a conflictos de intereses.

### Protección de Datos Desde el Diseño y Por Defecto (Artículo 25)

El responsable del tratamiento debe aplicar, tanto en el momento de determinar los medios como en el del propio tratamiento, medidas técnicas y organizativas apropiadas para garantizar y poder demostrar que el tratamiento es conforme con el RGPD.

- **Medidas a Implementar:**

- **Seudonimización y Minimización:** Tratar únicamente los datos personales necesarios para cada finalidad específica.
- **Limitación de Acceso:** Garantizar que, por defecto, los datos personales no sean accesibles a un número indeterminado de personas sin intervención del interesado.
- **Plazo de Conservación y Accesibilidad:** Aplicar medidas que afecten a la cantidad de datos recogidos, extensión del tratamiento, plazo de conservación y accesibilidad.
- **Certificación:** El cumplimiento de estas obligaciones puede demostrarse mediante mecanismos de certificación adecuados.

## Administración Electrónica

# Real Decreto 203/2021, de 30 de marzo, Reglamento de actuación y funcionamiento del sector público por medios electrónicos

Su objetivo es desarrollar y consolidar la administración electrónica, facilitando la relación entre los ciudadanos y las administraciones públicas.

### Objetivos Principales

- **Digitalización de procedimientos:** Impulsa la transformación digital de los procedimientos administrativos.
- **Accesibilidad y usabilidad:** Garantiza que los servicios electrónicos sean accesibles y fáciles de usar por todos los ciudadanos.
- **Seguridad jurídica:** Establece un marco normativo claro para el uso de medios electrónicos en el sector público.
- **Interoperabilidad:** Promueve la interoperabilidad entre sistemas y administraciones para facilitar el intercambio de información.

### Ámbito de Aplicación

Se aplica a todas las administraciones públicas, incluyendo:

- Administración General del Estado.
- Comunidades Autónomas.
- Entidades Locales.
- Sector público institucional.

### Derechos de los Ciudadanos

- **Elegir el canal de comunicación:** Derecho a relacionarse electrónicamente con las administraciones.
- **No aportar documentos redundantes:** No están obligados a presentar documentos que ya obren en poder de las administraciones.
- **Acceso a información y servicios:** Derecho a acceder a la información pública y a los servicios electrónicos de forma sencilla.

### Obligaciones de las Administraciones

- **Proporcionar medios electrónicos:** Deben facilitar los canales electrónicos necesarios para la comunicación con los ciudadanos.
- **Garantizar la seguridad:** Asegurar la protección de datos y la confidencialidad de las comunicaciones.
- **Transparencia:** Mantener actualizada y accesible la información en las sedes electrónicas.

### Identificación y Firma Electrónica

- **Sistemas admitidos:** DNI electrónico, certificados digitales reconocidos, sistemas de clave concertada.
- **Firma electrónica:** Se establece como medio para garantizar la autenticidad e integridad de los documentos electrónicos.

### Registro Electrónico

- **Presentación de documentos:** Permite la recepción de solicitudes, escritos y comunicaciones en formato electrónico.
- **Anotación de asientos:** Registra la fecha y hora de recepción para el cómputo de plazos.
- **Accesibilidad:** Disponible las 24 horas todos los días del año.

### Notificaciones Electrónicas

- **Obligatoriedad:** Determinados colectivos están obligados a recibir notificaciones por vía electrónica.
- **Disponibilidad:** Se consideran practicadas en el momento en que el interesado acceda a su contenido.
- **Rechazo:** Si transcurren 10 días naturales sin acceso, se entiende rechazada la notificación.

### Interoperabilidad y Seguridad

- **Esquema Nacional de Interoperabilidad:** Establece los criterios para asegurar la compatibilidad entre sistemas.
- **Esquema Nacional de Seguridad:** Define las medidas para proteger la información y los servicios electrónicos.

# Decreto 220/2014, de 12 de diciembre, del Consell, por el que se aprueba el Reglamento de Administración Electrónica de la Comunitat Valenciana.

## Objetivos Específicos

- **Implementación de servicios electrónicos:** Facilitar el acceso a los servicios públicos mediante medios electrónicos.
- **Participación ciudadana:** Fomentar la implicación de los ciudadanos en los asuntos públicos a través de plataformas digitales.
- **Transparencia y buen gobierno:** Mejorar la transparencia de la administración y la rendición de cuentas.

## Ámbito de Aplicación

Se aplica a:

- **Administración de la Generalitat:** Incluye todas las consellerías y organismos dependientes.
- **Sector público instrumental:** Empresas, fundaciones y otros entes públicos de la Comunitat Valenciana.

## Principios Rectores

- **Simplificación administrativa:** Reducir trámites y facilitar la gestión electrónica.
- **Accesibilidad universal:** Garantizar que todos los ciudadanos puedan acceder a los servicios electrónicos.
- **Calidad en la prestación de servicios:** Asegurar la eficacia y eficiencia en la atención al ciudadano.

## Servicios Electrónicos

- **Sede electrónica:** Punto de acceso general a los servicios y trámites electrónicos de la Generalitat.
- **Carpeta ciudadana:** Espacio personalizado donde los ciudadanos pueden consultar sus expedientes y comunicaciones.
- **Tablón electrónico:** Publicación oficial de actos y comunicaciones de la administración.

## Identificación y Autenticación

- **Medios admitidos:** Certificados electrónicos reconocidos, sistemas de clave concertada y otros medios seguros.

- **Registro de funcionarios habilitados:** Permite a funcionarios actuar en representación de ciudadanos que no disponen de medios electrónicos.

### Gestión Documental y Archivo Electrónico

- **Documento electrónico:** Establece los requisitos para la creación y conservación de documentos en formato digital.
- **Archivo electrónico único:** Centraliza la gestión documental para garantizar la integridad y disponibilidad a largo plazo.

### Interoperabilidad

- **Plataformas comunes:** Uso de plataformas y servicios compartidos para mejorar la coordinación entre administraciones.
- **Normas técnicas:** Adopción de estándares que faciliten la compatibilidad y el intercambio de información.

### Protección de Datos y Seguridad

- **Confidencialidad:** Garantizar la protección de los datos personales tratados por la administración.
- **Seguridad de la información:** Implementar medidas técnicas y organizativas para prevenir riesgos.

## Desarrollo web

# Arquitectura de Desarrollo en la Web

La arquitectura web define cómo los componentes de una aplicación web se organizan y comunican entre sí.

- **Modelo Cliente-Servidor:**
  - **Cliente:** Navegador web que realiza solicitudes.
  - **Servidor:** Procesa las solicitudes y devuelve respuestas (páginas web, datos).
- **Capas de Arquitectura:**
  - **Presentación:** Interfaz de usuario (front-end).
  - **Lógica de Negocio:** Procesamiento de datos y reglas de negocio (back-end).
  - **Acceso a Datos:** Interacción con bases de datos.

## Desarrollo Web Front-End

Se enfoca en la creación de la interfaz de usuario y experiencia interactiva.

- **Lenguajes Fundamentales:**
  - **HTML:** Estructura y contenido de la página.
  - **CSS:** Estilos y diseño visual.
  - **JavaScript:** Interactividad y comportamiento dinámico.
- **Frameworks y Librerías:**
  - **React:** Biblioteca para construir interfaces de usuario basadas en componentes.
  - **Angular:** Framework completo para aplicaciones web de una sola página (SPA).
  - **Vue.js:** Framework progresivo para la construcción de interfaces de usuario.
- **Herramientas y Tecnologías:**
  - **TypeScript:** Superset de JavaScript que añade tipado estático.
  - **SASS/LESS:** Preprocesadores CSS para facilitar la escritura de estilos.
  - **Webpack:** Empaquetador de módulos para aplicaciones JavaScript.

## Desarrollo Web en Servidor (Back-End) y Conexión a Bases de Datos

Gestiona la lógica del negocio, procesos del servidor y comunicación con bases de datos.

- **Lenguajes de Programación:**
  - **PHP:** Amplio uso en desarrollo web (WordPress, Laravel).
  - **Python:** Frameworks como Django y Flask.
  - **Java:** Uso empresarial con frameworks como Spring.
  - **Node.js:** Entorno para ejecutar JavaScript en el servidor.
  - **Ruby:** Usado con el framework Ruby on Rails.
- **Bases de Datos:**
  - **Relacionales (SQL):**
    - **MySQL:** Popular y de código abierto.
    - **PostgreSQL:** Avanzado y extensible.
    - **Oracle:** Orientado a empresas.
  - **NoSQL:**
    - **MongoDB:** Basado en documentos.
    - **Redis:** Almacenamiento en memoria clave-valor.
    - **Cassandra:** Altamente escalable.
- **ORM (Object-Relational Mapping):**
  - **Hibernate (Java), Entity Framework (.NET), Sequelize (Node.js).**
- **Servidores Web:**
  - **Apache:** Servidor HTTP de código abierto.
  - **Nginx:** Servidor ligero y de alto rendimiento.
- **Servicios y Arquitecturas:**
  - **Microservicios:** Aplicaciones divididas en pequeños servicios independientes.
  - **SOA (Arquitectura Orientada a Servicios):** Integración de servicios discretos.

## Interconexión con Sistemas y Servicios

Permite la comunicación y el intercambio de datos entre diferentes aplicaciones y sistemas.

- **APIs y Protocolos:**
  - **RESTful APIs:** Arquitectura para servicios web que utiliza HTTP.
  - **SOAP:** Protocolo basado en XML para intercambio de información.
  - **GraphQL:** Lenguaje de consulta para APIs que permite solicitar exactamente lo necesario.

- **Protocolos y Tecnologías de Comunicación:**
  - **HTTP/HTTPS:** Protocolos base para la comunicación web.
  - **WebSockets:** Comunicación bidireccional en tiempo real.
  - **gRPC:** Protocolo de llamada a procedimiento remoto de alto rendimiento.
- **Servicios en la Nube e Integraciones:**
  - **AWS (Amazon Web Services):** Amplia gama de servicios en la nube.
  - **Microsoft Azure:** Plataforma en la nube para servicios y aplicaciones.
  - **Google Cloud Platform:** Infraestructura y servicios de computación en la nube.
- **Mensajería y Colas:**
  - **RabbitMQ, Apache Kafka:** Sistemas para manejar mensajes y eventos.
- **Autenticación y Autorización:**
  - **OAuth2, JWT (JSON Web Tokens):** Estándares para autenticación segura.
  - **LDAP:** Protocolo para acceso a directorios y servicios de autenticación.

## Lenguajes y Herramientas para la Utilización en Redes Globales

Tecnologías y herramientas esenciales para desarrollar aplicaciones escalables y robustas en un entorno global.

- **Estándares Web Modernos:**
  - **HTML5:** Soporte multimedia y nuevas etiquetas semánticas.
  - **CSS3:** Nuevas características como transiciones, transformaciones y animaciones.
  - **ECMAScript 6+ (ES6+):** Actualizaciones del estándar JavaScript.
- **Control de Versiones y Colaboración:**
  - **Git:** Sistema de control de versiones distribuido.
  - **Plataformas: GitHub, GitLab, Bitbucket** para alojamiento y colaboración en código.
- **Herramientas de Construcción y Automatización:**
  - **npm y Yarn:** Gestores de paquetes para JavaScript.
  - **Webpack, Parcel:** Empaquetadores de módulos.
  - **Grunt, Gulp:** Herramientas para automatizar tareas.
- **Pruebas y Calidad de Código:**
  - **Jest, Mocha:** Frameworks de pruebas para JavaScript.

- **ESLint, Prettier:** Herramientas para análisis estático y formateo de código.
- **Seguridad y Rendimiento en Redes:**
  - **SSL/TLS:** Encriptación para comunicaciones seguras.
  - **HTTP/2 y HTTP/3:** Protocolos para mejorar la eficiencia y velocidad de carga.
  - **CDN (Content Delivery Network):** Distribución de contenido a nivel global para reducir latencia.
- **Protocolos y Estándares Internacionales:**
  - **UTF-8:** Codificación de caracteres para soporte multilingüe.
  - **ISO/IEC Estándares:** Normas internacionales para seguridad y calidad.
- **Despliegue y Contenedores:**
  - **Docker:** Plataforma para crear y administrar contenedores.
  - **Kubernetes:** Orquestación de contenedores para despliegue escalable.
- **Servicios y Arquitecturas de Red:**
  - **Microservicios:** Para escalabilidad y mantenimiento.
  - **Serverless Computing:** Ejecución de código sin gestión de servidores (AWS Lambda, Azure Functions).
- **Monitoreo y Logística:**
  - **Prometheus, Grafana:** Herramientas para monitoreo y visualización.
  - **ELK Stack (Elasticsearch, Logstash, Kibana):** Análisis y visualización de logs.

Tecnologías Web: HTML, CSS, Javascript, AngularJS

## **HTML, CSS, Javascript,...**

## Desarrollo de Aplicaciones Móviles

### Diseño y Desarrollo de Aplicaciones Móviles

El diseño y desarrollo de aplicaciones móviles requiere considerar el tipo de aplicación a crear, los principios de diseño adecuados y los entornos de trabajo disponibles. Las aplicaciones móviles se clasifican en tres categorías principales: **nativas**, **web** e **híbridas**.

**1. Aplicaciones nativas:** Se desarrollan específicamente para un sistema operativo móvil (Android, iOS, etc.) utilizando los lenguajes y herramientas propias de la plataforma. Estas aplicaciones aprovechan al máximo las características y funcionalidades del dispositivo, ofreciendo un rendimiento y experiencia de usuario superiores.

- **Ventajas:**

- Mayor rendimiento y velocidad de ejecución.
- Acceso completo a todas las funcionalidades del dispositivo (cámara, GPS, sensores, etc.).
- Mejor experiencia de usuario.
- Mayor visibilidad en las tiendas de aplicaciones.

- **Desventajas:**

- Mayor costo y tiempo de desarrollo, al requerir versiones específicas para cada sistema operativo.
- Mayor dificultad para actualizar y mantener.

- **Frameworks y lenguajes:**

- **Android:** Java y Kotlin.
- **iOS:** Objective-C y Swift.
- **Multiplataforma:** Xamarin.

**2. Aplicaciones web:** Se ejecutan en un navegador web, permitiendo el acceso desde cualquier dispositivo con conexión a Internet y un navegador compatible. Su desarrollo es independiente del sistema operativo.

- **Ventajas:**

- Mayor facilidad de desarrollo y mantenimiento.
- Mayor flexibilidad y escalabilidad.
- Mayor alcance y visibilidad.

- **Desventajas:**

- Menor rendimiento y velocidad de ejecución comparado con aplicaciones nativas.

- Acceso limitado a las funcionalidades del dispositivo.
- Experiencia de usuario menos fluida y consistente.
- **Frameworks y tecnologías:**
  - HTML5, CSS3 y JavaScript.
  - Frameworks como jQuery Mobile, AngularJS, React y Bootstrap.

**3. Aplicaciones híbridas:** Combinan elementos de aplicaciones nativas y web. Se desarrollan como aplicaciones web pero se empaquetan dentro de un contenedor nativo, permitiendo su distribución a través de las tiendas de aplicaciones y acceso a ciertas funcionalidades del dispositivo.

- **Ventajas:**
  - Desarrollo más rápido y económico al reutilizar código web.
  - Mayor alcance y visibilidad en tiendas de aplicaciones.
  - Flexibilidad y escalabilidad mejoradas.
- **Desventajas:**
  - Rendimiento y velocidad de ejecución inferiores a las aplicaciones nativas.
  - Experiencia de usuario menos fluida y consistente.
  - Acceso limitado a algunas funcionalidades del dispositivo.
- **Frameworks:**
  - Cordova, Ionic y Flutter.

## Principios de Diseño de Aplicaciones Móviles

Un buen diseño de aplicaciones móviles se basa en principios fundamentales como la **simplicidad, consistencia y navegación intuitiva**. La aplicación debe ser fácil de usar, coherente en su interfaz y reflejar la identidad de la marca.

- **Simplicidad:** Diseño limpio y sin elementos innecesarios que puedan distraer al usuario.
- **Consistencia:** Uso uniforme de elementos y comportamientos a lo largo de la aplicación.
- **Navegación intuitiva:** Estructura lógica que facilita al usuario moverse por la aplicación.

**Patrones de interacción:** Son soluciones probadas para problemas comunes en el diseño de aplicaciones, aplicados en aspectos como navegación, acciones, cuadros de diálogo, notificaciones y gestos.

**Diseño visual:** Debe ser atractivo y funcional, facilitando la interacción del usuario.

- **Tipografía:** En pantallas de baja resolución, es recomendable usar tipografías limpias, abiertas y sin serif (Sans-Serif).

- **Color:** Utilizar un sistema cromático consistente (por ejemplo, rojo para errores, amarillo para avisos y verde para confirmaciones).

# Aplicaciones Web para Móviles

Al desarrollar aplicaciones web para móviles, se puede optar por crear una web específica o utilizar un diseño responsive que se adapte a diferentes tamaños de pantalla.

## Reglas de usabilidad:

- Reducir la cantidad de contenido para facilitar la lectura en pantallas pequeñas.
- Utilizar una sola columna para presentar la información.
- Ocultar menús y elementos no esenciales.
- Minimizar las llamadas al servidor para mejorar el rendimiento.

## Tecnologías usadas:

- **HTML5:** Proporciona estructuras semánticas y capacidades multimedia sin necesidad de plugins.
- **CSS3:** Permite estilizar y adaptar el diseño a diferentes dispositivos.
- **JavaScript:** Añade interactividad y dinamismo.

## Principales frameworks:

- **jQuery Mobile:** Ofrece compatibilidad con una amplia gama de dispositivos, asegurando una experiencia consistente.
  - **Formas de crear páginas:**
    - Múltiples ficheros HTML con enlaces.
    - Un único fichero HTML con enlaces internos.
  - **Precarga de páginas:** Uso del atributo data-prefetch para mejorar el rendimiento.
- **AngularJS:** Framework para crear aplicaciones del lado del cliente usando el patrón MVC.
  - **Principales directivas:**
    - ng-app: Inicializa la aplicación.
    - \$scope: Contexto de ejecución de variables.
    - ng-controller: Define el ámbito del controlador.
    - ng-model: Enlaza campos de formulario con el ámbito.
    - ng-bind: Enlaza datos del modelo con la vista.
- **Bootstrap:** Framework frontend para diseño responsive.
  - Utiliza hojas de estilo LESS.
  - Basado en una cuadrícula estándar de 940 píxeles de ancho.

## Aplicaciones Nativas: Android

Las aplicaciones nativas para Android se desarrollan utilizando lenguajes como Java y Kotlin, ofreciendo una integración completa con el sistema operativo y el hardware.

### Ventajas:

- No requieren conexión a Internet para funcionar.
- Acceso completo a características hardware (cámara, GPS, etc.).
- Permiten notificaciones push.
- Distribución a través de la Play Store.

**Android:** Sistema operativo basado en Linux diseñado para dispositivos móviles, con una cuota de mercado superior al 80%.

### Arquitectura de Android:

- **Kernel de Linux:** Servicios básicos y manejo de hardware.
- **Hardware Abstraction Layer (HAL):** Interfaz estándar para acceder al hardware.
- **Android Runtime (ART):** Entorno de ejecución con compilación JIT.
- **Librerías Nativas (C/C++):** Funcionalidades básicas como gráficos y bases de datos.
- **Framework de API Java:** Acceso a componentes del sistema.
- **Aplicaciones del Sistema:** Aplicaciones preinstaladas.

**Java:** Compila a bytecodes ejecutables en cualquier JVM.

**Android SDK:** Herramientas de desarrollo incluyendo un depurador, bibliotecas y un emulador.

- **IDE oficial:** Android Studio.
- Las aplicaciones se empaquetan como .apk y se almacenan en /data/app.

### Principales clases para desarrollo:

- **ActivityManager:** Controla el ciclo de vida de las actividades.
- **View:** Construcción de interfaces.
- **NotificationManager:** Muestra avisos al usuario.
- **ContentProvider:** Intercambio estandarizado de datos.
- **ResourceManager:** Gestiona recursos no codificados.

### Tipos de aplicaciones:

- **Apps de primer plano:** Muestran una interfaz y pueden perder el foco.
- **Apps de segundo plano (Servicios):** Continúan ejecutándose tras cerrar la aplicación.
- **Widgets:** Interfaces pequeñas en el escritorio que se actualizan periódicamente.

**AndroidManifest.xml:** Declara metadatos y permisos requeridos, que deben ser concedidos por el usuario.

**Kotlin:** Lenguaje desarrollado por JetBrains, compatible con Java y oficial para Android.

- **Características:**

- Funciones con parámetros por defecto.
- Variables no nulas por defecto.
- Sobrecarga de operadores.
- Soporte para programación funcional.

**Construcción de UI:** Uso del patrón Modelo-Vista-Presentador (MVP).

- **Modelo:** Define datos y lógica.
- **Presentador:** Conecta modelo y vista.
- **Vista:** Muestra datos y gestiona la interacción del usuario.

**Frameworks adicionales:**

- **Titanium SDK:** Desarrollo multiplataforma con JavaScript.
- **Corona SDK (Solar2D):** Desarrollo en Lua para aplicaciones 2D.

## Aplicaciones Nativas: iOS

Las aplicaciones nativas para iOS se desarrollan en Objective-C o Swift, integrándose completamente con el sistema y hardware.

**iOS:** Sistema operativo basado en macOS, derivado de Unix, con una cuota de mercado del 10-15%.

**Arquitectura de iOS:**

- **Core OS Layer:** Servicios de bajo nivel y hardware.
- **Core Services Layer:** Servicios básicos como bases de datos.
- **Media Layer:** Capacidades gráficas y multimedia.
- **Cocoa Touch Layer:** Frameworks para desarrollo de interfaces.

**Objective-C:** Lenguaje orientado a objetos, superconjunto de C.

- **Características:**
  - Envío de mensajes a objetos.
  - Inclusión de código C.

**Cocoa Touch:** API para acceso a funciones del sistema.

- **Frameworks:**
  - **UIKit:** Manejo de la capa gráfica.
  - **Foundation Framework:** Clases básicas y servicios.
  - **AppKit:** Interfaz gráfica.
  - **Swift Standard Library:** Librería estándar para Swift.

**iOS SDK:** Herramientas para desarrollo de terceros.

**Swift:** Lenguaje compilado y multiparadigma para iOS y macOS.

- **Características:**
  - Sintaxis moderna.
  - Seguridad en gestión de memoria.
  - Programación orientada a objetos y funcional.

## Aplicaciones Nativas: Windows

Microsoft desarrolló sistemas operativos móviles como Windows Mobile, Windows Phone y Windows 10 Mobile, actualmente descontinuados.

- **Pocket PC / Windows Mobile:** Desarrollo en C++ o .NET.
- **Windows Phone:** Desarrollo en C#, Visual Basic .NET o C++.
- **Windows 10 Mobile:** Plataforma unificada, ahora abandonada.

## Aplicaciones Híbridas

Las aplicaciones híbridas combinan una aplicación web dentro de un contenedor nativo, utilizando un WebView para mostrar contenido y acceder a APIs nativas.

- **Ventajas:**
  - Desarrollo más rápido y económico.
  - Código reutilizable entre plataformas.
  - Distribución en tiendas de aplicaciones.
- **Desventajas:**
  - Rendimiento inferior al de aplicaciones nativas.
  - Experiencia de usuario menos fluida.
  - Acceso limitado a funcionalidades del dispositivo.

### Frameworks:

- **Ionic:** Basado en Angular y Cordova para acceso nativo.
- **Xamarin:** Genera aplicaciones nativas usando .NET y C#.
  - **Características:**
    - Código compartido en lógica de negocio.
    - Interfaces programadas independientemente.
    - **IDEs:** Xamarin Studio y Visual Studio.
- **Flutter:** SDK multiplataforma de Google usando Dart.
  - **Características:**
    - Alto rendimiento con motor gráfico propio.
    - Desarrollo rápido con Hot Reload.
- **React Native:** Framework de Facebook usando JavaScript y React.
  - **Características:**
    - Código nativo para mejor rendimiento.

- Código compartido entre plataformas.

### **Dalvik Virtual Machine (VM)**

La **Dalvik VM** es la máquina virtual utilizada en versiones anteriores de Android para ejecutar aplicaciones, ejecutando bytecode en formato .dex.

- **Características:**

- Optimizada para dispositivos con recursos limitados.
- Permite múltiples instancias con bajo consumo de memoria.
- Reemplazada por **ART (Android Runtime)** en versiones recientes.

## Accesibilidad y Usabilidad

### Accesibilidad y Usabilidad

**Accesibilidad:** Busca superar las discapacidades del usuario, garantizando el acceso igualitario a un sitio, producto o servicio para personas con diferentes habilidades o discapacidades. Se enfoca en la facilidad de uso de tecnologías, productos y servicios por parte de todas las personas, independientemente de sus capacidades, y requiere un sistema estandarizado para cada ámbito aplicable. Está vinculada al concepto de **diseño universal**, cuyo objetivo es crear productos usables por el mayor rango posible de capacidades y situaciones, con especial atención a personas con discapacidades o necesidades especiales.

- **Accesibilidad en las TIC:**

- **Hardware:**

- **Tecnología adaptativa:** Versiones específicas para personas con diversidad funcional (e.g., audífonos, pantallas braille).
    - **Tecnología asistiva:** Dispositivos con mecanismos de ayuda (e.g., teclados con letras grandes).

- **Software:**

- Herramientas como lectores de pantalla, lupas virtuales, y redundancia en canales de entrada (teclado, voz, ratón).

**Usabilidad:** Según la ISO 9241-11, se define como la "efectividad, eficiencia y satisfacción con la que usuarios específicos logran metas específicas en un entorno particular". Se centra en las características de la interacción entre el producto y el usuario, buscando optimizar la experiencia de uso.

- **Conceptos clave:**

- **Efectividad:** Precisión y completitud al alcanzar metas.
  - **Eficiencia:** Uso óptimo de recursos para alcanzar dichas metas.
  - **Satisfacción:** Confort y aceptabilidad percibidos por los usuarios.

- **Usabilidad en las TIC:**

- **Hardware:**

- Estandarización de teclados, facilidad en ratones y pantallas táctiles, uso de símbolos genéricos.

- **Software:**

- **Descubrimiento:** Identificación de características que satisfacen necesidades.
    - **Aprendizaje:** Comprensión de características para completar tareas.
    - **Eficiencia:** Uso sin necesidad de guías tras aprender su manejo.

### **World Wide Web Consortium (W3C)**

Organización internacional que desarrolla estándares y recomendaciones para la web, promoviendo su interoperabilidad y accesibilidad universal. Su misión incluye garantizar el crecimiento sostenible de la red mediante la creación de protocolos y directrices.

- **Aspectos clave:**
  - **Principios de estándares abiertos.**
  - **Principios de diseño.**
  - **Visión de una web universal y accesible.**
- **Proceso de estandarización:**
  - Etapas: **Working Draft, Last Call Working Draft, Candidate Recommendation, Proposed Recommendation, y W3C Recommendation/Web Standard.**

### **Web Accessibility Initiative (WAI)**

Iniciativa del W3C, busca maximizar la accesibilidad web para personas con discapacidades, permitiéndoles participar en igualdad de condiciones. Su campo de actuación incluye:

- **Contenido web.**
- **Herramientas de creación.**
- **Navegadores y otros agentes de usuario.**
- **Protocolos y formatos.**

### **Recomendaciones de la WAI**

- **WCAG 2.0 (Web Content Accessibility Guidelines):**
  - Directrices para contenidos web organizadas en **12 pautas dentro de 4 principios:**
    - **Perceptible.**
    - **Operable.**
    - **Entendible.**
    - **Robusto.**
  - **Niveles de conformidad: A, AA, AAA.**
  - **Ejemplos:**
    - Atributo "alt" para imágenes.
    - Navegación con teclado mediante "tabindex".

- Transcripciones de audio y video con <track>.
- **ATAG 2.0 (Authoring Tool Accessibility Guidelines):**
  - Directrices para herramientas de creación, como editores WYSIWYG y CMS.
  - Pautas generales:
    - Hacer accesible la interfaz de la herramienta.
    - Apoyar la creación de contenido accesible.
- **UAAG 1.0 (User Agent Accessibility Guidelines):**
  - Directrices para navegadores, reproductores multimedia y otros agentes de usuario.
  - Principios: **Perceptible, Operable, Entendible, Acceso programático, y Especificaciones y convenciones.**

Las especificaciones técnicas incluyen estándares como **HTML, CSS, SVG, y SMIL**.

## Diseño Universal

Proceso de crear productos que sean utilizables por el mayor número de personas posible, eliminando barreras y promoviendo la participación social inclusiva. No se limita a personas con discapacidades, sino que considera la diversidad humana en general.

- **Principios:**
  - Igualdad de uso.
  - Flexibilidad.
  - Simplicidad e intuición.
  - Información fácil de percibir.
  - Tolerancia a errores.
  - Mínimo esfuerzo físico.
  - Dimensiones apropiadas para el uso.

## Experiencia de Usuario (UX)

Engloba factores relacionados con la interacción del usuario con un entorno o dispositivo, influenciando la percepción del producto, servicio o sistema.

- **Enfoque:** Diseñar productos efectivos, eficientes y satisfactorios.
- **Aspectos clave:**
  - **Facilidad de uso.**
  - **Facilidad de memorización.**

- **Captura de errores.**
- **Metodologías:**
  - **Diseño centrado en el humano:** Proceso iterativo.
  - **Diseño centrado en el usuario:** Abordaje empático.
  - **Diseño centrado en la experiencia:** Orientado a las necesidades y expectativas.

### **Interfaz de Usuario (UI)**

Se centra en la forma en que un producto o servicio se presenta a los usuarios y cómo interactúan con él. Su objetivo es ofrecer una experiencia intuitiva, accesible y estética.

- **Principios:**
  - Usabilidad.
  - Accesibilidad.
  - Estética.
  - Coherencia.
- **Elementos clave:**
  - Disposición de la información.
  - Navegación.
  - Botones, menús y otros componentes interactivos.

## Arquitectura Orientada a Servicios (SOA)

# Arquitectura Orientada a Servicios (SOA)

La **Arquitectura Orientada a Servicios (SOA)** es un estilo de diseño que organiza la funcionalidad de un sistema en **pequeñas partes reutilizables llamadas "servicios"**, diseñadas para ser accesibles a través de **interfaces estandarizadas (APIs)**. Sus objetivos principales incluyen:

- **Agilidad:** Facilitar la planificación e implementación de soluciones empresariales.
- **Reutilización:** Maximizar el aprovechamiento de recursos.
- **Federación:** Unificación de criterios empresariales.

### Características clave de SOA:

- **Interoperabilidad:** Los servicios deben ser compatibles entre distintas plataformas.
- **Capacidad descriptiva:** Cada servicio debe tener una definición clara.
- **Reutilización:** Los servicios pueden integrarse en diferentes aplicaciones.
- **Descubrimiento:** Los consumidores pueden localizar servicios en un registro.
- **Composición:** Integración en procesos más complejos.
- **Auto-contenido:** Funcionan sin dependencias externas innecesarias.
- **Gestionabilidad:** Control eficiente para monitorización y actualización.

### Relación entre proveedor y consumidor:

- Se basa en **contratos** que definen las características del servicio.
- Implica el intercambio de mensajes con:
  - **Interoperabilidad sintáctica:** Uniformidad en el formato.
  - **Interoperabilidad semántica:** Claridad en el significado.

### Principios de la relación proveedor-consumidor:

1. **Independencia de dominios:** Pueden pertenecer al mismo sistema o a diferentes.
2. **Independencia de plataformas:** Los servicios se tratan como **cajas negras**.
3. **Independencia de protocolos:** Transformación de mensajes según el formato necesario.

Cada servicio consta de **tres elementos**:

- **Lógica:** Identificación única del servicio.
- **Descripción:** Definición de su funcionalidad.
- **Interfaz:** Punto de acceso para su uso.

Los servicios se registran en un **repositorio**, donde los consumidores pueden descubrirlos para su integración.

### **Modelo de Referencia SOA y Arquitectura de Capas**

El **Modelo de Referencia SOA** es independiente de la implementación y organiza los sistemas en una **arquitectura de capas**.

- **Capas verticales (funcionales):**
  1. **Operatividad:** Bases de datos, sistemas de monitorización, sistemas industriales, etc.
  2. **Componentes:** Desvinculación del servicio respecto a la tecnología.
  3. **Servicios:** Clasificados como simples o complejos.
  4. **Procesos de negocio:** Coordinación de tareas con un objetivo empresarial.
  5. **Consumidor:** Punto de visualización o acceso a los servicios.
- **Capas horizontales (transversales):**
  6. **Integración:** Conectividad entre servicios.
  7. **Calidad de Servicio (QoS):** Requisitos no funcionales, como seguridad, rendimiento y escalabilidad.
  8. **Información:** Representación y tratamiento de datos.
  9. **Gobierno:** Normas para el diseño, desarrollo y mantenimiento de los servicios.

### **Ciclo de Vida del Servicio SOA**

El desarrollo de un servicio SOA sigue un ciclo estructurado que incluye:

1. **Análisis de inventario:** Identificación de necesidades.
2. **Modelado del servicio:** Estructuración y definición.
3. **Diseño del contrato:** Especificación de interfaces y acuerdos.
4. **Diseño de la lógica:** Detalles técnicos del servicio.
5. **Desarrollo o implementación:** Creación técnica del servicio.
6. **Pruebas:** Validación de requisitos funcionales y no funcionales.
7. **Publicación:** Registro en repositorios accesibles.
8. **Monitorización:** Evaluación del rendimiento y uso.

9. **Mejora continua:** Actualización y optimización del servicio.

En la planificación estratégica de servicios, las fases clave son:

- **Acuerdo de usuario:** Definición de contratos.
- **Servicio:** Descripción detallada.
- **Interfaz:** Especificación de mensajes.
- **Implementación:** Desarrollo y mantenimiento.

### **Estilos de Composición de Tareas en SOA**

SOA permite la ejecución de tareas, definidas como **acciones atómicas** realizadas por actores humanos. Existen varios estilos para coordinar estas tareas:

1. **Orquestación:** Un elemento externo controla el flujo de tareas.
2. **Coreografía:** Relaciones predefinidas entre tareas, sin un control central.
3. **Colaboración:** Ejecución independiente con relaciones puntuales entre tareas.

### **Servicios Web y Tecnologías Asociadas**

Los **Servicios Web (WS)** son una tecnología clave en SOA, que utiliza estándares para facilitar la integración y la interoperabilidad entre aplicaciones.

**Definición según el W3C:** Un servicio web es un sistema software diseñado para soportar la interacción máquina-a-máquina a través de una red de forma interoperable. Sus características clave incluyen:

- **Interfaz estándar:** Definida en **WSDL**.
- **Mensajería estructurada:** Basada en **SOAP**.
- **Transporte:** Generalmente **HTTP**, con serialización en **XML**.

### **Estándares y herramientas utilizadas en los servicios web:**

1. **SOAP:** Protocolo para el intercambio de mensajes.
2. **WSDL:** Lenguaje para la descripción de interfaces.
3. **UDDI:** Registro para descubrimiento de servicios.
4. **REST:** Alternativa ligera basada en HTTP.
5. **\*WS- (Web Services Extensions):** Seguridad, transacciones y confiabilidad.
6. **WS-BPEL:** Orquestación y coreografía de servicios.

### **Principios de diseño de servicios web:**

- **Contrato de servicios estandarizados:** Interfaces bien definidas.

- **Desacoplamiento:** Reducción de dependencias entre sistemas.
- **Abstracción:** Ocultación de detalles internos.
- **Reutilización:** Uso eficiente de recursos.
- **Sin estado:** Los servicios no mantienen datos entre peticiones.
- **Granularidad:** Nivel adecuado de detalle.
- **Transparencia de ubicación:** El usuario no necesita conocer la localización física del servicio.

# Arquitectura de Servicios Web y Estándares

La arquitectura de servicios web (SOA) se basa en un diseño de software que permite reutilizar elementos a través de **interfaces de servicios**. Estas interfaces se comunican mediante una red utilizando un lenguaje común. Un servicio web, según el **W3C**, es un sistema diseñado para la interacción máquina-a-máquina a través de una red, de forma **interoperable**. Su interfaz está descrita en **WSDL**, permitiendo la interacción mediante el intercambio de mensajes **SOAP**, habitualmente serializados en XML sobre HTTP. Los estándares clave son **XML, SOAP, WSDL, UDDI, REST y WS-\***.

## SOAP (Simple Object Access Protocol)

Es un protocolo estándar para la comunicación entre procesos mediante XML. **SOAP** es **stateless** (sin estado) y se apoya en protocolos como HTTP o SMTP, permitiendo construir una capa base para otros protocolos web.

Sus partes principales incluyen:

- **Envelope**: Identifica el mensaje y cómo debe procesarse.
- **Header** (opcional): Extiende funcionalidades del mensaje.
- **Body**: Contiene la información de la llamada y la respuesta.
- **Fault**: Maneja errores durante el procesamiento.

Entre sus características destacan su **extensibilidad**, **neutralidad** respecto al protocolo subyacente, y **compatibilidad** con cualquier modelo de programación. Los mensajes SOAP deben ser **válidos** (cumplir DTD) y **bien formados** (etiquetas correctamente cerradas). Su estructura XML típica incluye las etiquetas <Envelope>, <Header> y <Body>.

El **modelo de procesamiento** de SOAP define roles:

- **SOAP Sender**: Emisor inicial del mensaje.
- **Ultimate SOAP Receiver**: Receptor final encargado del procesamiento.
- **SOAP Intermediary**: Puede actuar como receptor y reenviar el mensaje.

## REST (Representational State Transfer)

REST es un estilo de arquitectura cliente-servidor que utiliza HTTP para intercambiar datos (en XML, JSON u otros formatos) sin las abstracciones de protocolos como SOAP. Sus principios son:

- **Stateless** (sin estado).
- **Caché** opcional.
- **Sistemas por capas**: El cliente solo interactúa con la capa inmediata.
- **Interfaz uniforme**.

Una API **RESTful** sigue estos principios y utiliza **URI** para identificar recursos y métodos HTTP estándar (**GET, POST, PUT, DELETE, OPTIONS, HEAD**). Estos métodos se clasifican en:

- **Seguros** (no alteran recursos): Ej., GET.
- **Idempotentes** (el resultado no varía tras múltiples solicitudes): Ej., GET, PUT, DELETE. Códigos de respuesta comunes incluyen: **200 OK, 404 Not Found, 500 Internal Server Error**. Además, emplea cabeceras de **caché** como Cache-Control o Expires para optimizar el rendimiento.

## **SOAP vs. REST**

SOAP es un protocolo **orientado a servicios**, mientras que REST se basa en la **gestión de recursos**. SOAP utiliza XML exclusivamente, mientras REST admite JSON, XML y otros formatos, ofreciendo mayor flexibilidad.

### **Descripción y descubrimiento de servicios**

Los servicios web se describen mediante documentos como **WSDL** o **OpenAPI**, que detallan sus funcionalidades, parámetros y métodos de invocación. **UDDI** facilita el descubrimiento de servicios, aunque ha perdido relevancia frente a herramientas más modernas.

### **Protocolos WS-\***

El conjunto **WS-\*** incluye estándares como **WS-Policy, WS-Security, WS-Trust y WS-Reliable Messaging**, que ofrecen soporte para seguridad, confianza, y mensajería fiable en aplicaciones distribuidas.

### **WSDL (Web Services Description Language)**

WSDL, basado en XML, describe cómo interactuar con un servicio web. Aunque diseñado principalmente para SOAP, también soporta REST. Sus componentes incluyen:

- **Service**: Agrupación de funciones.
- **Binding**: Especifica protocolos y transportes.
- **PortType/Interface**: Define operaciones y mensajes permitidos.
- **Mensaje**: Describe el contenido de las operaciones.

Los patrones de mensaje son **one-way, notification, solicit-response y request-response**.

### **UDDI (Universal Description, Discovery and Integration)**

UDDI, basado en XML, permite registrar y buscar servicios web. Aunque ha sido sustituido por herramientas como WSDL o OpenAPI, UDDI organiza su contenido en:

- **Páginas blancas:** Datos básicos de identificación.
- **Páginas amarillas:** Clasificación industrial.
- **Páginas verdes:** Información técnica de los servicios.

### **WS-I (Web Services Interoperability)**

Esta organización fomenta la interoperabilidad entre servicios web mediante perfiles como **WS-I Basic Profile**, que agrupa especificaciones como SOAP o XML.

### **XML y JSON**

- **XML:** Formato extensible para representar datos estructurados, común en aplicaciones empresariales.
- **JSON:** Alternativa ligera y fácil de leer basada en JavaScript, ampliamente usada para la transferencia de datos en web.

### **MTOM (Message Transmission Optimization Mechanism)**

MTOM, definido por el W3C, optimiza la transmisión de datos codificados en base64 entre servicios web, mejorando la eficiencia en el manejo de datos binarios.

# Modelo de desarrollo de aplicaciones basado en microservicios

## Arquitectura de microservicios

La arquitectura de microservicios es un enfoque de diseño de software basado en la construcción de aplicaciones mediante la composición de pequeños servicios **independientes** que interactúan a través de **APIs** y suelen contar con almacenamiento propio. Cada microservicio es responsable de una funcionalidad específica del sistema, lo que permite su despliegue, escalado y mantenimiento de forma autónoma. Este modelo es una evolución de la arquitectura orientada a servicios (SOA), con un diseño **descentralizado y distribuido**.

Los **beneficios** de esta arquitectura incluyen:

- **Modularidad**, que facilita el desarrollo y mantenimiento.
- **Escalabilidad**, ya que los servicios se escalan de manera independiente.
- **Versatilidad** en la implementación tecnológica.
- **Rapidez de actuación** al aislar los cambios.
- **Mantenimiento más simple y económico**.
- **Agilidad** para responder a las necesidades del negocio.

Sin embargo, también presenta **desventajas**:

- **Consumo elevado de memoria**.
- **Alta complejidad en la gestión** del sistema.
- **Requiere perfiles especializados** de desarrolladores.
- **Dificultad en las pruebas**, dado el número de servicios involucrados.
- **Falta de uniformidad** entre servicios.
- **Coste elevado de implementación inicial**.

## Características de la arquitectura de microservicios

- Los componentes son **servicios independientes**.
- Se organiza en torno a las **funcionalidades del negocio**, integrando elementos como interfaces de usuario, persistencia de datos e interoperabilidad en cada servicio.
- Fomenta una mentalidad de **productos, no proyectos**, lo que implica que los equipos son responsables de los servicios durante todo su ciclo de vida.
- Sigue el principio de **extremos inteligentes, tuberías bobas**, lo que asegura bajo acoplamiento y alta cohesión.
- **Gobierno descentralizado**, permitiendo el uso de diferentes lenguajes y tecnologías según las necesidades de cada servicio.

- Gestión de datos también **descentralizada**, garantizando mayor independencia entre servicios.
- Diseño **tolerante a fallos**, incluyendo mecanismos como:
  - **Tiempos de espera máximos**, que realizan reintentos o encolan solicitudes fallidas.
  - **Disyuntores**, que actúan como “interruptores” para evitar sobrecargar el sistema al desconectar servicios cuando se alcanzan umbrales de fallos.
  - **Compartimentos estancos**, que aíslan fallos para evitar que afecten al sistema completo.
- Automatización de infraestructura mediante **CI/CD** (Integración y Despliegue Continuo).
- Fomenta un **diseño evolutivo**, adaptándose a las necesidades del negocio y las mejoras tecnológicas.

### Integración de servicios

Existen diferentes enfoques para coordinar los microservicios, dependiendo de las necesidades del sistema:

- **Orquestación**: Un servicio centralizado actúa como **orquestador**, controlando la ejecución de los demás servicios. Es útil para garantizar un mayor control y seguimiento, aunque puede generar una dependencia excesiva del orquestador y aumentar la complejidad del sistema.
- **Coreografía**: Los servicios interactúan de manera más **autónoma**, reduciendo la dependencia centralizada y mejorando la escalabilidad. Sin embargo, este enfoque puede requerir una mayor coordinación y ser más difícil de implementar.
- **Colaboración**: Los servicios trabajan de manera **informal**, sin una estructura rígida de coordinación. Esto ofrece mayor flexibilidad, pero implica tolerar cierta incertidumbre en los flujos de trabajo y puede ser complejo de gestionar.

### Soluciones para microservicios

Los microservicios suelen desplegarse en contenedores (por ejemplo, **Docker**) para garantizar su portabilidad y capacidad de ejecución en cualquier máquina o servidor. Esto facilita el despliegue y ofrece beneficios como:

- Mayor **flexibilidad** en la asignación de recursos.
- Mejor **disponibilidad** del sistema.
- Incremento en la **tolerancia a fallos**.

## Formatos usados para interoperabilidad de servicios: JSON y XML

### JSON (JavaScript Object Notation)

Es un formato abierto ampliamente utilizado para el intercambio de datos. Aunque originalmente es un subconjunto de la notación literal de objetos de JavaScript, su adopción masiva lo ha consolidado como un **formato independiente del lenguaje**. JSON se posiciona como una alternativa a XML, pero es habitual encontrar aplicaciones que combinan ambos formatos.

JSON destaca por su simplicidad, ya que es mucho más sencillo desarrollar un **parser** (analizador sintáctico) para JSON que para XML. Los tipos de datos admitidos en JSON incluyen **números, cadenas de texto, valores booleanos, null, arrays y objetos** (estructuras similares a diccionarios en otros lenguajes).

#### Modelos de procesamiento de JSON

- **Modelo de objeto:** Todo el contenido del JSON se carga en memoria como un árbol de datos, permitiendo una manipulación completa pero consumiendo más memoria.
- **Modelo de flujo:** Los datos se procesan de forma secuencial en bloques, lo que resulta más eficiente en memoria pero limita la accesibilidad directa al JSON completo.

#### Conversión de JSON a objetos del lenguaje

Una práctica común en lenguajes como JavaScript es convertir estructuras JSON en objetos nativos. Sin embargo, es importante evitar el uso de **eval()** debido a los riesgos de seguridad que implica, ya que eval ejecuta directamente el código. En su lugar, se recomienda usar **Function()**, que permite generar una función que solo se ejecutará bajo control explícito del usuario.

#### Validación de JSON

- **Validación sintáctica:** Verifica que el JSON esté correctamente formado según las reglas del formato, como el uso de comillas, comas, y delimitadores adecuados.
- **Validación semántica:** Comprueba que el JSON sea válido respecto a un esquema predefinido. Un esquema especifica la **gramática, estructura, contenido y significado** esperado, y puede definir modelos como “Persona”, “Automóvil” o “Usuario”.

#### MIME type de JSON

El **MIME type** asociado a JSON es **application/json**, y es esencial especificarlo al intercambiar datos a través de HTTP para garantizar el correcto reconocimiento del formato.

#### Manipulación de JSON en JavaScript

JavaScript ofrece métodos nativos para trabajar con JSON:

- **JSON.stringify()**: Convierte un objeto o estructura de datos en una cadena JSON.
- **JSON.parse()**: Transforma una cadena JSON válida en un objeto JavaScript.

## Programación sin código

# Programación Low-Code y No-Code

### Programación No-Code

Técnica diseñada para que usuarios con conocimientos básicos de programación puedan desarrollar aplicaciones y soluciones de software. Este enfoque se basa en el uso de **interfaces visuales** y una mínima cantidad de código, lo que **reduce la complejidad** del desarrollo y permite que los usuarios se concentren en la **solución de problemas** y la **definición de requisitos funcionales**.

Su audiencia principal son personas con **nociónes básicas** de programación, quienes pueden aprovechar estas herramientas para crear soluciones personalizadas sin la necesidad de ser programadores profesionales.

### Programación No-Code

Permite la creación de aplicaciones y soluciones de software sin escribir código en absoluto. Se basa en **plataformas intuitivas** que ofrecen **bloques de construcción preconfigurados** y componentes reutilizables que los usuarios pueden combinar mediante herramientas de arrastrar y soltar.

Está dirigida a personas **sin experiencia previa en programación**, democratizando el acceso al desarrollo de software y fomentando la creatividad en usuarios sin conocimientos técnicos.

### Plataformas más conocidas

Algunas de las plataformas más utilizadas en estos enfoques son:

- **WordPress**, popular para la creación de sitios web.
- **Honeycode**, para el desarrollo de aplicaciones.
- **AppSheet**, centrada en la construcción de aplicaciones móviles y web.
- **PowerApps**, que permite la integración con el ecosistema de Microsoft.
- **Figma**, orientada al diseño y prototipado de interfaces web y aplicaciones.

Estas herramientas se han consolidado como opciones líderes debido a su facilidad de uso y capacidad de adaptación a diferentes casos de uso.

### Ventajas

Las principales ventajas de la programación Low-Code y No-Code incluyen:

- **Agilidad**: Permite crear aplicaciones en menos tiempo.

- **Autonomía:** Usuarios no técnicos pueden desarrollar sin depender de programadores.
- **Ahorro:** Reduce costes al minimizar la necesidad de desarrolladores especializados.
- **Colaboración:** Fomenta el trabajo conjunto entre departamentos técnicos y no técnicos.
- **Facilidad de uso:** Interfaces intuitivas accesibles para usuarios con poca o ninguna formación.
- **Velocidad de desarrollo:** Ideal para prototipos o aplicaciones que deben desarrollarse rápidamente.
- **Mayor eficiencia:** Automatiza tareas repetitivas y simplifica el desarrollo.

### Desventajas

A pesar de sus ventajas, estos enfoques presentan **limitaciones** que deben considerarse:

- **Restricciones funcionales:** Las aplicaciones creadas pueden carecer de flexibilidad o funcionalidades avanzadas.
- **Dependencia de la herramienta:** Los usuarios quedan atados a las capacidades y licencias de la plataforma utilizada.
- **Conocimientos técnicos limitados:** Puede dificultar la personalización profunda o la resolución de problemas complejos.
- **Problemas de seguridad:** Algunas plataformas pueden no cumplir con estándares robustos de seguridad, exponiendo riesgos en aplicaciones críticas.

## Gestión Documental

### Gestión Documental

La **gestión documental** consiste en controlar de manera eficiente y sistemática la creación, recepción, mantenimiento, utilización y disposición de los documentos. Esto abarca desde la generación hasta la eliminación o conservación permanente de los mismos, siguiendo políticas establecidas para asegurar su integridad y accesibilidad.

#### Tratamiento de Imágenes y Proceso Electrónico de Documentos

El tratamiento de imágenes dentro del proceso electrónico de documentos incluye:

- **Digitalización:** Consiste en transformar un documento físico en un documento electrónico compuesto por una **imagen electrónica**, metadatos y, opcionalmente, una **firma electrónica**.
- **Imagen Electrónica:** Debe ser válida según las **Normas Técnicas de Interoperabilidad (NTIs)**.
- **Formatos Admitidos:** PNG, RTF, SVG o TIFF.
- **Resolución Mínima:** 200 ppp en blanco y negro, color o grises.
- **Requisitos Adicionales:** La imagen debe respetar la geometría del documento original y no incluir caracteres o gráficos no presentes en el documento fuente.
- **Proceso de Digitalización:** Debe ser automático para garantizar la integridad y evitar manipulación humana, abarcando captura, optimización, asignación de metadatos y firma electrónica si procede.
  - **Captura:** Mediante un proceso fotoeléctrico.
  - **Optimización:** Realizada si es necesario.
  - **Asignación de Metadatos:** Incluye información básica o complementaria como resolución, tamaño, idioma, etc.
  - **Firma Electrónica:** Si se aplica, el documento digitalizado puede sustituir legalmente al original, permitiendo su destrucción.

#### Beneficios de la Digitalización

Los beneficios de la digitalización son de naturaleza estratégica, financiera y técnica, mejorando la eficiencia, reduciendo costos y facilitando el acceso y gestión de los documentos.

## Elementos del Sistema de Gestión Documental

Un **gestor documental** es una aplicación que facilita la generación, tratamiento, publicación y conservación de documentos electrónicos. Los elementos clave de un sistema de gestión documental incluyen:

- **Esquema o Cuadro de Clasificación:** Permite la identificación, clasificación y codificación de documentos y expedientes al ser recibidos o producidos.
- **Calendario de Conservación:** Define los períodos de conservación y el destino final de los documentos, determinando cuándo serán eliminados o conservados como archivos permanentes.
- **Sistema de Archivo Corporativo:** Repositorio para la ordenación y preservación de la documentación que no requiere disponibilidad inmediata.
- **Sistema de Acceso a la Información:** Facilita la localización y acceso a la documentación, controlando accesos y gestionando permisos.
- **Tipos de Sistemas de Información Asociados:**
  - **Modelos Relacionales.**
  - **Datacéntricos:** La información depende del sistema, por ejemplo, bases de datos.
  - **Docucéntricos:** Los documentos son independientes del sistema, como en Alfresco, donde se almacenan en el sistema de ficheros y se relacionan mediante metadatos en la base de datos.

## Productos de Gestión Documental Basados en Modelos Relacionales

- **Content Management Systems (CMS):** Enfocados en la producción colaborativa de contenidos estructurados, como páginas web.
- **Document Management (DM):** Administran el flujo de documentos dentro de una organización.
- **Records Management (RM):** Gestionan registros que son evidencia de las actividades de una empresa.
- **Enterprise Content Management (ECM):** Gestión global de contenidos que integra CMS, DM, RM, entre otros.

## Requisitos de un Sistema de Gestión Documental (SGD)

- **Metadatos:** Información adjunta a un documento que permite su identificación, autenticación y contextualización, regulados por normas técnicas como las NTIs.
- **Integración:** Debe integrarse con sistemas productores de documentos y sistemas de ficheros, como Microsoft SharePoint, utilizando protocolos como WebDAV, CIFS, NFS, IMAP, etc.

- **Otros Requisitos:** Incluyen indexación, almacenamiento, recuperación, colaboración (flujos de trabajo, control de versiones), publicación y seguridad.

### Gestión de Contenidos o Content Management System (CMS)

Un **CMS** es una aplicación que permite crear estructuras de soporte de información para la creación y gestión posterior de contenidos. Sus características incluyen:

- **Publicación Web:** Permite la difusión de contenidos a través de Internet.
- **Indexación, Revisión, Búsqueda y Recuperación:** Facilitan la gestión eficiente de la información.

### Partes de un CMS

- **Web Pública:** Accesible a través de una URL.
- **Web Privada:** Parte interna que incluye:
  - **CMA (Content Management Application):** Permite crear, editar y eliminar contenidos.
  - **CDA (Content Dispensing Application):** Compila y publica la información en el sitio web.

### Capas del CMS

La **renderización** de un gestor de contenidos se compone de varias capas:

- **Capa de Base de Datos:** Administración, permisos, usuarios, utilizando tecnologías como MySQL.
- **Capa de Programación:** Responde a peticiones y muestra información, utilizando tecnologías como PHP.
- **Capa de Diseño:** Maqueta la página con tecnologías como HTML y CSS.

### Tipos de CMS

Incluyen sistemas como:

- **Learn Management System (LMS):** Ejemplo, Moodle.
- **Sistemas de Comercio Electrónico:** Ejemplo, Shopify.
- **Blogs, Foros, Wikis.**
- **Sistemas de Difusión de Contenidos Multimedia (DMS).**

## **Portafirmas Electrónico**

Es una herramienta para firmar electrónicamente documentos utilizando el certificado digital del firmante. **Port@firmas** es una aplicación que integra la firma electrónica en los flujos de trabajo de una organización, facilitando la autenticación y legalidad de los documentos electrónicos.

## **CSV (Código Seguro de Verificación)**

El **CSV** es un código único que identifica un documento electrónico, garantizando su integridad mediante el cotejo en las sedes electrónicas habilitadas, como Ministerios, Comunidades Autónomas y Entidades Locales.

## **Archivo Electrónico**

Un **archivo electrónico** se encarga del almacenamiento, custodia y conservación de documentos generados electrónicamente, así como de su consulta y recuperación. El **ciclo de vida del documento** incluye todas las etapas desde su identificación hasta su conservación permanente o destrucción reglamentaria.

## **Fases del Archivo**

- **Fase 1: Archivo Activo o de Gestión:** Reúne documentación en trámite, sometida a uso y consulta administrativa continua. Los documentos están en el gestor documental.
- **Fase 2: Archivo Semi-activo, Central o Intermedio:** Coordina y controla los archivos de gestión, reuniendo documentos una vez finalizado su trámite.
- **Fase 3: Archivo Inactivo o Histórico:** Conserva permanentemente documentos de valor histórico, siguiendo políticas definidas para su preservación o expuración.

## **Fases del Ciclo Vital del Documento**

- **Fase de Captura:** Incorporación del documento al sistema de gestión documental.
- **Fase de Mantenimiento y Uso:** Disponibilidad y validez administrativa de los documentos.
- **Fase de Conservación y Selección:** Eliminación reglamentaria de documentos efímeros y conservación de aquellos con valor a largo plazo.

## **InSide (Infraestructuras y Sistemas para el Documento Electrónico)**

**InSide** es un sistema para la gestión de documentos y expedientes electrónicos que cumple con los requisitos del ENI. Se utiliza en dos modos:

- **InSide Base:** Permite almacenar y modificar documentos y expedientes en gestores compatibles con el estándar CMIS, gestionando metadatos, asociaciones, índices, validaciones y firmas.
- **G-Inside (Generador de InSide):** Servicios web en la nube para validar y generar documentos y expedientes según el ENI, incluyendo la generación de PDFs.

### **Archivo Electrónico Longevo**

Un **archivo electrónico longevo** asegura el almacenamiento seguro, custodia, preservación, recuperación y consulta de documentos tras la finalización de sus fases activa y semi-activa.

### **Roles y Responsabilidades en un Sistema de Gestión Documental**

Incluyen la dirección, responsables de procesos de gestión, planificación, implantación y administración del programa de tratamiento de documentos, y responsables de las unidades administrativas que gestionan documentos electrónicos.

### **Tipos de Sistemas de Gestión Documental Electrónica**

- **Sistema de Gestión de Documentos Electrónicos (SGDE):** Para documentos que aún no han alcanzado su estado definitivo, permitiendo modificaciones, versionado y borrado.
- **Sistemas de Gestión de Documentos Electrónicos de Archivo (SGDEA)/Archivos Electrónicos Longevos:** Para documentos en su forma definitiva, garantizando su inmutabilidad.

### **Procesos de Gestión Documental y Archivo**

Incluyen captura, registro, clasificación, descripción, acceso y trazabilidad, calificación, conservación, transferencia, destrucción y eliminación, asignación de metadatos, documentación, formación, supervisión y auditoría, y gestión de la política.

### **Junta Calificadora de Documentos Administrativos (JCDA)**

En la **Generalitat Valenciana (GVA)**, la JCDA dicta sobre la valoración, conservación y eliminación de documentos a conservar por los archivos longevos.

### **OAIS (Open Archival Information System)**

Es un modelo conceptual destinado a la gestión, archivo y preservación a largo plazo de documentos. Define las funciones, responsabilidades y organización necesarias para preservar la información y garantizar el acceso a una comunidad de usuarios.

## Esquema Nacional de Interoperabilidad (ENI)

### Esquema Nacional de Interoperabilidad

El Real Decreto 4/2010 establece el Esquema Nacional de Interoperabilidad (ENI) en el ámbito de la Administración Electrónica. Su objetivo es comprender y definir el conjunto de criterios y recomendaciones que las Administraciones Públicas deben tener en cuenta para la toma de decisiones tecnológicas que garanticen la interoperabilidad.

El ENI busca asegurar un nivel adecuado de interoperabilidad en los datos, informaciones y servicios, evitando así la discriminación de los ciudadanos por razones de elección tecnológica. Se atiende, además, al Marco Europeo de Interoperabilidad.

#### Objeto

El ENI tiene como objeto establecer los criterios y recomendaciones en materia de **seguridad, normalización y conservación** de la información, formatos y aplicaciones utilizados por las Administraciones Públicas, garantizando así la interoperabilidad **organizativa, semántica y técnica**.

#### Ámbito de Aplicación

El ENI es de aplicación obligatoria para **todas las Administraciones Públicas** españolas.

#### Principios Básicos de la Interoperabilidad

La interoperabilidad en el ENI se basa en los siguientes principios:

- **Interoperabilidad como calidad integral:** Debe estar presente durante todo el ciclo de vida de los sistemas y servicios, incluyendo planificación, diseño, adquisición, implantación, despliegue, explotación y finalización.
- **Carácter multidimensional:** Abarca dimensiones organizativa, semántica y técnica, y considera también la interoperabilidad temporal.
- **Enfoque de soluciones multilaterales:** Se promueve el aprovechamiento de ventajas de escalado, arquitecturas modulares y multiplataforma, y la colaboración para compartir y reutilizar soluciones.

#### Interoperabilidad Organizativa

Se refiere a las condiciones de acceso y utilización de los servicios, datos y documentos en formato electrónico que se ponen a disposición del resto de Administraciones Públicas.

- **Servicios disponibles electrónicamente:** Las AAPP deben publicar las condiciones de acceso y uso de sus servicios, datos y documentos en la **Red de comunicaciones de las Administraciones Públicas españolas** o equivalente.
- **Uso de Nodos de Interoperabilidad:** Son entidades que gestionan la interoperabilidad de forma global o parcial.
- **Inventarios de Información Administrativa:** Cada AAPP debe mantener actualizado un inventario que incluye los procedimientos administrativos y servicios que prestan, clasificados y estructurados en familias, indicando su nivel de informatización. Este inventario debe integrarse con el de la Administración General del Estado.

### **Interoperabilidad Semántica**

Busca establecer un **lenguaje común de información** entre las AAPP.

- Se deben establecer y mantener actualizadas las relaciones de **modelos de datos de intercambio**.

### **Interoperabilidad Técnica**

Se enfoca en el uso de **estándares abiertos o de uso generalizado**.

- **Estándares Aplicables:** Se deben utilizar estándares abiertos o, en su defecto, estándares de uso generalizado. Si no existe alternativa abierta, se pueden utilizar estándares no abiertos.
- **Criterios de Selección:** Se consideran las especificaciones técnicas TIC, la definición de estándar abierto según la Ley 11/2007, la formalización de especificaciones y los costes que no supongan una dificultad de acceso.

### **Infraestructuras y Servicios Comunes**

Las AAPP deben enlazar sus infraestructuras y servicios con las de la Administración General del Estado para facilitar la interoperabilidad y la relación multilateral.

### **Comunicaciones de las Administraciones Públicas**

- **Uso Preferente de la Red SARA:** Las AAPP utilizarán preferentemente la **Red SARA** (Sistema de Aplicaciones y Redes para las Administraciones) para sus comunicaciones internas. Esta red conecta las redes de las AAPP españolas e instituciones europeas, facilitando el intercambio de información y el acceso a servicios.
- **Plan de Direccionamiento e Interconexión:** Se establece según las Normas Técnicas de Interoperabilidad.

- **Sincronización Horaria:** Las AAPP deben sincronizar sus sistemas con la hora oficial basada en el **Real Instituto y Observatorio de la Armada**, y con la hora oficial a nivel europeo cuando sea posible.

## Reutilización y Transferencia de Tecnología

- **Condiciones de Licenciamiento:** La licencia de las tecnologías debe ser libre y abierta, procurando aplicar la **Licencia Pública de la Unión Europea**.
- **Tecnología Propiedad de las AAPP:** Se promueve el aprovechamiento y reutilización de recursos públicos, protección contra apropiación por terceros, y ausencia de responsabilidad y asistencia técnica. Por defecto, se facilita sin contraprestación ni necesidad de convenio.
- **Tecnología Utilizada por las AAPP:** Debe permitir ejecución libre, acceso al código fuente, posibilidad de modificación y mejora, y libertad para redistribuir.
- **Directorios de Aplicaciones Reutilizables:** Se crean para favorecer el compartir, reutilizar y colaborar, mejorando la eficiencia. Los directorios propios deben ser accesibles desde el **Centro de Transferencia de Tecnología**.

## Firma Electrónica y Certificados

Las AAPP deben aprobar y publicar su **política de firma electrónica y de certificados** para regular la interoperabilidad en la autenticación y reconocimiento mutuo de firmas electrónicas dentro de su ámbito.

- **Interoperabilidad en la Política de Firma Electrónica y Certificados:**
  - Definida por la Administración General del Estado como marco general.
  - Aplicada por todos los organismos y entidades de Derecho Público de la AGE.
  - La no aplicación debe estar justificada y autorizada por la **Secretaría General de Administración Digital**.
  - Otras AAPP pueden desarrollar políticas propias, partiendo de la norma técnica y comunicándolas a la Secretaría General de Administración Digital.
- **Aspectos Definidos en las Políticas de Firma:**
  - Validación y aceptación de documentos electrónicos recibidos.
  - Interoperabilidad de las aplicaciones usuarias.
  - Características técnicas y operativas de la lista de prestadores de servicios de certificación de confianza.
- **Plataformas de Validación:**
  - Proporcionan servicios de confianza a las aplicaciones usuarias.
  - Centralizan elementos de confianza e interoperabilidad.

- Potencian la armonización técnica y el uso común de formatos, estándares y políticas.
- Incorporan listas de confianza de certificados interoperables entre AAPP nacionales y europeas.

### **Recuperación y Conservación del Documento Electrónico**

Las AAPP deben adoptar medidas técnicas y organizativas para garantizar la interoperabilidad en la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida.

- **Medidas a Implementar:**

- Políticas de gestión de documentos.
  - Expedientes con un índice electrónico.
  - Identificación única e inequívoca de cada documento.
  - Uso de metadatos mínimos obligatorios.
  - Clasificación y periodo de conservación definidos.
  - Acceso completo e inmediato a los documentos.
  - Conservación a largo plazo.
  - Registro de eliminación de documentos.
  - Formación del personal.
- **Seguridad:** Se aplicará el **Esquema Nacional de Seguridad** para garantizar la integridad, autenticidad, confidencialidad, disponibilidad, trazabilidad, calidad, protección, recuperación y conservación física y lógica de los documentos electrónicos, sus soportes y medios.
  - **Firma Electrónica en la Conservación:** Se seguirá la política de firma electrónica y de certificados, utilizando firmas longevas.
  - **Formatos de los Documentos:**
    - Se conservarán en el formato en que fueron elaborados, enviados o recibidos.
    - Preferentemente en estándares abiertos que perduren en el tiempo.
    - Si existe riesgo de obsolescencia o el formato deja de ser admitido en el ENI, se aplicarán procedimientos normalizados de **copiado auténtico**.
  - **Digitalización de Documentos en Papel:**
    - Se realizará según la Norma Técnica de Interoperabilidad correspondiente.
    - Considera aspectos como formatos estándar, resolución, garantía de imagen fiel e íntegra y metadatos mínimos obligatorios y complementarios asociados al proceso de digitalización.

### **Normas de Conformidad del ENI**

El cumplimiento del ENI es obligatorio en:

- **Sedes y registros electrónicos.**
- **Ciclo de vida de servicios y sistemas.**

Cada AAPP debe establecer sus mecanismos de control y publicar sus declaraciones de conformidad respecto al ENI.

Es necesaria una actualización permanente de la adecuación al ENI.

### **Normas Técnicas de Interoperabilidad**

Las Normas Técnicas de Interoperabilidad desarrollan aspectos específicos del ENI. Entre ellas se incluyen:

- **Catálogo de Estándares.**
- **Documento Electrónico.**
- **Digitalización de Documentos.**
- **Expediente Electrónico.**
- **Política de Firma Electrónica y de Certificados de la Administración.**
- **Protocolos de Intermediación de Datos.**
- **Relación de Modelos de Datos Comunes en la Administración.**
- **Política de Gestión de Documentos Electrónicos.**
- **Requisitos de Conexión a la Red SARA.**
- **Procedimientos de Copiado Auténtico y Conversión entre Documentos Electrónicos.**
- **Modelo de Datos para el Intercambio de Asientos entre Entidades Registrales.**

### **Instrumentos para la Interoperabilidad**

- **Inventario de Procedimientos Administrativos y Servicios Prestados:** Contiene información detallada de los procedimientos y servicios de las AAPP.
- **Centro de Interoperabilidad Semántica de la Administración:** Publica los modelos de datos de intercambio.
- **Directorio de Aplicaciones para su Libre Reutilización:** Incluye la relación de aplicaciones disponibles para reutilización, fomentando la eficiencia y colaboración entre las AAPP.

## Normas Técnicas de Interoperabilidad (NTI)

Las Normas Técnicas de Interoperabilidad (NTI) son un conjunto de directrices que establecen criterios y recomendaciones para garantizar la interoperabilidad técnica entre las Administraciones Públicas en España. Estas normas son esenciales para asegurar que los sistemas y servicios electrónicos puedan comunicarse y trabajar juntos de manera eficiente y segura.

### NTI de Expedientes Electrónicos

Esta norma establece la estructura y el formato que deben tener los expedientes electrónicos, así como las especificaciones para los servicios de remisión y puesta a disposición entre las Administraciones Públicas. Los expedientes electrónicos deben incluir una serie de **metadatos mínimos**, entre los que se encuentran:

- Versión de la NTI utilizada.
- Identificador único del expediente.
- Órgano administrativo responsable.
- Fecha de apertura del expediente.
- Clasificación o materia del expediente.
- Estado actual del expediente.
- Interesado o interesados involucrados.
- Tipo de firma electrónica aplicada.
- Código Seguro de Verificación (CSV).

Estos metadatos deben estar presentes en cualquier proceso de intercambio entre Administraciones Públicas y no deben ser modificados en ninguna fase posterior, excepto en caso de errores.

### NTI de Documento Electrónico

Esta norma define los **metadatos mínimos obligatorios** que deben acompañar a un documento electrónico, la asociación de los datos y metadatos de firma o de sellado de tiempo, así como otros metadatos complementarios asociados. También especifica los formatos que deben utilizarse para los documentos electrónicos.

Los metadatos mínimos incluyen:

- Versión de la NTI utilizada.
- Identificador único del documento.
- Órgano administrativo que emite el documento.

- Fecha de captura o creación del documento.
- Origen del documento.
- Estado de elaboración.
- Nombre del formato del documento.
- Tipo documental.
- Tipo de firma electrónica aplicada.
- Código Seguro de Verificación (CSV).
- Identificador del documento origen (si procede).

Estos metadatos garantizan la autenticidad, integridad y trazabilidad del documento electrónico en los procesos administrativos y en los intercambios entre Administraciones Públicas.

#### **NTI de Digitalización de Documentos**

Esta norma aborda los formatos y estándares aplicables en la digitalización de documentos, los niveles de calidad requeridos, las condiciones técnicas y los metadatos asociados al proceso de digitalización.

Los **requisitos de la imagen electrónica** resultante son:

- Utilizar formatos de imagen según el Catálogo de Estándares del Esquema Nacional de Interoperabilidad (ENI).
- Resolución mínima de 200 ppp (puntos por pulgada) en color, blanco y negro o escala de grises.
- Respetar la geometría original del documento, sin alteraciones.
- No contener caracteres o gráficos que no estuviesen en el documento de origen.

El **proceso de digitalización** debe incluir:

- Digitalización mediante un medio fotoeléctrico.
- Optimización automática de la imagen electrónica para garantizar su legibilidad, si procede.
- Asignación de los metadatos correspondientes.
- Firma de la imagen electrónica, si procede.

#### **NTI de Política de Firma Electrónica y Certificados de la Administración**

Esta norma trata sobre los formatos de firma, los algoritmos y longitudes mínimas de las claves, las reglas de creación y validación de la firma electrónica, la gestión de las políticas de firma, el uso de referencias temporales y de sellos de tiempo, así como la normalización de la

representación de la firma electrónica en pantalla y en papel para el ciudadano y en las relaciones entre Administraciones Públicas.

La política de firma electrónica debe definir:

- Los procesos de creación, validación y conservación de firmas electrónicas y sellos electrónicos.
- Las características y requisitos de los sistemas de firma electrónica, sellos electrónicos, certificados y sellos de tiempo.

Además, la política debe incluir:

- Definición del alcance y ámbito de aplicación.
- Datos para la identificación del documento y del responsable de su gestión.
- Reglas comunes y responsabilidades para el **firmante**, el **creador del sello** y el **verificador** de la firma o sello electrónicos.

Los **agentes involucrados** son:

- **Firmante**: Persona física que crea una firma electrónica.
- **Creador del sello**: Entidad que aplica un sello electrónico en representación de una persona jurídica.
- **Verificador**: Entidad o persona que valida la firma o sello electrónico.
- **Prestador de servicios de confianza**: Proveedor que emite certificados y servicios relacionados.
- **Emisor**: Entidad que emite el documento electrónico.
- **Gestor de la política de firma**: Responsable de la definición y mantenimiento de la política de firma electrónica.

### **NTI de Protocolos de Intermediación de Datos**

Esta norma establece las especificaciones de los protocolos de intermediación de datos que facilitan la integración y reutilización de servicios entre las Administraciones Públicas. Es aplicable tanto para los prestadores como para los consumidores de estos servicios.

Los **agentes en el intercambio de datos** son:

- **Cedente**: Entidad propietaria de los datos y responsable de su cesión.
- **Emisor**: Responsable del tratamiento tecnológico de los datos y de su transmisión.
- **Cesionario**: Organismo que necesita los datos para sus procedimientos y solicita su cesión.
- **Requirente**: Responsable del tratamiento tecnológico de los datos y de su recepción.

**El Protocolo de Acceso a Servicios Intermediados (SCSP)** es fundamental para garantizar un intercambio seguro y eficiente de datos entre las Administraciones Públicas, facilitando la integración de servicios y promoviendo la interoperabilidad.

# Interoperabilidad Europea, Nacional y Autonómica

## Interoperabilidad y Sistemas de Cooperación entre Administraciones Públicas

La **interoperabilidad** es la capacidad que tienen los sistemas de información y los procedimientos que estos soportan para compartir datos y posibilitar el intercambio de información y conocimiento entre ellos. Esta cualidad es esencial para garantizar una comunicación efectiva y eficiente entre diferentes entidades y niveles administrativos.

### Tipos de interoperabilidad:

- **Interoperabilidad Organizativa:** Se refiere al conjunto de políticas y acuerdos de colaboración entre organizaciones con estructuras internas y niveles de servicio distintos que desean intercambiar información. Facilita la coordinación y alineación de procesos entre entidades diversas.
- **Interoperabilidad Semántica:** Es la capacidad de distintos sistemas de información, definidos por organismos y orígenes diferentes, para entender y procesar la información de manera coherente. Asegura que el significado de los datos intercambiados sea interpretado de la misma forma por todos los sistemas involucrados.
- **Interoperabilidad Técnica:** Comprende el conjunto de características técnicas que garantizan el intercambio físico y lógico de datos entre los sistemas de información de diferentes organismos. Incluye protocolos, interfaces y estándares tecnológicos que permiten la comunicación efectiva entre sistemas.

### Aspectos relevantes de la interoperabilidad:

- **Identidad**
- **Intercambio de expedientes**
- **Intercambio de documentos**
- **Intercambio de datos**
- **Servicios de interoperabilidad**
- **Marco legal**

## Política de la Unión Europea y Normativa al Respecto

La Unión Europea promueve activamente la interoperabilidad entre las administraciones públicas de sus Estados miembros para facilitar la prestación de servicios públicos electrónicos y apoyar la aplicación de políticas comunitarias.

- **Programa ISA (Soluciones de Interoperabilidad para las Administraciones Públicas):** Su objetivo es apoyar la cooperación entre las administraciones públicas europeas,

posibilitando la prestación de servicios públicos electrónicos que fomenten la aplicación de políticas y actividades comunitarias.

- **NIFO (Observatorio de los Marcos Nacionales de Interoperabilidad):** Este observatorio realiza el seguimiento de las principales actividades de interoperabilidad, analiza las normativas nacionales y su alineamiento con el marco europeo, y proporciona información sobre las mejores prácticas en interoperabilidad.
- **Proyecto e-SENS (Servicios Electrónicos Europeos Simples e Interconectados):**
  - Facilita el acceso de los ciudadanos de cualquier país de la UE a los servicios públicos de los distintos países miembros.
  - Dota a los servicios públicos de una perspectiva transfronteriza.
  - Consolida soluciones existentes para proponer una infraestructura única y coherente.

### **Plataformas de Interoperabilidad**

Las plataformas de interoperabilidad son infraestructuras tecnológicas que facilitan el intercambio de datos entre administraciones públicas, simplificando la complejidad administrativa y organizando los servicios de interoperabilidad en un único punto común.

**Plataforma de Intermediación de Datos del Ministerio de Hacienda y Administraciones Públicas (MinHaP):** Facilita el intercambio de datos entre administraciones públicas para evitar solicitar al ciudadano información que ya obra en poder de la administración.

- **Servicios ofrecidos:** Datos de identidad, residencia, desempleo, información censal, títulos oficiales, estado al corriente de pagos con la Seguridad Social, información de renta y obligaciones tributarias, entre otros.

**Plataforma Autonómica de Interoperabilidad de la Generalitat Valenciana (PAI):** Tiene como objetivo ofrecer y facilitar servicios web para el intercambio de información a las diferentes entidades de la Comunitat Valenciana, incluida la propia Generalitat.

- **Servicios ofrecidos:** Verificación de datos de un ciudadano, como por ejemplo su identidad o situación administrativa.

**NISUE (Nodo de Interoperabilidad del Sistema Universitario Español):** Actúa como punto único para el intercambio de información universitaria.

- **Servicios ofrecidos:** Cesión de datos académicos, traslado de expedientes académicos, entre otros.

**Red SARA (Sistemas de Aplicaciones y Redes para las Administraciones):** Es un conjunto de infraestructuras de comunicaciones y servicios básicos que conecta a las administraciones

públicas españolas y a instituciones europeas, facilitando el intercambio de información y el acceso a servicios. Las administraciones públicas publicarán aquellos servicios que pongan a disposición de las demás administraciones a través de la red de comunicaciones de las administraciones públicas españolas, o de cualquier otra red equivalente o conectada a la misma que garantice el acceso seguro al resto de administraciones.

- **Características de la Red SARA:**
  - **Fiabilidad:** Operatividad 24x7x365.
  - **Seguridad:** Garantiza la protección y confidencialidad de la información.
  - **Capacidad:** Soporta un gran volumen de tráfico y usuarios.
  - **Calidad de Servicio (QoS):** Asegura un rendimiento óptimo en la prestación de servicios.
  - **Interoperabilidad:** Facilita la comunicación entre diferentes sistemas y plataformas.
  - **Flexibilidad:** Se adapta a las necesidades cambiantes de las administraciones.
- **Organismos responsables:**
  - Ministerio de Hacienda y Administraciones Públicas
  - Secretaría de Estado de Administraciones Públicas
  - Dirección de Tecnologías de la Información y las Comunicaciones
- **Alcance:** Conecta a más de 4,000 entidades, cubriendo al 93% de la población española.
- **Servicios ofrecidos:**
  - Verificación de datos (identidad, residencia, datos tributarios, catastro, desempleo, Seguridad Social, títulos académicos, etc.).
  - Plataforma de validación de firma electrónica (@Firma).
  - Comunicación de cambio de domicilio.
  - Punto de entrada centralizado para facturas electrónicas (FACE).
  - Pasarela de pago.
  - Registro electrónico común.
  - Consultas del estado de expedientes.
  - Catálogos de procedimientos de las administraciones públicas.
  - Servicios de correo electrónico SMTP, sincronización horaria NTP, resolución de nombres DNS, videoconferencia, Voz IP, entre otros.
- **Catálogo de Soluciones de Administración Digital:** Su propósito es difundir los servicios compartidos, infraestructuras y otras soluciones disponibles para las administraciones públicas.

## Plataforma Autonómica de Interoperabilidad de la Generalitat Valenciana (PAI)

La PAI facilita el intercambio de información entre los diferentes departamentos de la Generalitat y entre estos y el resto de las administraciones públicas.

### Detalles:

- Canaliza la relación con la Plataforma de Intermediación de Datos Estatal (PID) a través de la Red SARA.
- Centraliza el intercambio de información y gestiona las solicitudes e incidencias técnicas y organizativas.
- Potencia la interoperabilidad entre aplicaciones de diferentes entidades.

**Arquitectura:** Implementada sobre Oracle Service Bus (OSB).

### Componentes:

- **Bus de Verificación**
- **Bus Instrumental**
- **Bus de Innovación**

### Tecnologías y funcionalidades:

- **Autenticación y autorización:** Control de acceso seguro a los servicios.
- **Firmado y sellado electrónico:** Garantiza la integridad y autenticidad de la información.
- **Transformación de mensajes:** Adaptación de formatos para la interoperabilidad entre sistemas.
- **Registro y auditoría:** Seguimiento y control de las transacciones realizadas.
- **Orquestación de servicios:** Coordinación de múltiples servicios para cumplir procesos complejos.
- **Herramienta de administración:** Gestión y configuración de la plataforma.

### Roles de los participantes:

- **Proveedor de Servicios (Cedente):** Entidad que ofrece datos o servicios.
- **Consumidor de Servicios (Cesionario):** Entidad que consume datos o servicios.

**Servicios ofrecidos:**

- **Servicios de verificación de datos/intermediación:** Permiten verificar información para evitar solicitar al ciudadano documentación ya disponible en la administración.
  - **Ejemplos:**
    - Consulta de datos de identidad y verificación.
    - Verificación de títulos universitarios y no universitarios.
    - Comprobación de estar al corriente de pago con la Agencia Tributaria, Seguridad Social o Generalitat Valenciana.
    - Información sobre situación actual de desempleo e inscripción como demandante de empleo.
    - Grado y nivel de dependencia.
    - Datos de nacimiento, matrimonio y defunción.
    - Residencia legal y cambio de domicilio.
    - Inexistencia de antecedentes penales o delitos sexuales.
    - Consulta del grado de conocimiento de valenciano de la JQCV.
    - Verificación de título de familia numerosa.
- **Servicios Web Instrumentales:** Facilitan procesos internos en la gestión administrativa con el ciudadano.
  - **Tipos y ejemplos:**
    - **Componentes comunes de administración electrónica desarrollados o adaptados por la DGTIC:**
      - Comunicaciones y notificaciones.
      - Pasarela de pagos.
      - Localizador y generación de nuevos CSV.
      - Gestor documental.
      - Sistema de Autenticación y Firma Electrónica (SAFE).
      - Envío de correos electrónicos y SMS.
      - Portafirmas.
      - Servicios de traducción (SALT).
    - **Servicios de otras administraciones públicas:** Fogasa, Lexnet, FACE.
    - **Servicios ofrecidos a empresas:** Servicio de prohibidos.

### **Roles en la PAI y Contratos de Integración**

En el funcionamiento de la PAI participan diferentes roles esenciales para garantizar la interoperabilidad y el correcto intercambio de información.

#### **Roles:**

- **Cedente (Proveedor de Servicios):** Entidad que proporciona los datos o servicios. Es responsable de elaborar el contrato de integración y definir las condiciones y especificaciones del servicio ofrecido.
- **Cesionario (Consumidor de Servicios):** Entidad que solicita y consume los datos o servicios proporcionados por el cedente.

**Contrato de Integración:** Documento que establece las reglas y condiciones para consumir un servicio a través de la PAI. Incluye:

- Descripción detallada del sistema y del servicio ofrecido.
- Definición del intercambio de mensajes, incluyendo esquemas y formatos.
- Especificación de respuestas y posibles errores.
- Anexos con información adicional relevante.

## Infraestructuras de interoperabilidad

La interoperabilidad entre Administraciones Públicas se refiere a la capacidad de intercambiar información y servicios de manera eficiente y efectiva. Esto se logra mediante infraestructuras y servicios comunes y compartidos.

- **Infraestructuras:**

Incluyen redes de comunicación, sistemas de información y estándares técnicos de interoperabilidad. Ejemplos:

- **Comunicaciones SARA:** Red de comunicaciones segura.
- **Servicio unificado de telecomunicaciones:** Gestión centralizada.
- **Servicio de seguridad gestionada:** Protección de infraestructuras TIC.
- **Servicio de nube híbrida (nubeSARA):** Infraestructura cloud para la Administración.

- **Servicios comunes:**

Servicios utilizados por varias administraciones simultáneamente:

- Red de comunicaciones de las AAPP (SARA)
- DNI electrónico (DNIE)
- @Firma
- Plataforma de Intermediación de Datos (PID)
- Red 060
- Ventanilla Única (EUGO.ES)
- Pack Administración-e (ORVE, ACCEDA, PORTAFIRMAS, INSIDE, +PORTAL)
- Notificaciones electrónicas
- Reutilización de información pública

- **Servicios compartidos:**

Ofrecidos por una sola administración, pero accesibles para otras.

### Sistema de Información Administrativa (SIA)

El SIA es una aplicación informática que actúa como catálogo de información sobre tramitación administrativa. Es conocido como el "Inventario de información administrativa de la AGE" y organiza procedimientos administrativos para garantizar acceso centralizado y actualizado.

### Directorio común de unidades orgánicas y oficinas (DIR3)

El DIR3 es un directorio electrónico que contiene información actualizada sobre las unidades orgánicas y oficinas de las Administraciones Públicas españolas.

- **Objetivos:**

- Crear un inventario unificado y corresponsable de unidades orgánicas, oficinas y organismos públicos.
- Mejorar la localización, contacto e interoperabilidad entre administraciones.

### **Sistema de Interconexión de Registros (SIR)**

El SIR permite el intercambio seguro de asientos electrónicos de registro entre Administraciones Públicas, facilitando la interoperabilidad y la comunicación administrativa eficiente. Es considerado una infraestructura clave para el registro electrónico.

### **Cl@ve**

Cl@ve es un sistema de identificación y autenticación unificada para ciudadanos y empresas, diseñado para simplificar el acceso a servicios electrónicos públicos.

- **Tipos de acceso:**

- **Cl@ve PIN:** Contraseñas de un solo uso para accesos esporádicos.
- **Cl@ve Permanente:** Contraseñas de validez duradera para accesos habituales y firma en la nube.

### **Plataforma de Intermediación de Datos (PID)**

La PID permite a las Administraciones Públicas compartir y verificar datos de manera segura y estandarizada, asegurando la protección de la información y la optimización de trámites administrativos. Es el "servicio estatal de verificación y consulta".

### **Dirección Electrónica Habilitada (DEH)**

La DEH, reemplazada por la Dirección Electrónica Habilitada Única (DEHÚ), permite la recepción segura de notificaciones administrativas telemáticas.

- **Características:**

- Uso de certificados digitales.
- Disponible para personas físicas y jurídicas.
- Comunicación oficial segura con las administraciones.

### **INSIDE (Infraestructura y Sistemas de Documentación Electrónica)**

INSIDE es una plataforma para gestionar documentos y expedientes electrónicos según los estándares del Esquema Nacional de Interoperabilidad (ENI).

- **Funciones principales:**

- Gestión segura de documentos.
- Almacenamiento estándar de expedientes electrónicos.

## **ARCHIVE**

ARCHIVE es el sistema de archivo definitivo para expedientes y documentos electrónicos, asegurando su conservación y accesibilidad a largo plazo, cumpliendo con los estándares normativos.

## Identificación y firma electrónica

# Identificación y firma electrónica. Marco europeo y nacional. Certificados digitales. Claves privadas, públicas y concertadas. Formatos de firma electrónica. Servicios de directorio. Mecanismos de identificación y firma biométricos

### Servicios de autenticación

Los servicios de autenticación son fundamentales para garantizar la seguridad en sistemas informáticos y redes. Permiten verificar la identidad de usuarios y controlar el acceso a recursos y datos sensibles.

- **Definiciones (RD 1720/2007):**
  - **Identificación:** Procedimiento para reconocer la identidad de un usuario, por ejemplo, mediante nombre de usuario o DNI.
  - **Autenticación:** Procedimiento para comprobar la identidad de un usuario, como el uso de una contraseña.
  - **Control de accesos (autorización):** Mecanismo que permite, en función de la identidad autenticada, acceder a datos o recursos específicos.
- **Triple A (AAA):** Concepto que engloba:
  - **Authentication (Autenticación):** Verificación de identidad.
  - **Authorization (Autorización):** Control de permisos y accesos.
  - **Accounting (Auditoría):** Registro y monitoreo de actividades.
- **Métodos de autenticación:**
  - **Algo que sabemos:** Contraseñas, PINs.
  - **Algo que tenemos:** Tokens, tarjetas inteligentes.
  - **Algo que somos:** Características biométricas como huellas digitales.
- **Sistemas de autenticación:**
  - **Factor único:** Utiliza un solo método de autenticación.
  - **Doble factor:** Combina dos métodos, aumentando la seguridad.
  - **Multifactor:** Utiliza tres o más métodos para una autenticación más robusta.
- **Características deseables:**
  - **Fiabilidad:** Precisión en la identificación.
  - **Viabilidad:** Implementación práctica y eficiente.

- **Integridad:** Protección contra alteraciones no autorizadas.
- **Amigabilidad:** Facilidad de uso para los usuarios.

### **Identificación Digital (ID)**

La identificación digital es el conjunto de mecanismos y medios que garantizan la identidad de personas físicas o jurídicas en entornos digitales, incluyendo la gestión y administración de estos servicios.

- **Garantías que debe ofrecer:**
  - **Autenticación:** Confirmación de la identidad.
  - **Autorización:** Control de acceso a recursos.
  - **Integridad:** Aseguramiento de que la información no ha sido alterada.
  - **Confidencialidad:** Protección de la información contra accesos no autorizados.
- **Medios utilizados:**
  - Tarjetas RFID, DNI electrónico, certificados digitales, tokens, sistemas biométricos, entre otros.

### **Firma electrónica y firma digital**

La firma electrónica y la firma digital son herramientas que permiten garantizar la identidad del firmante y la integridad de los documentos electrónicos.

- **Firma digital:**
  - **Definición técnica:** Mecanismo criptográfico que permite identificar al emisor de un mensaje y asegurar que no ha sido alterado desde su emisión.
  - **Características:**
    - Garantiza la identidad del firmante.
    - Asegura la integridad del mensaje.
    - Proporciona validez jurídico-administrativa equiparable a la firma manuscrita.
  - **Naturaleza técnica.**
- **Firma electrónica:**
  - **Definición legal:** "Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante."
  - **Regulación:**
    - Ley 59/2003 (derogada).
    - Reglamento (UE) Nº 910/2014 (eIDAS).
  - **Propiedades:**

- Identidad.
- Integridad.
- No repudio.
- **Funciones:**
  - Identificar al firmante de manera inequívoca.
  - Asegurar la integridad del documento.
  - Garantizar el no repudio del documento firmado.
- **Tipos de firma electrónica:**
  - **Simple:** Medios básicos de identificación, como un login o PIN.
  - **Avanzada:** Permite identificar al firmante y detectar cualquier cambio en los datos firmados; está vinculada de manera única al firmante.
  - **Cualificada:** Es una firma avanzada creada mediante un dispositivo cualificado y basada en un certificado reconocido; tiene equivalencia legal con la firma manuscrita.
- **Formatos técnicos de firma electrónica:**
  - **CAdES:** Basado en CMS y sintaxis ASN.1.
  - **XAdES:** Basado en sintaxis y formato XML.
- **Modalidades de firma:**
  - **Básica:** Combinación de hash y clave privada.
  - **Fechada:** Firma básica más sello de tiempo.
  - **Completa (validada):** Firma fechada más Dispositivo Seguro de Creación de Firma (DSCF) y certificado reconocido.

## Certificados digitales

Un certificado digital es un documento electrónico firmado por un prestador de servicios de certificación que vincula una clave pública a una identidad, confirmando su autenticidad.

- **Funciones:**
  - Firma electrónica de documentos.
  - Cifrado de información transmitida.
  - Autenticación de identidad en comunicaciones.
- **Información básica contenida:**
  - Identidad del titular.
  - Periodo de validez.
  - Clave pública certificada.

- Emisor del certificado (Autoridad de Certificación).
- **Formatos de codificación (basados en X.509):**
  - **DER (Distinguished Encoding Rules):** Codificación binaria; extensiones .der, .cer, .crt.
  - **PEM (Privacy-enhanced Electronic Mail):** Texto ASCII Base64; extensiones .pem, .cer, .crt, .key.
  - **PKCS#7 (.p7b / .p7c):** Formato contenedor; no almacena claves privadas.
  - **PKCS#12 (.p12 / .pfx):** Almacena certificados y claves privadas cifradas en un único archivo.
- **Tipos de certificados:**
  - **Certificados del DNI electrónico:** Emitidos por el Cuerpo Nacional de Policía.
  - **Certificado de Sede Electrónica:** Identifica y autentica a un servidor como sede electrónica de una Administración Pública.
  - **Certificado de Empleado Público:** Para identificación y autenticación de empleados públicos en el ejercicio de sus funciones.
  - **Certificado de Sello Electrónico:** Para actuaciones administrativas automatizadas; identifica al órgano o entidad pública.
  - **Certificado de Firma de Código:** Garantiza la identidad del autor de software al firmar código ejecutable.

#### Tipos de sellos

- **Sello de tiempo:** Método que prueba que un conjunto de datos existió antes de un momento dado y que no ha sido modificado desde entonces.
- **Sello de tiempo cualificado:** Añade valor a la firma digital al proporcionar una marca temporal fiable de una entidad de confianza, evitando depender únicamente de la hora proporcionada por el firmante.

#### Huella digital

Conjunto de datos asociados a un mensaje que permiten asegurar que no ha sido modificado. Se obtiene aplicando una función hash al mensaje.

#### Sistemas criptográficos

- **Criptografía simétrica:**
  - Utiliza la misma clave para cifrar y descifrar.
  - Algoritmos comunes: DES, 3DES, RC5, AES, Blowfish, IDEA.
- **Criptografía asimétrica:**
  - Utiliza un par de claves: pública y privada.
  - Algoritmos comunes:

- **Diffie-Hellman:** Basado en exponenciación modular.
- **RSA:** Basado en la factorización de números primos.

### Estándar X.509 v3

- **Descripción:** Estándar de la UIT-T para infraestructuras de clave pública (PKI).
- **Características:**
  - Especifica formatos para certificados digitales y algoritmos de hash.
  - Utiliza un sistema jerárquico de autoridades de certificación.
  - Definido en lenguaje ASN.1.
  - Codificado mediante DER o PEM.

### Gestión del ciclo de vida de un certificado

Proceso normalizado que incluye:

1. **Verificación y confirmación de identidad:** La Autoridad de Certificación (CA) verifica la identidad del solicitante, a menudo requiriendo presencia física.
2. **Emisión del certificado:** La CA firma el certificado con su clave privada.
3. **Entrega del certificado:** La CA entrega el certificado al titular, sin mantener copias de la clave privada.

### Infraestructura de Clave Pública (PKI)

La PKI es un conjunto de componentes que permiten la emisión, gestión y validación de certificados digitales.

- **Funciones principales:**
  - **Confidencialidad:** Protección de la información.
  - **Integridad:** Garantía de que la información no ha sido alterada.
  - **Autenticación:** Verificación de identidades.
  - **No repudio:** Imposibilidad de negar la autoría de una acción.
- **Entidades involucradas:**
  - **Autoridad de Certificación (CA):** Emite y gestiona certificados.
  - **Autoridad de Registro (RA):** Verifica la identidad de los solicitantes.
  - **Autoridad de Depósito (AD):** Conserva de forma segura los certificados.
  - **Suscriptores:** Usuarios que solicitan y utilizan los certificados.
- **Otros componentes:**
  - **Política de Seguridad:** Reglas para mantener la seguridad.

- **Declaración de Prácticas de Certificados (CPS):** Detalla cómo se implementa la política de seguridad.
- **Sistema de Distribución de Certificados:** Distribuye y localiza certificados.
- **Listas de Revocación de Certificados (CRL):** Listas de certificados revocados.

#### Localización de claves públicas

- **PGP (Pretty Good Privacy):** Alternativa descentralizada a la PKI tradicional.
  - **Servidores de claves públicas:** Facilitan la distribución de claves.
  - **Anillos de confianza:** Los usuarios firman las claves de otros, estableciendo una red de confianza.

#### Prestación de servicios de certificación públicos y privados

- **Obligaciones de los prestadores:**
  - No almacenar ni copiar datos de firma sin autorización.
  - Proporcionar información clara a los solicitantes sobre sus obligaciones y derechos.
  - Mantener directorios actualizados de certificados y su estado.
  - Garantizar servicios de consulta sobre la vigencia de los certificados.
  - En caso de cese de actividad, comunicar con antelación y gestionar la continuidad o extinción de certificados.
- **Obligaciones adicionales para certificados reconocidos:**
  - Demostrar fiabilidad y certificaciones obtenidas.
  - Garantizar la precisión de fechas y horas.
  - Emplear personal cualificado y sistemas fiables.
  - Tomar medidas contra la falsificación.
  - Conservar información relativa a los certificados durante 15 años.
  - Disponer de un seguro de responsabilidad civil adecuado.

#### Autoridad de Certificación (CA)

- **Función principal:** Emitir y gestionar certificados digitales.
- **Jerarquía de autoridades:** Las CA pueden estar organizadas en una estructura jerárquica, donde cada CA es avalada por otra de nivel superior hasta llegar a una CA raíz.
- **Principales CA en España:**
  - **Para particulares y empresas:**
    - Fábrica Nacional de Moneda y Timbre (FNMT).

- Agència Catalana de Certificació (CATCert).
- Autoritat de Certificació de la Comunitat Valenciana (ACCV).
- IZENPE.
- DNI electrónico (Dirección General de la Policía).
- **Para empresas:**
  - Agencia Notarial de Certificación (ANCERT).
  - ANF Autoridad de Certificación (ANF AC).
  - Autoridad de Certificación de la Abogacía (ACA).
  - Camerfirma.
  - EDICOM.
  - Firma Profesional.

### Servicios de directorio

Los servicios de directorio son aplicaciones y componentes que permiten gestionar y acceder a información de directorios en una red.

- **Características:**
  - **Dinamismo:** Datos modificables en tiempo real.
  - **Flexibilidad:** Organización y tipos de datos adaptables.
  - **Seguridad:** Gestión de accesos y autenticación.
  - **Personalización:** Información y acceso según el tipo de usuario.
- **Protocolos y estándares:**
  - **X.500:** Conjunto de estándares para servicios de directorio.
  - **LDAP (Lightweight Directory Access Protocol):** Protocolo para acceder y mantener servicios de directorio distribuidos.
    - Basado en TCP/IP.
    - Utiliza estructuras ASN.1.
    - Organiza datos en un árbol de directorio (DIT).
- **Elementos clave:**
  - **DN (Distinguished Name):** Identificador único de cada objeto en el directorio.
  - **LDIF (LDAP Data Interchange Format):** Formato estándar para intercambiar datos de directorio.
- **Funciones de un servicio de directorio:**
  - Autenticación de usuarios.

- Integración con otras aplicaciones y servicios.
- Implementación de políticas de seguridad.
- Gestión y distribución de certificados digitales.
- **Implementaciones de LDAP:**
  - **Active Directory:** De Microsoft.
  - **OpenLDAP:** Proyecto de código abierto.

## Marcos de autenticación

Conjunto de protocolos y tecnologías que permiten autenticar usuarios y gestionar identidades.

- **Funciones:**
  - Autenticar usuarios.
  - Aplicar políticas de acceso.
  - Gestionar credenciales.
- **Categorías:**
  - **Tecnologías delegadas de control de acceso:**
    - **Kerberos:** Protocolo de autenticación en redes que utiliza cifrado simétrico y una tercera entidad de confianza.
    - **RADIUS (Remote Authentication Dial-In User Service):** Protocolo para autenticación y autorización.
    - **Estándar 802.1x:** Control de acceso a redes basado en puertos.
  - **Tecnologías para gestión de identidades federadas:**
    - **OpenID:** Protocolo de autenticación descentralizado que permite a los usuarios acceder a múltiples servicios con una sola identidad.
    - **SAML (Security Assertion Markup Language):** Estándar para intercambio de datos de autenticación y autorización.
    - **XACML (eXtensible Access Control Markup Language):** Estándar para control de acceso basado en atributos.
    - **SPML (Service Provisioning Markup Language):** Estándar para aprovisionamiento de servicios.
- **Otros protocolos y métodos de autenticación:**
  - **RPC seguro (Remote Procedure Call):** Permite llamadas a procedimientos en red con seguridad.
  - **PAM (Pluggable Authentication Module):** Sistema modular para autenticación en Unix.

- **SASL (Simple Authentication and Security Layer):** Proporciona autenticación y seguridad en protocolos de internet.
- **SSH (Secure Shell):** Protocolo para acceso remoto seguro.
- **DIAMETER:** Evolución de RADIUS, utilizado para AAA (Autenticación, Autorización y Accounting).

### Mecanismos de identificación y firma biométricos

Los sistemas biométricos utilizan características físicas o comportamentales para identificar y autenticar a los usuarios.

- **Factores biométricos comunes:**

- **Huellas dactilares.**
- **Iris y retina.**
- **Reconocimiento facial.**
- **Geometría de la mano.**
- **Venas del dedo o mano.**
- **Voz.**

- **Ventajas:**

- Difíciles de falsificar.
- No requieren memorizar contraseñas.
- Proporcionan alta seguridad.

- **Consideraciones:**

- **Privacidad y protección de datos personales.**
- **Necesidad de equipos especializados.**
- **Posibles errores de lectura o identificación.**

### Tipos de claves

- **Clave privada:**

- Conocida solo por el propietario.
- Utilizada para descifrar información cifrada con la clave pública correspondiente.
- También se usa para firmar digitalmente.

- **Clave pública:**

- Disponible para cualquier persona.
- Utilizada para cifrar información destinada al propietario de la clave privada.

- Permite verificar firmas digitales.
- **Clave concertada:**
  - Compartida entre dos o más partes.
  - Utilizada para autenticar identidades y cifrar comunicaciones en entornos donde se requiere confianza mutua.

### Certificados del DNI electrónico

- **Tipos de certificados:**
  - **Certificado de Componente:** Asociado al chip del DNIE.
  - **Certificado de Autenticación:** Permite autenticar la identidad del ciudadano.
  - **Certificado de Firma:** Permite realizar firma electrónica reconocida.

### Protocolos de verificación de certificados

- **OCSP (Online Certificate Status Protocol):**
  - Permite determinar el estado de revocación de un certificado en tiempo real.
  - Más eficiente que consultar listas CRL completas.
- **Listas de Revocación de Certificados (CRL):**
  - Listas que contienen certificados revocados antes de su fecha de expiración.
  - Deben ser consultadas para verificar la validez de un certificado.

## Sistemas de Información Geográfica (SIG)

### Sistemas de Información Geográfica (SIG)

Son herramientas esenciales para la gestión y análisis de datos geográficos, integrando información gráfica y alfanumérica. Estos sistemas permiten trabajar con planos digitales y datos asociados, ofreciendo múltiples funcionalidades y aplicaciones prácticas.

- **Concepto:** Sistemas diseñados para gestionar bases de datos geográficas, combinando mapas digitales con datos alfanuméricos.
- **Visualización y estructura:** Se asemejan a una serie de mapas superpuestos que representan diferentes capas de información (altitudes, redes fluviales, tipos de suelo, etc.).
- **Funcionalidades principales:**
  - Consulta y visualización de información geográfica.
  - Medición de distancias, áreas y perímetros.
  - Edición y actualización de datos.
  - Búsqueda y análisis espacial.
  - Explicación de fenómenos y predicción de sucesos.
  - Planificación estratégica y soporte en la toma de decisiones.
- **Problemas que resuelven:**
  - **Localización:** Identificación de la posición exacta de un objeto o fenómeno.
  - **Condiciones:** Determinación de características y atributos asociados a un lugar.
  - **Tendencias:** Análisis de cambios temporales en el espacio geográfico.
  - **Rutas:** Identificación de caminos óptimos.
  - **Pautas:** Detección de patrones espaciales y relaciones.
  - **Modelación:** Simulación de escenarios basados en datos geográficos.

#### Datos en un SIG

La información gestionada en los SIG se organiza según formatos y representaciones específicas, dependiendo de su naturaleza y propósito.

- **Sistemas de coordenadas:**

- Uso del **Sistema Universal Transversal de Mercator (UTM)**, que divide la Tierra en 60 husos de 6º de longitud. En la Comunidad Valenciana se utiliza el huso 30N.
- Las coordenadas se expresan en metros y son precisas al nivel del mar.
- **Representación de objetos geográficos:**
  - **Modelo raster:** Divide el espacio en una matriz de celdas o píxeles. Usos: imágenes satelitales, modelos digitales del terreno (MDT), fotografías aéreas.
    - **Formatos comunes:** GeoTIFF, ECW, MrSID, JPG georreferenciado, ESRI Grid.
  - **Modelo vectorial:** Representa objetos mediante puntos, líneas y polígonos.
    - **Formatos comunes:** Shapefile (SHP), bases de datos espaciales (MySQL, Oracle Spatial), formatos CAD (DXF, DWG), GML/XML, KML.
- **Fuentes de datos geográficos:**
  - **Topografía:** Mediciones detalladas del terreno.
  - **Geodesia:** Ciencia que mide y representa la Tierra.
  - **Posicionamiento por satélite:** GPS y otros sistemas globales.
  - **Fotogrametría:** Uso de drones o aviones para tomar imágenes aéreas.
  - **Teledetección:** Obtención de datos mediante sensores en satélites o aviones no tripulados.
  - **LIDAR:** Tecnología basada en láser para obtener modelos digitales precisos.
  - **Institut Cartogràfic Valencià (ICV):** Fuente principal de datos cartográficos en la Comunidad Valenciana.

## Proyecto gvSIG

El **Proyecto gvSIG** es una iniciativa de la Generalitat Valenciana para proporcionar herramientas SIG de código abierto adaptadas a las necesidades de los usuarios.

- **Características destacadas:**
  - Portable y modular.
  - De código abierto, bajo licencia GPL.
  - Sin costos de licencias.
  - Interoperable con soluciones preexistentes.
  - Basado en estándares internacionales.
- **Plataformas disponibles:**
  - **gvSIG Desktop:** Herramienta para uso en ordenadores.

- **gvSIG Mobile:** Versión optimizada para dispositivos móviles.

### **Incorporación de la componente geográfica en los Sistemas de Información**

La integración de datos geográficos en sistemas de información permite ampliar sus capacidades y aplicaciones.

- **Geocodificación:** Proceso de asignar coordenadas geográficas a objetos previamente no georreferenciados. Se basa en direcciones u otros identificadores espaciales.
- **Datum geodésico:** Sistema de referencia que describe la forma y tamaño de la Tierra. Define un origen para los sistemas de coordenadas y permite una representación precisa del espacio geográfico.

## Infraestructuras de Datos Espaciales (IDE)

# Definición y Componentes. Arquitectura y Servicios Web de una IDE

**Infraestructuras de Datos Espaciales (IDE):** Son plataformas de interoperabilidad diseñadas para compartir información geográfica de forma eficiente. Integran datos espaciales de diferentes organismos mediante tecnologías, políticas, acuerdos institucionales, datos y servicios estandarizados, facilitando su acceso, manejo, intercambio y distribución a través de Internet.

### Características Principales de una IDE

- **Geoportal o Sitio Web:** Se materializan a través de un portal que ofrece aplicaciones de visualización, catálogos y nomenclátores.
- **Interoperabilidad:** Integran información espacial de diversos orígenes, garantizando su compatibilidad.
- **Accesibilidad:** Permiten el acceso público a datos geográficos actualizados y de calidad.

### Componentes de una IDE

- **Componentes Geográficos:**
  - **Datos:**
    - **De Referencia:** Cartografía, fotografías aéreas, modelos digitales del terreno.
    - **Temáticos:** Información sobre clima, suelo, población, etc.
  - **Metadatos:** Descripciones detalladas que proporcionan información sobre los datos, como su origen, formato, calidad y restricciones de uso.
- **Componentes Tecnológicos:**
  - **Estándares:**
    - **OGC (Open Geospatial Consortium):** Organismo que desarrolla especificaciones para asegurar la interoperabilidad.
    - **ISO:** Estándares internacionales para la información geográfica.
    - **Grupo de Trabajo IDEE:** En España, coordina la implementación de estándares en las IDE.
  - **Servicios:**
    - **WMS (Web Map Service):** Proporciona imágenes de mapas georreferenciados.

- **WMTS (Web Map Tile Service)**: Ofrece mapas mediante teselas para una carga más rápida.
- **WFS (Web Feature Service)**: Permite el acceso y manipulación de datos vectoriales en formato **GML (Geography Markup Language)**.
- **WCS (Web Coverage Service)**: Proporciona acceso a datos raster, como imágenes satelitales.
- **CSW (Catalog Service for the Web)**: Facilita la búsqueda y consulta de metadatos.
- **Gazetteer (Servicio de Nomenclátor)**: Localiza elementos geográficos por su nombre.
- **Infraestructura de Comunicaciones**: Red de Internet que soporta la transferencia y acceso a los datos geoespaciales.
- **Componentes Políticos**:
  - **Políticas y Normativas**: Regulaciones que establecen cómo se recolectan, mantienen y usan los datos geográficos.
  - **Acuerdos Institucionales**: Colaboración entre entidades para compartir y gestionar información espacial.
- **Componentes Sociales**:
  - **Usuarios**: Comunidad de profesionales, instituciones y público en general que utilizan y contribuyen a la IDE.

## Legislación Relacionada

- **Directiva INSPIRE**: Norma europea que establece una infraestructura de datos espaciales común en la Unión Europea.
- **Ley 14/2010 (LISIGE)**: Transpone la Directiva INSPIRE al marco legal español, regulando la infraestructura de información geográfica en España.
- **Sistema Cartográfico Nacional (SCN)**: La Generalitat Valenciana se integra en este sistema para coordinar la información geográfica a nivel nacional.

## IDE en España y la Comunitat Valenciana

- **Infraestructura de Datos Espaciales de España (IDEE)**:
  - Integra datos, metadatos y servicios geográficos producidos en España.
  - Gestionada por la **Dirección General del Instituto Geográfico Nacional**.
  - Ofrece un geoportal que centraliza el acceso a la información geoespacial.
- **Infraestructura de Datos Espaciales de la Comunitat Valenciana (IDECV)**:

- Plataforma que promueve la cooperación entre entidades públicas y privadas para hacer accesible la información geográfica del territorio valenciano.
- Gestionada por el **Institut Cartogràfic Valencià**.

## Arquitectura de una IDE

La arquitectura de una IDE se basa en el modelo **Cliente-Servidor** y utiliza estándares abiertos para garantizar la interoperabilidad.

- **Tecnologías Utilizadas:**
  - **XML:** Lenguaje utilizado para la descripción de servicios web y metadatos.
  - **GML:** Basado en XML, describe objetos geográficos para facilitar su intercambio.
- **Bases de Datos:**
  - Almacenan información cartográfica, datos alfanuméricos, imágenes y metadatos geoespaciales.
- **Servicios Web:**
  - **WMS, WFS, WCS, CSW**, entre otros, que permiten el acceso y manipulación de datos geográficos.
- **Tipos de Clientes:**
  - **Clientes Pesados:** Software de escritorio como ArcGIS, gvSIG, QGIS, que ofrecen funcionalidades avanzadas de SIG.
  - **Clientes Ligeros:** Geoportales y visores web que permiten acceder a la información geográfica sin necesidad de instalar software especializado.

## Servicios Web de una IDE

Los servicios web de una IDE están basados en una arquitectura orientada a servicios (**SOA**) y utilizan interfaces estandarizadas para asegurar la interoperabilidad.

- **Servicios de Visualización:**
  - **WMS:** Genera imágenes de mapas a partir de datos geográficos.
  - **WMTS:** Mejora la velocidad de carga mediante el uso de teselas pre-renderizadas.
- **Servicios de Catálogo:**
  - **CSW:** Permite buscar y acceder a metadatos de datos y servicios geográficos, facilitando su localización por temas, palabras clave, área geográfica, fecha, formato, escala u organización.
- **Servicios de Descarga:**

- **WFS:** Proporciona acceso directo a datos vectoriales, permitiendo su consulta y edición.
- **WCS:** Similar al WFS, pero para datos raster, como imágenes y coberturas.
- **Servicios de Geoprocесamiento:**
  - **WPS (Web Processing Service):** Define una interfaz estándar para publicar y ejecutar procesos geoespaciales, como análisis y modelos, sobre datos georreferenciados.
- **Servicios de Observación de Sensores:**
  - **SOS (Sensor Observation Service):** Facilita el acceso a datos de sensores, permitiendo solicitar, filtrar y recuperar observaciones y descripciones de sistemas de sensores.
- **Servicio de Nomenclátor:**
  - **Gazetteer:** Permite encontrar la ubicación geográfica de un lugar a partir de su nombre, proporcionando sus coordenadas y otra información relevante.

## Aplicaciones Geoespaciales Asociadas

- **Clientes SIG de Escritorio:**
  - **ArcGIS, gvSIG, QGIS, Geomedia:** Herramientas avanzadas para el análisis y gestión de datos geoespaciales.
- **Aplicaciones SIG en la Nube:**
  - **ArcGIS Online, CartoDB, MapBox, My Maps:** Plataformas que ofrecen funcionalidades SIG a través de servicios web.
- **Clientes Ligeros Web:**
  - **OpenLayers, MapBender, MapFish:** Frameworks y bibliotecas para desarrollar aplicaciones web de mapas.
- **Bases de Datos Geográficas:**
  - **ArcSDE, PostGIS, MySQL Spatial:** Sistemas de gestión de bases de datos que soportan datos espaciales.
- **Servidores Web Geoespaciales:**
  - **ArcGIS for Server, MapServer, MapGuide, GeoServer:** Software que permite publicar y administrar servicios web geoespaciales.
- **Catálogos de Metadatos:**
  - **GeoNetwork, PyCSW:** Aplicaciones para la gestión y distribución de metadatos geográficos.
- **Bibliotecas Geoespaciales:**

- **GDAL (Geospatial Data Abstraction Library), Sextante:** Conjuntos de herramientas para el procesamiento y análisis de datos geoespaciales.

## Redes de computadores

### Red de computadores: Componentes, Categorías, dispositivos,...

Una red de computadores es un conjunto de equipos, conocidos como nodos, y software conectados entre sí mediante dispositivos físicos que transmiten y reciben datos a través de impulsos eléctricos, ondas electromagnéticas u otros medios. Su finalidad es compartir información, recursos y ofrecer servicios entre los dispositivos conectados.

#### Componentes de una red

- **Emisor:** Dispositivo que envía el mensaje.
- **Mensaje:** Información que se desea transmitir.
- **Medio:** Canal a través del cual se transmite el mensaje.
- **Receptor:** Dispositivo que recibe el mensaje.

#### Categorías de una red

- **Capa física:** Incluye los elementos tangibles utilizados por un equipo para comunicarse con otros dentro de la red, como tarjetas de red, cables y antenas.
- **Capa lógica:** Establece normas y protocolos que permiten proporcionar servicios de comunicación entre dispositivos.

#### Componentes básicos de las redes

- **Hardware:** Dispositivos físicos que conforman la red, como routers, switches y servidores.
- **Software:** Programas y aplicaciones que gestionan la comunicación y el flujo de datos en la red.
- **Protocolos:** Conjuntos de reglas que permiten la comunicación eficiente y segura entre dispositivos de diferentes fabricantes.

#### Dispositivos de red

- **Conmutador de red (switch):** Interconecta dos o más hosts, pasando datos de un segmento a otro según la dirección MAC de destino de las tramas, y elimina la conexión una vez finalizada.
- **Enrutador (router):** Interconecta redes con distintos prefijos en sus direcciones IP, estableciendo la mejor ruta para que cada paquete de datos llegue a su destino.

- **Puente de red (bridge):** Interconecta segmentos de red transfiriendo datos de una red a otra basándose en la dirección física de destino de cada paquete.
- **Puente de red y enrutador (brouter):** Combina las funciones de un puente de red y un enrutador, permitiendo interconectar redes y segmentar el tráfico.
- **Punto de acceso inalámbrico (Wireless Access Point, WAP):** Dispositivo que interconecta equipos de comunicación inalámbricos para formar una red inalámbrica que conecta dispositivos móviles o tarjetas de red inalámbricas.

### Clasificación de las redes por alcance

- **Red de área personal (Personal Area Network, PAN):** Red utilizada para la comunicación entre dispositivos cercanos a una persona, como smartphones y relojes inteligentes.
- **Red inalámbrica de área personal (Wireless Personal Area Network, WPAN):** Similar a la PAN pero inalámbrica, permite la comunicación entre dispositivos cercanos al punto de acceso, generalmente en un rango de pocos metros (ejemplo: Bluetooth).
- **Red de área local (Local Area Network, LAN):** Red que se limita a un área geográfica pequeña, como una habitación, un edificio o una nave industrial.
- **Red de área local inalámbrica (Wireless Local Area Network, WLAN):** Sistema de comunicación de datos inalámbrico que utiliza tecnología de radiofrecuencia para conectar dispositivos dentro de un área local.
- **Red de área de campus (Campus Area Network, CAN):** Red de alta velocidad que conecta redes LAN en un área geográfica limitada, como un campus universitario o un parque tecnológico.
- **Red de área metropolitana (Metropolitan Area Network, MAN):** Red de alta velocidad que cubre un área geográfica más extensa que una CAN, como una ciudad o un conjunto de edificios públicos.
- **Red de área amplia (Wide Area Network, WAN):** Red que se extiende sobre un área geográfica extensa, utilizando medios como satélites, cables interoceánicos, Internet o fibras ópticas públicas.

### Clasificación de las redes por topología

- **Red en bus (lineal):** Se caracteriza por tener un único canal de comunicaciones al cual se conectan todos los dispositivos. Es sencilla y económica, pero si el canal falla, toda la red se interrumpe.
- **Red en anillo (ring):** Cada estación está conectada a la siguiente y la última está conectada a la primera, formando un círculo cerrado. Los datos circulan en una dirección y cada nodo actúa como repetidor.

- **Red en estrella (star):** Todas las estaciones están conectadas directamente a un punto central, generalmente un switch o hub, y las comunicaciones se realizan a través de este. Es fácil de administrar y escalar.
- **Red en malla (mesh):** Cada nodo está conectado a todos los demás, proporcionando múltiples rutas para la transmisión de datos. Ofrece alta redundancia y fiabilidad.
- **Red en árbol (tree):** Los nodos están organizados en forma jerárquica, similar a la estructura de un árbol, combinando características de las topologías en estrella y bus.
- **Red híbrida o mixta:** Combinación de dos o más topologías de red mencionadas anteriormente, adaptándose a necesidades específicas.

### Clasificación de las redes por direccionalidad de datos

- **Simplex (unidireccional):** La comunicación se realiza en un solo sentido; un dispositivo transmite y otro recibe, como en las transmisiones de radio.
- **Half-duplex (semidúplex):** La comunicación es bidireccional pero no simultánea; los dispositivos pueden transmitir y recibir, pero no al mismo tiempo, como en el uso de walkie-talkies.
- **Full-duplex (dúplex):** La comunicación es bidireccional y simultánea; ambos dispositivos pueden transmitir y recibir al mismo tiempo, como en una conversación telefónica.

### Clasificación de las redes por medios de transmisión

- **Medios guiados:**
  - **Cable de par trenzado:** Consiste en pares de cables entrelazados para reducir la interferencia electromagnética. Se utiliza comúnmente en redes LAN.
  - **Cable coaxial:** Cable con un conductor interno rodeado por un aislante y una malla conductora que sirve como blindaje. Fue popular en redes Ethernet antiguas.
  - **Fibra óptica:** Utiliza hilos de vidrio o plástico para transmitir datos en forma de pulsos de luz, ofreciendo altas velocidades y mayor inmunidad a interferencias.
- **Medios no guiados:**
  - **Red por radio:** Utiliza ondas de radio para la transmisión inalámbrica de datos, como en redes Wi-Fi.
  - **Red por infrarrojos:** Emplea luz infrarroja para la comunicación entre dispositivos en línea de visión directa, aunque es susceptible a interferencias y obstrucciones.
  - **Red por microondas:** Utiliza señales de microondas para la transmisión de datos a largas distancias, incluyendo enlaces satelitales.

## Cálculo de redes

Para dividir una red en subredes, se utilizan cálculos basados en el número de bits reservados para la identificación de redes y hosts.

**Ejemplo:** Dividir la red 192.169.48.0 con máscara 255.255.255.0 en 4 subredes.

- **Número de subredes:** Necesitamos 4 subredes, lo cual implica que  $2^n=4 \Rightarrow n=2$ , donde  $n=2$  es el número de bits adicionales que debemos reservar para las subredes.
- **Actualización de la máscara de subred:** Reservamos 2 bits en la parte de host de la máscara original, obteniendo una nueva máscara: 255.255.255.**192** (los dos primeros bits del último octeto en uno: 11000000).
- **Número de direcciones por subred:** Cada subred tiene  $2^{8-n}=2^{8-2}=2^6=64$  direcciones posibles (8 bits originales menos 2 bits reservados para subredes).
- **Direcciones utilizables por subred:** Restamos las direcciones reservadas para red y broadcast en cada subred:  $64 - 2 = 62$  **direcciones de host** disponibles por subred.

## Redes de Área Extensa (WAN)

Las redes de área extensa (WAN, *Wide Area Network*) son redes de computadoras que interconectan múltiples redes de ámbito geográfico menor, como redes de área local (LAN), permitiendo la comunicación entre dispositivos que no se encuentran en la misma ubicación física. Las WAN son esenciales para conectar sucursales de empresas, instituciones gubernamentales y para el funcionamiento global de internet. Pueden ser privadas, diseñadas y gestionadas por organizaciones, o públicas, administradas por proveedores de servicios de internet (ISP).

La mayoría de los enlaces WAN son **enlaces punto a punto**, conectando directamente dos ubicaciones específicas. Esto facilita una comunicación directa y constante entre los puntos finales.

### Infraestructura de una WAN

- **Equipamiento local del cliente (CPE):** Dispositivos y cables ubicados en las instalaciones del cliente que se conectan a la red del proveedor.
- **Equipo de comunicación de datos (DCE):** Dispositivos que proporcionan la interfaz entre el CPE y la red del proveedor, como módems y multiplexores.
- **Equipo terminal de datos (DTE):** Dispositivos del cliente que generan y consumen datos, como computadoras y routers.
- **Punto de demarcación:** Límite físico que separa las responsabilidades de mantenimiento entre el cliente y el proveedor de servicios.
- **Bucle local:** Conexión física que une el CPE con la central del proveedor.
- **Centralita de comunicaciones:** Instalación del proveedor donde se gestionan las conexiones y el tráfico de datos.
- **Red interurbana:** Infraestructura que conecta diferentes áreas geográficas, facilitando la comunicación a larga distancia.

### Tipos de Redes WAN

- **Conmutación de circuitos:** Establece un circuito dedicado entre las terminales de los usuarios antes de la transmisión de datos. Este circuito permanece reservado durante toda la comunicación. Ejemplo: la red telefónica tradicional.
- **Conmutación de paquetes:** Los datos se dividen en paquetes que se envían a través de una red compartida. Cada paquete puede tomar rutas diferentes y se reensambla en el destino. Ejemplo: internet.
- **Conmutación de mensajes:** Los mensajes completos se transmiten de nodo en nodo, almacenándose temporalmente en cada uno antes de ser reenviados. Este método es menos común en la actualidad.

## Tipos de conexiones a una WAN

### 1. Conexiones de un Suscriptor a una WAN

- **Línea dedicada:** Conexión punto a punto permanente y exclusiva entre dos puntos. Ofrece alta fiabilidad y seguridad.
  - **Protocolos asociados:** PPP (Point-to-Point Protocol), HDLC (High-Level Data Link Control), SDLC (Synchronous Data Link Control), HNAS.
- **Comutación de circuitos:** Se establece un circuito dedicado temporal para cada sesión de comunicación.
  - **Protocolos asociados:** PPP, ISDN (Integrated Services Digital Network).
- **Comutación de paquetes:** Los datos se transmiten en paquetes a través de enlaces compartidos.
  - **Protocolos con estado:** X.25, Frame Relay.
  - **Protocolos sin estado:** IPv4, IPv6.
- **Comutación de celdas:** Similar a la comutación de paquetes, pero utiliza celdas de longitud fija.
  - **Protocolo asociado:** ATM (Asynchronous Transfer Mode).
- **Internet:** Utiliza la infraestructura global de internet para la transmisión de datos.
  - **Protocolos asociados:** VPN (Virtual Private Network), DSL (Digital Subscriber Line), módem por cable, conexiones inalámbricas.

### 2. Conexiones a la WAN con Medios Guiados

- **Líneas dedicadas:** Para conexiones permanentes que requieren alta disponibilidad y ancho de banda garantizado.
- **Acceso telefónico (dial-up):** Utiliza líneas telefónicas analógicas; es lento y se usa cuando no hay otras opciones disponibles.
- **RDSI (Red Digital de Servicios Integrados):** Permite la transmisión digital de voz y datos a través de líneas telefónicas tradicionales.
- **Frame Relay:** Tecnología de capa 2 que ofrece comutación rápida de paquetes para interconectar LANs distantes.
- **ATM (Modo de Transferencia Asíncrona):** Transmite datos en celdas de tamaño fijo, adecuado para voz, vídeo y datos.
- **WAN Ethernet:** Utiliza estándares Ethernet avanzados sobre fibra óptica para conexiones de alta velocidad.
- **MPLS (Comutación de Etiquetas Multiprotocolo):** Dirige datos basándose en etiquetas cortas en lugar de direcciones IP, mejorando la eficiencia.
- **WAN DSL:** Utiliza líneas telefónicas de cobre para proporcionar acceso a internet de banda ancha.

- **Cable:** Usa la infraestructura de televisión por cable para ofrecer servicios de internet.
- **Fibra óptica:** Ofrece las velocidades más altas y es inmune a las interferencias electromagnéticas.

### 3. Conexiones a la WAN de Manera Inalámbrica

- **VSAT (Very Small Aperture Terminal):** Utiliza comunicaciones satelitales para crear una WAN privada, ideal para áreas remotas.
- **Tecnologías inalámbricas:**
  - **Wi-Fi Municipal:** Redes inalámbricas que brindan acceso a internet en áreas urbanas extensas.
  - **WiMAX:** Ofrece acceso inalámbrico de banda ancha en un radio amplio, similar a la cobertura celular.
  - **Datos móviles:** Tecnologías celulares como 3G, 4G/LTE y 5G que permiten acceso a internet móvil de alta velocidad.

### Telefonía Móvil y Nuevas Tecnologías

La telefonía móvil ha evolucionado desde servicios básicos de voz hasta ofrecer conexiones de datos de alta velocidad:

- **3G:** Introdujo servicios de datos más rápidos, permitiendo navegación web y aplicaciones básicas.
- **4G/LTE (Long Term Evolution):** Mejoró significativamente las velocidades de datos, habilitando streaming de vídeo y aplicaciones en tiempo real.
- **5G:** Proporciona velocidades ultra rápidas, baja latencia y capacidad para una gran cantidad de dispositivos, impulsando el Internet de las Cosas (IoT) y aplicaciones avanzadas como realidad aumentada.

### Nuevos Protocolos

La innovación en tecnologías WAN ha dado lugar a nuevos protocolos:

- **IPv6:** Expande el espacio de direcciones IP, mejora la seguridad y la eficiencia enrutamiento.
- **MPLS:** Mejora la velocidad y gestión del tráfico en redes complejas mediante la utilización de etiquetas.
- **VPN:** Permite crear conexiones seguras a través de redes públicas, utilizando protocolos como IPsec o SSL/TLS.

### Redes por Software (SDN)

Las **Redes Definidas por Software (SDN)** representan una nueva aproximación en la gestión de redes:

- **Separación de planos:** Dividen el plano de control (inteligencia de enrutamiento) del plano de datos (encaminamiento del tráfico), permitiendo una gestión centralizada.
- **Flexibilidad y automatización:** Facilitan la configuración y adaptación de la red a las necesidades cambiantes mediante software.
- **Protocolos asociados:** OpenFlow es uno de los estándares más utilizados para la comunicación entre el controlador SDN y los dispositivos de red.

## Modelos de interconexión de sistemas abiertos: Modelo OSI vs Modelo TCP/IP

### Modelo de Referencia OSI (Open Systems Interconnection)

El Modelo OSI es un marco de referencia lógico y conceptual diseñado para estandarizar y normalizar la interconexión de sistemas abiertos, facilitando la compatibilidad entre diferentes tecnologías de red. Creado en 1980 por la **ISO** (International Organization for Standardization), no es un modelo de red específico ni define protocolos concretos, pero sí establece las funcionalidades que deben cumplir los protocolos de comunicación para lograr un estándar común.

#### Arquitectura del Modelo OSI: 7 Capas ("FER Tiene Su Pipi Amarillo")

El modelo se compone de siete capas jerárquicas, cada una encargada de funciones específicas en el proceso de comunicación:

- **Capa 7: Aplicación**
  - **Responsabilidad:** Proporcionar servicios de red directamente a las aplicaciones del usuario.
  - **Función:** Facilitar APIs de alto nivel para actividades como compartir recursos, acceso remoto a archivos y servicios de correo electrónico.
  - **Unidad de Datos:** Datos.
- **Capa 6: Presentación**
  - **Responsabilidad:** Transformar y adaptar el formato de los datos para asegurar que la información enviada por la capa de aplicación de un sistema sea entendible por la capa de aplicación de otro.
  - **Función:** Gestionar la codificación de caracteres, compresión de datos y cifrado/descifrado para la seguridad y eficiencia de la información.
  - **Unidad de Datos:** Datos.
- **Capa 5: Sesión**
  - **Responsabilidad:** Establecer, mantener y finalizar sesiones de comunicación entre aplicaciones en diferentes dispositivos.
  - **Función:** Manejar el diálogo entre sistemas, controlando quién transmite y durante cuánto tiempo.
  - **Características Adicionales:**
    - **Control del Diálogo:** Define si la comunicación es bidireccional simultánea (**full-duplex**) o alternada (**half-duplex**).

- **Agrupamiento:** Permite organizar el flujo de datos en unidades lógicas o transacciones.
- **Recuperación:** Implementa puntos de comprobación para reiniciar la comunicación desde el último punto válido en caso de fallo.
- **Unidad de Datos:** Datos.
- **Capa 4: Transporte**
  - **Responsabilidad:** Proporcionar una transferencia de datos confiable y transparente entre extremos, ajustándose a los requisitos de calidad de servicio.
  - **Función:** Realizar la segmentación y reensamblado de datos, control de flujo, detección y corrección de errores, y multiplexación de conexiones.
  - **Unidad de Datos:** Segmento o Datagrama.
  - **Tipos de Servicios:**
    - **Conmutación de Datagramas (Stateless):** Cada paquete es independiente y se enruta individualmente.
    - **Circuitos Virtuales (Stateful):** Se establece una ruta predefinida por la que todos los paquetes transitan en orden.
- **Capa 3: Red**
  - **Responsabilidad:** Determinar cómo se enrutan los datos desde el origen hasta el destino a través de múltiples nodos.
  - **Función:** Gestionar el direccionamiento lógico, el enrutamiento y el control de congestión en la red.
  - **Unidad de Datos:** Paquete.
- **Capa 2: Enlace de Datos**
  - **Responsabilidad:** Proporcionar transferencia de datos libre de errores entre dos nodos conectados físicamente.
  - **Función:** Encapsular paquetes en tramas, gestionar direcciones físicas (**MAC**), detección y corrección de errores a nivel de enlace.
  - **Unidad de Datos:** Trama.
- **Capa 1: Física**
  - **Responsabilidad:** Definir las características eléctricas, mecánicas y funcionales para activar, mantener y desactivar conexiones físicas.
  - **Función:** Transmitir bits individuales a través de un medio físico, incluyendo aspectos como voltajes, sincronización y velocidades de transmisión.
  - **Unidad de Datos:** Bits.

## Modelo TCP/IP o Internet Protocol Suite

El Modelo TCP/IP es un conjunto de protocolos de comunicación fundamentales para Internet y redes similares. Desarrollado en 1973 por **DARPA** (Defense Advanced Research Projects Agency), precede al Modelo OSI y define protocolos específicos para la comunicación en red, estableciendo estándares prácticos que permiten la interoperabilidad entre sistemas heterogéneos.

### Arquitectura del Modelo TCP/IP: 4 Capas ("Ana Toca Iguanas Eléctricas")

El modelo consta de cuatro capas, cada una con roles definidos:

- **Capa de Aplicación**
  - **Función:** Proporcionar servicios de red a las aplicaciones del usuario final.
  - **Protocolos Comunes:**
    - **HTTP (HyperText Transfer Protocol):** Transferencia de documentos web.
    - **FTP (File Transfer Protocol):** Transferencia de archivos entre sistemas.
    - **DNS (Domain Name System):** Resolución de nombres de dominio.
    - **SMTP (Simple Mail Transfer Protocol), POP (Post Office Protocol), IMAP (Internet Message Access Protocol):** Servicios de correo electrónico.
    - **Telnet:** Acceso remoto a servidores.
- **Capa de Transporte**
  - **Función:** Proporcionar comunicación de extremo a extremo y control de flujo.
  - **Protocolos:**
    - **TCP (Transmission Control Protocol):** Protocolo orientado a conexión que garantiza la entrega confiable de datos.
    - **UDP (User Datagram Protocol):** Protocolo sin conexión que permite el envío rápido de datagramas sin garantizar su entrega.
    - **TLS (Transport Layer Security):** Protocolo de seguridad para comunicaciones cifradas.
- **Capa de Internet**
  - **Función:** Encargada del direccionamiento y enrutamiento de paquetes entre redes.
  - **Características:**
    - Los paquetes pueden seguir rutas diferentes entre origen y destino.

- No se garantiza la entrega en orden ni la integridad de los datos; estas funciones son manejadas por capas superiores si es necesario.
- **Protocolos:**
  - **IP (Internet Protocol):** Proporciona direccionamiento lógico y enrutamiento de paquetes.
  - **ICMP (Internet Control Message Protocol):** Utilizado para mensajes de control y diagnóstico.
  - **ARP (Address Resolution Protocol):** Resuelve direcciones IP a direcciones MAC.
  - **RARP (Reverse ARP):** Resuelve direcciones MAC a direcciones IP.
- **Capa de Enlace o Acceso a la Red**
  - **Función:** Gestionar la transmisión física de datos en el medio de comunicación de la red.
  - **Protocolos y Tecnologías:**
    - **Ethernet, Fast Ethernet:** Estándares para redes de área local (**LAN**).
    - **Token Ring, Token Bus:** Tecnologías de acceso al medio basadas en paso de testigo.
    - **FDDI (Fiber Distributed Data Interface):** Tecnología para redes de alta velocidad usando fibra óptica.
    - **X.25, Frame Relay, ATM (Asynchronous Transfer Mode):** Tecnologías para redes de área amplia (**WAN**).

## Comparativa entre modelos

Modelo OSI	Modelo TCP/IP	Protocol Data Unit	Protocolos
Capa de Aplicación		Datos	HTTP, FTP, DNS, SMPT, Telnet..
Capa de Presentación	Capa de Aplicación	Datos	*SSL, TLS, MPEG, JPEG,...
Capa de Sesión		Datos	*RPC, SCP, NetBIOS, PPTP, Sockets
Capa de Transporte	Capa de Transporte	Segmento o Datagrama	TCP, UDP, TLS
Capa de Red	Capa de Internet	Paquete	IP, IPSec, ICMP, Router
Capa de Enlace	Capa de Enlace o Acceso a la Red	Trama	Ethernet, PPP, Switch, Bridge
Capa Física		Bit, Baudios	Cables, Fibra, Repeaters, Hub,...

## Virtualización de redes

### Virtualización de redes

Es una tecnología que combina hardware y software para presentar una vista lógica de la red que difiere de la infraestructura física subyacente. Esta técnica permite **combinar múltiples redes físicas en una sola red virtual** o, por el contrario, **dividir una red física en varias redes virtuales independientes**. Cada red virtual puede tener sus propias características y configuraciones, lo que proporciona una gran flexibilidad en la gestión de recursos.

Al **desvincular los servicios de red del hardware subyacente**, la virtualización permite el aprovisionamiento y la administración de la red de forma más eficiente.

#### Beneficios principales:

- **Aumento de la productividad** al facilitar el despliegue y la gestión de recursos.
- **Mejora de la eficiencia** en el uso de la infraestructura existente.
- **Ahorro de costes** al reducir la necesidad de hardware adicional.
- **Facilidad de administración** gracias a una gestión centralizada.
- **Mayor flexibilidad** para adaptarse a las necesidades cambiantes del negocio.

#### Tipos de virtualización de red:

- **Virtualización externa:** Utiliza dispositivos externos, como routers o switches, para dividir una red física en varias redes virtuales.
- **Virtualización interna:** Emplea componentes internos, como tarjetas de red o placas base, para crear redes virtuales dentro de una misma infraestructura física.

## Redes definidas por software (SDN)

Las **Redes Definidas por Software (SDN)** representan un enfoque innovador en la gestión de redes, donde se utiliza software o interfaces de programación de aplicaciones (**API**) para dirigir el tráfico y comunicarse con el hardware subyacente. La SDN **separa el plano de control de la red del plano de datos**, es decir, las decisiones sobre cómo se enruta el tráfico se separan de los dispositivos que efectúan el enrutamiento.

**Objetivo principal de las SDN:** Facilitar la implementación y gestión de servicios de red de manera **determinista, dinámica y escalable**, evitando que los administradores tengan que gestionar servicios a bajo nivel.

### Características clave:

- **Centralización del control de la red**, permitiendo una visión global y unificada.
- **Programabilidad**, facilitando la automatización y adaptación de la red.
- **Virtualización y abstracción de la red**, simplificando la gestión de recursos.
- **Separación de planos**: el **plano de control** toma decisiones, mientras que el **plano de datos** ejecuta el reenvío de paquetes.
- **Flexibilidad y actualización en tiempo real**, adaptándose rápidamente a las necesidades cambiantes.

### Arquitectura de SDN:

- **Capa de aplicación**: Proporciona aplicaciones específicas que utilizan la red, comunicando solicitudes de recursos o información sobre el estado global de la red.
- **Capa de control**: Actúa como el cerebro de la red, tomando decisiones sobre el enrutamiento y configurando los dispositivos de conmutación y enrutamiento según las necesidades de las aplicaciones.
- **Capa de infraestructura**: Constituye el plano físico, donde los dispositivos de red ejecutan las instrucciones recibidas, encargándose de la conmutación y el enrutamiento del tráfico.

### Protocolos de control:

- **OpenFlow**: Estándar abierto que define un protocolo de comunicaciones entre el plano de control y el plano de datos.
- Otros protocolos y plataformas como **OpenDaylight (ODL)** y **OnePK**.

**Clasificación de modelos de SDN:**

- **Abierta:** Basada en estándares abiertos, favoreciendo la interoperabilidad.
- **Por API:** Utiliza interfaces de programación para interactuar con dispositivos específicos.
- **De superposición:** Crea redes virtuales sobre la infraestructura física existente.
- **Híbrida:** Combina elementos de los modelos anteriores para adaptarse a necesidades específicas.

## Redes de área amplia definidas por software (SD-WAN)

Las **Redes de Área Amplia Definidas por Software (SD-WAN)** son una evolución de las redes WAN tradicionales, que incorporan automatización y programabilidad para **encaminar el tráfico de forma dinámica y segura**. Basándose en políticas de aplicación, condiciones de la red o prioridades de los circuitos WAN, las SD-WAN optimizan el enrutamiento sin necesidad de redirigir el tráfico a ubicaciones centrales, lo que **reduce costes y mejora la eficiencia**.

### Beneficios de las SD-WAN:

- **Simplificación de la red**, facilitando su gestión y configuración.
- **Mejora del rendimiento y la fiabilidad**, al optimizar el uso de los enlaces disponibles.
- **Control avanzado del tráfico de datos**, permitiendo priorizar aplicaciones críticas.
- **Flexibilidad en la conexión de dispositivos**, utilizando diversos tipos de enlaces como banda ancha, líneas privadas y conexiones a internet.
- **Actualizaciones y cambios de configuración sin reemplazo de hardware**, gracias a su naturaleza definida por software.

La **SD-WAN basada en Inteligencia Artificial (IA)** añade una capa adicional de inteligencia, proporcionando:

- **Conocimientos basados en IA** para optimizar el rendimiento.
- **Detección de anomalías y resolución automatizada de problemas**, reduciendo el tiempo de inactividad.
- **Mejora de la experiencia del usuario final**, al garantizar un servicio de red más estable y eficiente.
- **Reducción de la carga operativa** para el personal de TI, al automatizar tareas rutinarias.

Finalmente, el concepto de **SASE (Secure Access Service Edge)** integra las funcionalidades de SD-WAN con servicios de seguridad en la nube. Esta solución ofrece:

- **Seguridad de red unificada**, tanto física como basada en la nube, en todos los puntos del perímetro de la red.
- **Acceso seguro y eficiente** a recursos corporativos desde cualquier ubicación.
- **Simplificación de la arquitectura de seguridad**, consolidando múltiples servicios en una sola plataforma.

# Orquestación y Gestión Centralizada de Dispositivos de Comunicaciones

## Orquestación y Gestión Centralizada de Dispositivos de Comunicaciones

La **orquestación y gestión centralizada** son prácticas clave para administrar dispositivos de red de manera eficiente mediante tecnologías como las **redes definidas por software (SDN)**. Permiten un **control centralizado**, optimizando el tráfico, la configuración y el rendimiento de toda la infraestructura de red.

### Redes Definidas por Software (SDN)

- Separan el control de la red del hardware, gestionándolo mediante software.
- Ofrecen **flexibilidad**, permitiendo ajustes rápidos en políticas y configuraciones.
- Aseguran **escalabilidad**, adaptándose a las necesidades cambiantes de la red.

### Visión Global y Control Centralizado

- **Monitoreo en tiempo real:** Supervisión continua del rendimiento y estado de los dispositivos.
- **Resolución rápida de problemas:** Identificación y mitigación eficiente de fallos.
- **Gestión del tráfico:** Priorización de aplicaciones críticas y optimización del ancho de banda.
- **Seguridad uniforme:** Aplicación de políticas de seguridad en toda la red.

### Orquestación

- **Automatización:**
  - Configuración masiva mediante scripts y plantillas.
  - Reducción de errores humanos.
- **Despliegue rápido:**
  - Integración eficiente de nuevos dispositivos con configuraciones predefinidas.
- **Actualización centralizada:**
  - Distribución uniforme de parches y actualizaciones de firmware.

### Gestión Centralizada

- **Consola única:**

- Control y supervisión unificada de todos los dispositivos.
- **Análisis y reportes:**
  - Generación de informes detallados sobre rendimiento y uso.
- **Configuración centralizada:**
  - Cambios y ajustes uniformes desde un único punto.
- **Seguridad integrada:**
  - Protección y monitorización proactiva contra amenazas.

### **Beneficios Clave**

- **Eficiencia:** Automatización y centralización reducen costos y tiempos de gestión.
- **Flexibilidad:** Adaptación rápida a nuevas necesidades o tecnologías.
- **Seguridad mejorada:** Protección uniforme y actualizada.
- **Mayor disponibilidad:** Menor tiempo de inactividad por fallos o ataques.
- **Optimización de recursos:** Uso eficiente del ancho de banda y priorización inteligente.

## Redes de emergencia

### Redes de emergencia

Las redes de emergencia son sistemas de comunicación diseñados para ser utilizados en situaciones de emergencia o crisis. Su objetivo principal es garantizar la comunicación efectiva entre los diferentes servicios de emergencia, como bomberos, policías y servicios médicos.

- **Definición:** "*Conjunto de nodos y enlaces que proporcionan conexiones entre dos o más puntos definidos para intercambiar información, ya sea mediante un canal de voz, vídeo y/o datos, con el objeto de gestionar operaciones de socorro o alertar catástrofes*".

#### Características principales:

- **Uso privado y seguro:** Acceso restringido a usuarios autorizados, garantizando la confidencialidad y seguridad de las comunicaciones.
- **Alta disponibilidad y resistencia:** Diseñadas para operar en condiciones adversas, asegurando el restablecimiento rápido del servicio en caso de fallo.
- **Independencia de redes comerciales:** Funcionan de manera autónoma respecto a las redes públicas para asegurar operatividad en situaciones críticas.
- **Interoperabilidad y trato prioritario:** Capaces de establecer comunicaciones prioritarias y garantizar la interoperabilidad entre las subredes que las conforman.

#### Requisitos mínimos:

- **Tratamiento prioritario del tráfico:** Identificación y gestión preferente del tráfico de emergencia.
- **Seguridad y confidencialidad:** Protección contra accesos no autorizados, manipulaciones e intercepciones.
- **Restablecimiento rápido:** Capacidad para reanudar el servicio eficientemente tras una interrupción.
- **Conectividad amplia:** Integración con otras redes para proporcionar cobertura extensa, incluso a nivel internacional.
- **Compatibilidad y movilidad:** Infraestructuras compatibles que faciliten el transporte y despliegue en diferentes ubicaciones.
- **Cobertura ubicua:** Alcance en grandes zonas geográficas para asegurar comunicación en cualquier lugar.
- **Resistencia a catástrofes:** Diseño robusto para mantener operatividad frente a desastres.

- **Transmisión de voz de calidad:** Comunicaciones claras y sin interferencias.
- **Ancho de banda adaptable:** Capacidad elástica para ajustarse a las necesidades en situaciones de emergencia.
- **Fiabilidad y disponibilidad:** Alto grado de confianza en el desempeño continuo del servicio.

### Tecnologías utilizadas en telecomunicaciones de emergencia: Redes de radio

En las telecomunicaciones de emergencia se emplean principalmente redes de radio, esenciales para asegurar comunicaciones fiables cuando otras infraestructuras pueden fallar.

#### Tipos de redes de radio en Europa:

- **Redes analógicas:** Tienen cobertura limitada y requieren repetidores para ampliar su alcance. Presentan limitaciones en calidad y seguridad.
- **Redes con sistema de acceso troncalizado (Trunking):** Ofrecen servicios de intercomunicación de voz y/o datos para grupos cerrados de usuarios mediante redes independientes de las públicas.
  - **Trunking analógico:** Tecnología obsoleta reemplazada por sistemas digitales.
  - **Trunking digital:** Mejora la calidad de audio, reduce interferencias y permite funcionalidades avanzadas como llamadas en grupo e integración de sistemas de localización.

#### Tecnologías de radio digitales usadas en Europa:

- **TETRA (Terrestrial Trunked Radio):** Sistema de radio trunking digital que conecta múltiples puntos y bases de radio, formando redes extensas que pueden cubrir países enteros.
  - **Características:**
    - Protocolo abierto.
    - Transmisión de voz y datos (mensajes de estado, datos cortos y datos en modo paquete).
    - Utiliza multiplexación por división de tiempo (TDMA) con 4 canales en 25 kHz.
    - Operable en España en la banda de 380-400 MHz para servicios de seguridad y emergencia.
- **TETRAPOL:** Tecnología europea de radiocomunicaciones digitales adaptada a usuarios profesionales de redes privadas de radio (PMR).
  - **Características:**

- Funciona en la banda de 380-400 MHz.
  - Cifrado de extremo a extremo, ofreciendo mayor seguridad que TETRA.
  - Protocolo propietario.
- **LTE (Long Term Evolution):** Soporta un amplio rango de frecuencias y proporciona alto rendimiento a altas velocidades, alcanzando tasas de transferencia superiores a 100 Mbps.
    - **Limitaciones:**
      - Menor resiliencia para comunicaciones críticas.
      - Uso en soluciones mixtas (LTE-TETRA) en proyectos puntuales.

### **Redes de Comunicaciones de Emergencias de ámbito estatal y autonómico**

- **SIRDEE (Sistema de Radiocomunicaciones Digitales de Emergencia del Estado):** Red nacional de radio trunking digital basada en TETRAPOL para las Fuerzas y Cuerpos de Seguridad del Estado.
- **REMER (Red Radio de Emergencia):** Complementaria de la Dirección General de Protección Civil y Emergencias, formada por alrededor de 7.000 radioaficionados.
- **COMDES (Comunicaciones Móviles Digitales de Emergencias y Seguridad de la Comunitat Valenciana):** Red de la Generalitat basada en tecnología TETRA, que ofrece servicios a organizaciones y flotas de emergencias y seguridad en la comunidad.
- **RENEM (Red Nacional de Emergencias):** "Sistema de Sistemas de Información y Telecomunicaciones" que integra sistemas de la Administración General del Estado, Comunidades Autónomas y corporaciones privadas de infraestructuras críticas.
  - **Infraestructura:** Utiliza redes terrestres (Red Iris, Red Sara, WAN PG, Internet) y satelitales (SPAINSAT, XTAR-EU y redes civiles).

## **Red COMDES (Comunicaciones Móviles Digitales de Emergencias y Seguridad de la Comunitat Valenciana)**

La Red COMDES es la infraestructura de telecomunicaciones que la Generalitat ofrece a organizaciones y flotas de prevención, rescate, emergencias y seguridad en la Comunidad Valenciana.

### **Funcionamiento:**

- Opera como una red privada virtual para cada flota.
- Permite intercomunicación mediante grupos de comunicación comunes para facilitar la operativa local, comarcal y autonómica.

### **Infraestructura:**

- **193 estaciones base** que cubren el 98% del territorio y el 99,5% de la población.
- **Capacidad para más de 1.445 comunicaciones** de voz y datos simultáneas.
- **Interconexión con otras redes** públicas y privadas de voz y datos.

### **Servicios ofrecidos:**

- Llamadas individuales y de grupo.
- Configuración dinámica de grupos de comunicación intra e inter flotas.
- Autenticación de terminales y encriptación de comunicaciones.
- Envío de mensajes de texto y posicionamiento GPS.
- Comunicaciones de datos y aplicaciones instalables en terminales y servicios centrales.
- Comunicaciones de voz y datos con redes externas.

### **Organización:**

- **Operador de red:**
  - **Funciones:** Planificación, gestión y supervisión técnica, operativa y administrativa de la red.
  - **Entidad responsable:** Dirección General de Tecnologías de la Información y las Comunicaciones.
- **Usuarios:**
  - **Funciones:** Gestión operativa y uso de la red como apoyo a sus servicios.
  - **Incluye:**
    - Servicios de intervención: Sanitarios, bomberos, protección civil.

- Servicios de seguridad: Policías locales y nacionales.
- Centro de Coordinación de Emergencias de la Comunidad Valenciana: Elabora protocolos y organiza comunicaciones.
- **Proveedores externos:**
  - **Funciones:** Mantenimiento de equipamiento y servicios relacionados.
  - **Incluye:** Empresas contratadas por el operador de red o usuarios para mantenimiento, suministro de terminales, plataformas externas (ej.: 112) y aplicaciones.

## Estándar TETRA (Terrestrial Trunked Radio)

El estándar TETRA es un sistema de comunicación digital móvil desarrollado para redes de emergencia y servicios críticos, mejorando la calidad y seguridad respecto a sistemas analógicos.

### Características:

- **Frecuencia utilizada:** 380-400 MHz.
- **Cobertura extendida:** Usa bandas más bajas que GSM para mayor alcance.
- **Infraestructura independiente:** Separada de redes de telefonía móvil, asegurando operatividad en situaciones donde estas pueden fallar.
- **Modo directo (terminal a terminal):** Comunicación sin necesidad de infraestructura intermedia.
- **Calidad de sonido superior a GSM:** Comunicaciones claras y sin interferencias.
- **Modos de comunicación:** Semidúplex (como radios) y dúplex (como teléfonos).
- **Baja saturación:** Menor riesgo de congestión, garantizando capacidad en alta demanda.
- **Comunicaciones grupales:** Facilita coordinación entre múltiples usuarios.

### Arquitectura del sistema TETRA:

- **Terminales móviles:** Dispositivos de usuario final para comunicación en la red.
- **Estaciones base:** Transmiten y reciben señales de terminales, cubriendo áreas específicas.
- **Sistema de control:** Gestiona la red, llamadas y acceso.
- **Sistema de red:** Conectividad entre componentes, asegurando interoperabilidad.

### Servicios ofrecidos por TETRA:

- **Servicios de voz y datos:** Comunicación eficiente y segura.
- **Llamadas individuales y grupales:** Flexibilidad en comunicaciones.
- **Mensajes de texto y estado:** Información rápida y discreta.
- **Servicios de localización y seguimiento:** Integración GPS para posicionamiento.
- **Acceso a bases de datos y sistemas de información:** Información en tiempo real.

### Seguridad en TETRA:

- **Encriptación de comunicaciones:** Protege contra escuchas no autorizadas.

- **Autenticación de usuarios:** Asegura acceso exclusivo a usuarios autorizados.
- **Protección contra ataques:** Prevención y detección de intrusiones o interferencias.

#### Aplicaciones de TETRA:

- **Servicios de emergencia:** Coordinación en policías, bomberos y servicios médicos.
- **Empresas y eventos masivos:** Comunicación interna en corporaciones y gestión de eventos.
- **Transporte y logística:** Comunicación en transporte público y gestión de flotas.

#### Evolución y tendencias para servicios de datos en banda ancha

La creciente demanda de datos en tiempo real en servicios de emergencia impulsa la evolución de TETRA hacia la integración con tecnologías de banda ancha.

#### Tendencias actuales:

- **Integración con LTE y 5G:** Combinación de la fiabilidad de TETRA con la alta velocidad de datos de redes móviles avanzadas.
- **Desarrollo de estándares abiertos:** Facilita interoperabilidad y reduce dependencia de tecnologías propietarias.
- **Soluciones híbridas:** Sistemas que utilizan TETRA para voz crítica y LTE para datos de banda ancha.
- **Avances en seguridad:** Incorporación de ciberseguridad avanzada para proteger comunicaciones en redes más complejas.

#### Desafíos:

- **Resiliencia y fiabilidad:** Mantener altos estándares de disponibilidad en nuevas tecnologías.
- **Compatibilidad e interoperabilidad:** Asegurar interacción con infraestructuras existentes.
- **Asignación de espectro:** Necesidad de frecuencias dedicadas para servicios de emergencia en bandas aptas para banda ancha.

## Internet de las Cosas (IoT)

### Internet de las Cosas (IoT)

La **Internet de las Cosas (IoT)** es una red de dispositivos conectados que pueden recopilar y compartir datos a través de internet. Estos dispositivos no solo se comunican entre sí, sino que también pueden tomar decisiones de manera autónoma.

El **objetivo principal** del IoT es enviar, recibir y analizar datos para mejorar procesos y tomar decisiones informadas.

#### Componentes del IoT:

- **Objetos conectados:** Dispositivos equipados con sensores y actuadores.
- **Tecnologías de red:** Infraestructura que permite la comunicación entre dispositivos.
- **Protocolos de comunicación:** Reglas y estándares que facilitan el intercambio de datos.
- **Plataforma IoT:** Entorno donde se procesan y gestionan los datos recopilados.
- **Aplicaciones de usuario:** Interfaces mediante las cuales los usuarios interactúan con el sistema.

#### Actores en el IoT:

- **Operadores de telefonía:** Proveen la conectividad necesaria.
- **Industria:** Desarrolla dispositivos y soluciones IoT.
- **Administraciones:** Regulan y promueven el uso del IoT.
- **Usuarios:** Finales y empresariales que utilizan las aplicaciones y servicios.

#### Tipos de dispositivos:

- **Interruptores:** Envían instrucciones a otros objetos.
- **Sensores:** Recopilan datos y los envían para su análisis.

#### Modelos de comunicación:

- **Dispositivo a dispositivo:** Comunicación directa entre dispositivos.
- **Dispositivo a la nube:** Los dispositivos se conectan a servicios en la nube para procesamiento y almacenamiento.
- **Dispositivo a puerta de enlace:** Uso de un intermediario que gestiona la comunicación.

- **Intercambio de datos a través del backend:** Los datos se comparten y procesan en sistemas de respaldo.

#### Ventajas del IoT:

- Conectividad de múltiples dispositivos a la red.
- Intercambio de información rápido y en tiempo real.
- Ahorro energético y procesos más sostenibles.
- Comunicación eficiente con el entorno directo.

#### Desventajas del IoT:

- Problemas de **seguridad y privacidad**.
- Costes asociados a la implementación y mantenimiento.
- Falta de **compatibilidad** entre diferentes dispositivos y estándares.

#### Tipos de arquitecturas:

- **Arquitectura de tres niveles con objetos conectados sin protocolo IP:** Incluye dispositivos, una puerta de enlace y la nube.
- **Arquitectura de dos niveles con objetos conectados con protocolo IP:** Los dispositivos se conectan directamente a la nube usando IP.
- **Arquitectura de dos niveles con objetos conectados sin protocolo IP:** Los dispositivos se conectan a la nube a través de una puerta de enlace sin usar IP.

#### Ecosistema del IoT:

- **Capa de nodos:** Dispositivos y sensores que recopilan datos.
- **Capa de datos:** Almacenamiento y gestión de la información recopilada.
- **Capa de conectividad:** Redes y protocolos que permiten la comunicación.
- **Capa de aplicación:** Servicios y aplicaciones que utilizan los datos para proporcionar valor al usuario.

#### Protocolos del IoT:

- **AMQP (Advanced Message Queuing Protocol)**
- **CoAP (Constrained Application Protocol)**
- **DDS (Servicio de Distribución de Datos)**

- **MQTT (Message Queue Telemetry Transport)**
- **M2M (Protocolo de Comunicaciones entre Máquinas)**
- **XMPP (Extensible Messaging and Presence Protocol)**
- **Tecnologías inalámbricas:** Bluetooth, Zigbee, Z-Wave, 6LoWPAN, Thread, Wi-Fi, NFC.
- **Redes de largo alcance:** Sigfox, LoRaWAN.
- **Conectividad celular:** Redes móviles tradicionales.

## Redes de Sensores

Las **redes de sensores** son sistemas que utilizan dispositivos para recopilar y transmitir datos sobre condiciones físicas o ambientales, como temperatura, sonido o presión. Consisten en una red de pequeños ordenadores o **nodos**, equipados con sensores que colaboran en una o más tareas comunes. Estas redes forman parte de conceptos como la **inteligencia ambiental** y la **computación ubicua**.

### Tipos de redes:

- **Redes de corto alcance o PAN (Personal Area Network):**
  - Alcance limitado, generalmente de menos de 10 metros.
  - Utilizadas en aplicaciones de hogar y edificios inteligentes.
  - **Ejemplos:** Bluetooth, Wi-Fi, Zigbee, NFC, RFID, Z-Wave, 6LoWPAN, IR, UWB, bandas ISM.
- **Redes de largo alcance o WAN (Wide Area Network):**
  - Alcance mucho mayor, utilizadas para transmitir datos a largas distancias.
  - Empleadas en aplicaciones de monitoreo ambiental y transporte.
  - **Ejemplos:** LoRaWAN, Sigfox, LTE-M, NB-IoT, 5G.

### Variantes de redes de sensores:

- **Wireless Sensor Network (WSN):** Redes de sensores autónomos distribuidos espacialmente para monitorear condiciones ambientales.
- **Mobile Wireless Sensor Network (MWSN):** Variante de WSN donde los nodos son móviles, lo que aumenta la flexibilidad y el alcance de la red.

### Factores que pueden afectar a la comunicación:

- **Rendimiento y potencia** de los dispositivos.
- **Ruido y frecuencia** en el entorno de comunicación.
- **Pérdida de espacio libre y difracción** de las señales.
- **Multitrayectoria y absorción** que pueden degradar la señal.
- Características del **terreno** y obstáculos físicos.
- Calidad de las **antenas** y el **alcance** efectivo de la comunicación.

## Ciudades Inteligentes (Smart Cities)

# Ciudades Inteligentes (Smart Cities)

### Definiciones:

- **Ciudad inteligente:** Es una visión holística que aplica las tecnologías de la información y la comunicación (TIC) para mejorar la calidad de vida y la accesibilidad de sus habitantes, asegurando un desarrollo sostenible en los ámbitos económico, social y ambiental. Permite a los ciudadanos interactuar de forma multidisciplinar y adaptarse en tiempo real a sus necesidades, ofreciendo datos abiertos, soluciones y servicios eficientes en calidad y costes. Esto aborda los efectos del crecimiento urbano en ámbitos públicos y privados mediante la integración innovadora de infraestructuras con sistemas de gestión inteligente. En este contexto, la participación del **Internet de las Cosas (IoT)** se vuelve imprescindible.
- **Smart City Platforms (SCPs):** Son plataformas urbanas que ofrecen integración directa entre sistemas y plataformas urbanas, con el fin de proporcionar operaciones y servicios que apoyen el funcionamiento de los servicios urbanos, mejorando la eficiencia, el rendimiento, la seguridad y la escalabilidad.

\***Retos:** Las ciudades inteligentes enfrentan desafíos como la escalabilidad, las tecnologías heredadas (legacy), la gobernanza, la falta de bancos de pruebas (testbeds), la interoperabilidad y la reutilización.

### Tecnologías Clave

- **IoT (Internet de las Cosas):** Incluye hardware como sensores y actuadores, middleware y recolección de datos.
- **Big Data:** Comprende el procesamiento, almacenamiento, análisis y visualización de datos.
- **Sistemas Ciberfísicos:** Integran la computación en sistemas físicos y permiten la actuación en la ciudad.
- **Cloud Computing:** Ofrece servicios de hosting, almacenamiento, computación, elasticidad y escalabilidad.

### Arquitectura Tecnológica de una Plataforma Urbana

Se centra en el uso de sensores y dispositivos IoT para recopilar datos sobre la ciudad, facilitando la toma de decisiones y mejorando los servicios urbanos.

**Estándares Internacionales:** Para garantizar la interoperabilidad y calidad, se siguen estándares como **ITU-T Y.4201**, **ISO/IEC 24039**, **UNE 178104:2017**, **DIN 91357-2017** y **FIWARE**.

### **Capas Comunes (5):**

- **Capa de Adquisición:** Se encarga de la adquisición e integración de datos de sistemas de información y dispositivos IoT. Incluye sensores desplegados en la ciudad (semáforos, farolas, riego de parques, temperatura, aforo, etc.), sistemas de información e infraestructuras externas, dispositivos ciudadanos (aplicaciones móviles) y redes sociales. Se recomienda el uso de protocolos estándar.
- **Capa de Conocimiento:** Responsable del procesamiento y análisis de la información. Debe integrar software y herramientas para la gestión y tratamiento de datos, minería de datos, análisis de ingeniería, control de sistemas, aprendizaje automático, evaluación medioambiental y análisis económicos y sociales. Además, debe compartir datos e información entre las partes interesadas de la ciudad e integrar herramientas de modelización como SIG, CIM y BIM.
- **Capa de Interoperabilidad:** Proporciona interfaces estándar y abiertas que garantizan el envío y acceso a los datos por parte de diferentes aplicaciones y sistemas. Los datos abiertos deben estructurarse en torno a normas bien definidas y acompañarse de los metadatos correspondientes. La licencia asociada a los datos debe indicar claramente si pueden ser compartidos y utilizados libremente por terceros, y se deben anonimizar los datos cuando sea necesario.
- **Capa de Servicios Inteligentes:** Integra herramientas específicas para interactuar con los ciudadanos, la administración, proveedores de servicios, profesionales y visitantes. Se debe difundir información a diferentes grupos y recibir información, comentarios y peticiones de las partes interesadas de la ciudad.
- **Capa de Soporte:** Se encarga de la gestión y soporte de la seguridad, incluyendo servicios de auditoría, monitorización, seguridad, registro (logging), operaciones, administración, gestión y configuración (OAM). Debe ofrecer una visión única y centralizada.

**Interfaces:** Se definen interfaces de adquisición, de servicios y de interoperabilidad.

### **Soluciones**

Las soluciones en ciudades inteligentes abarcan la sensorización medioambiental, eficiencia energética, iluminación inteligente, tráfico inteligente, gestión de residuos urbanos, aplicaciones para la promoción del comercio y movilidad urbana inteligente.

### **Gobierno**

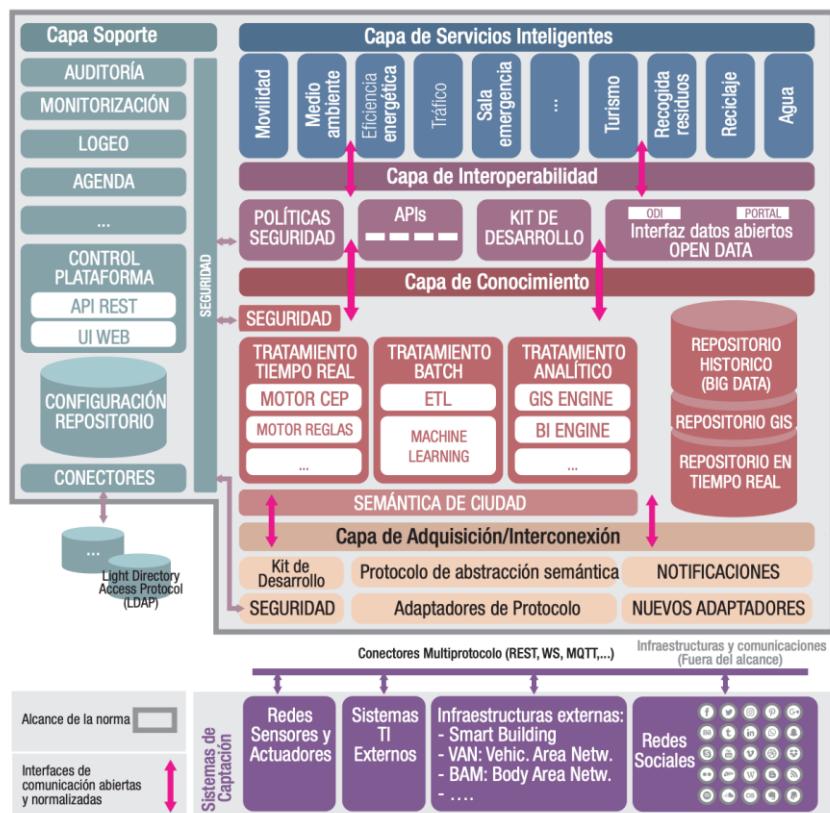
El gobierno en las ciudades inteligentes busca crear un marco para el desarrollo y despliegue de soluciones, así como el establecimiento de políticas y reglamentos que garanticen un uso ético y responsable. La gobernanza en torno a la plataforma de datos de la ciudad es crucial, y la cooperación y colaboración entre los ámbitos público y privado son esenciales.

## Norma Y.4201

La **Norma Y.4201** ("Requisitos de alto nivel y marco de referencia de las plataformas de ciudades inteligentes") es un estándar internacional que establece los requisitos y el marco de referencia para plataformas de ciudades inteligentes. Garantiza la calidad y la interoperabilidad de estas plataformas, definiendo los requisitos para su implementación y proporcionando un marco para su diseño y desarrollo.

### Aspectos principales:

- **Integración de Datos:** Requisitos para la integración de datos de diferentes fuentes y sistemas en una plataforma de ciudad inteligente.
- **Interoperabilidad:** Requisitos para garantizar la interoperabilidad entre diferentes sistemas y servicios en una plataforma de ciudad inteligente.
- **Seguridad y Privacidad:** Requisitos para garantizar la seguridad y la privacidad de los datos y la información en una plataforma de ciudad inteligente.
- **Gestión de Cambios:** Requisitos para la gestión de cambios en una plataforma de ciudad inteligente, incluyendo la implementación de nuevos servicios y la actualización de sistemas existentes.



## Redes inalámbricas

### Redes inalámbricas

Las redes inalámbricas permiten la conexión de nodos mediante ondas electromagnéticas, eliminando la necesidad de una red cableada. Son esenciales en entornos donde la movilidad y la flexibilidad son prioritarias.

#### Tipos de redes inalámbricas por alcance

- **WPAN (Wireless Personal Area Network)**

Red para la comunicación entre dispositivos cercanos al punto de acceso.

- **Ejemplos:** Bluetooth (2-6 Mbits; 2.4-5 GHz; 5-20 m), RFID, NFC, ZigBee.
  - **Alcance:** 10-100 m.

- **WLAN (Wireless Local Area Network)**

Red de comunicación para distancias cortas basada en ondas de radio o infrarrojas.

- **Ejemplos:** Wi-Fi (802.11) → (+600 Mbits; 2.4-5 GHz; 50-250 m).
  - **Alcance:** 100 m-1 km.

- **WMAN (Wireless Metropolitan Area Network)**

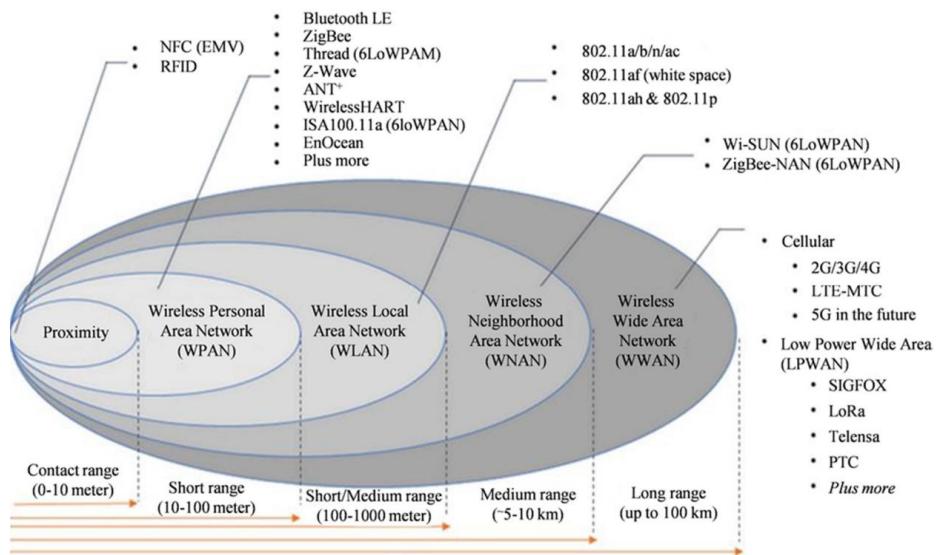
Red de banda ancha para cubrir áreas geográficas extensas.

- **Ejemplos:** WiMAX (+70 Mbits; 2-11 GHz; 50 km).
  - **Alcance:** 1-50 km.

- **WWAN (Wireless Wide Area Network)**

Red que utiliza tecnologías de comunicación móvil.

- **Ejemplos:** 2G, 3G, 4G LTE, 5G, WiMAX, UMTS, GPRS, EDGE, CDMA2000, GSM, CDPD, Mobitex, HSPA.
  - **Alcance:** Hasta 100 km.



### Tipos de redes inalámbricas por el rango de frecuencias

- **Microondas terrestres:**  
Utilizan antenas parabólicas ( $\varnothing$  3 m) que requieren alineación para conexiones punto-a-punto.
- **Microondas por satélite:**  
Enlazan estaciones terrestres (base) con un satélite.
  - **Señal ascendente:** Emitida por la estación terrestre.
  - **Señal descendente:** Retransmitida por el satélite en otra banda de frecuencia.
- **Infrarrojos:**  
Utilizan transmisores y receptores que modulan luz infrarroja no coherente.

### Estándares IEEE 802

- **IEEE 802.1 (LAN, MAN, WAN)**
  - 802.1D: Puentes MAC.
  - 802.1Q: VLANs.
  - 802.1X: Control de acceso a la red basado en puertos (autenticación).
- **IEEE 802.2 (LLC)**  
Control lógico de enlace (LLC).
- **IEEE 802.3 (Ethernet)**  
Redes Ethernet cableadas.

- **IEEE 802.11 (WLAN)**

Redes Ethernet inalámbricas → WiFi (+600 Mbits; 2.4-5 GHz; 50-250 m).

- Estándar "n" o superior: Admite múltiples frecuencias (2.4/5/6 GHz).
- Subestándares:
  - **a**: 5 GHz.
  - **n**: Estándar actual.

- **IEEE 802.15 (WPAN)**

Redes de área personal inalámbricas (Bluetooth: 50 Mbits; 2.4 GHz; 0.5-100 m).

- **IEEE 802.16 (WMAN)**

Redes metropolitanas inalámbricas (WiMAX).

### Conceptos generales IEEE 802.11

- **Estaciones**: Dispositivos con interfaz de red.

- **Medio**: Radiofrecuencias o infrarrojos.

- **Punto de acceso (AP)**:

- Funciona como un puente, conectando redes con niveles de enlace similares o distintos.
- Realiza conversiones de tramas.

- **Sistema de distribución**:

- Proporciona movilidad entre APs.
- Controla la ubicación de las estaciones para enviar tramas correctamente.

- **Conjunto de Servicio Básico (BSS)**: Grupo de estaciones intercomunicadas.

- **Independientes**: Comunicación directa entre estaciones.
- **Infraestructura**: Comunicación a través de un punto de acceso.

- **Conjunto de Servicio Extendido (ESS)**: Unión de varios BSS.

- **Área de servicio básico**:

- Define la capacidad de movilidad entre terminales cambiando de BSS.
- La transición es correcta dentro del mismo ESS.

- **Límites de la red**:

- Difusos debido al solapamiento de diferentes BSS.

Generation	IEEE Standard	Maximum Linkrate (Mbit/s)	Adopted	Radio Frequency (GHz)
Wi-Fi 7	802.11be	40000	TBA	2.4/5/6
Wi-Fi 6E	802.11ax	600 to 9608	2020	2.4/5/6
Wi-Fi 6			2019	2.4/5
Wi-Fi 5	802.11ac	433 to 6933	2014	5
Wi-Fi 4	802.11n	72 to 600	2008	2.4/5
(Wi-Fi 3*)	802.11g	6 to 54	2003	2.4
(Wi-Fi 2*)	802.11a	6 to 54	1999	5
(Wi-Fi 1*)	802.11b	1 to 11	1999	2.4
(Wi-Fi 0*)	802.11	1 to 2	1997	2.4

Enmienda	Fecha de publicación	Descripción
<u>802.11i</u>	2004	Agrega mecanismos de <b>identificación y encriptación de datos</b> (WPA), para reemplazar el algoritmo WEP original del estándar 802.11 que está obsoleto.
<u>802.11w</u>	2009	<b>Aumenta la seguridad</b> de los marcos de gestión.

## Redes 5G y Programa ÚNICO-Banda Ancha

### Redes 5G

La quinta generación de comunicaciones móviles (5G) se caracteriza por su capacidad para ofrecer **mayor velocidad, menor latencia y mayor capacidad de conectividad**. No es una tecnología estática, ya que evoluciona mediante la publicación de nuevas “releases”. Esta red inalámbrica se adapta a diversos casos de uso, proporcionando soluciones especializadas según el tipo de conexión.

#### Características básicas de las redes 5G

- **Velocidad máxima:** 20 Gbps de bajada y 10 Gbps de subida.
- **Latencia:** 1 ms.
- **Disponibilidad:** 99,999%.
- **Capacidad de volumen de datos:** Hasta 10 TB/s por km<sup>2</sup>.
- **Dispositivos conectados:** Soporta hasta 1 millón de dispositivos por km<sup>2</sup>.
- **Eficiencia energética:** 90% más eficiente que 4G.

#### Bandas de frecuencia utilizadas

- **Banda de 700 MHz** (694-790 MHz): Ideal para amplias coberturas rurales.
- **Banda de 3,5 GHz** (3,4-3,8 GHz): Banda principal para ofrecer altas velocidades.
- **Banda de 26 GHz** (24,25-27,5 GHz): Proporciona capacidades para zonas densamente pobladas.

#### Tipos de comunicaciones en 5G

- **Banda ancha móvil mejorada (eMBB):** Alta tasa de transmisión de datos en movilidad (10-20 Gbps de bajada, 1-10 Gbps de subida).
- **Comunicaciones de baja latencia y alta fiabilidad (URLLC):** Comunicaciones críticas con latencia de 1-10 ms y fiabilidad del 99,999%.
- **Comunicaciones masivas para IoT (mMTC):** Orientadas a dispositivos de bajo coste y bajo consumo, con capacidad para conectar hasta 1 millón de nodos por km<sup>2</sup>.

#### Multi-access Edge Computing (MEC)

Permite la ejecución de aplicaciones en los bordes de la red, reduciendo la latencia y mejorando la eficiencia al procesar los datos más cerca de donde se generan.

#### Organizaciones de normalización del 5G

- **3GPP:** Asociación del Proyecto de 3<sup>a</sup> Generación.
- **ETSI:** Instituto Europeo de Normas de Telecomunicaciones.
- **UIT-T:** Sector de Normalización de las Telecomunicaciones de la UIT.

- **IETF:** Grupo de Trabajo de Ingeniería de Internet.
- **IEEE:** Instituto de Ingenieros Eléctricos y Electrónicos.

### Tecnología básica de redes 5G

- Uso de **bandas de alta y ultra alta frecuencia**.
- Empleo de técnicas avanzadas de modulación y codificación para mejorar la eficiencia de transmisión.
- Utilización de tecnologías de multiplexación como **FDMA**, **TDMA** y **CDMA** para transmitir múltiples señales simultáneamente.

### Aplicaciones del 5G

- **Industria 4.0:** Automatización y robótica avanzada.
- **Agricultura de precisión:** Uso de UAVs para aplicación en tiempo real de fitosanitarios.
- **Ingeniería y construcción:** Modelos digitales de proyectos.
- **Infraestructuras digitales:** Smart Cities.
- **Control de fronteras:** Sistemas de defensa y seguridad avanzados.
- **Sector audiovisual:** Producción y distribución de contenidos con alta conectividad.
- **Ciencia aplicada:** Aplicaciones en metaversos e Internet de los sentidos (IoS).

### Programa de Universalización de Infraestructuras Digitales para la Cohesión (UNICO)

Este programa fomenta la universalización del acceso a la banda ancha ultra rápida y la extensión del 5G mediante convocatorias específicas.

Los principales subprogramas son:

- **UNICO-Banda Ancha**
- **UNICO-Servicios Públicos**
- **UNICO-Industria y Empresas**
- **UNICO-Bono Social**
- **UNICO-Edificios**
- **UNICO 5G I+D**
- **UNICO 5G Redes – Pasivas y Backhaul Fibra Óptica**
- **UNICO-Bono Pyme**
- **UNICO-Demanda Rural**
- **UNICO I+D 6G**
- **UNICO Sectorial 5G**

## Programa UNICO-Banda Ancha

El objetivo principal es facilitar el despliegue de infraestructuras de banda ancha de muy alta velocidad mediante ayudas dirigidas a operadores de telecomunicaciones.

### Características

- Servicios de velocidad simétrica entre **300 Mbps y 1 Gbps**.

### Actuaciones

- **UNICO Banda Ancha Acceso:** Proporcionar velocidades de 300 Mbps (actualizables a 1 Gbps) en zonas sin cobertura.
- **UNICO Banda Ancha Interconexión terrestre:** Ampliar la conectividad a 1 Gbps para entidades públicas, centros educativos, redes de investigación y defensa.
- **UNICO Banda Ancha Interconexión submarina:** Incrementar la capacidad en cables submarinos para instituciones públicas y redes de defensa.

### Objetivos

- Garantizar el acceso universal a internet de alta velocidad para todos los hogares y empresas en España.
- Impulsar la competitividad y el desarrollo económico.
- Desplegar infraestructuras avanzadas como fibra óptica y tecnologías móviles de última generación (5G).

## Seguridad en las Comunicaciones

# Seguridad en las Comunicaciones

La seguridad en las comunicaciones protege la integridad, confidencialidad y disponibilidad de los datos durante su transmisión a través de redes. Incluye medidas, políticas y tecnologías que mitigan riesgos y previenen accesos no autorizados.

### Seguridad Perimetral: Firewalls NGFW y Dispositivos de Gestión de Tráfico

La **seguridad perimetral** resguarda los límites de una red para prevenir accesos no autorizados. Los **firewalls** son componentes clave que controlan el tráfico según reglas definidas.

#### Tipos de Firewalls:

- **Filtrado de paquetes:** Inspeccionan las direcciones IP y las tramas para permitir o bloquear el tráfico entre redes.
- **De estado:** Registran conexiones activas para un control más dinámico.
- **De aplicación:** Analizan protocolos en el nivel de aplicación, detectando usos indebidos o amenazas específicas.

#### Topologías de Firewalls:

- **Bastion Host:** Firewall instalado directamente en un equipo clave.
- **Encaminador con filtrado:** Un router que bloquea tráfico entre redes o nodos específicos.
- **Host con doble conexión:** Un servidor con dos interfaces separadas que conecta redes internas y externas sin reenvío directo.
- **Screened Host:** Combina un bastion host con un router de filtrado, asegurando que solo el bastion host sea accesible desde Internet.
- **Screened Subnet:** Establece una subred aislada entre las redes interna y externa, añadiendo capas de seguridad.

#### Políticas de Firewalls:

- **Restrictiva:** Bloquea todo el tráfico excepto el explícitamente permitido.
- **Permisiva:** Permite todo el tráfico salvo el explícitamente denegado.

#### Firewalls Avanzados:

- **UTM (Unified Threat Management):** Integran funcionalidades como antivirus, VPN y detección de intrusos. Ideales para PyMEs.
- **NGFW (Next-Generation Firewall):** Evolución de los firewalls tradicionales, ofrecen:
  - **Inspección profunda** en múltiples niveles.

- **IDS/IPS** (detección y prevención de intrusiones).
- **Prevención de amenazas (TPS)**.
- **Control granular** de aplicaciones y contenido.
- **Análisis detallado** y generación de informes.

#### **Dispositivos de Gestión de Tráfico:**

- **Funcionalidades:**
  - Monitorización del tráfico.
  - Control de acceso y filtrado de paquetes.
  - Gestión del ancho de banda.
- **Dispositivos:** Firewalls, routers y switches gestionables.

#### **Servidores y Servicios AAA (Autenticación, Autorización y Accounting)**

El modelo **AAA** garantiza acceso seguro a sistemas y redes, respondiendo a tres preguntas fundamentales:

- **Autenticación ("¿Quién eres?")**: Verifica la identidad del usuario o dispositivo.
- **Autorización ("¿Qué puedes hacer?")**: Determina permisos y recursos accesibles.
- **Accounting ("¿Qué has hecho?")**: Registra y audita actividades para trazabilidad.

#### **Protocolos AAA:**

- **RADIUS**: Autenticación centralizada para acceso remoto, VPN y puntos de acceso inalámbricos.
- **Kerberos**: Utiliza tickets para autenticar usuarios sin transmitir contraseñas.

#### **Seguridad en el Acceso a Redes de Usuario (NAC)**

El **Network Access Control (NAC)** asegura que solo dispositivos conformes a políticas corporativas accedan a la red.

#### **Beneficios:**

- Evita accesos no autorizados o inseguros.
- Refuerza el cumplimiento de políticas corporativas.
- Segmenta y controla dispositivos de forma dinámica.

#### **Implementaciones:**

- **Out of Band**: Menor impacto en la red; rápido despliegue.
- **In-line**: Control continuo del tráfico; supervisa y aplica restricciones tras el acceso.

**Herramientas Complementarias:**

- Gestión de parches.
- Escáneres de vulnerabilidades.
- Sistemas de prevención de intrusos (IPS).

## Seguridad Inalámbrica

La **seguridad inalámbrica** protege redes Wi-Fi mediante autenticación, cifrado y otras medidas que minimizan riesgos.

### Prácticas Recomendadas:

- Cambiar contraseñas predeterminadas del router y Wi-Fi.
- Configurar cifrado WPA2 o WPA3.
- Actualizar firmware del router.
- Deshabilitar funciones no seguras (WPS, UPnP, administración remota).
- Configurar redes para invitados.

### Protocolos de Seguridad Inalámbrica:

- **WEP (Wired Equivalent Privacy):** Cifrado RC4, actualmente obsoleto por vulnerabilidades.
- **WPA (Wi-Fi Protected Access):** Cifrado TKIP con RC4; seguro si se usan contraseñas fuertes.
- **WPA2:** Estándar basado en AES y CCMP; versiones:
  - **Personal:** Autenticación con contraseña compartida.
  - **Enterprise:** Autenticación con servidor RADIUS.
- **WPA3:** Última generación, utiliza GCMP-256, claves más robustas y mayor simplicidad de configuración.

### Protocolos de Autenticación:

- **RADIUS:** Ideal para redes empresariales, centraliza la autenticación.
- **Kerberos:** Autenticación segura basada en tickets, sin transmitir contraseñas.

## Acceso seguro a redes corporativas

### Acceso seguro a redes corporativas

El acceso seguro a redes corporativas permite a los usuarios conectarse de manera protegida a los recursos de una red corporativa desde ubicaciones remotas, garantizando la integridad, confidencialidad y autenticidad de la información transmitida. Esto se logra mediante tecnologías como **VPN** (Virtual Private Network) e **IPSec** (Internet Protocol Security).

#### 1. Redes Privadas Virtuales (VPN)

Una VPN establece un “túnel” seguro sobre una red física insegura (ej.: Internet). Este túnel encapsula y cifra los datos, proporcionando la funcionalidad, seguridad y políticas de una red privada.

##### Características básicas:

- **Autenticación y autorización:** Verificación de identidad del usuario.
- **Integridad:** Protección contra alteraciones no autorizadas de los datos.
- **Confidencialidad y privacidad:** Cifrado de datos transmitidos.
- **No repudio:** Prevención de la negación de acciones realizadas.
- **Control de acceso:** Restricción de accesos no autorizados.
- **Auditoría y registro de actividades:** Trazabilidad de accesos.
- **Calidad del servicio (QoS):** Priorización del tráfico en la red.

##### Requisitos básicos:

- **Identificación de usuario:** Credenciales (usuario y contraseña).
- **Cifrado de datos:** Algoritmos como DES, 3DES, AES o SEAL (más rápido).
- **Administración de claves:** Gestión de claves criptográficas.

##### Tipos de VPN:

- **VPN site-to-site:** Comunicación segura entre redes de diferentes sedes.
- **VPN de acceso remoto:** Conexión entre un usuario remoto y la red interna.
- **VPN de equipo a equipo:** Seguridad en las comunicaciones entre dispositivos.
- **VPN Cloud:** Acceso simultáneo a recursos de la nube y de la organización.

##### Tecnologías de VPN según nivel:

- **Aplicación:** Túneles SSH (proxy).
- **Transporte:** VPN TLS.

- **Red:** IPSec, WireGuard.
- **Enlace:** VPNs basadas en MACsec.

#### Protocolos de VPN:

- **PPP (Point-to-Point Protocol):** Conexión directa entre dos nodos.
- **PPTP (Point-to-Point Tunneling Protocol):** Limitado a un único túnel, ya no es seguro.
- **L2TP (Layer 2 Tunneling Protocol):** Mejoras sobre PPTP, más seguro.

**Concentrador VPN:** Dispositivo que gestiona múltiples túneles encriptados, permitiendo conexiones remotas para numerosos usuarios simultáneamente.

**Funcionamiento:** Los datos se encapsulan en un túnel que simula una conexión punto a punto, garantizando la seguridad incluso en redes públicas.

## 2. IPSec (Internet Protocol Security)

IPSec opera en la capa de red, proporcionando un estándar abierto y transparente para aplicaciones. Garantiza la seguridad de las comunicaciones mediante cifrado y autenticación.

#### Características:

- **Autenticación:** Verificación de origen de los datos.
- **Confidencialidad:** Cifrado de paquetes IP.
- **Protección anti-reenvíos:** Evita ataques por repetición.
- **Transparencia:** No requiere modificación en las aplicaciones.
- **Perfect Forward Secrecy:** Protección frente a compromisos futuros de claves.

#### Modos de funcionamiento:

- **Modo transporte:** Protege los datos del nivel de transporte.
- **Modo túnel:** Encripta el paquete IP completo, usado en VPN.

#### Protocolos de seguridad:

- **AH (Authentication Header):** Integridad y autenticación de paquetes.
  - Algoritmo HMAC.
  - Funciona en el puerto 51.
- **ESP (Encapsulating Security Payload):** Confidencialidad, integridad y autenticación.
  - Cifra solo el contenido de los paquetes, no las cabeceras.
  - Funciona en el puerto 50.

#### Protocolos complementarios:

- **IKE (Internet Key Exchange)**: Intercambio de claves y establecimiento de SA (Security Association). Funciona en el puerto 500 de UDP.
- **IPComp**: Compresión de datos antes del cifrado.

**Protocolos SSL/TLS**: Securizan el nivel de transporte, proporcionando conexiones cifradas para protocolos como HTTP.

### Gestión de identidades y accesos

El acceso remoto requiere autenticación previa para garantizar la identidad del usuario.

#### Funciones principales:

- Gestión de cuentas y contraseñas según políticas de la empresa.
- **Centralización de permisos**: Uso de directorios (ej.: LDAP).
- Esquema de autorizaciones: Unificación de autorizaciones en un único punto.
- **Single Sign-On (SSO)**: Acceso a múltiples sistemas con una única autenticación.

#### Mecanismos de autenticación:

- **Usuario y contraseña**.
- **Certificados digitales**.
- **Autenticación multifactor**: Combinación de métodos.

#### Modelos de autorización:

- **DAC (Discretionary Access Control)**: Basado en la identidad del usuario.
- **RBAC (Role-Based Access Control)**: Control granular según roles.
- **MAC (Mandatory Access Control)**: Políticas estrictas mediante etiquetado de elementos.

### Acceso remoto seguro (SSH)

SSH reemplaza a Telnet como protocolo de acceso remoto seguro, proporcionando autenticación por clave pública y cifrado robusto para conexiones a través del puerto 22.



FINAL DEL DOCUMENTO