Apuntes de la asignatura

Gestión de la Información

Grado en Gestión y Administración Pública

Autor: Prof. Ignacio Díaz Cano

Curso: 2025/2026

Índice general

Índice de figuras

Índice de tablas

Acrónimos

AEPD Agencia Española de Protección de Datos. 61, 75

AGE Administración General del Estado. 17, 20, 38, 51

API Interfaz de Programación de Aplicaciones. 77

ARCO Acceso, Rectificación, Cancelación y Oposición. 64, 65

ARPA Agencia de Proyectos de Investigación Avanzada. 48

BCP Business Continuity Plan. 73

BD Bases de Datos. 29, 32, 34, 36, 39, 40

BDR Bases de Datos Relacionales. 31

BIA Business Impact Analysis. 73

BYOD *Bring Your Own Device*. 76, 78, 79

CCN Centro Criptológico Nacional. 69

CCN-CERT Centro Criptológico Nacional *Computer Emergency Response Team*. 62, 69

CISO *Chief Information Security Officer*. 69, 70, 74

CSIRT Equipo de Respuesta a Incidentes de Seguridad Informática. 74

DDL *Data Definition Language*. 36

DEHú Dirección Electrónica Habilitada Única. 17, 19, 21, 40

DIR3 Directorio Común de Unidades Orgánicas y Oficinas. 39

DLP Prevención de Pérdida de Datos. 79

DNS *Domain Name System*. 49

DPD Delegado/a de Protección de Datos. 60, 61, 68, 74

DRP Disaster Recovery Plan. 73

EIPD Evaluaciones de impacto. 60, 61, 66

ENI Esquema Nacional de Interoperabilidad. 5, 18, 22

ENS Esquema Nacional de Seguridad. 4, 18, 22, 59, 60, 62, 67–71, 75, 78

FTP *File Transfer Protocol*. 47

HTTP *Hypertext Transfer Protocol*. 47

IA Inteligencia Artificial. 3

IDS Sistema de Detección de Intrusiones. 74

INCIBE Instituto Nacional de Ciberseguridad. 69, 70

INSS Instituto Nacional de la Seguridad Social. 18

IOC Indicador de Compromiso. 74

IOT *Internet Of Things*. 32

IPS Sistema de Prevención de Intrusiones. 74

ITS Instrucciones Técnicas de Seguridad. 62

LAN *Local Area Network*. 44

LOPDGDD Ley Orgánica de Protección de Datos y Derechos de Garantías Digitales. 4, 59–62, 67

MAN *Metropolitan Area Network*. 44

MFA Autenticación MultiFactor. 79

MTD *Mobile Threat Defense*. 78

MTTR Tiempo Medio de Recuperación. 76

NIST Instituto Nacional de Estándares y Tecnología. 71

NoSQL Bases de Datos No Relacionales. 32

OGP *Open Government Partnership*. 7

ORVE Oficina de Registro Virtual de Entidades. 39

OSI *Open Systems Interconnection*. 45

OTP Código de un Solo Uso. 16

REGAGE Registro Electrónico General. 38

RETA Régimen Especial de Trabajadores Autónomos. 19

RGPD Reglamento General de Protección de Datos. 4, 15, 22, 59–62, 67, 75, 78

RPA Automatización de Procesos. 14

RPO Recovery Point Objective. 73, 78

RTO Recovery Time Objective. 73, 78

SARA Sistema de Aplicaciones y Redes para las Administraciones. 20, 22, 54

SEDESS Sede Electrónica de la Seguridad Social. 18, 19

SGAD Secretaría General de Administración Digital. 20

SGBD Sistema Gestor de Bases de Datos. 30, 33, 35–37

SGEE Sistema de Gestión Electrónica de Expedientes. 3

SGSI Sistema de Gestión de Seguridad. 62, 67, 71

SI Sistema de Información. 1, 2, 4, 5, 14

SIA Sistema de Información Administrativa. 39

SIEM Sistema de Gestión de Eventos e Información de Seguridad. 74

SIGP Herramientas de Gestión de Personal. 51

SIR Sistemas de Interconexión de Registros. 5, 20

SLA Acuerdo de Nivel de Servicio de seguridad. 74, 78

SOC *Security Operations Center*. 69, 74

SQL *Structured Query Language*. 36, 37

SSO Inicio de Sesión Único. 79

TCP/IP *Transmission Control Protocol/Internet Protocol*. 46

TGSS Tesorería General de la Seguridad Social. 18

TIC Tecnologías de la Información y las Comunicaciones. 14

TLS Seguridad de la Capa de Transporte. 78

UE Unión Europea. 15, 21, 59

VPN Red Privada Virtual. 78

WAN *Wide Area Network*. 45

WWW *World Wide Web*. 49

Capítulo 1

Sistemas de Información para la Administración Pública

1.1. Introducción a los sistemas de información en la administración pública

En la actualidad, la gestión pública requiere del uso sistemático de tecnologías de la información para poder responder a las demandas ciudadanas de forma eficiente, transparente y responsable. Un Sistema de Información (SI) no se limita al uso de ordenadores o programas, sino que representa una estructura integrada que permite a las organizaciones públicas cumplir sus objetivos estratégicos (European Commission, 2017).

1.1.1. Definición de sistema de información

Un sistema de información puede definirse como un conjunto interrelacionado de elementos (hardware, software, datos, personas y procesos) diseñado para recolectar, procesar, almacenar y distribuir información que apoye la toma de decisiones y el control dentro de una organización (Laudon and Laudon, 2020).

Los SI pueden ser utilizados para:

- Automatizar tareas administrativas (registro, archivo, cálculo), aumentando así la productividad de los procesos.

- Mejorar la comunicación interna y externa, haciendo a ésta más eficiente y fiable, desde el punto de vista administrativo y humano. La comunicación podría tener un carácter más general o particular, dependiendo del contexto y de las herramientas empleadas para su transmisión.

- Analizar grandes cantidades de datos para la planificación estratégica. Algo que sería imposible realizar solo con conocimiento y aplicación humana, ya que esta, por más que se aumente su número, siempre sería limitada.

- Facilitar el acceso a la información pública, de una forma más segura, más fiable y precisa. Haciendo que la información sea garante de los procesos en los que interviene, y facilitando al ciudadano su localización.

1.1.2. Componentes básicos de un sistema de información

Hardware: Equipos físicos como servidores, ordenadores, impresoras, escáneres y dispositivos móviles. Constituyen la infraestructura tecnológica sobre la que operan los SI.

Software: Programas que permiten ejecutar tareas específicas. Incluye tanto software de base (sistemas operativos) como software de aplicación (gestores documentales, bases de datos, sistemas de gestión).

Datos: Elementos básicos que se transforman en información significativa a través del procesamiento. Su calidad, integridad y actualidad son fundamentales. En el caso en el que los datos no tengan un mínimo de calidad y son coherentes los resultados pueden ser deficientes.

Personas: Usuarios finales, técnicos informáticos, administradores de sistemas, responsables funcionales, etc. La interacción humano-tecnología es clave.

Procesos: Conjunto de actividades estructuradas que permiten transformar los datos en información útil. Generalmente se usa el principio de "caja negra" donde se conoce la información que entra (datos) y la de salida (resultados), pero no cómo se realizan los procesos en el interior de los SI.

En la Figura 1.1 se puede observar la unión entre los diferentes componentes de un sistema de información. Todos los componentes desembocan en el propio sistema y deben tener una estrecha relación con él en todo momento.

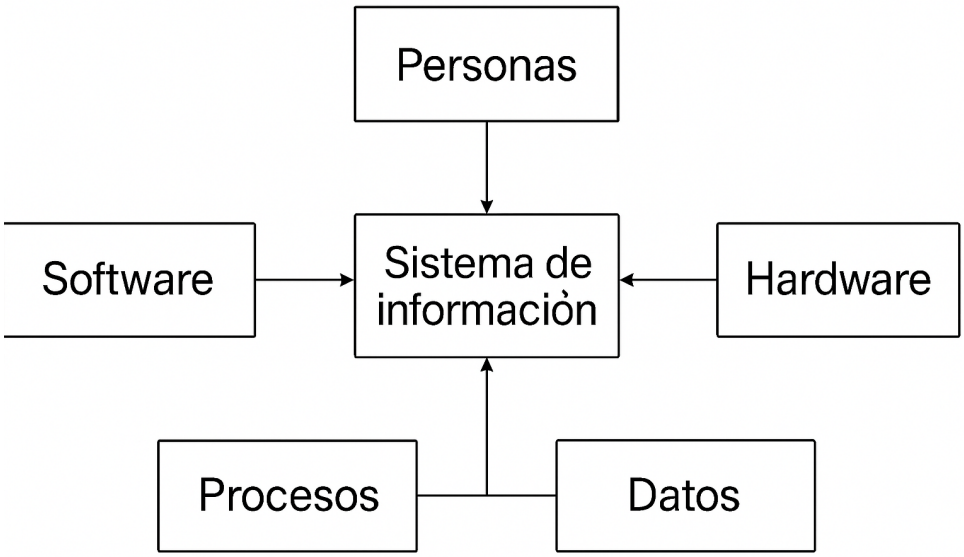

Figura 1.1: Diagrama de bloques con los cinco componentes interconectados.

1.2. Funciones y objetivos de los sistemas de información públicos

Los SI en la administración no tienen una función puramente técnica. Son herramientas estratégicas que permiten transformar la manera en que se gestionan los servicios públicos.

La digitalización de los procedimientos administrativos es una de las transformaciones más relevantes en la administración pública contemporánea. Entre las aplicaciones más extendidas se encuentra el Sistema de Gestión Electrónica de Expedientes (SGEE), cuyo objetivo es sustituir los expedientes físicos en papel por documentos y procesos íntegramente digitales. Los objetivos del SGEE son:

- Eliminar el uso de papel en la tramitación de expedientes.
- Permitir el acceso remoto y en tiempo real a los documentos.
- Garantizar la trazabilidad, integridad y seguridad jurídica de los procedimientos.
- Reducir los tiempos de resolución y aumentar la eficiencia administrativa.
- Asegurar el cumplimiento de la normativa sobre administración electrónica (Ley 39/2015. y Ley 40/2015).

A continuación, se detallan sus principales funciones y objetivos:

1.2.1. Apoyo a la toma de decisiones

Los gestores públicos requieren datos consolidados, precisos y actuales para tomar decisiones efectivas. Por ejemplo, los datos demográficos de una región pueden guiar el diseño de políticas educativas o sanitarias (Turban et al., 2018).

Además, los SI permiten la simulación de escenarios, la elaboración de informes automatizados y el análisis comparativo entre unidades administrativas. Además el uso de la Inteligencia Artificial (IA) permite que esta toma de decisiones tenga el aval de un sistema revolucionario que es capaz de "ver" e inferir cuestiones y datos que el ser humano no sería capaz de relacionar, debido a la complejidad y tamaño de los mismos (Davenport and Bean, 2018).

El apoyo a la toma de decisiones es una de las funciones más relevantes de los sistemas de información en la Administración Pública. Consiste en facilitar a responsables y directivos los datos, indicadores y herramientas necesarios para seleccionar la mejor alternativa en un contexto determinado.

En el ámbito público, la toma de decisiones no se limita a criterios económicos o de rentabilidad, como en el sector privado, sino que debe incorporar dimensiones sociales, jurídicas, éticas y políticas. Esto hace que el apoyo que brindan los sistemas de información sea más complejo y multifactorial (Power, 2021). Así, los objetivos que persigue la toma de decisiones en el ámbito público son los siguientes:

- Reducir la incertidumbre en situaciones con múltiples variables.
- Optimizar recursos públicos (humanos, económicos y técnicos).
- Asegurar la legalidad de las decisiones.
- Favorecer la transparencia y rendición de cuentas ante la ciudadanía.
- Alinear las decisiones con las políticas y planes estratégicos de la Administración.

Beneficios del uso de sistemas de información en la toma de decisiones

En la Tabla 1.1 se pueden observar los beneficios que nos otorga el uso de los SI a la hora de tomar decisiones. Se pueden ver como un complemento de ayuda a una persona o grupo que deban decidir cualquier cuestión sencilla o compleja.

Beneficio	**Descripción**	**Ejemplo**
Rapidez	Acceso inmediato a datos procesados.	Informe instantáneo sobre disponibilidad de personal.
Mayor precisión	Uso de datos actualizados y fiables.	Estadísticas de uso real de un servicio.
Simulación de escenarios	Comparación de alternativas sin riesgo real.	Probar virtualmente la reorganización de líneas de autobús.
Transparencia y trazabilidad	Registro de datos y decisiones.	Publicar los criterios de adjudicación de contratos.
Optimización de recursos	Uso más eficiente del presupuesto público.	Reducir gastos energéticos mediante sensores IoT.

Tabla 1.1: Beneficios del uso de sistemas de información en la toma de decisiones

Limitaciones y precauciones

Como en cualquier cuestión es importante tener presente no solo parte beneficiosa, sino también el apartado de las limitaciones y posibles precauciones que debemos tomar para no incurrir en gastos, problemas o incoherencias innecesarias. En la Figura 1.2 se puede observar un flujo típico que se suele emplear a la hora de tomar decisiones dentro de la Administración Pública (OECD, 2020). A continuación, se definen las posibles limitaciones que nos podemos encontrar, así como las precauciones que debemos tener en cuenta:

- **Dependencia de la calidad de los datos:** decisiones basadas en datos incompletos o erróneos pueden ser inadecuadas.
- **Sesgos algorítmicos:** modelos predictivos pueden perpetuar desigualdades si se entrenan con datos históricos sesgados.
- **Resistencia al cambio:** el personal puede mostrar reticencias a sustituir procesos manuales.
- **Costes de implantación y mantenimiento:** algunos sistemas requieren inversiones considerables.

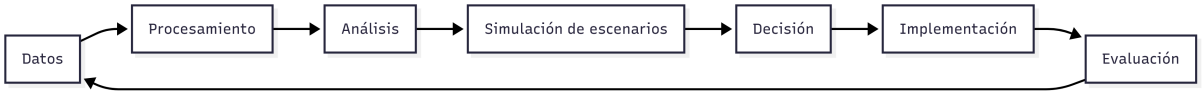

Figura 1.2: Diagrama de flujo para el apoyo a decisiones en la Administración Pública

1.2.2. Mejora de la eficiencia administrativa

Los SI permiten:

- Reducir tiempos de tramitación.
- Eliminar redundancias de datos.
- Minimizar errores humanos.
- Facilitar el seguimiento de expedientes.

Ejemplo práctico: implementación de un sistema de gestión electrónica de expedientes que sustituye los archivos en papel y permite el acceso en línea

Ayuntamiento medio en España. El Ayuntamiento de VillaNueva, con una población de 60.000 habitantes, decide en 2023 implementar un SGEE para modernizar su gestión administrativa. El sistema afecta inicialmente a tres áreas clave:

- Urbanismo
- Recursos Humanos
- Servicios Sociales

A continuación se muestran las fases del proyecto:

- Diagnóstico inicial
  - Evaluación del volumen y tipo de expedientes tramitados.
  - Identificación de flujos documentales críticos.
  - Análisis del grado de madurez digital del personal.
- Selección de la plataforma tecnológica.
  - El Ayuntamiento opta por una solución basada en software libre interoperable con el Sistemas de Interconexión de Registros (SIR) y con compatibilidad con la plataforma `@firma` y `Cl@ve`.
  - Integración con la sede electrónica existente.
- Digitalización y carga de expedientes
  - Los expedientes en papel activos se escanean e indexan.
  - Se definen metadatos según el Esquema Nacional de Interoperabilidad (ENI).
- Formación del personal
  - Se imparten talleres prácticos sobre el uso del nuevo sistema.
  - Se entrega un manual digital de usuario.
- Despliegue y seguimiento
  - La implantación se realiza por fases.

- Se habilita una mesa de soporte técnico interno.

Otros aspectos que se relacionan a continuación con el ejemplo de proyecto son los siguientes:

- Ventajas obtenidas
  - Reducción del 60 % en el tiempo de tramitación de licencias urbanísticas.
  - Ahorro anual de 4.000 € en papel, carpetas y almacenamiento físico.
  - Posibilidad de seguimiento online por parte de la ciudadanía.
  - Mayor control sobre los plazos legales.
- Cumplimiento legal. El sistema implementado respeta los principios de:
  - Integridad documental (mediante firmas electrónicas),
  - Accesibilidad universal (adaptado a la (Ley 11/2007. y la Ley 39/2015.
  - Seguridad (conforme al Esquema Nacional de Seguridad),
  - Archivo electrónico conforme a la Norma Técnica de Interoperabilidad de Política de Gestión de Documentos Electrónicos.

En la Figura 1.3 se puede comprobar el flujo de gestión de un expediente electrónico, de manera tradicional.

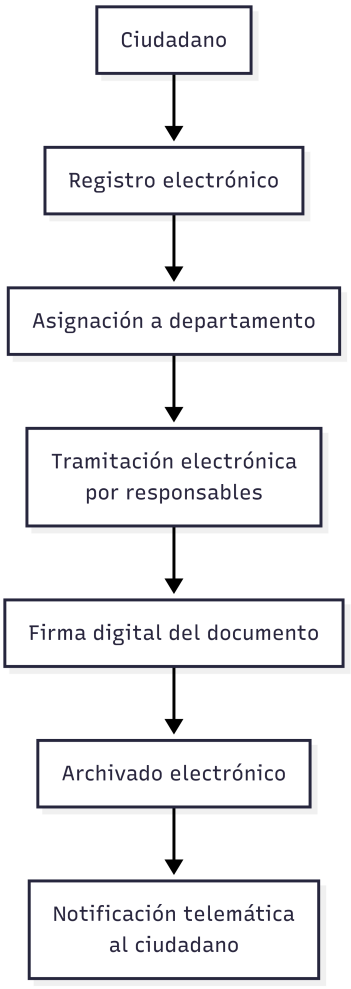

Figura 1.3: Diagrama de flujo de gestión de un expediente electrónico

1.2.3. Transparencia y rendición de cuentas

La transparencia y la rendición de cuentas constituyen dos pilares fundamentales de la gestión pública moderna. En un contexto de transformación digital y creciente exigencia ciudadana, estos conceptos han pasado de ser principios abstractos a convertirse en obligaciones operativas respaldadas por normativas nacionales e internacionales.

Mediante portales de transparencia y sistemas de datos abiertos, los ciudadanos pueden consultar información relativa a presupuestos, contratación pública o estadísticas. Esto contribuye a:

- Aumentar la confianza ciudadana.
- Prevenir la corrupción.
- Impulsar la participación ciudadana.

Definición y alcance

A continuación se muestran las definiciones y el alcance que deben tener una buena transparencia y rendicion de cuentas en la Administración Pública. En la Figura 1.4 se puede observar el diagrama de flujo que deberían tener los datos que se generan en una Administración Pública para que puedan ser lo más transparentes posibles de cada a los ciudadanos.

Transparencia: Implica la disponibilidad y accesibilidad de la información pública de manera proactiva, clara y comprensible, sin barreras técnicas ni jurídicas innecesarias. No se limita a publicar datos, sino que busca que estos sean relevantes, actualizados, reutilizables y verificables.

Rendición de cuentas (*accountability*): Es el proceso mediante el cual las instituciones públicas informan, justifican y asumen la responsabilidad por sus decisiones, acciones y uso de recursos ante la ciudadanía y otros organismos de control.

Marco normativo

Para acompañar y asegurar la transparencia de los datos al cidudadano, en nuestro país se cuenta tanto con un marco normativo estatal como internacional. :

- En el ámbito nacional tenemos la (Ley 19/2013, de transparencia, acceso a la información pública y buen gobierno establece las obligaciones básicas de las administraciones para garantizar el derecho de acceso a la información.
- En el ámbito internacional, destacan:
  - La (Directiva (UE) 2019/1024, sobre datos abiertos y reutilización de la información del sector público.
  - Iniciativa de Gobierno Abierto, con su acrónimo en inglés *Open Government Partnership* (OGP), que promueve políticas de apertura y participación (OCDE, 2017).

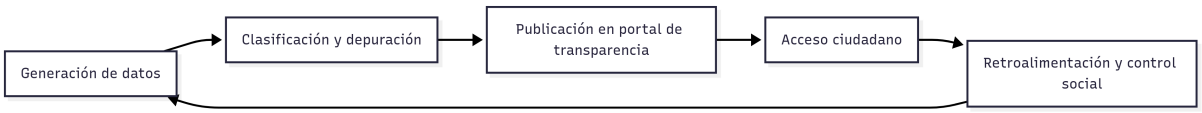

Figura 1.4: Diagrama de flujo de la transparencia de datos en una Administración Pública

1.3. Gestión de la información en el contexto público

En el ámbito de la Administración Pública, la gestión de la información constituye un pilar fundamental para garantizar la eficacia, eficiencia y transparencia en la prestación de servicios a la ciudadanía.

Se trata de un proceso estratégico que abarca la captura, organización, almacenamiento, análisis, difusión y preservación de datos e informaciones relevantes para la toma de decisiones y la ejecución de políticas públicas (OCDE, 2019).

A diferencia del sector privado, donde la información se orienta principalmente a objetivos de rentabilidad y competitividad, en el contexto público su valor radica en respaldar el interés general, promover la rendición de cuentas y asegurar el acceso equitativo a los recursos informativos.

La transformación digital de las administraciones, impulsada por las tecnologías de la información y la comunicación (TIC), ha multiplicado la capacidad de generar y procesar datos, pero también ha planteado retos en materia de interoperabilidad, seguridad, privacidad y reutilización de la información, haciendo imprescindible un enfoque integral de gestión que combine normativa, buenas prácticas y soluciones tecnológicas.

1.3.1. Ciclo de vida de la información

El ciclo de vida de la información describe las distintas fases por las que transitan los datos y documentos dentro de una organización, desde su creación o captura hasta su disposición final.

En el contexto de la Administración Pública, este ciclo adquiere especial relevancia, dado que la información es un recurso estratégico que debe gestionarse conforme a principios de legalidad, eficiencia, seguridad y transparencia.

La correcta administración de este ciclo permite garantizar que la información esté disponible, íntegra, accesible y protegida en todo momento, reduciendo riesgos y facilitando la rendición de cuentas.

La información en las instituciones públicas sigue un ciclo que incluye diversas fases, que puede observarse de forma gráfica en la Figura 1.5. Su adecuada gestión implica establecer políticas claras para cada etapa.

Diversos modelos teóricos proponen variantes en el número de fases, pero en el ámbito de la gestión documental y la gobernanza de datos en el sector público suelen identificarse las siguientes etapas (ISO, 2016).

En la Tabla 1.2 se ofrece una comparativa de los objetivos y riesgos que se pueden encontrar en las fases del ciclo de vida de la información dentro de la Administración Pública:

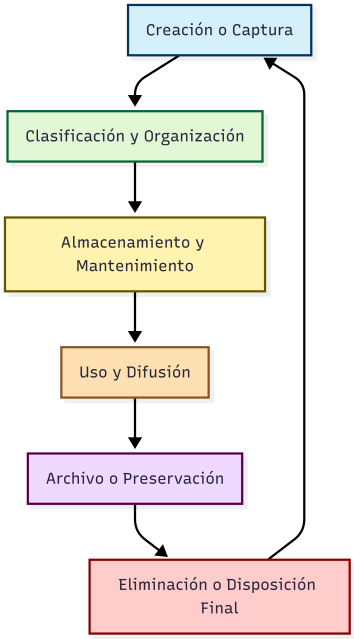

Figura 1.5: Ciclo de vida de la información en la Administración Pública

1. **Creación o captura**
   - Incluye la generación de nueva información o la incorporación de datos externos a los sistemas de la organización. Puede originarse a partir de documentos en papel digitalizados, formularios electrónicos, transacciones en línea, sensores IoT o registros administrativos.
   - Ejemplo: Registro de una solicitud ciudadana en una plataforma de administración electrónica.
2. **Clasificación y organización**
   - Se estructura la información según taxonomías, metadatos o criterios normativos, para facilitar su localización y uso posterior.
   - Ejemplo: Clasificar expedientes por tipo de procedimiento y fecha de entrada.
3. **Almacenamiento y mantenimiento**
   - Conservación en soportes físicos o digitales, asegurando su disponibilidad y protección contra pérdida o deterioro. Incluye la gestión de respaldos, migraciones de formato y control de acceso.
   - Ejemplo: Almacenar documentos en un gestor documental con copia en la nube cifrada.
4. **Uso y difusión**
   - Consiste en el acceso, consulta, análisis y reutilización de la información para la toma de decisiones, prestación de servicios o cumplimiento de obligaciones de transparencia.
   - Ejemplo: Publicar estadísticas de uso de un servicio público en el portal de datos abiertos.

5. **Archivo o preservación.**
   - Transferencia de la información de uso frecuente a repositorios de conservación a largo plazo, siguiendo criterios archivísticos y normativos.
   - Ejemplo: Archivar digitalmente expedientes cerrados según el calendario de conservación.
6. **Eliminación o disposición final.**
   - Supone la destrucción segura o la depuración de datos que ya no son necesarios, siempre respetando la legislación vigente sobre protección de datos y archivo histórico.
   - Ejemplo: Eliminar registros de solicitudes caducadas después del periodo legal de conservación.

Fase	**Objetivo**	**Riesgos**
Creación	Recoger información de manera precisa y completa desde su origen.	Errores de captura, duplicación de datos, información incompleta o sesgada.
Clasificación y Organización	Estructurar y categorizar la información para facilitar su búsqueda y recuperación.	Mala categorización, pérdida de contexto, exceso de clasificaciones irrelevantes.
Almacenamiento y Mantenimiento	Garantizar la conservación y accesibilidad segura de la información.	Fallos técnicos, corrupción de datos, obsolescencia tecnológica.
Uso y Difusión	Utilizar y compartir la información para la toma de decisiones o prestación de servicios.	Filtraciones no autorizadas, uso indebido, falta de actualización.
Archivo	Conservar información relevante para referencia histórica o legal.	Degradación del soporte, incompatibilidad de formatos, pérdida de metadatos.
Eliminación	Descartar información que ya no es necesaria cumpliendo normativas.	Eliminación prematura, destrucción incompleta, incumplimiento legal.

Tabla 1.2: Objetivos y riesgos en las fases del ciclo de vida de la información en la Administración Pública

1.3.2. Calidad de la información

La calidad de la información es un aspecto fundamental en la gestión de datos dentro de la Administración Pública, ya que de ella depende la efectividad de los procesos administrativos, la transparencia de la gestión y la confianza de la ciudadanía.

No basta con disponer de grandes volúmenes de información: es imprescindible que esta cumpla con criterios que la hagan útil, fiable y pertinente para los objetivos institucionales (Wang and Strong, 1996). Así, en el contexto público, una información de calidad permite:

- Sustentar decisiones en datos veraces y actualizados.
- Optimizar recursos evitando duplicidades y correcciones posteriores.
- Cumplir con obligaciones legales en materia de transparencia, protección de datos y archivo.
- Fomentar la confianza ciudadana al ofrecer información clara y verificable.

Dimensiones de la calidad de la información

Existen diversos marcos y modelos (por ejemplo, el de la ISO 8000 o el de Wang y Strong, 1996) que identifican atributos clave para medir la calidad de la información. Adaptando estos al ámbito de la Administración Pública, se destacan los siguientes atributos clave, que también se encuentran representados gráficamente en la Figura 1.6:

1. **Exactitud.**
   - La información debe representar correctamente la realidad que describe.
   - Ejemplo: el número de habitantes censados debe coincidir con los datos oficiales del Instituto Nacional de Estadística.
   - Riesgo: errores de digitación o registros desactualizados que induzcan a decisiones erróneas.
2. **Integridad.**
   - La información debe estar completa, sin omitir datos relevantes.
   - Ejemplo: un expediente de licitación debe contener todas las resoluciones, informes y anexos pertinentes.
   - Riesgo: ausencia de documentos clave que afecte la validez del proceso.
3. **Consistencia.**
   - Los datos deben ser coherentes entre distintos sistemas y fuentes.
   - Ejemplo: la dirección postal de un ciudadano debe coincidir en el padrón municipal y en el registro de tributos.
   - Riesgo: inconsistencias que generen duplicación de trámites o errores administrativos.

4. **Actualidad (o Temporalidad).**
   - La información debe estar al día para que las decisiones sean pertinentes.
   - Ejemplo: estadísticas de empleo publicadas mensualmente sin retrasos.
   - Riesgo: decisiones basadas en datos obsoletos.
5. **Accesibilidad.**
   - La información debe poder consultarse cuando y donde se necesite, respetando las restricciones legales.
   - Ejemplo: acceso en línea a expedientes para funcionarios autorizados.
   - Riesgo: retrasos por sistemas caídos o barreras burocráticas innecesarias.
6. **Comprensibilidad.**
   - La información debe presentarse en un formato y lenguaje que facilite su interpretación.
   - Ejemplo: informes de gasto público con gráficos y lenguaje claro.
   - Riesgo: información técnica inaccesible para la ciudadanía no especializada.

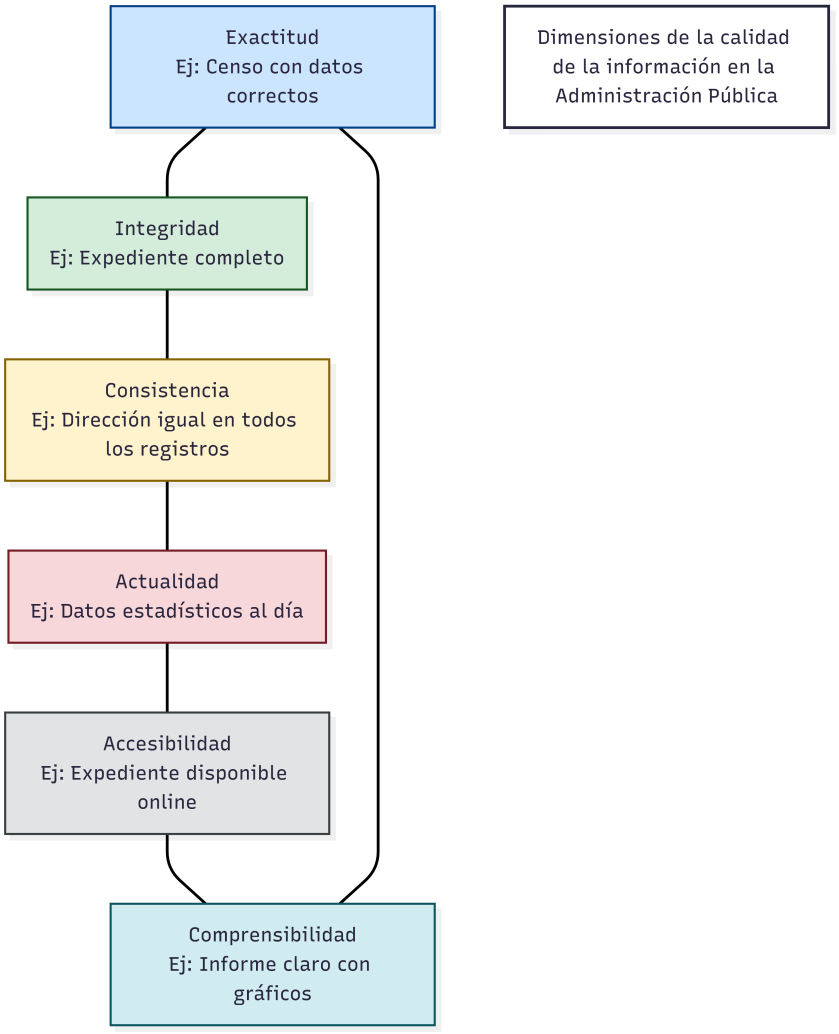

Figura 1.6: Dimensiones de la calidad de la información en la Administración Pública

Evaluación de la calidad de la información

En la Administración Pública, también es muy importante evaluar la calidad. Esto implica tres importantes características a tener en cuenta:

- Definir indicadores para cada dimensión (por ejemplo, porcentaje de registros correctos, tiempo medio de actualización, número de accesos autorizados fallidos).
- Auditar periódicamente las bases de datos y documentos clave.
- Implementar controles automáticos en los sistemas de información para detectar y corregir errores.

Herramientas para asegurar la calidad

Para asegurar la calidad de la información en la Administración Pública se cuenta con una serie de importantes herramientas que nos van a ayudar a monitorizar esa calidad de una forma más exhaustiva:

- **Normas y estándares:** como la ISO 8000 (calidad de los datos) (ISO, 2015) y la ISO 15489 (gestión documental) (ISO, 2016).
- **Sistemas de validación:** reglas que impiden registrar datos incorrectos o incompletos.
- **Capacitación del personal:** para que los responsables de introducir y gestionar datos comprendan la importancia de su labor.
- **Integración de sistemas:** que evite inconsistencias mediante sincronización automática.

Relación con la confianza ciudadana

Una información pública de calidad es esencial para la transparencia y la rendición de cuentas. Los portales de datos abiertos (*Open Data*) y los informes de gestión son útiles únicamente si la información que contienen es fiable y verificable. La falta de calidad puede erosionar la confianza pública y derivar en conflictos, reclamaciones o incluso sanciones legales.

1.3.3. Normativas y marcos regulatorios

A lo largo de este capítulo se ha hecho mención a la legislación a nivel nacional e internacional en materia de Información en relación a la Administración Pública. Aunque existen más leyes en este sentido, no se va a comentar por no estar en el alcance de la asignatura. No obstante, la gestión de la información en la Administración Pública no puede entenderse de forma aislada de su contexto legal. La información que se crea, recibe, almacena y distribuye en el sector público está sujeta a un conjunto de normas, leyes y estándares que determinan cómo debe ser tratada para garantizar su integridad, disponibilidad, confidencialidad y utilidad.

En este sentido, las normativas y marcos regulatorios no solo establecen obligaciones, sino que también proporcionan buenas prácticas y referentes internacionales que ayudan a las instituciones a cumplir con principios como la transparencia, la rendición de cuentas, la eficiencia y la protección de derechos fundamentales.

1.4. Sistemas de información como herramientas de modernización

En el contexto de la Administración Pública, los SI se han consolidado como instrumentos clave para la modernización organizativa y la mejora de los servicios. Más allá de su función tecnológica, constituyen una plataforma estratégica que integra datos, procesos y personas, permitiendo optimizar la toma de decisiones, reducir tiempos de tramitación y facilitar la transparencia.

La implantación de soluciones como los sistemas de gestión documental, plataformas de administración electrónica o portales de datos abiertos no solo incrementa la eficiencia operativa, sino que también fortalece la relación con la ciudadanía, impulsando un modelo de gestión más ágil, participativo y orientado a resultados. En este sentido, el desarrollo y uso adecuado de los sistemas de información representan un pilar fundamental para la transformación digital del sector público.

1.4.1. E-administración

La E-administración (o administración electrónica) hace referencia al uso de las Tecnologías de la Información y las Comunicaciones (TIC) por parte de las Administraciones Públicas para mejorar la prestación de servicios, optimizar la gestión interna y facilitar la interacción con la ciudadanía y las empresas. Su objetivo principal es transformar los procedimientos administrativos tradicionales, basados en el papel y la presencialidad, en procesos digitales, eficientes, accesibles y transparentes (Ramilo Araujo and López Subires, 2017).

Concepto y evolución

La E-administración surge como consecuencia de la creciente digitalización de la sociedad y de la necesidad de que el sector público adopte modelos de gestión más ágiles y orientados al ciudadano. En sus inicios, se centraba en ofrecer información básica en páginas web institucionales (Soriano Díaz and Alonso Ibáñez, 2015).

Con el tiempo, evolucionó hacia la prestación de servicios interactivos, como trámites en línea, solicitudes electrónicas o consultas de expedientes. Actualmente, se encuentra en una fase más avanzada, donde se integran tecnologías como la firma digital, la identidad electrónica, la Automatización de Procesos (RPA) y, en algunos casos, el uso de inteligencia artificial para mejorar la experiencia del usuario y la eficiencia interna.

En este sentido, la E-administración no es únicamente un proyecto tecnológico, sino una política pública de transformación que requiere la implicación de todos los niveles administrativos y el rediseño de procedimientos conforme a la Ley 39/2015 del Procedimiento Administrativo Común y la Ley 40/2015 de Régimen Jurídico del Sector Público. La administración electrónica busca facilitar la relación entre ciudadanos y administración mediante medios digitales.

Reforma digital: más allá de la informatización

La reforma digital supone ir más allá de la simple informatización de tareas. Implica:

- Reingeniería de procesos (Business Process Reengineering), adaptando los procedimientos a un entorno digital.
- Integración de sistemas de información para garantizar la interoperabilidad y la trazabilidad de datos.
- Gestión del cambio organizativo, formando al personal y adaptando las estructuras internas a nuevos flujos de trabajo digitales.
- Ciberseguridad y protección de datos, conforme al Reglamento General de Protección de Datos (RGPD) y la normativa (eIDAS de la Unión Europea (UE).

La reforma digital está estrechamente vinculada a conceptos como la gobernanza digital, la inteligencia de datos y la automatización inteligente, abriendo el camino hacia modelos de Administración 4.0 donde tecnologías como la inteligencia artificial, el *Blockchain* o el análisis masivo de datos (*Big Data*) se integran en la gestión pública.

Beneficios esperados

La implantación de la E-administración dentro de una estrategia de reforma digital aporta beneficios tanto internos (eficiencia, reducción de costes, mejora de la gestión documental) como externos (accesibilidad, transparencia, confianza ciudadana) (Gil-García et al., 2012).

Asimismo, potencia la resiliencia administrativa frente a contingencias como pandemias, desastres naturales o crisis económicas, al permitir la continuidad de los servicios públicos de forma no presencial.

Entre los beneficios visibles más importantes tenemos: tramitación 24/7, menor coste de gestión, reducción de desplazamientos.

Retos y limitaciones

A pesar de sus ventajas y beneficios quue se espera la reforma digital, el uso de tecnología ya implica de por sí una serie de cuestiones a tener en cuenta. Uniendo estas cuestiones a los desafíos actuales, tenemos lo siguiente:

- Brecha digital entre distintos sectores de la población.
- Resistencia al cambio por parte de empleados y estructuras administrativas.
- Necesidad de inversión continua en infraestructura tecnológica.
- Riesgos de ciberseguridad y vulnerabilidad de los sistemas.

1.4.2. Plataformas electrónicas en la Administración Pública

1.4.2.1. Sistema Cl@ve de identificación ciudadana

El Sistema Cl@ve es una plataforma de autenticación e identificación electrónica impulsada por el Gobierno de España, diseñada para centralizar y simplificar el acceso de la ciudadanía a los servicios electrónicos de las administraciones públicas. Su finalidad principal es unificar los métodos de identificación y firma electrónica, evitando que el usuario deba recordar múltiples credenciales para distintos organismos (Gobierno de España, 2025c).

Este sistema forma parte de la infraestructura de la Administración Electrónica española y responde a lo establecido en la Ley 39/2015 del Procedimiento Administrativo Común de las Administraciones Públicas, que reconoce el derecho de las personas a relacionarse electrónicamente con las Administraciones Públicas, así como a identificarse y firmar de manera digital en sus trámites (Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática, 2010b).

Objetivos del sistema

El Sistema Cl@ve busca como objetivos los siguientes:

- **Unificación de credenciales:** permitir que un único usuario y contraseña sirvan para múltiples servicios públicos.
- **Simplificación del acceso:** reducir la complejidad técnica para usuarios no expertos en certificados digitales.
- Seguridad y fiabilidad: garantizar la autenticidad del usuario y la integridad de las transacciones electrónicas.
- **Adaptabilidad multicanal:** ofrecer opciones de uso tanto desde ordenadores como desde dispositivos móviles.

Modalidades de identificación

El sistema ofrece varias formas de autenticación adaptadas a diferentes niveles de seguridad:

- **Cl@ve PIN:** Identificación temporal basada en un código enviado al dispositivo móvil del usuario. Está pensada para accesos puntuales y de corta duración.
- **Cl@ve Permanente:** Basada en usuario y contraseña fijos, reforzada con un Código de un Solo Uso (OTP) para mayor seguridad. Orientada a usuarios frecuentes.
- **Certificado digital/DNIe:** El sistema Cl@ve admite también el uso de certificados electrónicos y el Documento Nacional de Identidad electrónico para usuarios que requieran el máximo nivel de seguridad.

Integración con otros servicios

Cl@ve está integrado con múltiples plataformas y sistemas administrativos, para facilitar los trámites a los ciudadanos y al personal de las diferentes Administraciones Públicas:

- Agencia Tributaria (presentación de impuestos).
- Seguridad Social (consulta de vida laboral, pensiones, trámites).
- Carpeta Ciudadana (seguimiento de expedientes y notificaciones). Se verá en el siguiente epígrafe.
- Tramitadores de servicios autonómicos y locales que se han adherido al sistema.

Ventajas y retos

Ventajas:

- Mejora la experiencia de usuario en la relación con la Administración.
- Refuerza la seguridad frente a accesos no autorizados.
- Reduce la fragmentación de sistemas de identificación.

Retos:

- Persistencia de la brecha digital para colectivos menos familiarizados con la tecnología.
- Necesidad de actualización continua frente a nuevas amenazas de ciberseguridad.
- Coordinación y homogeneización tecnológica entre organismos adheridos.

1.4.2.2. Carpeta Ciudadana

La Carpeta Ciudadana es un servicio electrónico de la Administración General del Estado (AGE) de España que actúa como punto único de acceso para que las personas puedan consultar de forma centralizada la información y los trámites que mantienen con diferentes administraciones públicas. Se trata de una herramienta clave dentro de la estrategia de modernización administrativa y gobierno digital, ya que materializa el principio de "ventanilla única" en el ámbito electrónico (Gobierno de España, 2025a).

Su objetivo principal es facilitar la relación de la ciudadanía con las administraciones, evitando que la persona usuaria deba visitar múltiples sedes electrónicas o recordar en qué organismo inició un trámite. La Carpeta Ciudadana integra información procedente de distintas fuentes administrativas, presentándola de manera unificada y accesible (Gobierno de España, 2021).

Funcionalidades principales

Las funciones principales que nos ofrece la carpeta ciudadana son las siguientes:

- Consultar expedientes en curso: visualizar el estado y el historial de tramitación.
- Acceder a notificaciones electrónicas recibidas a través de la Dirección Electrónica Habilitada Única (DEHú).
- Ver datos personales en poder de la Administración (por ejemplo, padrón, títulos académicos, situación tributaria).

- Acceder a documentación archivada vinculada a trámites anteriores.
- Recibir avisos y alertas personalizadas sobre plazos y novedades de procedimientos en curso.

Integración y alcance

La Carpeta Ciudadana no se limita a los servicios de la Administración General del Estado, sino que está diseñada para interoperar con las administraciones autonómicas y locales que se adhieran a la plataforma, cumpliendo con el ENI. Esto permite que un ciudadano pueda, por ejemplo, consultar en un único espacio un expediente iniciado en un ayuntamiento y otro tramitado por un ministerio, sin necesidad de entrar en portales distintos.

Acceso y seguridad

El acceso a la Carpeta Ciudadana requiere identificación electrónica que asegure que quien accede a un perfil es exactamente la persona titular del mismo. Esta identificación se consigue mediante:

- Sistema Cl@ve (PIN, Permanente, certificado digital o DNI electrónico).
- Conexión cifrada bajo protocolo HTTPS y cumplimiento del ENS.

Beneficios para la gestión pública

Desde la perspectiva administrativa, la Carpeta Ciudadana aporta los siguientes beneficios:

- Reduce la carga de atención presencial, disminuyendo tiempos y costes.
- Aumenta la transparencia, ya que permite al ciudadano monitorizar el avance de sus trámites.
- Fomenta la confianza en la Administración, al ofrecer un servicio unificado y claro.
- Evita duplicidad de gestiones, pues el ciudadano puede aportar documentación digital ya en poder de otra administración.

1.4.2.3. Sede Electrónica de la Seguridad Social

La Sede Electrónica de la Seguridad Social (SEDESS) es la plataforma oficial que la Tesorería General de la Seguridad Social (TGSS) y el Instituto Nacional de la Seguridad Social (INSS) ponen a disposición de la ciudadanía, empresas y profesionales para realizar gestiones, consultas y trámites de forma electrónica, con plena validez jurídica y sin necesidad de desplazarse a una oficina física.

Esta herramienta se enmarca dentro de las políticas de administración electrónica y modernización de los servicios públicos, y responde al derecho de las personas a relacionarse electrónicamente con las administraciones.

Objetivos de la SEDESS

Los objetivos que pretende conseguir la SEDESS son los siguientes:

- Facilitar el acceso a los servicios de la Seguridad Social durante las 24 horas del día, los 365 días del año.
- Reducir la carga administrativa en las oficinas físicas, optimizando la gestión de recursos.
- Garantizar la seguridad y la validez jurídica de los trámites electrónicos.
- Centralizar en un único punto todos los servicios disponibles para ciudadanos, empresas y profesionales autorizados.

Principales funcionalidades

La SEDESS ofrece una amplia variedad de servicios, entre ellos:

- Consulta y descarga de la vida laboral y bases de cotización.
- Solicitud y seguimiento de prestaciones (jubilación, incapacidad, maternidad/paternidad, ingreso mínimo vital).
- Afiliación y variaciones de datos en el Régimen Especial de Trabajadores Autónomos (RETA).
- Inscripción y gestión de empresas y trabajadores por cuenta ajena.
- Cita previa y gestión de comunicaciones.
- Recepción y consulta de notificaciones electrónicas mediante la DEHú.

Acceso y métodos de identificación

Para acceder a los servicios de la SEDESS se requiere identificación electrónica mediante:

- Sistema Cl@ve.
- Certificado digital de la FNMT u otros reconocidos.
- Autenticación vía SMS para determinados trámites simplificados.

Ventajas y beneficios

Según el estamento se pueden distinguir diversos beneficios y ventajas. Así:

- Para la ciudadanía:
  - Tramitación rápida y sin desplazamientos.
  - Disponibilidad continua.
  - Transparencia y trazabilidad de los procedimientos.

- Para la administración:
  - Ahorro de costes y optimización de recursos.
  - Reducción de tiempos de gestión.
  - Menor congestión en oficinas presenciales.

1.4.3. Integración interinstitucional. Red SARA

La Red SARA (Sistema de Aplicaciones y Redes para las Administraciones) es una infraestructura de comunicaciones y servicios de interconexión que conecta de forma segura a las distintas administraciones públicas en España: AGE, comunidades autónomas, entidades locales, y, en algunos casos, instituciones europeas (Ministerio para la Transformación Digital y de la Función Pública, 2025).

Su principal finalidad es garantizar la interoperabilidad y el intercambio de información entre organismos públicos, facilitando la tramitación de procedimientos y reduciendo la necesidad de que la ciudadanía aporte documentos que ya están en poder de otras administraciones, en cumplimiento del principio de "solo una vez" (*once-only principle*) establecido en la normativa europea de administración digital (Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática, 2010a).

La Red SARA está gestionada por el Ministerio para la Transformación Digital y de la Función Pública, a través de la Secretaría General de Administración Digital (SGAD). En la Figura 1.7 se observa la red de entidades que están conectadas a la Red SARA.

Objetivos principales

La Red SARA fue creada persiguiendo unos objetivos claros que se muestran a continuación:

- Interoperabilidad técnica y organizativa entre sistemas informáticos de distintas administraciones.
- Seguridad en las comunicaciones, protegiendo la confidencialidad y la integridad de los datos.
- Eficiencia administrativa, reduciendo duplicidades y acelerando el intercambio de información.
- Soporte a servicios electrónicos transversales como notificaciones, registros electrónicos y verificación de datos.

Servicios que soporta

La Red SARA proporciona la infraestructura para múltiples servicios de administración electrónica, entre ellos:

- **Plataforma de Intermediación de Datos:** permite a una administración consultar datos custodiados por otra (por ejemplo, el padrón, la situación tributaria o el título universitario de un ciudadano).
- **El SIR:** permite el envío electrónico de asientos registrales entre administraciones.

- **Notificaciones electrónicas:** soporte para la DEHú.
- **Acceso a servicios europeos:** conexión con la red TESTA-ng[1].

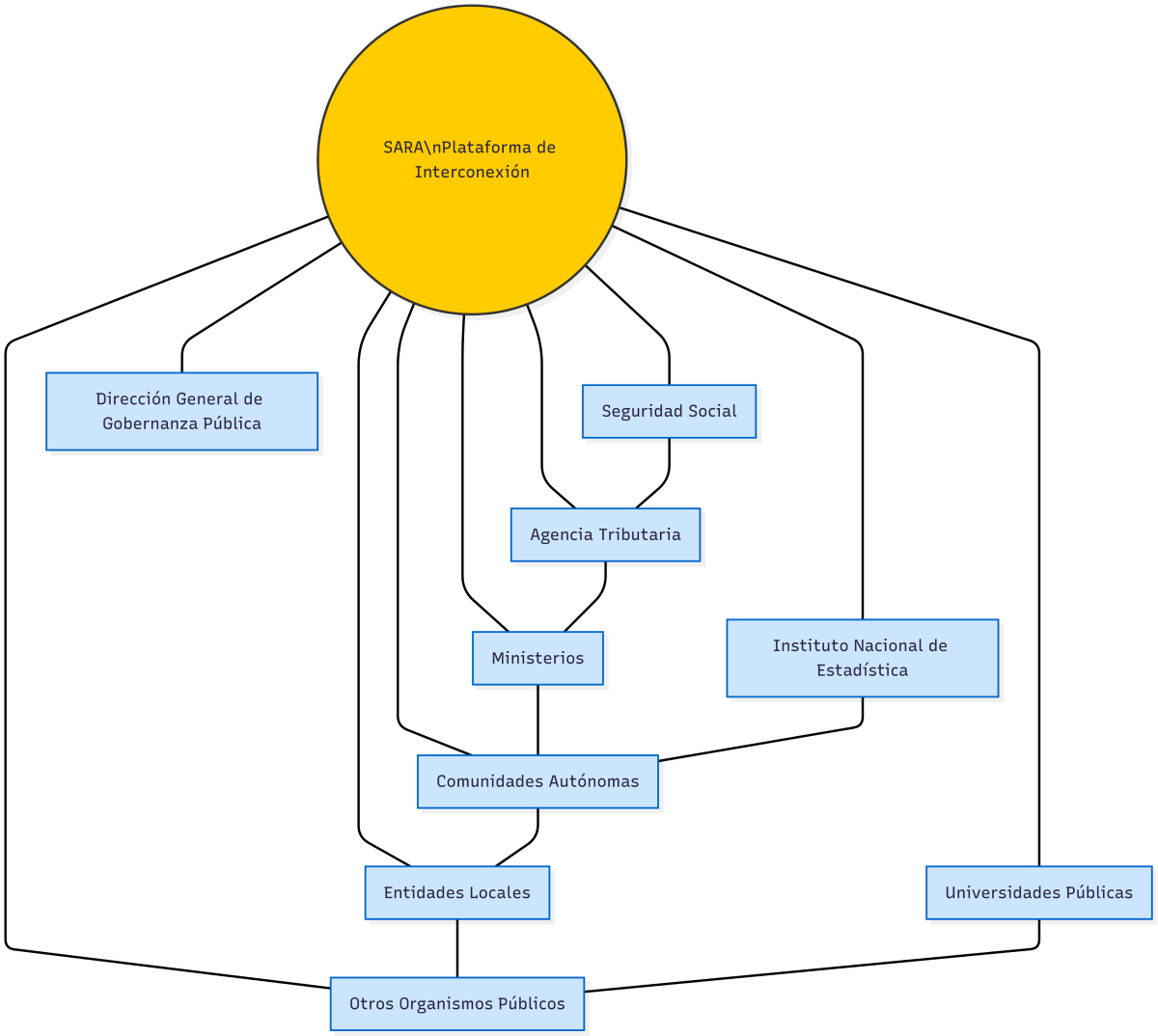

Figura 1.7: Red de entidades conectadas por la plataforma SARA

1.5. Tendencias actuales en la gestión de la información

En el contexto de la Administración Pública, la gestión de la información ha experimentado en la última década una profunda transformación impulsada por el avance tecnológico, la globalización de los datos y la creciente demanda ciudadana de transparencia y eficiencia. Estas tendencias no solo afectan a las herramientas utilizadas, sino también a los procesos, competencias profesionales y marcos normativos que rigen la información pública (Ponjuán Dante, 2013).

[1]red privada gestionada por la Comisión Europea destinada al intercambio seguro de datos entre administraciones de la UE

1.5.1. Digitalización e interoperabilidad

La digitalización integral de procesos administrativos se ha consolidado como la piedra angular de la modernización. Esto incluye la conversión de procedimientos tradicionales en formatos electrónicos y la implantación de sistemas interoperables que permiten el intercambio seguro de información entre distintas administraciones.

La interoperabilidad —favorecida por el ENI garantiza que los sistemas de información, bases de datos y servicios electrónicos puedan comunicarse de manera eficiente, reduciendo duplicidades y tiempos de tramitación.

Ejemplo: el uso de plataformas como Red SARA o la Plataforma de Intermediación de Datos para validar información sin necesidad de que el ciudadano aporte documentos que ya posee la Administración.

1.5.2. Gobierno del dato y datos abiertos

La administración contemporánea adopta políticas de gobierno del dato que establecen normas, estándares y responsabilidades para garantizar la calidad, integridad y disponibilidad de la información (Secretaría de Estado de Digitalización e Inteligencia Artificial, 2025).

La publicación de datos abiertos (*Open Data*) no solo fomenta la transparencia, sino que también impulsa la reutilización de la información por parte de empresas, investigadores y ciudadanos, generando valor económico y social.

Plataformas como `datos.gob.es` centralizan conjuntos de datos públicos en formatos reutilizables y bajo licencias abiertas.

1.5.3. Ciberseguridad y protección de datos personales

El incremento de la tramitación electrónica y el almacenamiento masivo de información exige un reforzamiento constante de las medidas de seguridad, siguiendo el ENS y el RGPD (Chaffey, 2019).

La gestión de la información ya no se concibe únicamente en términos de eficiencia, sino también de confidencialidad, integridad y disponibilidad.

Se promueve la formación del personal en buenas prácticas de seguridad y el uso de tecnologías de autenticación robustas como el Sistema Cl@ve.

1.5.4. Inteligencia artificial y analítica avanzada

Las herramientas de analítica de datos, *machine learning* y procesamiento de lenguaje natural permiten extraer patrones, predecir tendencias y automatizar decisiones administrativas (Delgado García and López Álvarez, 2021).

Aplicaciones: detección de fraude, predicción de demanda de servicios sociales o análisis de sentimiento en redes sociales sobre políticas públicas.

Retos: garantizar que los algoritmos sean transparentes, éticos y auditables.

1.6. Conclusiones

En la era digital, los sistemas de información se han consolidado como un pilar esencial para la modernización de la Administración Pública. La correcta integración de hardware, software, datos, procesos y capital humano no solo incrementa la eficiencia operativa, sino que también potencia la transparencia y la rendición de cuentas ante la ciudadanía.

La e-Administración y las reformas digitales han abierto nuevas oportunidades para repensar los servicios públicos, impulsando la interoperabilidad entre organismos, la simplificación de trámites y la accesibilidad universal. Iniciativas como el Sistema Cl@ve, la Carpeta Ciudadana, la Sede Electrónica de la Seguridad Social y la Red SARA constituyen ejemplos concretos de cómo la tecnología puede facilitar la relación entre ciudadanos y Estado, reduciendo barreras burocráticas y optimizando tiempos de gestión.

Asimismo, las tendencias actuales en gestión de la información —marcadas por la inteligencia artificial, el análisis masivo de datos, la ciberseguridad y la apertura de datos públicos— redefinen el perfil del gestor público, que debe combinar competencias tecnológicas con un conocimiento profundo de la normativa vigente. En este contexto, la formación continua y la adaptación al cambio se convierten en factores críticos para garantizar el éxito de las políticas de transformación digital.

En definitiva, la digitalización administrativa no debe entenderse únicamente como la implantación de nuevas herramientas tecnológicas, sino como una estrategia integral orientada a mejorar la calidad de los servicios públicos, fortalecer la confianza ciudadana y asegurar que la Administración Pública esté preparada para afrontar los retos de un entorno globalizado, interconectado y en constante evolución.

Capítulo 2

Organización de datos y de información. Bases de datos

2.1. Datos, información y conocimiento: distinciones clave

Concepto de dato

En el ámbito de la gestión de la información, un dato se define como una representación simbólica, numérica, alfanumérica o gráfica de un hecho, fenómeno o concepto, carente de significado por sí mismo hasta que se contextualiza. Los datos constituyen la materia prima sobre la que se construyen procesos analíticos y de toma de decisiones (Davenport and Prusak, 1998).

En la administración pública, los datos pueden presentarse en diversas formas: registros de ciudadanos, indicadores económicos, inventarios de bienes públicos o estadísticas de uso de servicios. Estos elementos, aunque relevantes, no aportan valor real hasta que se interpretan en un marco de referencia que les otorgue sentido (de Asuntos Económicos y Transformación Digital, 2023).

Proceso de conversión de datos en información útil

La transición de dato a información implica un proceso de contextualización, organización y análisis (Rowley, 2007). Este proceso, conocido como *data processing*, requiere de (Connolly and Begg, 2014):

- **Recopilación:** obtención de datos relevantes y fiables, a menudo provenientes de sistemas transaccionales, encuestas o registros administrativos.
- **Validación:** verificación de la exactitud y consistencia de los datos.
- **Organización:** clasificación y estructuración para facilitar su interpretación.
- **Interpretación:** análisis que permite identificar patrones, relaciones o tendencias.

En este sentido, la información es dato procesado con un propósito, capaz de responder a preguntas concretas o de apoyar una decisión. En el sector público, un ejemplo sería el análisis de las cifras de desempleo desagregadas por región y sector económico para orientar políticas de empleo.

Valor del conocimiento en la administración pública

Cuando la información se combina con la experiencia, las competencias y el juicio humano, se transforma en conocimiento. Este se entiende como la capacidad de utilizar la información para tomar decisiones eficaces, resolver problemas y generar innovación en la gestión pública. En la Administración, el conocimiento organizativo incluye:

- La experiencia acumulada en la gestión de políticas públicas.
- Procedimientos y buenas prácticas administrativas.
- Redes de colaboración interinstitucional.

El valor del conocimiento reside en su potencial para mejorar la eficiencia, anticipar necesidades ciudadanas y formular políticas más efectivas. En un entorno de cambio constante, la gestión del conocimiento se convierte en un activo estratégico, requiriendo sistemas que lo capturen, almacenen y difundan entre los distintos niveles administrativos (Nonaka and Takeuchi, 1995).

2.2. Modelos de organización de la información

La organización de la información constituye el armazón lógico que permite encontrar, comprender, relacionar y reutilizar contenidos dentro de una organización. En la Administración Pública, elegir y gobernar bien estos modelos tiene impacto directo en la eficiencia administrativa, la interoperabilidad y la transparencia. A continuación se presentan tres enfoques complementarios: los sistemas jerárquicos, la clasificación/codificación/metadatos y las ontologías y taxonomías con orientación aplicada.

2.2.1. Sistemas jerárquicos

Los sistemas jerárquicos estructuran los contenidos en forma de árbol (relaciones padre–hijo), de lo general a lo particular. Son ampliamente utilizados por su simplicidad cognitiva y porque reflejan bien estructuras orgánicas o funcionales. En la Figura 2.1 se puede observar un ejemplo de un diagrama jerárquico representando la clasificación de un expediente administrativo.

Características:

Las características principales de los sistemas jerárquicos son las siguientes:

- **Unidimensionalidad:** un único criterio principal ordena las ramas (por ejemplo, función → proceso → actividad).
- **Herencia de contexto:** la posición en el árbol aporta significado (una hoja "Expedientes de subvenciones" bajo "Políticas de empleo" no significa lo mismo que bajo "Cultura").
- **Control de versiones y estabilidad:** se busca estabilidad terminológica para no romper referencias y enlaces.

Ventajas:

El uso de sistemas jerárquicos en los modelos de organización de la información ofrece al usuario una serie de ventajas que se describen a continuación:

- Facilidad de navegación para personas usuarias.
- Governanza más sencilla (comités reducidos, cambios pautados).
- Buena base para planes de clasificación de documentos y cuadros de clasificación funcional (registros y archivo) en línea con ISO 15489 (International Organization for Standardization, 2016) e ISO 23081 (International Organization for Standardization, 2017).

Limitaciones:

El sistema jerárquico, a pesar de ser un buen sistema para la organización de la información, también presenta una serie de limitaciones:

- Rigidez ante nuevas perspectivas: con este sistema es complicado representar las relaciones múltiples o polijerarquías.
- Riesgo de sobre-especificación: este riesgo aparece cuando se crean árboles demasiado profundos que dificultan la búsqueda.
- No capturan bien relaciones semánticas laterales: equivalencias, asociaciones.

Buenas prácticas:

Aunque el uso del sistema jerárquico es libre, y se podría decir que hasta bastante creativo, hay dos buenas prácticas que si se siguen se pueden evitar problemas y salvar las limitaciones del sistema jerárquico:

- Diseñar jerarquías funcionales (qué hace la organización) más que orgánicas (quién lo hace) para que sobrevivan a reorganizaciones.
- Limitar la profundidad (3–4 niveles) y el ancho de cada nivel.

2.2.2. Clasificación, codificación y metadatos

Esta capa traduce la estructura conceptual en etiquetas manejables por personas y máquinas.

Clasificación

Asigna categorías a recursos (expedientes, *datasets*, trámites). Puede ser enumerativa (listas cerradas) o facetada (combinación de facetas: tema, territorio, tiempo, población, etc.). En el sector público, las clasificaciones facetadas permiten filtrar trámites o conjuntos de datos por ámbito territorial, materia o servicio.

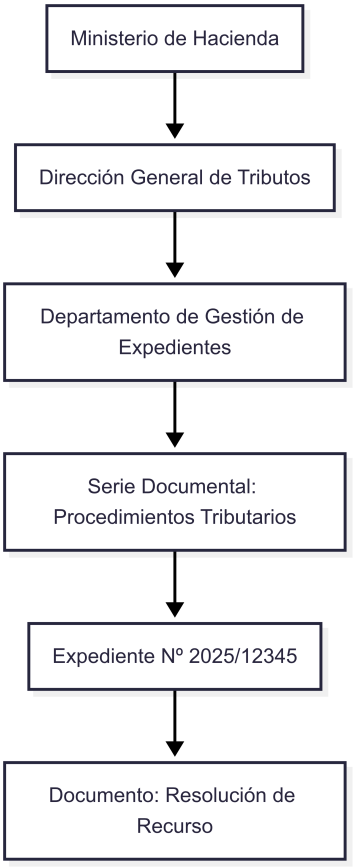

Figura 2.1: Diagrama jerárquico que representa la clasificación de expedientes administrativos

Codificación

Consiste en asociar identificadores persistentes y únicos (códigos) a entidades (p. ej., códigos de procedimiento, de entidad local, de norma). Los códigos:

- Favorecen la trazabilidad y la interoperabilidad.
- Permiten crear tablas de referencia (codelists) reutilizables (p. ej., estados de expediente, tipos de vía).
- Deben ser estables, opacos (no depender de atributos cambiantes) y resolubles mediante URI cuando sea posible.

Metadatos

Son datos sobre los datos. Proveen contexto para descubrir, entender y reutilizar recursos. Tipologías comunes:

- **Descriptivos:** título, resumen, palabras clave: Dublin Core.
- **Administrativos:** creador, fechas, responsable, versión.
- **Técnicos:** formato, tamaño, esquema, software.
- **Derechos:** licencias, restricciones.

- **Estructurales:** (relación entre partes de un objeto complejo).
- **Preservación:** eventos, comprobaciones de integridad: PREMIS[1] (PREMIS Editorial Committee, 2015).

2.2.3. Ontologías y taxonomías aplicadas

Las taxonomías son estructuras jerárquicas de conceptos (p. ej., materias, tipos de trámite). Los tesauros amplían las taxonomías incorporando relaciones semánticas (equivalencia, asociación, jerarquía) y notas de alcance (Group, 2012). Las ontologías modelan dominios con mayor expresividad lógica (clases, propiedades, restricciones) y permiten razonamiento automático. La Figura 2.2 contiene el esquema de capas donde se muestra la evolución de la organización de la información.

Aplicaciones en la Administración Pública

LAs aplicaciones de las ontologías y taxonomías en la Administración Pública pueden ser variadas:

- **Catálogos de procedimientos y ventanillas únicas:** desambiguación, navegación por temas/públicos/vida-eventos.
- **Datos abiertos:** mejora de la descubribilidad[2] mediante etiquetas controladas y enlaces a vocabularios externos (GeoNames, EuroVoc).
- **Búsqueda semántica y recomendación:** expansión de consultas, sugerencia de trámites/*datasets* relacionados.
- **Grafos de conocimiento institucionales:** integración de registros dispersos (organigramas, normativa, contratos, subvenciones) con consultas SPARQL.

2.3. Introducción a las bases de datos

2.3.1. Concepto y finalidad

Una Bases de Datos (BD) es un conjunto organizado de datos almacenados de forma electrónica, diseñado para permitir su acceso, gestión y actualización de manera eficiente. Su propósito fundamental es proporcionar una estructura que facilite la recuperación, modificación y administración de la información, garantizando su integridad, coherencia y disponibilidad (Date, 2004).

En la Administración Pública, las BD permiten gestionar grandes volúmenes de información de manera segura y estructurada, como por ejemplo registros de ciudadanos, expedientes administrativos, inventarios, datos estadísticos y documentación legal.

[1] *Preservation Metadata Implementation Strategies*. Es un estándar internacional de metadatos diseñado para describir la información necesaria para preservar objetos digitales a largo plazo.

[2] En el contexto digital, es la capacidad de un contenido, producto o servicio para ser encontrado por los usuarios de forma fácil y natural, incluso sin que estos lo busquen activamente

Figura 2.2: Esquema de capas donde se muestre la evolución de la organización de la información

En la Figura 2.3 se muestran usuarios, aplicaciones, el Sistema Gestor de Bases de Datos (SGBD) y el almacenamiento.Las finalidades principales de una base de datos se muestran a continuación:

- Centralizar la información para evitar redundancias.
- Garantizar la integridad y exactitud de los datos.
- Permitir el acceso simultáneo de múltiples usuarios.
- Facilitar la búsqueda y generación de informes.
- Proteger la información mediante mecanismos de seguridad.

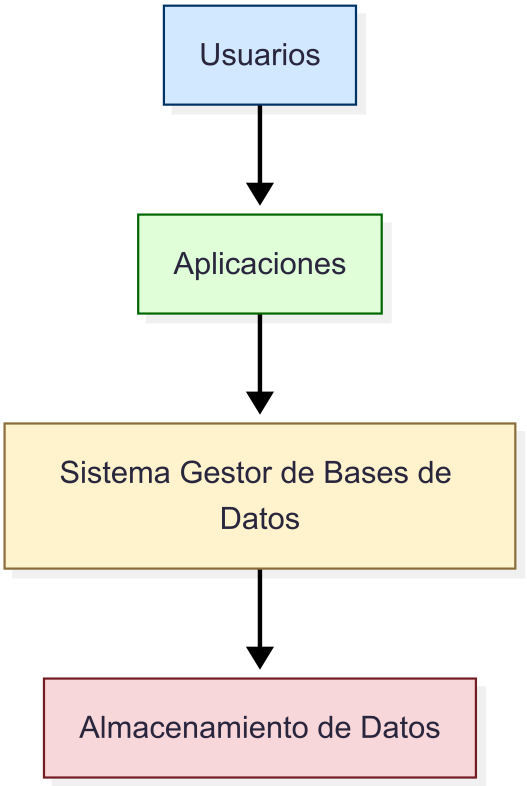

Figura 2.3: Esquema de arquitectura básica de una base de datos

2.3.2. Bases de datos relacionales: tablas, registros, campos, claves

Las Bases de Datos Relacionales (BDR) son el modelo más utilizado en entornos administrativos y empresariales. Organizan los datos en tablas (también llamadas relaciones) compuestas por filas y columnas.

- **Tabla:** conjunto de datos organizados por un tema específico.
- **Registro (o fila):** conjunto de datos relacionados que representan una entidad concreta.
- **Campo (o columna):** atributo específico de la entidad.
- **Clave primaria (*Primary Key*):** campo que identifica de manera única cada registro.
- **Clave foránea (*Foreign Key*):** campo que enlaza registros entre tablas diferentes, permitiendo relaciones.

Ejemplo en administración pública

Una base de datos del Registro Civil puede tener una tabla Ciudadanos con campos como `ID_Ciudadano` (clave primaria), `Nombre`, `Apellidos` y `Fecha_Nacimiento`, y otra tabla Expedientes con un campo `ID_Ciudadano` como clave foránea para vincular el expediente a la persona correspondiente. En la Figura 2.4 se puede ver gráficamente esta estructura en lo que se denomina, diagrama Entidad-Relación.

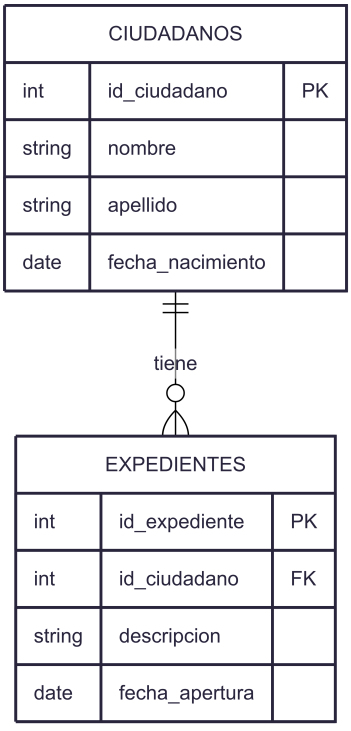

Figura 2.4: Diagrama Entidad-Relación (ER), de una BD con dos tablas relacionadas

2.3.3. Bases de datos no relacionales: características y aplicaciones

Las Bases de Datos No Relacionales (NoSQL) surgieron para manejar grandes volúmenes de datos no estructurados o semiestructurados, que no encajan bien en el modelo de tablas. Ejemplos de tecnologías NoSQL: MongoDB (documentos), Redis (clave-valor), Neo4j (grafos), Cassandra (columnas) (Han et al., 2011). En la Figura 2.5 se puede observar una diferencia visual de la estructura de una BD Relacional y una NoSQL.

Características principales

Las características principales de estas BD son:

- Flexibilidad en el esquema: no requieren una estructura fija de campos.
- Alta escalabilidad y rendimiento en entornos distribuidos.
- Diversos modelos: clave-valor, documentos, grafos y columnas.
- Mejor adaptadas a datos heterogéneos, multimedia o generados en tiempo real.

Aplicaciones

Dentro de la Administración Pública las Bases de Datos NoSQL tienen múltiples aplicaciones. Entre las que destacan:

- Gestión de grandes volúmenes de datos abiertos (*Open Data*).
- Análisis de redes sociales para la comunicación institucional.
- Sistemas de sensores *Internet Of Things* (IOT) o Internet de la Cosas, para gestión urbana (tráfico, medio ambiente).
- Bases de datos documentales para archivar normativas y legislación.

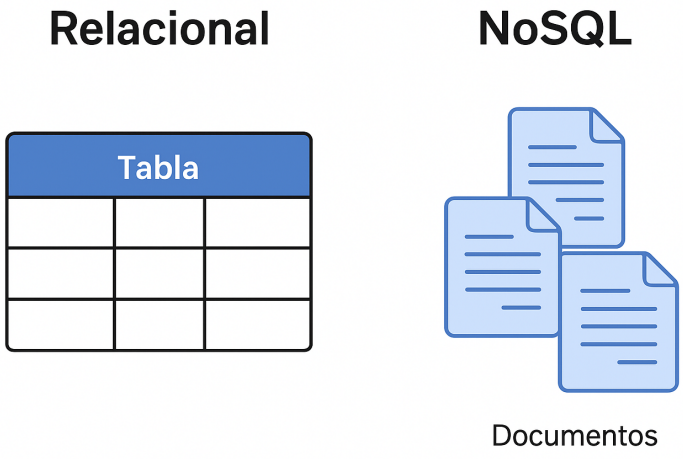

Figura 2.5: Diferencia visual entre las Bases de Datos Relacionales y No Relacionales

2.4. Diseño lógico y físico de bases de datos

El diseño de bases de datos constituye una de las fases más críticas en la gestión de la información, pues determina cómo se almacenan, organizan y recuperan los datos. A grandes rasgos, podemos distinguir dos niveles:

- **Diseño lógico:** se centra en la estructura conceptual de los datos, independiente de su implementación técnica. Aquí se definen entidades, relaciones, atributos y reglas de integridad.
- **Diseño físico:** se ocupa de la implementación concreta en un SGBD, considerando aspectos técnicos como índices, almacenamiento y rendimiento.

Ambos niveles son complementarios: el lógico garantiza la coherencia de la información y el físico asegura eficiencia y accesibilidad.

2.4.1. Modelado entidad-relación (E-R)

El modelo entidad-relación, propuesto por Peter Chen (1976), es una técnica de representación gráfica que facilita el diseño lógico de bases de datos (Chen, 1976). Consta de los siguientes elementos:

- **Entidad:** objeto o concepto del mundo real sobre el que se desea almacenar información (ej.: Ciudadano, Expediente).
- **Atributo:** característica de la entidad (ej.: nombre, DNI, fecha de nacimiento).
- **Relación:** asociación entre entidades (ej.: Ciudadano presenta Expediente).
- **Cardinalidad:** número de instancias de una entidad que pueden asociarse con otra (1:1, 1:N, N:M).

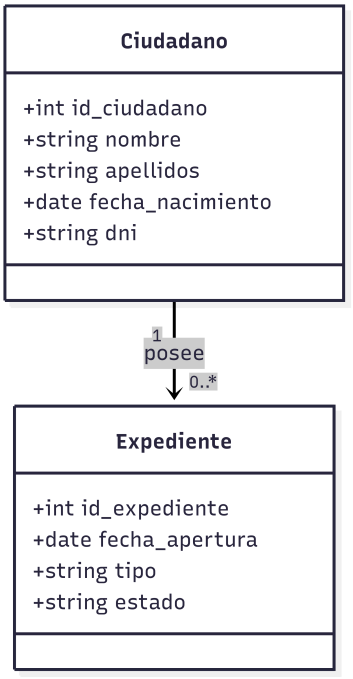

Figura 2.6: Diagrama E-R del ejemplo Ciudadano-Expediente

Ejemplo en Administración Pública, que se puede observar gráficamente en la Figura 2.6:

- **Entidad:** Ciudadano con atributos DNI, Nombre, Dirección.
- **Entidad:** Expediente con atributos Número, Tipo, Fecha.
- **Relación:** Presenta entre Ciudadano y Expediente, de cardinalidad 1:N (un ciudadano puede presentar varios expedientes, y un expediente en concreto solo puede ser presentado por un ciudado).

2.4.2. Niveles de abstracción en bases de datos

Dentro del modelo ANSI/SPARC se especifican tres niveles de abstracción en una BD (Silberschatz et al., 2019):

Nivel Conceptual

Representa la visión global de los datos de la organización, independiente de cómo se almacenan físicamente o de las aplicaciones que los usan. En este nivel se emplea el diagrama E-R para representar la información. En la Figura 2.7 se puede observar un diagrama E-R con tres tablas y dos relaciones.

- Describe qué datos existen y cómo se relacionan.
- Se centra en el significado de la información.
- No incluye detalles técnicos de almacenamiento.

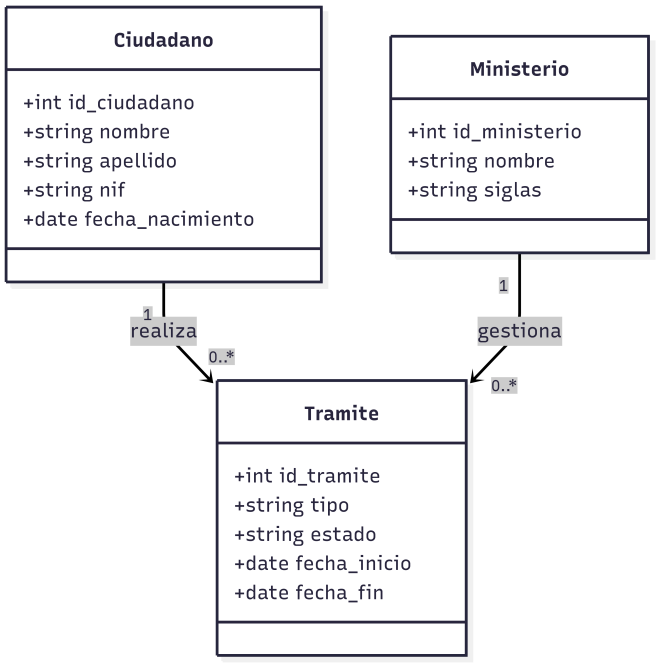

Figura 2.7: Ejemplo diagrama E-R con dos relaciones. Nivel Conceptual

CIUDADANOS		
string	DNI	PK
string	Nombre	
string	Apellido	
date	FechaNacimiento	

Figura 2.8: Ejemplo Tabla. Nivel Lógico

Nivel Lógico

Es la traducción del nivel conceptual al modelo lógico de la base de datos elegida (relacional, documental, grafos, etc.). La información se representa mediante Tablas, junto sus características, como se puede apreciar en la Figura 2.8

- Define tablas, atributos, tipos de datos, claves primarias y foráneas.
- Es dependiente del modelo de datos (ej: relacional → tablas).
- Todavía es independiente del almacenamiento físico.

Nivel Físico

Representa cómo se almacenan realmente los datos en los dispositivos físicos (discos, SSD, clústeres, etc.) junto a sus índices. En la Figura 2.9 se puede observar una tabla, almacenada con un tipo de índice en concreto y replicada en dos servidores por seguridad.

- Incluye índices, particiones, estructuras de almacenamiento, páginas de memoria, clusters, replicación.
- Optimiza el rendimiento y la seguridad.
- Es completamente dependiente del SGBD y del *hardware*.

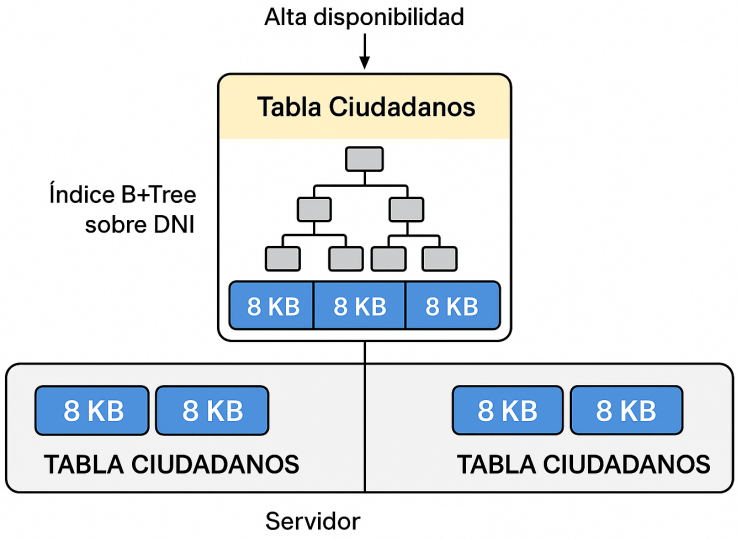

Figura 2.9: Ejemplo esquema. Nivel Físico

2.4.3. Consideraciones técnicas básicas

En el diseño físico, entran en juego los aspectos técnicos de implementación (Elmasri and Navathe, 2017) (de Hacienda Función Pública, 2022):

- **Selección del SGBD**: relacional (PostgreSQL, MySQL, Oracle) o NoSQL (MongoDB, Cassandra).
- **Definición de índices:** estructuras que aceleran la búsqueda (ej.: índice sobre el DNI en la tabla de ciudadanos).
- **Gestión del almacenamiento:** tamaño de las tablas, particionamiento y replicación en sistemas distribuidos.
- **Seguridad y acceso:** definición de roles y permisos (ej.: funcionario puede leer expedientes, pero no modificarlos).
- **Rendimiento:** optimización de consultas SQL, uso de caché y balanceo de cargas.
- **Respaldo y recuperación:** planes de *backup* y *disaster recovery*.

2.5. Herramientas y lenguajes de bases de datos

El trabajo con BD requiere tanto de lenguajes específicos como de herramientas de gestión que faciliten la interacción con la información. En la administración pública, donde el volumen de datos es creciente y las necesidades de interoperabilidad son críticas, resulta esencial comprender, tanto el *Structured Query Language* (SQL) o lenguaje de consulta estandarizado, como las interfaces que permiten gestionar la información de forma accesible (Date, 2003).

2.5.1. Introducción al lenguaje SQL

El SQL es el lenguaje estándar para la gestión de bases de datos relacionales. Fue desarrollado inicialmente por IBM en los años setenta y posteriormente estandarizado por ANSI e ISO (Melton, 2011). Sus principales características son:

- Permite definir estructuras de datos (*Data Definition Language* (DDL)).
- Facilita la manipulación de la información (DML: Data Manipulation Language).
- Ofrece mecanismos de control de acceso y seguridad (DCL: Data Control Language).

Listing 2.1: Ejemplo de creación de una tabla en SQL

```
CREATE TABLE Ciudadanos (
    DNI CHAR(9) PRIMARY KEY,
    Nombre VARCHAR(100),
    Direccion VARCHAR(200),
    FechaNacimiento DATE
);
```

2.5.2. Consultas básicas y filtrado de información

Las consultas SQL permiten extraer información de manera flexible. Algunas de las operaciones más comunes son:

Selección de datos

Listing 2.2: Consulta sencilla. SQL

```
SELECT Nombre, Direccion
FROM Ciudadanos;
```

Filtrado con condiciones

Listing 2.3: Consulta sencilla. SQL

```
SELECT *
FROM Ciudadanos
WHERE Direccion LIKE '%Madrid%';
```

Ordenación

Listing 2.4: Consulta sencilla. SQL

```
SELECT Nombre, FechaNacimiento
FROM Ciudadanos
ORDER BY FechaNacimiento DESC;
```

2.5.3. Interfaz de gestión de bases de datos

Aunque SQL es el lenguaje universal de interacción, muchos usuarios de la administración utilizan interfaces gráficas de gestión que simplifican la manipulación de datos sin necesidad de escribir código. Algunos ejemplos:

- **Microsoft Access:** muy usado en administraciones locales y regionales para aplicaciones de gestión interna (ej.: registros de inventario, listados de personal).
- **LibreOffice Base (The Document Foundation, 2025):** software libre que permite diseñar bases de datos sencillas, crear formularios y realizar consultas gráficas.
- **PostgreSQL pgAdmin (PostgreSQL Global Development Group, 2025):** interfaz gráfica avanzada para uno de los SGBD más potentes y usados en la administración. Permite consultas, monitoreo de rendimiento y administración de usuarios.

Ejemplo en la Administración Pública.

- Un ayuntamiento podría usar LibreOffice Base para gestionar el registro de asociaciones ciudadanas.
- Un ministerio emplearía PostgreSQL con pgAdmin para manejar millones de expedientes administrativos con seguridad y eficiencia.

2.6. Bases de datos en la Administración Pública

La gestión de la información en el sector público requiere infraestructuras sólidas que garanticen la eficiencia, la seguridad jurídica y la interoperabilidad. En este sentido, las bases de datos administrativas se han convertido en pilares esenciales de la administración digital, tanto para el funcionamiento interno como para la relación con la ciudadanía.

2.6.1. Registros administrativos electrónicos

Los registros administrativos electrónicos son sistemas donde se inscriben, clasifican y gestionan actos administrativos, solicitudes, documentos y comunicaciones oficiales en formato digital. A continuación se va a definir la función principal que tiene, un ejemplo que podría aplicarse a la Administración Pública en España y las ventajas que nos ofrece este sistema. En la Figura 2.10 se puede observar gráficamente el recorrido que realiza un escrito dentro de la Administración Pública electrónica.

- **Función principal:** garantizar la validez legal, la trazabilidad y la transparencia de las actuaciones administrativas.
- **Ejemplo en España:** el Registro Electrónico General (REGAGE) (Gobierno de España, 2025b), que permite a los ciudadanos presentar escritos dirigidos a cualquier órgano de la AGE.
- **Ventajas.**
  - Reducción de tiempos en la tramitación.
  - Supresión del papel y ahorro de costes.
  - Garantía de acceso permanente para la ciudadanía.

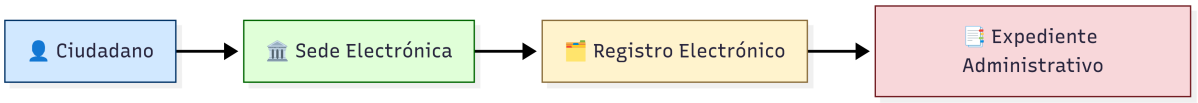

Figura 2.10: Diagrama de interoperabilidad entre BD públicas

2.7. Interoperabilidad entre bases de datos públicas

Uno de los grandes retos de la administración digital es lograr que diferentes bases de datos de organismos públicos puedan comunicarse entre sí de manera segura y eficiente (Cordero, 2018). En España y la Unión Europea, la interoperabilidad se sustenta en varios principios:

- **Técnico:** compatibilidad de formatos, estándares abiertos, servicios web.
- **Semántico:** uso de taxonomías y ontologías comunes (ej.: DIR3 para identificar unidades administrativas).
- **Organizativo:** acuerdos institucionales que permiten compartir información.

Ejemplo detallado de interoperatibilidad

entre BD públicas. Cuando un ciudadano solicita una beca universitaria, la administración puede consultar directamente en la Agencia Tributaria y en la Seguridad Social sus datos económicos y laborales, evitando que tenga que presentar documentos en papel. En la Figura 2.11 se puede ver un diagrama del procedimiento.

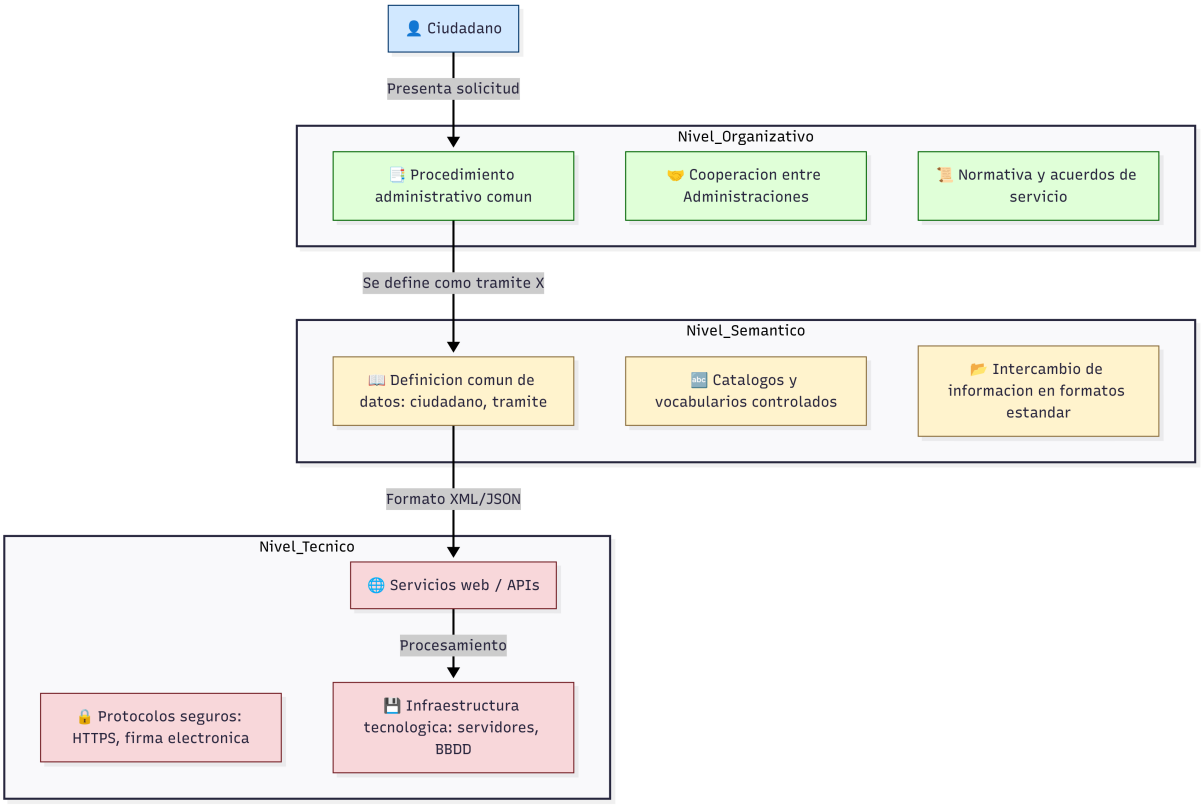

Figura 2.11: Diagrama de principios de interoperabilidad entre BD públicas

2.8. Principales sistemas de bases de datos utilizados en la gestión pública

Existen varias plataformas y sistemas clave que garantizan la organización y el acceso a la información en la AGE y en las comunidades autónomas:

- **Sistema de Información Administrativa (SIA) (Gobierno de España-SIA, 2025):** catálogo oficial de procedimientos y servicios de la Administración General del Estado. Permite localizar, identificar y acceder a los trámites disponibles.
- **Directorio Común de Unidades Orgánicas y Oficinas (DIR3) (Gobierno de España-DIR3, 2025):** clasifica y codifica todas las unidades administrativas, órganos y oficinas de registro, facilitando la interoperabilidad.
- **Oficina de Registro Virtual de Entidades (ORVE) (Gobierno de España-ORVE, 2025):** permite digitalizar documentos presentados en papel en cualquier oficina de registro y remitirlos electrónicamente a su destino.

- **Dirección Electrónica Habilitada Única (DEHú):** como ya se ha visto anteriormente, son BD que centraliza notificaciones administrativas electrónicas dirigidas a ciudadanos y empresas.

En la Tabla 2.1 se muestra una comparativa de los diferentes sistemas que nos encontramos en las Adminsitraciones Públicas de nuestro país.

Sistema	**Finalidad**	**Ejemplo de uso admo.**
Sede Electrónica	Punto de acceso digital para los ciudadanos a los servicios públicos.	Presentación de solicitudes, acceso a notificaciones y consulta de expedientes.
Registro Electrónico	Garantizar la entrada y salida de documentos de manera oficial y segura.	Registro de una instancia general presentada por un ciudadano.
Gestor de Expedientes	Organizar, almacenar y dar seguimiento al ciclo de vida de los expedientes administrativos.	Tramitación de un expediente de licencia urbanística.
Plataforma de Interoperabilidad	Facilitar el intercambio de datos entre diferentes administraciones y organismos.	Consulta de datos de empadronamiento en el Sistema de Verificación de Datos.
Firma Electrónica	Validar la identidad y asegurar la integridad de los documentos electrónicos.	Firma de un contrato administrativo por parte de un funcionario habilitado.

Tabla 2.1: Comparativa de sistemas en la Administración Pública

Capítulo 3

Telecomunicaciones, redes e Internet

3.1. Fundamentos de telecomunicaciones

3.1.1. Concepto de telecomunicación

El término telecomunicación proviene del griego tele (lejos) y del latín *communicare* (compartir) (Stallings, 2007). En un sentido amplio, hace referencia al proceso de transmisión y recepción de información a distancia, mediante medios técnicos. Esta información puede adoptar diferentes formas: voz, datos, texto, imágenes o vídeo.

En la actualidad, las telecomunicaciones son el soporte esencial de la sociedad de la información y de la transformación digital, constituyendo la infraestructura que permite la interconexión global a través de redes fijas, móviles y satelitales, así como de Internet.

Definición académica

La telecomunicación es todo proceso que permite el intercambio de información entre dos o más puntos separados físicamente, valiéndose de señales codificadas transmitidas a través de un medio de propagación y utilizando un conjunto de técnicas, dispositivos y protocolos (Tanenbaum and Wetherall, 2011). En la Tabla 3.1 se puede ver un modelo de comunicación aplicado a la telefonía.

Elemento	**Función principal**	**Ejemplo en telefonía**
Emisor	Generar y enviar la información	Usuario que habla
Mensaje	Contenido de la comunicación	Voz transmitida
Código	Transformación de la información en símbolos/señales	PCM (Pulse Code Modulation)
Canal	Medio de transmisión	Fibra óptica, ondas de radio
Receptor	Recibir y reconstruir el mensaje	Usuario que escucha

Tabla 3.1: Modelo de comunicación aplicado a la telefonía

3.1.2. Elementos básicos de un sistema de telecomunicación

Todo proceso de telecomunicación se puede analizar mediante un modelo general de comunicación, que incluye los siguientes elementos fundamentales (Forouzan, 2012):

- **Emisor:** la entidad (persona, dispositivo o sistema) que origina la información.
- **Mensaje:** la información a transmitir (voz, datos, vídeo, etc.).
- **Código:** el conjunto de reglas y símbolos que permiten representar la información (ejemplo: alfabeto, binario, codificación digital).
- **Canal:** el medio físico o lógico por el cual viaja la señal (cable coaxial, fibra óptica, ondas de radio, Internet).
- **Receptor:** la entidad que recibe la señal y la decodifica para reconstruir el mensaje.

En la Figura 3.1 se puede ver un diagrama que muestra la evolución de las telecomunicaciones hasta nuestros días. Como se puede comprobar de una forma u otra la humanidad siempre ha usado algún tipo de counicación a distancia.

Ejemplo clásico: una llamada telefónica

- Emisor = usuario que habla.
- Mensaje = voz.
- Código = digitalización PCM de la voz.
- Canal = red de telecomunicaciones (cobre, fibra, radio).
- Receptor = usuario que escucha.

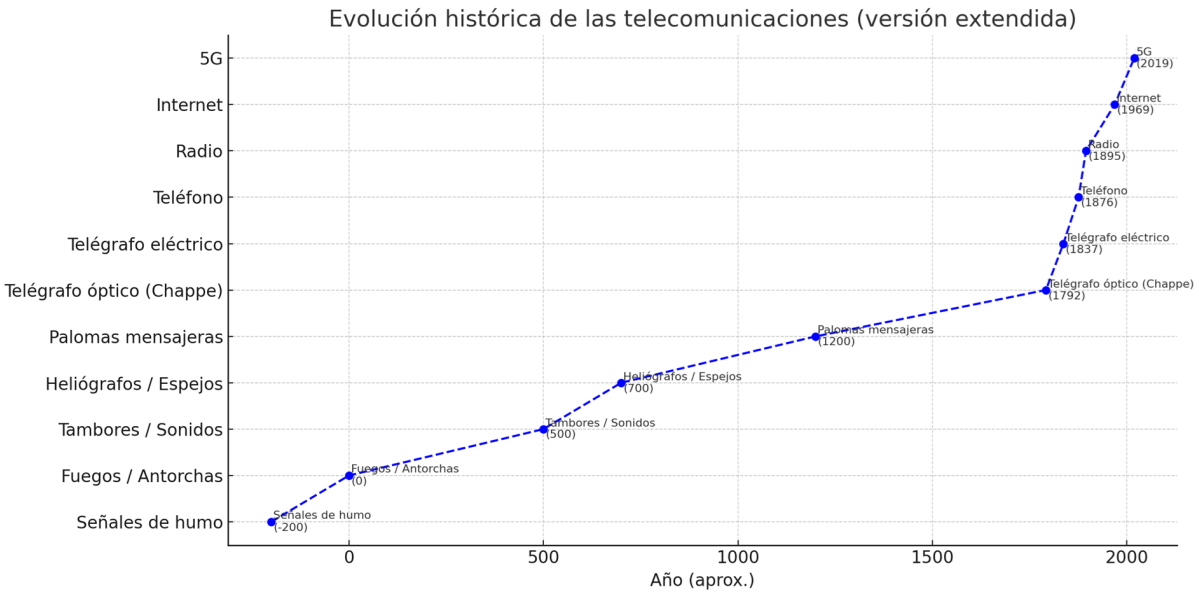

Figura 3.1: Evolución de las telecomunicaciones

Característica	Señal analógica	Señal digital
Representación	Continua	Discreta (bits)
Ejemplo	Onda de voz	Archivo de audio MP3
Ventaja	Menor complejidad técnica	Resistencia al ruido, compresión
Desventaja	Vulnerable al ruido	Necesita conversión (ADC[1]/DAC[2])

Tabla 3.2: Comparación entre señales analógicas y digitales

3.1.3. Tipos de señales y medios de transmisión

La información no se transmite directamente, sino mediante señales, que son representaciones físicas de la información en forma de variaciones de magnitudes (eléctricas, ópticas o electromagnéticas) (Haykin, 2000). En la Tabla 3.2 se muestra una comparativa de las características de cada una de las señales que existen: analógicas y digitales (International Telecommunication Union (ITU), 2020).

Tipos de señales

- **Señales analógicas**: Representan la información de forma continua.
  - **Ejemplo:** una onda de voz en telefonía tradicional.
  - **Ventaja:** simplicidad en la generación y transmisión.
  - **Desventaja:** alta susceptibilidad al ruido y degradación.
- **Señales digitales:** Representan la información mediante valores discretos (bits: 0 y 1).
  - **Ejemplo:** transmisión de datos por Internet.
  - **Ventaja:** robustez frente al ruido, facilidad de almacenamiento y procesamiento.
  - **Desventaja:** necesidad de procesos de conversión (digitalización).

Medios de transmisión

Las señales requieren un medio de propagación. En la Tabla 3.3 se muestra una comparattiva de tales medios. Estos medios de transmisión se clasifican en:

- **Medios guiados (alámbricos).**
  - **Par trenzado:** utilizado en redes telefónicas y Ethernet.
  - **Cable coaxial:** usado en televisión por cable.
  - **Fibra óptica:** gran capacidad de transmisión y baja atenuación.

[1]Analog to Digital Converter → Conversor Analógico a Digital
[2]Digital to Analog Converter → Conversor Digital a Analógico.

- **Medios no guiados (inalámbricos).**
  - **Ondas de radio:** AM/FM, WiFi, telefonía móvil.
  - **Microondas:** enlaces de largo alcance, comunicaciones satelitales.
  - **Infrarrojo y láser:** comunicaciones de corto alcance.

Medio	Tipo	Ventaja principal	Limitación
Par trenzado	Guiado	Bajo coste, fácil instalación	Distancias limitadas
Fibra óptica	Guiado	Alta velocidad, gran capacidad	Costo de instalación
Radiofrecuencia	No guiado	Movilidad, acceso inalámbrico	Interferencias
Satélite	No guiado	Cobertura global	Retardo (latencia)

Tabla 3.3: Comparación de medios de transmisión guiados y no guiados

3.2. Redes de Computadoras

Las redes de computadoras constituyen la base tecnológica que permite la interconexión de sistemas de información y usuarios a escala local y global. Su finalidad es compartir recursos, facilitar la comunicación y garantizar el acceso a datos y servicios, independientemente de la localización física de los equipos.

Desde una perspectiva de gestión pública y empresarial, las redes no solo representan una infraestructura técnica, sino también un recurso estratégico que soporta procesos administrativos, económicos y sociales en la era digital.

3.2.1. Tipos de redes: LAN, MAN, WAN

Las redes se clasifican principalmente en función de su alcance geográfico y propósito. Aunque existen diferentes clasificaciones, las tres categorías más comunes son:

- ***Local Area Network* (LAN) o Red de Área Local.**
  - Cobertura: edificios, oficinas, campus universitarios.
  - Alta velocidad y baja latencia.
  - **Ejemplo:** red interna de una universidad.
  - **Tecnología común:** Ethernet, WiFi.
- ***Metropolitan Area Network* (MAN) o Red de Área Metropolitana.**
  - **Cobertura:** ciudades o áreas metropolitanas.
  - Mayor alcance que una LAN, pero más limitada que una WAN.
  - Usada por universidades, empresas o entidades públicas con varias sedes en una misma ciudad.
  - **Ejemplo:** red metropolitana de transporte que conecta estaciones.

- ***Wide Area Network* (WAN) o Red de Área Extensa.**
  - Cobertura: nacional o internacional.
  - Conecta múltiples LAN y MAN a través de infraestructuras públicas y privadas.
  - **Ejemplo:** Internet.
  - **Tecnologías:** enlaces satelitales, fibra óptica submarina, móviles (4G, 5G).

En la Tabla 3.4 se muestra una comparación de los tres tipos de redes más comunes.

Tipo de red	**Alcance**	**Velocidad típica**	**Ejemplo**
LAN	Local (edificio)	Muy alta (1–10 Gbps)	Red de oficina o campus
MAN	Ciudad/región	Alta (100 Mbps–1 Gbps)	Red de universidades de una ciudad
WAN	Global	Variable (10 Mbps–100 Gbps)	Internet, redes bancarias

Tabla 3.4: Comparación de los tipos de redes: LAN, MAN y WAN

3.2.2. Componentes de las redes

Las redes requieren una serie de componentes físicos y lógicos que hacen posible la transmisión de datos. En la Figura 2.11 se muestra un diagrama estructurado de los componentes que forman las redes. Entre los más relevantes destacan:

- ***Routers.***
  - Dispositivos que interconectan redes diferentes.
  - Determinan la mejor ruta para enviar los paquetes de datos.
  - **Ejemplo:** un router doméstico que conecta la red local a Internet.
- ***Switches* (conmutadores)**
  - Dispositivos que interconectan equipos dentro de una misma red local.
  - Operan a nivel de enlace de datos (Capa 2 del modelo *Open Systems Interconnection* (OSI) o de Interconexión de Sistemas Abiertos[3]).
  - Mejoran el rendimiento al enviar datos solo al destinatario correspondiente.
- **Servidores.**
  - Computadoras dedicadas a proporcionar servicios (correo electrónico, páginas web, bases de datos).
  - Suelen estar optimizados para disponibilidad, capacidad de almacenamiento y redundancia.
  - **Ejemplo:** servidor de aplicaciones en una administración pública.

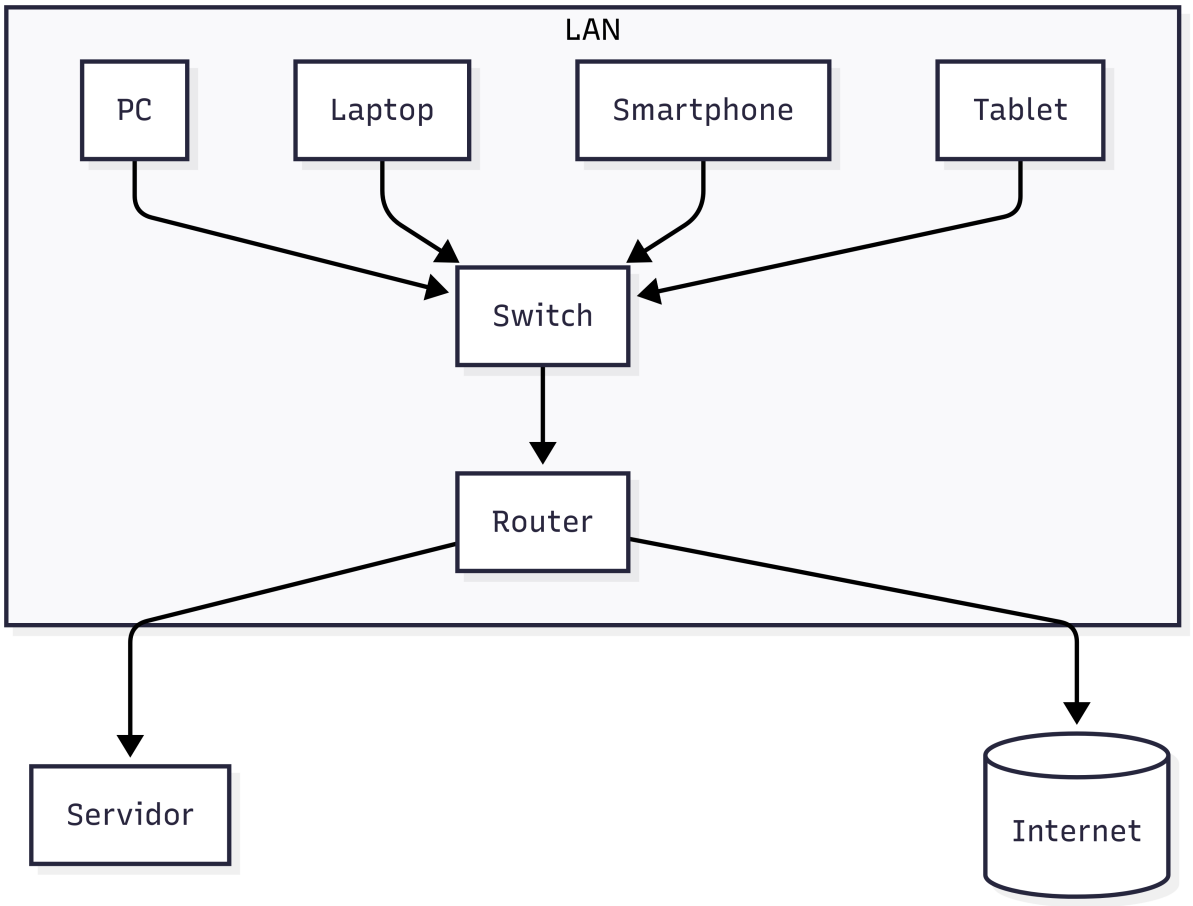

Figura 3.2: Diagrama de redes y sus componentes

3.2.3. Protocolos de comunicación

Una red no solo requiere de *hardware*, sino también de protocolos, es decir, conjuntos de reglas y convenciones que permiten a los dispositivos comunicarse entre sí de forma eficiente y segura (IETF, 2023). En la Tabla 3.5 se pueden observar un resumen de los protocolos de comunicación más importantes junto a su función principal y ejemplos de uso. Así mismo, en la Figura 3.3 se puede observar un esquema de las capas del modelo TCP/IP (Kurose and Ross, 2017).

***Transmission Control Protocol/Internet Protocol* (TCP/IP)**

Conjunto de protocolos que constituye la base de Internet. Posee las siguientes características:

- **IP:** direcciona los paquetes de datos (cada equipo tiene una dirección IP).
- **TCP:** garantiza la entrega correcta y ordenada de los datos.
- Modelo práctico con 4 capas: Aplicación, Transporte, Internet, Acceso.

Protocolo	Función principal	Ejemplo de uso
TCP/IP	Base de Internet, transporte y direccionamiento	Envío de correos, navegación web
HTTP	Transmisión de páginas web	Acceso a un sitio web
FTP	Transferencia de archivos	Subida de documentos a un servidor

Tabla 3.5: Ejemplos de protocolos y sus funciones principales

***Hypertext Transfer Protocol* (HTTP)**

Protocolo de aplicación para la transmisión de páginas web. Su versión segura es HTTPS, que añade cifrado mediante TLS. Permite la comunicación entre navegadores y servidores (W3C, 2023).

***File Transfer Protocol* (FTP)**

Protocolo para la transferencia de archivos entre sistemas, que permite subir y descargar datos en servidores remotos. A menudo reemplazado en entornos seguros por SFTP (*Secure FTP*).

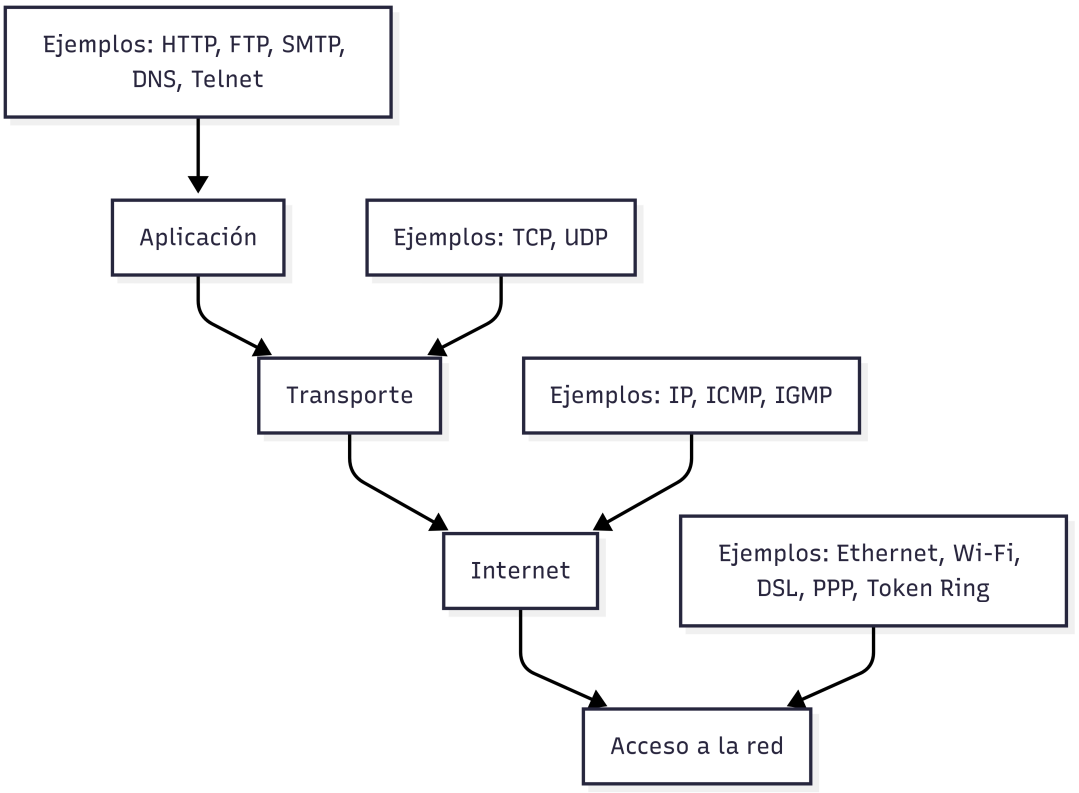

Figura 3.3: Esquema de las capas del modelo TCP/IP

[3]Marco conceptual que divide las comunicaciones de red en siete capas distintas, cada una con funciones específicas

3.3. Internet como infraestructura para la gestión y administración pública

La infraestructura de Internet se ha consolidado como un recurso estratégico para la gestión pública moderna. Permite la digitalización de servicios administrativos, la comunicación con los ciudadanos y la interoperabilidad entre organismos. Comprender su historia, sus servicios y las herramientas de acceso es fundamental para los futuros gestores públicos en la era digital.

Internet ha pasado de ser un instrumento militar y posteriormente académico, a convertirse en una infraestructura crítica para la administración pública, la educación, la economía y la interacción social. En la Figura 3.4 se muestran gráficamente los hitos más importantes relacionados con la aparación e historia de Internet.

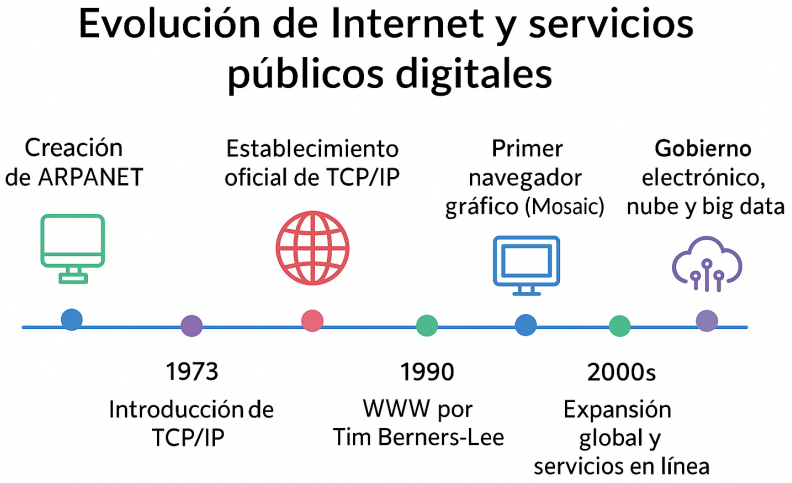

Figura 3.4: Hitos clave de la evolución de Internet

3.3.1. Historia y evolución de Internet

Internet tiene sus orígenes en la ARPANET, desarrollada a finales de los años 60 en Estados Unidos por la Agencia de Proyectos de Investigación Avanzada (ARPA) del Departamento de Defensa. Su objetivo inicial era crear una red resistente a fallos y capaz de interconectar centros militares ante el temor de una invasión de la Unión Soviética, en plena guerra fría.

Posteriormente, su uso fue ampliándose a universidades y centros de investigación. Hasta que el 1 de enero de 1983 nace lo que hoy se conoce como Internet. Una red global que se desligó de la parte militar, para pasar a tener un uso totalmente civil, al alcance de la humanidad. En la Tabla 3.6 se recogen los principales hitos o fechas relevantes sobre Internet.

Año	Hito importante
1969	Creación de ARPANET
1973	Introducción de protocolos TCP/IP
1983	Asentamiento de TCP/IP y nacimiento oficial de Internet
1990	Desarrollo de la World Wide Web por Tim Berners-Lee
1993	Primer navegador gráfico (Mosaic)
2000s	Expansión global y servicios públicos en línea
2010s	Gobierno electrónico, nube y big data

Tabla 3.6: Hitos históricos de Internet

3.3.2. Servicios básicos de Internet

La funcionalidad, acciones o tareas que se pueden hacer en Internet se denominan, servicios. Los servicios de Internet permiten la gestión eficiente de información y la comunicación entre ciudadanos y organismos públicos. Entre los más usados se destacan los siguientes:

- ***World Wide Web* (WWW).**
  - Sistema de documentos interconectados mediante hipervínculos.
  - Accesible mediante navegadores web.
  - Ejemplo en gestión pública: portales de administración electrónica que permiten realizar trámites en línea.
- **Correo electrónico.**
  - Servicio de comunicación digital rápido y económico.
  - Permite el envío y recepción de mensajes, documentos y notificaciones.
  - **Ejemplo:** notificaciones electrónicas de impuestos o citaciones administrativas.
- ***Domain Name System* (DNS) o Sistema de nombres de dominio.**
  - Traduce nombres de dominio legibles por humanos (como www.gob.es) a direcciones IP necesarias para la transmisión de datos.
  - Fundamental para la usabilidad y la localización de recursos en la red.

3.3.3. Navegadores y buscadores

El acceso a Internet se realiza principalmente mediante navegadores web y se optimiza con buscadores, herramientas que permiten localizar información de forma rápida y precisa.

Navegadores

. Las características de los navegadores son las siguientes:

- **Definición:** software que interpreta los contenidos de la web y permite su visualización.
- **Ejemplos:** Chrome, Firefox, Edge.
- **Funciones clave:** renderización de páginas HTML, ejecución de scripts, seguridad en la navegación.

Buscadores

En el caso de los buscadores tenemos las siguientes características breves:

- **Definición:** motores que indexan y recuperan información de la web mediante algoritmos de búsqueda.
- **Ejemplos:** Google, Bing, DuckDuckGo.
- **Función en gestión pública:** facilitar el acceso a normativas, formularios, informes estadísticos y datos abiertos.

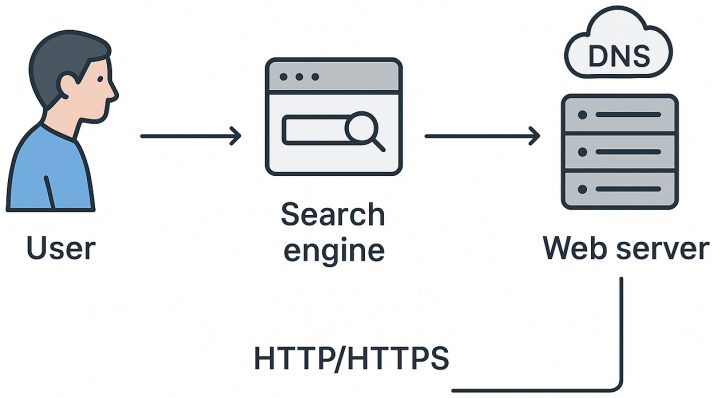

Figura 3.5: Esquema de las capas del modelo TCP/IP

3.4. Administración en red

La transformación digital de las administraciones públicas no se limita a la implantación de sedes electrónicas y registros administrativos. También implica el uso de redes corporativas y servicios en la nube, que permiten nuevas formas de comunicación interna, colaboración y provisión de servicios. En la Figura 3.6 se observa cómo una serie de departamentos compartirían una misma red intranet de la misma corporación.

3.4.1. Intranet institucional

Las intranets institucionales son redes privadas utilizadas dentro de un organismo público (Rosenbaum, 2020). Se diseñan para:

- Compartir información interna (normativas, circulares, comunicados, manuales).
- Facilitar la comunicación entre departamentos y unidades administrativas.
- Ofrecer servicios corporativos como gestión de vacaciones, solicitudes internas, acceso a bases de datos administrativas, etc.
- Ejemplo en la administración española: la intranet de la AGE ofrece acceso a Herramientas de Gestión de Personal (SIGP), recursos de formación y documentación administrativa de uso interno.

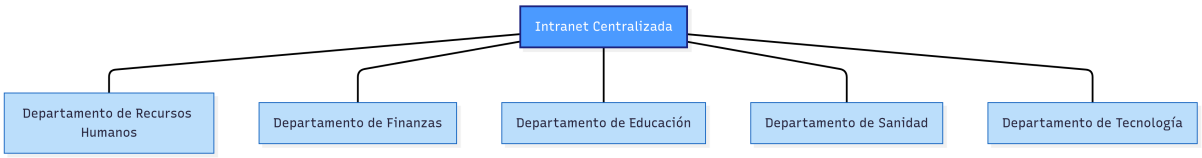

Figura 3.6: Departamentos de un ministerio conectados a una intranet centralizada.

3.4.2. Plataformas colaborativas

Las plataformas colaborativas son espacios digitales diseñados para fomentar el trabajo en equipo y la gestión compartida de proyectos dentro de la Administración Pública (Martínez, 2019). En la Figura 3.7 se pueden encontrar una serie de diferencias entre correo electrónico, intranet y plataformas colaborativas (Meijer, 2018). Dentro de las características principales de plataformas colaborativas encontramos:

- **Gestión documental:** repositorios compartidos con control de versiones.
- **Comunicación síncrona y asíncrona:** chats internos, foros, videoconferencias.
- **Gestión de proyectos:** calendarios, asignación de tareas, seguimiento de hitos.

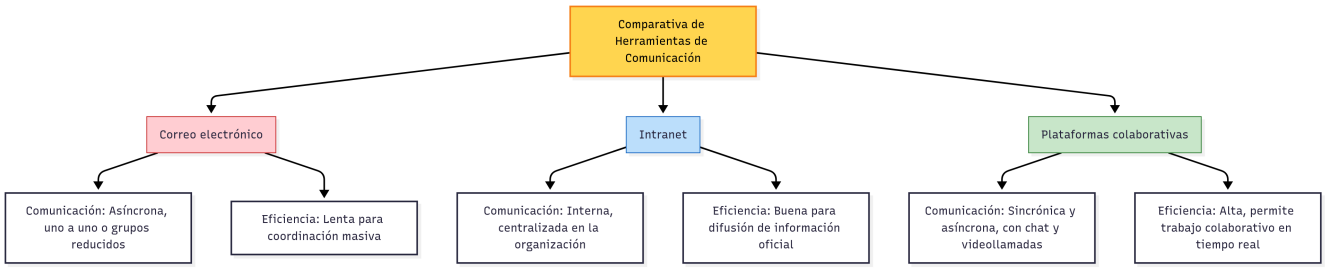

Figura 3.7: Diagrama comparativo entre correo electrónico, intranet y plataformas colaborativas

3.4.3. Computación en la nube

El *cloud computing* (computación en la nube) consiste en el uso de infraestructuras, plataformas y aplicaciones alojadas en servidores externos y accesibles por Internet, bajo demanda (Ministerio de Asuntos Económicos y Transformación Digital, 2024).

Definición

La administración pública puede acceder a servicios en la nube para almacenar, procesar y gestionar datos sin necesidad de infraestructura física propia. En la Tabla 3.7 se ofrece una comparativa de las ventajas y riesgos que debemos tener en cuenta si queremos implementar soluciones de computación en la nube.

Ventajas

Las ventajas que nos ofrece la computación en la nube son las siguientes:

- **Reducción de costes:** menos gasto en servidores y mantenimiento.
- **Escalabilidad:** se adapta a la demanda en tiempo real.
- **Accesibilidad:** disponible desde cualquier ubicación, favoreciendo la movilidad de empleados públicos.
- **Resiliencia:** copias de seguridad y recuperación ante desastres.

Riesgos

A pesar de que la computación en la nube ofrece una serie de ventajas, además muy novedosas, este sistema también presenta una serie de riesgos que hay que tener en cuenta:

- **Seguridad y confidencialidad:** riesgo de accesos no autorizados a datos sensibles.
- **Dependencia de proveedores:** la administración puede quedar sujeta a contratos con empresas privadas.
- **Cumplimiento normativo:** necesidad de garantizar la protección de datos personales según el RGPD y la (Ley Orgánica 3/2018) en España.

Ventajas del *Cloud Computing*	**Riesgos del *Cloud Computing***
Reducción de costes en infraestructura y mantenimiento de sistemas.	Dependencia de proveedores externos para el almacenamiento y procesamiento de datos.
Escalabilidad flexible para adaptarse a la demanda de servicios públicos digitales.	Riesgos de seguridad y privacidad en el manejo de datos sensibles de los ciudadanos.
Acceso remoto a aplicaciones y servicios desde cualquier lugar.	Posible interrupción del servicio por fallos en la nube o ataques cibernéticos.
Facilita la interoperabilidad entre organismos de la administración.	Cumplimiento complejo de normativas legales y protección de datos (ej. RGPD).
Actualizaciones automáticas y acceso a tecnología de vanguardia.	Pérdida de control directo sobre la infraestructura tecnológica.

Tabla 3.7: Ventajas y riesgos del Cloud Computing en la Administración Pública

3.5. Conectividad y brecha digital en la administración pública

La digitalización de la administración pública depende no solo de la modernización de sus sistemas internos, sino también de la capacidad de la ciudadanía para acceder y utilizar los servicios electrónicos en igualdad de condiciones. En este sentido, la brecha digital constituye uno de los mayores retos de la gobernanza electrónica, pues refleja las desigualdades existentes en materia de acceso, uso y competencias digitales (Castells, 2021).

3.5.1. Acceso equitativo a los servicios digitales

La equidad en el acceso a los servicios digitales implica garantizar que todos los ciudadanos, con independencia de su lugar de residencia, nivel económico, edad o capacidades, puedan relacionarse con la administración pública a través de medios electrónicos (Simões and Carvalho, 2020). Los principales factores que condicionan el acceso son:

- **Disponibilidad de conexión a Internet:** la cobertura desigual entre zonas urbanas y rurales genera una brecha geográfica.
- **Dispositivos tecnológicos:** ordenadores, tabletas y smartphones no están igualmente distribuidos entre la población.
- **Competencias digitales:** las habilidades necesarias para manejar certificados digitales, sedes electrónicas o formularios *online* varían según edad y nivel educativo.
- **Ejemplo:** En España, la implantación de la Carpeta Ciudadana ha permitido centralizar servicios digitales, pero su uso se ve limitado en colectivos con baja alfabetización digital o escaso acceso a redes de banda ancha.

3.5.2. Estrategias públicas contra la brecha digital

Para hacer frente a la brecha digital, las administraciones han puesto en marcha diversas políticas de inclusión digital que buscan no solo ampliar el acceso técnico, sino también mejorar las capacidades de uso de los servicios públicos digitales.

Medidas habituales.

Las medidas habituales que se suelen emplear contra la brecha digital se comentan a continuación:

1. **Extensión de infraestructuras de telecomunicaciones.**
   - Programas de despliegue de fibra óptica en la España rural (Plan PEBA-NGA).
   - Impulso de la conectividad 5G a nivel nacional y europeo.
2. Formación en competencias digitales.
   - Cursos y talleres para mayores sobre uso de certificados electrónicos y trámites online.

- Programas de capacitación en centros de acceso público a Internet (telecentros, bibliotecas digitales).

3. Accesibilidad universal.
   - Diseño de sedes electrónicas y aplicaciones bajo criterios de accesibilidad web (WCAG 2.1).
   - Servicios específicos para personas con discapacidad (lectores de pantalla, interfaces simplificadas).
4. **Políticas de apoyo económico.**
   - Subvenciones o ayudas para adquisición de dispositivos.
   - Tarifas sociales de acceso a Internet.

3.5.3. Infraestructuras críticas de red

La provisión de servicios digitales por parte de la administración depende de la existencia de infraestructuras críticas de red robustas y seguras. Estas infraestructuras no solo garantizan la conectividad, sino que también permiten la continuidad de los servicios esenciales en caso de incidentes. Para conseguir este esquema se necesitan algunos elementos clave:

- **Centros de datos gubernamentales:** donde se alojan bases de datos críticas (SIA, DIR3, registros civiles electrónicos, historiales clínicos). (Ver Capítulo 2)
- **Red Sistema de Aplicaciones y Redes para las Administraciones (SARA):** infraestructura troncal que interconecta organismos públicos en España (ver Capítulo 1)
- **Servidores de respaldo y copias de seguridad:** ubicados en diferentes regiones para garantizar la resiliencia ante catástrofes o ciberataques.
- **Protección frente a ciberamenazas:**
  - Sistemas de ciberseguridad gestionados por el CCN-CERT (Centro Criptológico Nacional) (Centro Criptológico Nacional, 2023).
  - Estrategias europeas de ciberresiliencia y protección de datos sensibles.

Capítulo 4

Seguridad y privacidad

4.1. Seguridad de la información en la administración

La seguridad de la información constituye un pilar esencial en el ámbito de la Administración Pública, dado que los organismos gubernamentales gestionan datos sensibles relacionados con ciudadanos, empresas e infraestructuras críticas. Garantizar la protección de esta información no solo es una cuestión técnica, sino también un imperativo legal, ético y social (INCIBE, 2023).

A continuación, se analizan los fundamentos y mecanismos básicos de la seguridad de la información en la administración, organizados en tres apartados: principios, amenazas y herramientas.

4.1.1. Principios básicos de la seguridad y la privacidad

En el ámbito de la seguridad de la información se habla comúnmente de la tríada CID (Confidencialidad, Integridad, Disponibilidad), un marco conceptual que orienta la creación de políticas y medidas de protección (NIST, 2023). En la Figura 4.1 se muestra gráficamente cómo cada principio básico de la seguridad de la información representa un vértice del triángulo.

Confidencialidad

Para la confidencialidad vamos a tener en cuenta lo siguiente:

- **Definición:** asegura que la información solo sea accesible por personas, entidades o sistemas autorizados.
- **Ejemplo en la administración:** garantizar que los datos fiscales de un ciudadano solo estén disponibles para el personal autorizado de la Agencia Tributaria.
- **Mecanismos:** control de accesos, autenticación robusta, cifrado.

Integridad

En el caso de la integridad podemos nombrar una serie de características que la definen:

- **Definición:** implica que la información no pueda ser alterada de manera indebida, accidental o maliciosa.

- **Ejemplo:** evitar que un expediente electrónico sea manipulado sin dejar trazabilidad.
- **Mecanismos:** sumas de verificación, firmas digitales, sistemas de control de versiones.

Disponibilidad

Para la disponibilidad tenemos las siguientes características:

- **Definición:** trata de que la información y los servicios deben estar accesibles cuando se necesiten.
- **Ejemplo:** mantener operativos los portales de trámites electrónicos 24/7 para los ciudadanos.
- **Mecanismos:** redundancia de sistemas, planes de contingencia, centros de respaldo.

Figura 4.1: Triángulo de la seguridad de la información (CIA)

4.1.2. Amenazas comunes

Las administraciones públicas son objetivos frecuentes de ataques cibernéticos debido al valor estratégico de la información que gestionan (Gobierno de España, 2021). En la Tabla 4.1 se puede observar una comparativa de las amenazas más comunes. Entre estas amenazan destacan:

Malware (software malicioso)

Cualquier malware tiene las siguientes características que debemos tener en cuenta:

- **Definición:** programas diseñados para dañar sistemas, robar datos o interrumpir servicios.

- **Tipos:** virus (comportamientos no deseados de los sistemas informáticos), gusanos(ralentizan el sistema), troyanos(los *hackers* pueden tomar el control del sistema), ransomware (encriptan la información.
- **Ejemplo:** ataques de *ransomware* a ayuntamientos europeos que han bloqueado sus sistemas de gestión tributaria.

Phishing

Para esta técnica de engaño vamos a tener en cuenta lo siguiente:

- **Definición:** técnica de ingeniería social que consiste en el envío de correos electrónicos o mensajes fraudulentos que simulan ser de instituciones legítimas.
- Objetivo: engañar al usuario para que revele credenciales o datos bancarios.
- **Ejemplo:** correos falsos en nombre de la Seguridad Social solicitando actualización de datos.

Acceso no autorizado

En este caso vamos a tener en cuenta las siguientes características:

- **Definición:** ocurre cuando personas o sistemas sin los permisos adecuados logran penetrar en redes gubernamentales.
- **Riesgo:** robo de expedientes electrónicos, manipulación de datos o filtraciones masivas.
- **Medidas:** autenticación multifactor, políticas de contraseñas, monitorización continua.

Amenaza	**Descripción breve**	**Ejemplo en la Administración**	**Medida preventiva principal**
Malware	Software malicioso que infecta sistemas	Ransomware en servidores municipales	Antivirus, copias de seguridad
Phishing	Correos o webs fraudulentas	Emails falsos de Seguridad Social	Educación al usuario, filtros
Acceso no autorizado	Intrusión sin permisos en sistemas	Ataques a expedientes judiciales	MFA, monitorización SIEM

Tabla 4.1: Ejemplos de amenazas informáticas y medidas preventivas en la Administración Pública

4.1.3. Herramientas de seguridad

Las organizaciones públicas implementan un conjunto de herramientas técnicas para mitigar riesgos y proteger la infraestructura digital (Stallings, 2018). En la Figura 4.2se muestra un ejemplo gráfico de funcionamiento de las herramientas de seguridad más relevantes. Entre ellas se destacan las siguientes:

Antivirus y *antimalware*.

En cuanto a los antivirus debemos tener en cuenta lo siguiente:

- **Definición:** software destinado a detectar, neutralizar y eliminar programas maliciosos (Anderson, 2020a).
- **Uso en la administración:** proteger estaciones de trabajo de funcionarios y servidores que almacenan expedientes digitales.
- **Ejemplo:** detección temprana de *ransomware* en equipos de gestión documental.

Firewalls (cortafuegos).

Los cortafuegos van a ser muy importantes en el sistema. Vamos a ver sus características:

- Definición: dispositivos o programas que filtran el tráfico de red, permitiendo únicamente las comunicaciones autorizadas.
- **Uso en la administración:** segmentar redes internas, protegiendo sistemas sensibles como los registros civiles frente al acceso desde internet.
- **Tipos:** existen *firewalls* tradicionales (basados en reglas) y de nueva generación (con inspección profunda de paquetes).

Cifrado.

En esta herramienta se van a tener en cuenta las siguientes características:

- **Definición:** técnica que convierte los datos en información ilegible para quien no disponga de la clave adecuada.
- **Uso en la administración:** comunicaciones cifradas entre ciudadanos y portales web (HTTPS), cifrado de bases de datos de padrones municipales.
- **Algoritmos habituales:** AES, RSA.

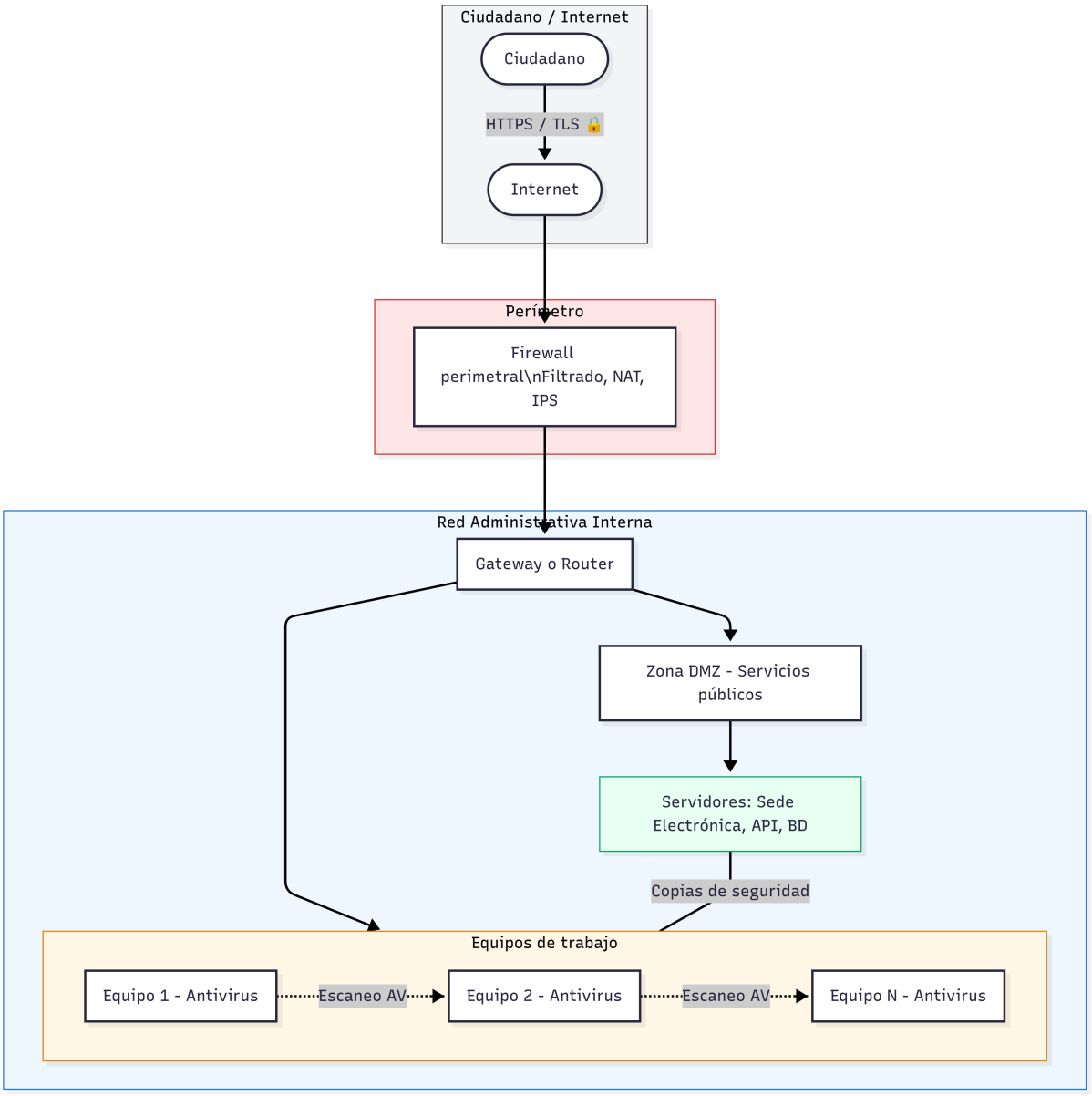

Figura 4.2: Red con firewall en perímetro, antivirus en equipos de trabajo y comunicación cifrada (HTTPS/TLS)

4.2. Marco legal de la seguridad y la protección de datos

La Administración Pública española opera bajo un marco normativo multinivel que integra el Derecho de la UE Unión Europea, la legislación estatal y los estándares de seguridad aplicables al sector público.

Tres piezas resultan esenciales: el RGPD, la (Ley Orgánica 3/2018) o Ley Orgánica de Protección de Datos y Derechos de Garantías Digitales (LOPDGDD), y el ENS. Así, de forma sintética podemos establecer las siguientes diferencias y complementos entre los tres conceptos:

- **RGPD**: fija principios y derechos.
- **LOPDGDD**: los desarrolla y adapta al ordenamiento español —incluyendo los derechos digitales—.
- **ENS**: establece los requisitos técnicos y organizativos mínimos de ciberseguridad para los sistemas del sector público y entidades que los soportan.

4.2.1. Reglamento General de Protección de Datos (RGPD)

Para tratar este reglamento se han realizado una serie de apartados que a continuación se muestran (UE, 2016).

Finalidad y ámbito

El (Reglamento 2016/679(RGPD)) es de aplicación directa en todos los Estados miembros y regula el tratamiento de datos personales por parte de entidades públicas y privadas, con excepciones específicas. En el sector público, el RGPD exige licitud, transparencia, rendición de cuentas y seguridad en todos los tratamientos.

Principios y bases jurídicas

El RGPD articula, entre otros, los principios de licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; integridad y confidencialidad; y responsabilidad proactiva (*accountability*). Las bases jurídicas más habituales en la Administración son el cumplimiento de una misión realizada en interés público o el ejercicio de poderes públicos, además del cumplimiento de obligaciones legales.

Derechos de las personas interesadas

Garantiza los derechos de acceso, rectificación, supresión, limitación, oposición, portabilidad y protección frente a decisiones automatizadas (incluida la elaboración de perfiles), con especial atención a la transparencia y los deberes de información que recaen sobre el responsable del tratamiento.

Gobernanza y cumplimiento

A continuación se muestra un repaso de los artículos más importantes, relacionados con la gestión de la información, dentro del RGPD:

- Responsable/Encargado del tratamiento y contratos con garantías (art. 28).
- Evaluaciones de impacto (EIPD): cuando el tratamiento entrañe alto riesgo (art. 35).
- Delegado/a de Protección de Datos (DPD): obligada su presencia para autoridades u organismos públicos (art. 37.1.a).
- Notificación de brechas de seguridad a la autoridad de control y, en su caso, a los interesados (arts. 33–34).

4.2.2. Ley Orgánica de Protección de Datos y Derechos de Garantías Digitales (LOPDGDD)

A lo largo de esta sección se va a proceder a analizar el contenido de esta importante Ley Orgánica de nuestro país, base de la protección de datos. Para entender mejor ambas regulaciones, en la Tabla 4.2 se exponen las difrencias más notables entre cada una de ellas (de España, 2018).

Rol de la LOPDGDD

La (Ley Orgánica 3/2018) de 5 de diciembre, adapta y complementa el RGPD en España: define particularidades del sector público, regula aspectos concretos (p. ej., tratamientos en el empleo público, videovigilancia), y consagra los derechos digitales en su Título X. Establece, además, la edad mínima de 14 años para el consentimiento en servicios de la sociedad de la información.

Aspectos destacables para la Administración

Los aspectos más destacables de esta Ley, para la Administración Pública son los siguientes:

- Tratamientos con base en interés público y ejercicio de poderes públicos: la ley clarifica condiciones y garantías.
- Designación y funciones del DPD en AAPP: refuerza su papel de interlocución con la AEPD y la ciudadanía.
- Régimen de transparencia y acceso: coordinación con la normativa de transparencia y procedimiento administrativo.
- Derechos digitales (Título X): derecho a la seguridad digital, neutralidad de Internet, acceso universal, educación digital, desconexión digital en el ámbito laboral, entre otros.
- Régimen sancionador con graduación conforme a RGPD.

Guías y apoyo institucional

La Agencia Española de Protección de Datos (AEPD) (Agencia Española de Protección de Datos, 2025) proporciona guías, orientaciones y modelos específicos para Administraciones Públicas (p. ej., EIPD, gestión de brechas, contratos con encargados, canal del DPD), útiles para operacionalizar el cumplimiento.

Materia	RGPD (marco UE)	LOPDGDD (desarrollo España)
Obligación DPD	Autoridades u organismos públicos	Refuerzo del rol y relación con AEPD
Edad de consentimiento	No fija (corresponde a Estados 13–16)	**14 años**
Derechos digitales	No desarrolla catálogo específico	**Título X** (seguridad, educación, desconexión, etc.)
Tratamientos sectoriales	Principios y bases generales	Reglas y matices para empleo público, videovigilancia, etc.

Tabla 4.2: Comparativa entre RGPD y LOPDGDD en la Administración Pública

4.2.3. Esquema Nacional de Seguridad (ENS)

Naturaleza y objetivos

El ENS, ya nombrado y comentado anteriormente, es el marco de referencia de ciberseguridad para el sector público español. Regulamentado actualmente por el Real Decreto 311/2022, fija los principios básicos y requisitos mínimos que deben observar los sistemas que soportan servicios públicos, así como las entidades privadas que los prestan o mantienen. Sustituye y actualiza al (RD 3/2010), incorporando novedades (p. ej., gestión de riesgos actualizada, cadena de suministro, servicios en la nube).

Principios, medidas y conformidad

El (RD 311/2022) que regula actualmente el ENS establece:

- **Principios**, tales como: seguridad como proceso integral; prevención, detección y corrección; reevaluación periódica del riesgo.
- **Requisitos mínimos y medidas** organizativas, operativas y de protección, con adecuación a categorías de seguridad del sistema (Bajo/Medio/Alto).
- **Instrucciones Técnicas de Seguridad (ITS)** de obligado cumplimiento, y guías CCN-STIC[1] (CCN-CERT, 2024) como apoyo a la implantación (p. ej., valoración de sistemas, ámbito de aplicación).
- **Funciones del Centro Criptológico Nacional *Computer Emergency Response Team* (CCN-CERT)** (CCN-CERT, 2025) como órgano de referencia técnica para el sector público.

Como nota didáctica general que englobe a los tres conceptos que se han descrito en esta sección se debe comentar que: la **LOPDGDD/ RGPD** aseguran legalidad y derechos; el **ENS** asegura seguridad técnica y organizativa. Ambos planos se complementan, y deben integrarse en el denominado Sistema de Gestión de Seguridad (SGSI) de la entidad.

[1]Las Series CCN-STIC son normas, instrucciones, guías y recomendaciones desarrolladas por el Centro Criptológico Nacional con el fin de mejorar el grado de ciberseguridad de las organizaciones.

4.3. Gestión de la privacidad en entornos digitales

La gestión de la privacidad en la Administración Pública exige integrar principios jurídicos y controles técnicos en todo el ciclo de vida del dato: desde el diseño del trámite hasta la prestación del servicio y la retención/eliminación de la información (Kuneva et al., 2014). En entornos digitales, esta gestión se apoya en tres grandes pilares: consentimiento informado cuando proceda, garantía efectiva de derechos y medidas proactivas basadas en evaluación de riesgos (Anderson, 2020b).

4.3.1. Consentimiento informado

Concepto y requisitos de validez

El consentimiento es la manifestación de voluntad del ciudadano para el tratamiento de sus datos cuando la Administración no pueda apoyarse en otra base jurídica (p. ej., consentimiento para comunicaciones adicionales, envío de boletines, o tratamientos no necesarios para el procedimiento) (European Data Protection Board, 2020). Para que sea válido debe ser:

- **Libre** (sin coacciones ni condicionamientos indebidos; evitar "empaquetar" consentimientos).
- **Específico** (vinculado a finalidades determinadas, no genéricas).
- **Informado** (el interesado conoce quién trata sus datos, con qué fines, qué derechos tiene y cómo ejercerlos).
- **Inequívoco** (acción afirmativa clara: marcar una casilla, firmar digitalmente, etc.; no valen casillas premarcadas ni silencio).
- **Granular** (una opción por cada finalidad).
- **Verificable** (prueba del consentimiento).
- **Revocable:** con la misma facilidad con la que se otorgó.

Nota sector público: en la mayoría de trámites administrativos, la base jurídica suele ser el cumplimiento de una obligación legal o el interés público/ejercicio de poderes públicos. El consentimiento se reserva para finalidades no necesarias para el procedimiento (Agencia Española de Protección de Datos, 2024). En la Tabla 4.3 se muestra un posible *checklist* para comprobar que se cumplen todos los requisitos de validez de un consentimiento informado, además de posibles evidencias que justifiquen el cumplimiento de cada requisito.

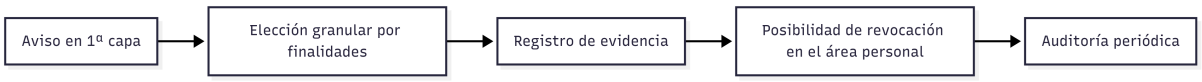

Figura 4.3: Flujo de consentimiento digital

Prácticas recomendadas en sedes y apps públicas

En la Figura 4.3 se puede observar el flujo adecuado que se debe aplicar para un buen consentimiento digital. Las buenas prácticas recomendadas que se deben dar en las diferentes sedes son las siguientes:

- **Capas informativas:** un aviso breve (quién, para qué, derechos, enlace a info ampliada) + política completa accesible.
- **Diseño sin "patrones oscuros":** evitar interfaces que induzcan a aceptar por defecto (p. ej., cookies no esenciales).
- **Gestión de cookies:** separar cookies técnicas (no requieren consentimiento) de analíticas/marketing (requieren consentimiento explícito en entornos públicos).
- **Consentimiento de menores:** reforzar la autenticación/representación cuando proceda; controles parentales en servicios educativos.
- **Registro de evidencias:** sellado temporal del consentimiento, logs y versión del texto mostrado.

Derechos de los ciudadano (ARCO)

Alcance y finalidad

Los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) constituyen el núcleo histórico de la tutela del ciudadano:

- **Acceso:** conocer si se tratan sus datos y obtener copia e información asociada (finalidades, categorías, cesiones, plazos, etc.).
- **Rectificación:** corregir datos inexactos o incompletos.
- **Cancelación/Supresión:** eliminación cuando ya no sean necesarios, el ciudadano retire el consentimiento o exista obligación legal de suprimir.
- **Oposición:** oponerse al tratamiento en determinadas circunstancias (especialmente tratamientos no necesarios para el servicio público concreto).

Criterio	¿Se cumple?	Evidencia/Control
Libre	❑ / ✓	Sin casillas premarcadas, sin bloqueo
Específico	❑ / ✓	Finalidades separadas
Informado	❑ / ✓	1ª capa + política completa
Inequívoco	❑ / ✓	Acción afirmativa, registro de logs
Revocable	❑ / ✓	Botón "retirar" en el área personal

Tabla 4.3: Posible formulario de criterios de validez del consentimiento y sus evidencias de control

Extensión en el marco actual: además de ARCO, el marco vigente reconoce limitación del tratamiento, portabilidad y no ser objeto de decisiones automatizadas. En entornos públicos, la oposición y la supresión pueden estar limitadas por obligaciones legales o por el interés público prevalente, pero el organismo debe motivar y documentar dichas limitaciones.

Gestión operativa en Administraciones Públicas

En una Administación Pública se debe conforme a una serie de principios, que se comentan a continuación:

- **Canales accesibles:** sede electrónica, oficinas de registro, y canal del DPD (Delegado/a de Protección de Datos).
- **Autenticación robusta:** identificación mediante certificados, sistemas clave PIN, o equivalentes para evitar entrega a terceros.
- **Plazos de respuesta:** procedimientos internos que aseguren la respuesta en plazo legal, con posibilidad de ampliación motivada en casos complejos.
- **Trazabilidad:** registro de solicitudes, decisiones, fechas, personas responsables y documentación entregada.
- **Interacción con terceros:** si existen encargados del tratamiento, establecer flujos para recuperar/bloquear/suprimir en sus sistemas.
- **Excepciones motivadas:** cuando prevalezcan obligaciones legales (p. ej., conservación por archivo público o procedimiento judicial).

4.3.2. Evaluaciones de impacto y medidas proactivas

Enfoque de riesgo

La responsabilidad proactiva exige que la organización no solo cumpla, sino que demuestre el cumplimiento. En la práctica, esto se materializa en:

- ***Privacy by design (ENISA, 2015):*** integrar la privacidad desde el inicio del proyecto (p. ej., minimización de datos, seudonimización, partición de finalidades, controles de acceso).

- ***Privacy by default (National Institute of Standards and Technology, 2023):*** la configuración por defecto debe ser la más protectora (p. ej., desactivar por defecto analíticas no esenciales).
- **Inventario de tratamientos:** registro actualizado con finalidades, bases jurídicas, categorías de datos, cesiones, plazos y medidas.
- **Gobernanza:** roles claros (Responsable, Encargado, DPD), políticas, formación y auditorías.

Evaluaciones de Impacto en Protección de Datos (EIPD)

Una EIPD es obligatoria cuando un tratamiento pueda implicar alto riesgo para los derechos y libertades (p. ej., evaluación sistemática y extensa, uso de categorías especiales de datos, observación a gran escala de zonas de acceso público, biometría, perfiles que produzcan efectos jurídicos relevantes, etc.).

Fases típicas de una EIPD.

- **Descripción sistemática del tratamiento:** finalidad, contexto, datos, actores, ciclo de vida.
- **Necesidad y proporcionalidad:** base jurídica, idoneidad y alternativas menos intrusivas.
- **Análisis de riesgos:** identificación de amenazas, probabilidad/impacto, escenarios de abuso o error.
- **Medidas previstas:** técnicas (cifrado, seudonimización, control de accesos, retención) y organizativas (políticas, formación, auditoría).
- **Resultado:** riesgo residual aceptable o consulta previa a la autoridad de control si persiste el alto riesgo.
- **Plan de revisión:** reevaluación periódica o ante cambios sustantivos (nuevas finalidades, nuevas fuentes de datos, IA, etc.).

Riesgo identificado	**Medida proactiva principal**
Acceso indebido a expedientes	MFA[2], segregación de funciones, registro de accesos
Reutilización no autorizada de datos	Catalogación de finalidades, controles contractuales
Exposición en datos abiertos	Anonimización/Seudonimización + revisión manual
Errores en plazos de conservación	Políticas de retención y borrado automatizado
Pérdida de confidencialidad en la nube	Cifrado E2E, claves gestionadas, evaluación de proveedor
Decisiones automatizadas sin garantías	Evaluación algorítmica, revisión humana significativa

Tabla 4.4: Mapa de riesgos y medidas proactivas en protección de datos

Catálogo de medidas proactivas

Dentro de las medidas proactivas, destacamos las siguientes como más necesarias, importantes e ineludibles a implantar en cualquier Administración Pública. Además, en la Tabla 4.4 se puede observar un mapa de riesgos y medidas proactivas que podrían tomarse para paliarlo:

- **Minimización:** recoger solo los datos necesarios para cada finalidad.
- **Seudonimización/Anonimización:** reducir el vínculo directo con el interesado en analítica o publicación de datos abiertos.
- **Retención y borrado:** calendarios de conservación con bloqueo cuando lo exija el archivo público.
- **Transparencia:** panel de privacidad en la sede electrónica con estado de consentimientos, bases jurídicas y derechos.
- **Seguridad:** cifrado en tránsito y reposo; autenticación multifactor para perfiles con acceso a expedientes; registro y correlación de eventos.
- **Evaluación de terceros:** cláusulas y auditorías a encargados y proveedores cloud (transferencias internacionales, subencargados, certificaciones).
- **Formación y cultura:** programas periódicos, simulacros (p. ej., *phishing*), métricas de madurez.

4.4. Políticas de seguridad en la Administración Pública

Las políticas de seguridad constituyen el marco de gobierno que ordena la protección de la información y los servicios públicos digitales. Ya hemos visto que en el sector público, estas políticas deben alinearse con el marco legal (RGPD/LOPDGDD) y normativo-técnico (ENS, normas ISO/IEC, NIST, guías CCN-STIC) (Centro Criptológico Nacional (CCN), 2023), a la vez que se operativizan mediante planes, protocolos, formación y estructuras de responsabilidad como el DPD. Su objetivo último es sostener la continuidad del servicio, la confianza ciudadana y la resiliencia frente a amenazas.

4.4.1. Planes internos de seguridad, protocolos de actuación, formación y la figura del CISO

Planes internos de seguridad (SGSI y planificación)

En una administración moderna, el pilar es unSGSI, ya que este se va a encargar de tomar las siguientes acciones:

- Define el alcance (servicios, unidades, sistemas).

[2]Método de seguridad que requiere dos o más formas diferentes de verificación de identidad para iniciar sesión en una cuenta, aplicación o sistema

- Establece la política marco de seguridad aprobada por la alta dirección (principios, roles, cumplimiento ENS) (European Union Agency for Cybersecurity (ENISA), 2020).

- Despliega políticas y normas específicas (clasificación, control de accesos, copias, cifrado, continuidad, registro y monitorización, desarrollo seguro, cloud, móviles/-teletrabajo).

- Opera un ciclo PDCA (*Plan–Do–Check–Act*)[3] con métricas y auditorías periódicas.

- Integra la gestión de riesgos (identificación, análisis, tratamiento y aceptación del riesgo) y la continuidad de negocio

Protocolos de actuación (procedimientos operativos)

Una vez descritos los planes internos de seguridad se deben establecer los protocolos que traducen la política a acciones repetibles (National Institute of Standards and Technology (NIST), 2010). Resultan críticos:

- **Gestión de incidentes** (detección → análisis → contención → erradicación → recuperación → aprendizaje). Más adelante se tratará esta gestión. En la Figura 4.6 se observa un diagrama sobre los pasos a seguir en la gestión de incidentes de ciberseguridad y la acción más importante que lo describe. *Playbooks* específicos[4]: *ransomware*, fuga de datos, compromiso de credenciales, indisponibilidad de sede electrónica, etc.

- **Gestión de vulnerabilidades y parches** (inventario, escaneo periódico, priorización, ventana de mantenimiento, verificación post-parche).

- **Gestión de cambios** (evaluación de impacto, autorización, rollback plan[5]).

- **Copias de seguridad** (3–2–1, copias *offline*/inmutables, pruebas de restauración).

- Alta, modificación y baja de usuarios (uniones, cambios de puesto, cese).

- **Relación con terceros** (*onboarding*[6], requisitos ENS, SLA de seguridad[7], auditorías, *offboarding*[8]).

- **Notificación de brechas** (circuitos internos, valoración de impacto, coordinación con DPD y en su caso a la autoridad competente).

[3]Metodología de gestión para la mejora continua de procesos, que consta de cuatro pasos cíclicos: Planificar (identificar el problema y el objetivo), Hacer (ejecutar el plan), Verificar (medir y evaluar los resultados) y Actuar (implementar las acciones)

[4]Proporciona pasos de análisis detallados para un incidente de *ransomware*

[5]Pasos que permiten revertir cambios no deseados en un sistema de software o infraestructura tecnológica a un estado anterior y estable

[6]Proceso de integración y adaptación de un nuevo empleado en una empresa

[7]Contrato entre un proveedor de servicios de seguridad y un cliente que detalla el nivel de seguridad, las métricas y las responsabilidades que el proveedor se compromete a cumplir

[8]Proceso de salida de un empleado de una empresa

Formación y concienciación de empleados públicos

Un factor importante en toda acción a ejecutar en el plano de un equipo, grupo, o a nivel de la Adminsitración Pública, es la formación. La formación continua es medida estratégica: el vector humano concentra gran parte del riesgo (p. ej., phishing). Para ello se debe interponer acciones formativas de los empleados, de forma anual, con carácter de reciclaje y concienciador:

- Módulos base (política marco, manejo de información, phishing, contraseñas, movilidad y teletrabajo).
- Formación por roles (técnicos TI, gestores de expedientes, atención ciudadana, responsables de área, directivos).
- Simulaciones de *phishing*, campañas temáticas y otros riesgos.
- Evaluación (tests, métricas de mejora) y certificación interna.

La figura del CISO en organismos públicos

El/la *Chief Information Security Officer* (CISO) o Director/a de seguridad de la información es la máxima autoridad técnica en seguridad de la información. En el sector público se destacan las siguientes características:

- **Funciones:** gobernanza del SGSI, gestión de riesgos, coordinación de incidentes, interlocución con CCN-CERT e Instituto Nacional de Ciberseguridad (INCIBE) INCIBE (según ámbito), supervisión de continuidad, reporte a dirección.
- **Relaciones:** coordinación con DPD, comunicaciones institucionales, asesoría jurídica, responsables de negocio y proveedores.
- **Independencia y capacidad de reportar:** debe disponer de autoridad suficiente y acceso directo a alta dirección/comités (evitar conflictos de interés).
- **Estructura de soporte:** *Security Operations Center* (SOC) o Centro de Operaciones de Seguridad interno o externalizado, gestores de vulnerabilidades, arquitectura y cumplimiento ENS, riesgos y continuidad.

4.4.2. Organismos clave en España en la Ciberseguridad

CCN-CERT

El CCN-CERT, dependiente del Centro Criptológico Nacional (CCN), es el equipo de respuesta y el órgano de referencia para la ciberseguridad del sector público en España y para empresas que prestan servicios a éste. Sus líneas de actuación incluyen, entre otras:

- Prevención, detección y respuesta frente a ciberamenazas que afecten a sistemas del sector público.
- Normativa y guías CCN-STIC que operativizan el ENS (medidas técnicas y organizativas, valoración de sistemas, auditoría, buenas prácticas).
- Alerta temprana y coordinación de incidentes, intercambio de inteligencia de amenazas y campañas.

- Formación y ejercicios especializados para administraciones.

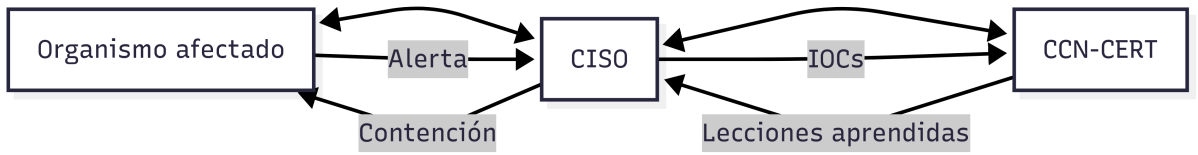

Figura 4.4: Flujo de coordinación de incidentes

En la Figura 4.4 se refleja gráficamente el flujo de coordinación de los diferentes actores ante un incidente. Destaca la posición del CISO en el centro de la coordinación. Los IOCs[9]

INCIBE

El INCIBE (Instituto Nacional de Ciberseguridad, 2025) es el referente nacional para ciudadanía, empresas y ecosistema económico. A través de INCIBE-CERT presta servicios de prevención y respuesta a incidentes a operadores privados y sectores económicos (según ámbito competencial), además de:

- Línea 017 gratuita, de ayuda y asesoramiento.
- Programas de concienciación y recursos didácticos para ciudadanía, pymes y menores.
- **Soporte a empresas**: (guías, herramientas, ejercicios, apoyo a la industria y talento).
- **Complementariedad**: CCN-CERT / INCIBE-CERT
- **CCN-CERT**: foco en Administraciones Públicas (y empresas que les prestan servicios en el marco del ENS).
- **INCIBE-CERT:** foco en tejido empresarial y ciudadanía.
- **Ambos coordinan la respuesta nacional** y comparten inteligencia y buenas prácticas.

4.4.3. Madurez, métricas y mejora continua

El hecho de integrar políticas y organismos de referencia con eficacia y sentido, debe traducirse en planes concretos y medibles, como los que se muestran a continuación:

- Modelo de madurez (inicial → gestionado → definido → medido → optimizado) con autoevaluación anual.
- Cuadro de mando: KPIs de 4.4.1.B + indicadores de formación (% plantilla formada, tasa de clic en phishing simulado), ENS (% medidas implantadas por categoría), auditoría (no conformidades resueltas).
- Lecciones aprendidas de incidentes y ejercicios — incorporación a políticas.
- Revisión del SGSI por la dirección con prioridades y presupuesto.

[9]Son pistas o datos forenses que señalan una actividad maliciosa o un posible ataque cibernético en un sistema, red o dispositivo

Radar de madurez

La lectura de los ejes y valores de la Figura4.5 que describe un rada de madurez se detalla a continuación:

- Gobernanza → 4/5 → Nivel alto de madurez, existe estructura y supervisión sólida.
- Técnica → 3/5 → Madurez intermedia, con margen para mejorar en herramientas, procesos técnicos o automatización.
- Respuesta → 5/5 → Dominio más fuerte: excelente capacidad de reacción ante incidentes.
- Continuidad → 2/5 → Punto débil: planes de continuidad y resiliencia aún poco desarrollados o sin pruebas suficientes.
- Terceros → 3/5 → Gestión aceptable de proveedores y riesgos externos, pero no robusta.
- Formación → 4/5 → Alto nivel en concienciación y capacitación del personal, aunque todavía se puede afinar.

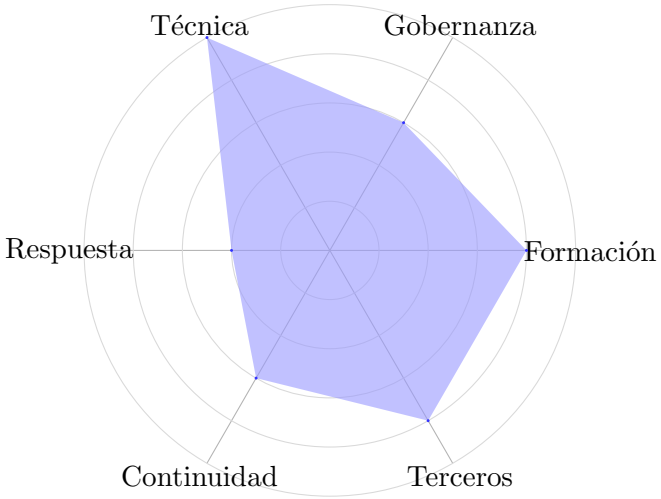

Figura 4.5: Radar de madurez por dominios

4.5. Continuidad del servicio y gestión de incidentes

La continuidad del servicio y la gestión de incidentes son dos vectores críticos de la ciber-resiliencia en la Administración Pública. Mientras la continuidad se ocupa de garantizar que los servicios esenciales permanezcan disponibles ante fallos o desastres, la gestión de incidentes cubre la detección, respuesta y recuperación tras eventos de seguridad (ciberataques, fallos masivos, desastres naturales) (National Institute of Standards and Technology (NIST), 2010). Ambos ámbitos deben integrarse en el SGSI y enlazarse con el ENS y los marcos internacionales (ISO/IEC 27001 (ISO, 2022), ISO 22301 (ISO, 2019), Instituto Nacional de Estándares y Tecnología (NIST)[10]).

[10]Es una agencia estadounidense no reguladora que promueve la innovación mediante el fomento de la ciencia, los estándares y la tecnología de la medición, y cuyos estándares son reconocidos y seguidos por la comunidad internacional.

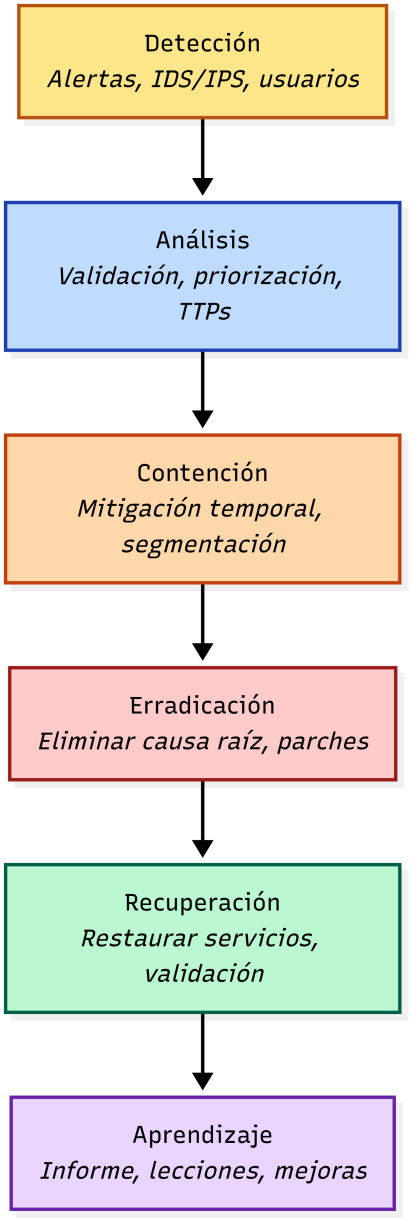

Figura 4.6: Flujo de gestión de incidentes de ciberseguridad

4.5.1. Importancia de planes de contingencia, copias de seguridad y DRP

Concepto y alcance

A continuación se van a definir los conceptos que se van a tratar en esta sección.

- **Copias de seguridad (*backups*)**: mecanismos para preservar datos e imágenes de sistema que permitan la recuperación. La estrategia de *backups* define retención, periodicidad, tipos (completo / incremental / diferencial), ubicación (*on-prem*[11] / *off-site*[12]/ *cloud)* y medidas de protección (cifrado, inmutabilidad).

[11]En el servidor
[12]Fuera del servidor

- **Business Continuity Plan (BCP) o Plan de contingencia**: conjunto de procedimientos organizados para mantener o restablecer las funciones críticas ante una interrupción. Incluye análisis de impacto al negocio (BIA), identificación de funciones críticas, prioridades de recuperación y planes operativos.

- **Disaster Recovery Plan (DRP) o Plan de Recuperación ante Desastres**: subplan técnico focalizado en la recuperación de infraestructuras y sistemas (servidores, bases de datos, comunicaciones) tras un desastre. Normalmente define procesos de *failover*[13], recuperación desde copias y roles técnicos.

Principios y buenas prácticas

A continuación se explican un conjunto de buenas prácticas y principios que se deben tener en cuenta a la hora de trabajar con información en formato digital:

- **3-2-1:**tener al menos 3 copias de los datos, en 2 medios distintos, con 1 copia off-site.

- ***Backups* inmutables (*WORM / air-gapped*)**: para mitigar ransomware que cifra o borra copias.

- **Versionado y pruebas periódicas de restauración:** una copia no probada no es una copia fiable.

- **Planificación por capas**: aplicaciones críticas tienen DRP con replicación síncrona o asíncrona; servicios no críticos con backups diarios/semanales.

- **Documentación y actualización continua:**los planes deben revisarse tras cambios en arquitectura, aplicaciones o proveedores.

- Recovery Time Objective (RTO) u Objetivo de Tiempo de Recuperación[14] y Recovery Point Objective (RPO) u Objetivo de Punto de Recuperación[15], deben definirse por servicio crítico tras el Business Impact Analysis (BIA) o Análisis de Impacto en el Negocio[16]

4.5.2. Coordinación en caso de ciberataques

Anteriormente se habían indicado las fases a tener en cuenta ante un incidente de seguridad (Centro Criptológico Nacional (CCN), 2023). En la Figura 4.6 se muestra brevemente una explicación de lo que se tiene que atender en cada una de esas fases de forma gráfica. A continuación se exponen de forma más detallada cada una de dichas fases:

[13]Los procesos de *failover* son mecanismos para asegurar la continuidad de un servicio o sistema mediante la transferencia automática o manual de operaciones de un componente principal que ha fallado a uno o más componentes redundantes.

[14]Período máximo de tiempo que una empresa puede tolerar que sus sistemas, aplicaciones o servicios estén inactivos tras un incidente o desastre

[15]Cantidad máxima de datos que una organización puede permitirse perder en caso de una interrupción o desastre

[16]Identificar los procesos y activos críticos de una organización y evaluar el impacto de un incidente de seguridad en ellos.

- **Detección:** alertas Sistema de Gestión de Eventos e Información de Seguridad (SIEM), Sistema de Detección de Intrusiones (IDS)/Sistema de Prevención de Intrusiones (IPS), monitoreo de tráfico anómalo, reportes de usuarios.
- **Clasificación/Contención:** determinar alcance, aislar sistemas afectados para evitar propagación (segmentación, bloqueo de cuentas comprometidas).
- **Erradicación:** eliminar causa raíz (malware, credenciales comprometidas, vulnerabilidad explotada).
- **Recuperación:**restaurar servicios desde copias seguras.
- **Lecciones aprendidas:** informe post-mortem, actualizar playbooks y políticas, comunicar resultados a dirección y a autoridades si procede.

Roles y estructura de respuesta

Para crear una respuesta funcional y efectiva, éste debe estar bien estructurada y cada ente tiene que tener un rol bien definido. En la Tabla4.5 se muestra un ejemplo de clasificación de incidentes basado en su SLA. A continuación se explican cada una de las entidades que deben aparecer y actuar ante un incidente de ciberseguridad:

- **Equipo de Respuesta a Incidentes (CSIRT/SOC):** responsables técnicos de detección, contención y recuperación[17].
- **Comité de Crisis (CISO, DPD, Jurídico, Comunicación, Dirección)**: decisiones estratégicas, comunicación externa, coordinación legal.
- **Punto de contacto con CCN-CERT / INCIBE-CERT:** notificación temprana, intercambio de IOC, soporte en mitigaciones nacionales.
- **Relación con proveedores/*cloud*:** activar SLA, coordinación con subcontratas, uso de canales de emergencia.

Nivel	**Descripción**	**Respuesta inmediata**	**Comunicación interna**	**Escalado externo**
1 (Crítico)	Servicio clave caído, datos sensibles comprometidos	Inmediata (0–1 h)	Sí, Exec + prensa	Notificar CCN/INCIBE
2 (Alto)	Interferencia grave en funciones esenciales	1–4 h	Sí, equipos + dirección	Posible
3 (Medio)	Incidente operativo limitado	4–24 h	Equipos TI	No, salvo agravamiento
4 (Bajo)	Incidentes menores (p.ej. spam)	24–72 h	Registro / Seguimiento	No

Tabla 4.5: Niveles de incidentes y criterios de respuesta

[17]CSIRT es un equipo especializado en la gestión y respuesta a incidentes de seguridad informática, mientras que SOC se enfoca en la monitorización continua y la detección temprana de amenazas

4.5.3. Coordinación interinstitucional

Otro factor importante a tener en cuenta es la coordinación que se debe hacer entre instituciones cuando se ha producio un incidente de ciberseguridad. Así, brevemente comentamos lo siguiente:

- **Establecer protocolos de notificación** (quién, cómo, cuándo) a CCN-CERT/INCIBE y autoridades competentes.
- **Compartir conocimientos (IOCs)** y participar en ejercicios conjuntos.
- **Comunicación pública:** disponer de planes de comunicación para prensa y ciudadanos que eviten pánico y ofrezcan instrucciones concretas.

4.5.4. Comunicación, aspectos legales y notificación

Cuando se produce un incidente de seguridad, se debe tener en cuenta cómo solucionarlo, atajarlo, sin duda. Pero no menos importante es la comunicación y los aspectos legales y notificaciones que se deben realizar para la ocasión:

- **Comunicación interna debe estar contemplada en el plan:** mensajes para empleados, instrucciones de confinamiento, prioridades de recuperación.
- **Comunicación externa:** designar portavoces, mensajes oficiales y canales alternativos para informar a la ciudadanía sin comprometer la investigación forense.
- **Notificaciones reglamentarias:** si hay afectación de datos personales, el RGPD exige notificar brechas a la autoridad de control AEPD y, cuando proceda, a los interesados; ENS y normativa sectorial pueden imponer obligaciones adicionales.
- **Preservación de evidencias:** protocolos forenses (no sobrescribir logs, conservar imágenes disco, cadena de custodia) para permitir investigación y posibles acciones legales.

4.5.5. Arquitectura de resiliencia y consideraciones técnicas Estrategias técnicas clave

Es imposible establecer alguna estrategia que implique una total seguridad en el sistema, es decir, siempre hay un riesgo de que un sistema sea atacado. Pero sí se pueden establecer ciertas consieraciones técnicas o estrategias clave que puedan mitigar esos ataques, y sus consecuencias, en el caso de que se produzcan. Es lo que se llama la arquitectura de resiliencia, basada en conceptos que ya se han visto anteriormente en diferentes secciones:

- **Redundancia geográfica:** replicación entre centros de datos y/o regiones *cloud* para tolerancia a fallos de zona/país.
- **Segregación de redes:** segmentación por funciones (administración, usuarios, servicios críticos) para limitar movimiento lateral.
- **Replicación y *snapshots*:** uso de replicación síncrona para RTO bajos; asíncrona para eficiencia de ancho de banda.

- ***Backups* inmutables y retención prolongada:** protegidos contra eliminación maliciosa.
- **Automatización de *failover:*** scripts y orquestación para reducir Tiempo Medio de Recuperación (MTTR); siempre con procedimientos manuales de *rollback*.
- **Pruebas periódicas y métricas:** ejercicios programados, validación de integridad, tiempos de restauración medidos.

4.6. Ciberseguridad en servicios en la nube y entornos móviles

La adopción de servicios en la nube (*cloud computing*) y la movilidad (dispositivos móviles, *Bring Your Own Device* (BYOD) o Traer tu propio dispositivo) ha transformado la provisión de servicios públicos, pero también introduce riesgos y retos específicos para la ciberseguridad de la Administración Pública. Esta sección revisa de forma académica los principales riesgos de la nube, las contramedidas organizativas y técnicas, y los retos de la movilidad —incluyendo estrategias de gobernanza, herramientas y métricas— con sugerencias de tablas, diagramas y listas prácticas para su aplicación en entornos públicos.

4.6.1. Riesgos específicos de la nube

Naturaleza del riesgo

La nube modifica el perímetro tradicional y plantea riesgos por la externalización de infraestructura y servicios, la compartición lógica de recursos, la pérdida de visibilidad y control, y por la complejidad de las cadenas de suministro (proveedores, subcontratas, servicios gestionados). Los riesgos se manifiestan en ámbitos técnicos, operativos, contractuales y de cumplimiento legal.

Riesgos clave

Es importante tener en cuenta los riesgos clave que hay que asumir sin se opta por mantener servicios en la nube o en entornos móviles. A continuación se enumeran estos riesgos clave:

1. **Ubicación de datos y jurisdicción.**
   - *Riesgo:* datos almacenados en centros de datos situados en jurisdicciones con normativas distintas (acceso por autoridades, transferencia internacional).
   - *Impacto:* incumplimiento de requisitos de protección de datos (p. ej. RGPD), exigencia de localización o cifrado adicional.
2. **Dependencia del proveedor.**
   - *Riesgo:* dificultad para migrar o recuperar datos y servicios por formatos propietarios, APIs o costos de salida.
   - Impacto: problemas de continuidad, coste elevado en cambio de proveedor.
3. **Responsabilidad compartida.**

- *Riesgo:* confusión sobre quién es responsable de qué (proveedor vs cliente).
- *Impacto:* lagunas en seguridad si no se definen claramente responsabilidades (p. ej. configuración de IAM, protección de datos en reposo).

4. **Configuraciones erróneas y exposición pública.**
   - *Riesgo:* reglas de *firewall* abiertas, roles con privilegios excesivos.
   - *Impacto:* exposición masiva de datos, escalada de privilegios.
5. **Falta de visibilidad y telemetría.**
   - *Riesgo: logs* delegados o deshabilitados, dificultades para correlacionar eventos.
   - *Impacto:* detección tardía de incidentes y pobre respuesta forense.
6. **Accesos compartidos y credenciales comprometidas.**
   - *Riesgo:* claves de Interfaz de Programación de Aplicaciones (API)[18], credenciales con privilegios elevados almacenadas en código o repositorios públicos.
   - *Impacto:* compromiso total del entorno *cloud*.
7. **Seguridad de la cadena de suministro (subprocesadores).**
   - *Riesgo:* proveedores de servicios gestionados, microservicios que introducen vulnerabilidades.
   - *Impacto:* vector de entrada indirecto[19], responsabilidad contractual.
8. **Aislamiento insuficiente.**
   - *Riesgo:* fallo en aislamiento lógico entre clientes (p.ej. escape de contenedores o unidades virtuales).
   - *Impacto:* fuga de información entre inquilinos.
9. **Gestión de claves y cifrado.**
   - *Riesgo:* claves gestionadas por el proveedor sin control del cliente (no se controla la revocación, acceso de administrador del proveedor).
   - Impacto: acceso no autorizado a datos cifrados.
10. **Continuidad y recuperación.**
    - *Riesgo:* arquitecturas *cloud* diseñadas sin estrategias de *backup* adecuadas (por ejemplo, *backups* en la misma región sin replicación).
    - *Impacto:* incapacidad para recuperar tras una pérdida masiva o fallo regional.

[18]Es un conjunto de reglas y protocolos que permite que diferentes programas de software se comuniquen entre sí

[19]Camino menos obvio de entrada a un sistema informático

4.6.2. Buenas prácticas de gobernanza y contratación en *cloud*

Las buenas prácticas que podemos adquirir en el terreno de la gobernanza y contratación de la computación en la nube son las siguientes:

- **Acuerdos sobre el procesamiento de datos:** incluir obligaciones de protección de datos RGPD, subprocesadores, plazos de notificación de brechas, ubicación de datos, y derechos de auditoría.
- **SLA:** definir RTO/RPO, disponibilidad, créditos por incumplimiento, tiempos de respuesta ante incidentes de seguridad.
- **Cláusulas de salida:**exportación completa de datos en formatos abiertos, procedimiento de borrado certificado, plazos y costes.
- **Auditorías y certificaciones:** exigir ISO/IEC 27001, ISO/IEC 27701, certificaciones *cloud* específicas y registros de cumplimiento ENS cuando aplique.

4.6.3. Retos y medidas para entornos móviles y BYOD

El uso de entornos móviles y dejar que se expanda el uso del BYOD confiere una serie de retos y medidas que deben tenerse en cuenta y que a continuación se van a exponer:

1. **Pérdida o robo de dispositivo.**
   - *Riesgo:* acceso físico a información almacenada o sesiones abiertas.
   - *Mitigación:* cifrado del dispositivo, bloqueo remoto, borrado remoto, autenticación fuerte.
2. **Dispositivos inseguros.**
   - *Riesgo:* vulnerabilidades elevadas, *bypass* de controles de seguridad.
   - *Mitigación:* políticas de no admisión (*blocklist*), *Mobile Threat Defense* (MTD)[20], verificación de integridad.
3. **Conexiones inseguras (Wi-Fi pública).**
   - Riesgo: ataques *man-in-the-middle*[21], interceptación de credenciales.
   - *Mitigación:* Red Privada Virtual (VPN)[22]obligatoria para acceso a recursos sensibles, Seguridad de la Capa de Transporte (TLS)[23] obligatorio, certificados de cliente.
4. **Aplicaciones maliciosas o de terceros no controladas.**

[20]Es un marco de ciberseguridad que protege los dispositivos móviles y los datos empresariales de una amplia gama de amenazas

[21]Es un ciberataque en el que un atacante se interpone secretamente entre dos partes que se están comunicando

[22]Crea un túnel cifrado a través de Internet para proteger tu actividad en línea, ocultar tu dirección IP y encriptar tus datos

[23]Protocolo de seguridad que cifra y autentica las comunicaciones en Internet

- *Riesgo:* exfiltración de datos, *keylogging*[24], sesiones secuestradas.
- *Mitigación:* listas blancas de apps, *sandboxing* o zonas de ejecución seguras.

5. **Parches.**
   - *Riesgo:* dispositivos con vulnerabilidades conocidas.
   - *Mitigación:* políticas de actualización forzadas, bloqueo de acceso si el Sistema Operativo está desactualizado.
6. **Separación de datos personal/profesional.**
   - *Riesgo:* fuga de datos por uso personal (copias a nubes personales, compartir).
   - *Mitigación:* contenedorización, Prevención de Pérdida de Datos (DLP)[25], DLP móvil, políticas BYOD claras.
7. **Autenticación débil.**
   - *Riesgo:* uso de PINs simples o ausencia de Autenticación MultiFactor (MFA).
   - *Mitigación:* Inicio de Sesión Único (SSO) con MFA, autenticación adaptativa

[24]Es el acto de grabar encubiertamente las teclas que se pulsan en un teclado, ya sea mediante software o hardware, para recopilar información confidencial

[25]Estrategia de seguridad que utiliza herramientas para identificar, monitorear y proteger información confidencial

Bibliografía

Agencia Española de Protección de Datos (2024). Guías y herramientas para administraciones públicas. https://www.aepd.es/areas-de-actuacion/administraciones-publicas.

Agencia Española de Protección de Datos (2025). Administraciones públicas: Guías, informes y documentos (aepd). https://www.aepd.es/areas-de-actuacion/administraciones-publicas.

Anderson, R. (2020a). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley, 3rd edition.

Anderson, R. (2020b). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley, 3rd edition.

Castells, M. (2021). *La sociedad red: la era de la información*. Alianza Editorial, Madrid.

CCN-CERT (2024). Ccn-stic 830: Ámbito de aplicación del ens. https://www.ccn-cert.cni.es/es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1674-ccn-stic-830-ambito-aplicacion-ens/file.html.

CCN-CERT (2025). Ccn-stic 803: Valoración de sistemas en el ens. https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/682-ccn-stic-803-valoracion-de-sistemas-en-el-ens-1/file.html.

Centro Criptológico Nacional (2023). Informe anual del ccn-cert sobre ciberseguridad en las administraciones públicas. https://www.ccn-cert.cni.es. Consultado el 18 de agosto de 2025.

Centro Criptológico Nacional (CCN) (2023). Guías ccn-stic sobre continuidad y recuperación. https://www.ccn-cert.cni.es.

Chaffey, D. (2019). *Digital Business and E-Commerce Management: Strategy, Implementation and Practice*. Pearson Education, Harlow, UK.

Chen, P. P. (1976). The entity-relationship model—toward a unified view of data. *ACM Transactions on Database Systems*, 1(1):9–36.

Connolly, T. and Begg, C. (2014). *Database Systems: A Practical Approach to Design, Implementation, and Management*. Pearson, Harlow, UK, 6th edition.

Cordero, J. (2018). *Administración electrónica e interoperabilidad en España*. Dykinson, Madrid.

Date, C. (2004). *Introducción a los sistemas de bases de datos*. Pearson Educación, Madrid.

Date, C. J. (2003). *An Introduction to Database Systems*. Addison-Wesley, Boston, 8th edition.

Davenport, T. H. and Bean, R. (2018). How analytics and ai are transforming decision making. *Harvard Business Review*, 96(5):40–48.

Davenport, T. H. and Prusak, L. (1998). *Working Knowledge: How Organizations Manage What They Know*. Harvard Business School Press, Boston, MA.

de Asuntos Económicos y Transformación Digital, M. (2023). Gestión de bases de datos en la administración pública. `https://administracionelectronica.gob.es/`. Consultado el 14 de agosto de 2025.

de España, G. (2018). Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. `https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673`.

de Hacienda Función Pública, M. (2022). Buenas prácticas en el diseño de bases de datos en la administración pública. `https://administracionelectronica.gob.es/`. Consultado el 18 de agosto de 2025.

Delgado García, M. and López Álvarez, J. (2021). Aplicaciones de la inteligencia artificial en la gestión pública. *Revista de Estudios de la Administración Local y Autonómica*, 15:45–63.

Elmasri, R. and Navathe, S. B. (2017). *Fundamentals of Database Systems*. Pearson, Boston, 7th edition.

ENISA (2015). Privacy by design in big data. `https://www.enisa.europa.eu/`.

European Commission (2017). European egovernment action plan 2016-2020. Technical report, Publications Office of the European Union, Luxembourg.

European Data Protection Board (2020). Edpb guidelines on data protection impact assessment (dpia). `https://edpb.europa.eu/`.

European Union Agency for Cybersecurity (ENISA) (2020). Enisa good practices for incident management. `https://www.enisa.europa.eu`.

Forouzan, B. A. (2012). *Data Communications and Networking*. McGraw-Hill, 5th edition.

Gil-García, R., Luna-Reyes, L. F., and Purón-Cid, G. (2012). Gobierno electrónico y reforma administrativa: hacia la transformación de las administraciones públicas en iberoamérica. *Revista del CLAD Reforma y Democracia*, 54:1–22.

Gobierno de España (2021). Agenda españa digital 2026 - plan para la digitalización del país. `https://espanadigital.gob.es/`. Consultado el 13 de agosto de 2025.

Gobierno de España (2025a). Carpeta ciudadana - punto de acceso único a la información y servicios de las administraciones públicas. `https://carpetaciudadana.gob.es/`. Consultado el 13 de agosto de 2025.

Gobierno de España (2025b). Registro electrónico general de la administración general del estado (regage). https://sede.administracion.gob.es. Consultado el 18 de agosto de 2025.

Gobierno de España (2025c). Sistema cl@ve - plataforma común de identificación, autenticación y firma electrónica. https://clave.gob.es/clave_Home/. Consultado el 13 de agosto de 2025.

Gobierno de España-DIR3 (2025). Dir3: Directorio común de unidades orgánicas y oficinas. https://administracionelectronica.gob.es/ctt/dir3. Consultado el 18 de agosto de 2025.

Gobierno de España-ORVE (2025). Orve: Oficina de registro virtual de entidades. https://administracionelectronica.gob.es/ctt/orve. Consultado el 18 de agosto de 2025.

Gobierno de España-SIA (2025). Sistema de información administrativa (sia). https://administracionelectronica.gob.es/ctt/sia. Consultado el 18 de agosto de 2025.

Group, W. O. W. (2012). Owl 2 web ontology language document overview (second edition). Technical report, W3C. W3C Recommendation.

Han, J., Haihong, E., Le, G., and Du, J. (2011). Nosql: New sql for cloud-based databases. *Proceedings of the International Conference on Cloud and Service Computing*, pages 401–408.

Haykin, S. (2000). *Communication Systems*. Wiley, 4th edition.

IETF (2023). Internet engineering task force (ietf) standards. https://www.ietf.org/standards/.

INCIBE (2023). Guía de seguridad en la administración pública. https://www.incibe.es/.

Instituto Nacional de Ciberseguridad (2025). Recursos y servicios de incibe e incibe-cert. https://www.incibe.es.

International Organization for Standardization (2016). Iso 15489-1:2016 information and documentation — records management — part 1: Concepts and principles. https://www.iso.org/standard/62542.html. Records management.

International Organization for Standardization (2017). Iso 23081-1:2017 information and documentation — managing metadata for records — part 1: Principles. https://www.iso.org/standard/67842.html. Metadata for records.

International Telecommunication Union (ITU) (2020). Fundamentals of telecommunications. https://www.itu.int.

ISO (2015). Iso 8000: Data quality. International Organization for Standardization, disponible en: https://www.iso.org/iso-8000-data-quality.html.

ISO (2016). Iso 15489-1:2016 information and documentation — records management — part 1: Concepts and principles. Ginebra, Suiza.

ISO (2019). Iso 22301:2019 security and resilience — business continuity management systems.

ISO (2022). Iso/iec 27001:2022 information security, cybersecurity and privacy protection — information security management systems.

Kuneva, M. et al. (2014). *Privacy and Data Protection*. European Commission.

Kurose, J. F. and Ross, K. W. (2017). *Computer Networking: A Top-Down Approach*. Pearson, 7th edition.

Laudon, K. C. and Laudon, J. P. (2020). *Sistemas de información gerenciales*. Pearson Educación, México, 15 edition.

Martínez, L. (2019). *Gobierno digital: tecnologías de la información en la administración pública*. Tirant lo Blanch, Valencia.

Meijer, A. (2018). Collaborative platforms in public administration: Opportunities and challenges. *Government Information Quarterly*, 35(4):567–575.

Melton, J. (2011). *SQL: 2011*. Morgan Kaufmann, San Francisco.

Ministerio de Asuntos Económicos y Transformación Digital (2024). Guía para el uso de servicios en la nube en el sector público. `https://administracionelectronica.gob.es`. Consultado el 18 de agosto de 2025.

Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática (2010a). Esquema nacional de interoperabilidad en el ámbito de la administración electrónica. `https://www.boe.es/buscar/doc.php?id=BOE-A-2010-1331`. Real Decreto 4/2010, de 8 de enero.

Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática (2010b). Esquema nacional de seguridad en el ámbito de la administración electrónica. `https://www.boe.es/buscar/doc.php?id=BOE-A-2010-1330`. Real Decreto 3/2010, de 8 de enero.

Ministerio para la Transformación Digital y de la Función Pública (2025). Red sara - sistema de aplicaciones y redes para las administraciones. `https://administracionelectronica.gob.es/ctt/sara`. Consultado el 14 de agosto de 2025.

National Institute of Standards and Technology (2023). Nist privacy framework: A tool for improving privacy through enterprise risk management. `https://www.nist.gov/privacy-framework`.

National Institute of Standards and Technology (NIST) (2010). Contingency planning guide for information technology systems (nist sp 800-34 rev. 1). `https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf`.

NIST (2023). Framework for improving critical infrastructure cybersecurity. `https://www.nist.gov/cyberframework`.

Nonaka, I. and Takeuchi, H. (1995). The knowledge-creating company. *Harvard Business Review*, pages 162–171.

OCDE (2017). *Recomendación del Consejo sobre Gobierno Abierto*. Organización para la Cooperación y el Desarrollo Económicos. Disponible en línea, consultado el 9 de agosto de 2025.

OCDE (2019). *Principios de Gobernanza de Datos en el Sector Público*. Organización para la Cooperación y el Desarrollo Económicos, París, Francia.

OECD (2020). The path to becoming a data-driven public sector. `https://doi.org/10.1787/059814a7-en`. Accedido el 8 de agosto de 2025.

Ponjuán Dante, G. (2013). *Gestión de la información y del conocimiento en las organizaciones*. Cengage Learning, México.

PostgreSQL Global Development Group (2025). pgadmin: Postgresql tools. `https://www.pgadmin.org/`. Consultado el 18 de agosto de 2025.

Power, D. J. (2021). *Decision Support, Analytics, and Business Intelligence*. Business Expert Press, New York, USA, 4 edition.

PREMIS Editorial Committee (2015). Premis data dictionary for preservation metadata, version 3.0. Technical report, PREMIS Editorial Committee.

Ramilo Araujo, M. C. and López Subires, M. (2017). *Administración electrónica y servicios públicos digitales*. Editorial UOC, Barcelona.

Rosenbaum, P. (2020). Intranets y plataformas colaborativas en el sector público. *Revista de Gestión Pública*, 12(1):55–74.

Rowley, J. (2007). *Knowledge Management: An Introduction*. Facet Publishing, London.

Secretaría de Estado de Digitalización e Inteligencia Artificial (2025). Portal de datos abiertos de españa - datos.gob.es. `https://datos.gob.es`. Consultado el 14 de agosto de 2025.

Silberschatz, A., Korth, H. F., and Sudarshan, S. (2019). *Database System Concepts*. McGraw-Hill, New York, 7th edition.

Simões, A. and Carvalho, T. (2020). Digital divide in public services: Challenges and responses. *Public Policy Review*, 18(2):123–141.

Soriano Díaz, R. and Alonso Ibáñez, M. d. C. (2015). La e-administración como instrumento de modernización de las administraciones públicas. *Revista de Estudios de la Administración Local y Autonómica*, 3:7–27.

Stallings, W. (2007). *Data and Computer Communications*. Prentice Hall, 8th edition.

Stallings, W. (2018). *Cryptography and Network Security: Principles and Practice*. Pearson, 8th edition.

Tanenbaum, A. S. and Wetherall, D. J. (2011). *Computer Networks*. Prentice Hall, 5th edition.

The Document Foundation (2025). Libreoffice base: The database frontend. `https://www.libreoffice.org/discover/base/`. Consultado el 18 de agosto de 2025.

Turban, E., Sharda, R., and Delen, D. (2018). Decision support systems and intelligent systems. *Journal of Decision Systems*, 27(Sup1):38–49.

UE (2016). Reglamento (ue) 2016/679 del parlamento europeo y del consejo, de 27 de abril de 2016 (rgpd). `https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679`.

W3C (2023). World wide web consortium (w3c): Http/https. `https://www.w3.org/Protocols/`.

Wang, R. Y. and Strong, D. M. (1996). Beyond accuracy: What data quality means to data consumers. *Journal of Management Information Systems*, 12(4):5–33.