CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

Gobierno de Datos

Integración con Seguridad de la Información y Privacidad

ALIGNMENT
SOLUCIONES ESTRATÉGICAS

DIPLOMADO
CIBERSEGURIDAD

Agenda

- Presentación del curso
- Introducción al Dato
- Introducción al Gobierno de Datos
- Modelos y estándares en la Gobierno de Datos

Profesor del Curso - Carlos Lobos de Medina

https://www.linkedin.com/in/clobos/

- Ingeniero Civil en Informática y Magister en Informática © de la Universidad de Santiago de Chile, Diplomado en Auditoría de Sistemas, Postitulado en Seguridad Computacional y Gestión de Procesos de Negocios de la Universidad de Chile.
- Especialista en gobernanza, gestión y control de tecnologías de información empleando modelos como COBIT, ITIL, ISO 27001 e ISO 22301. Posee certificaciones internacionales CISA, CISM, COBIT, ISO Lead Auditor 27001, ISO Lead Auditor BS 25599 e ITIL V3, entre otras.
- Director de los Programas de Ciberseguridad de Capacitación USACH. CEO Alignment SpA

Introducción al Dato

¿Qué son los datos?

- Un datos es el nivel de abstracción mínima que posibilita la generación de información y conocimiento.

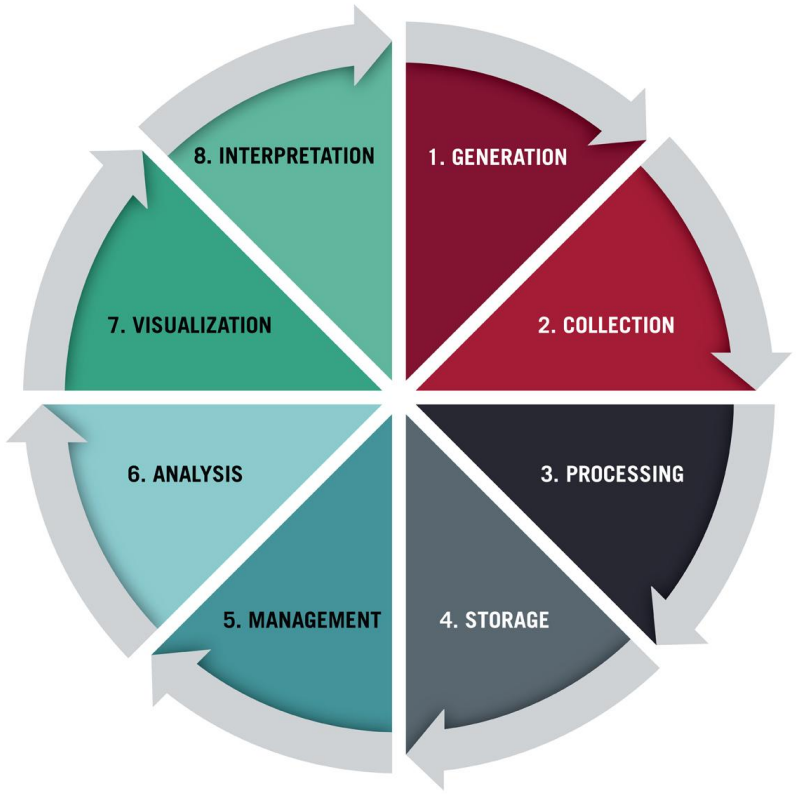
- Es una representación simbólica que puede ser un valor, un texto, un archivo, un audio, una imagen…….. en formato digital o físico.

Dato
- Representación
- Abstracto

Información
- Datos
- Contexto

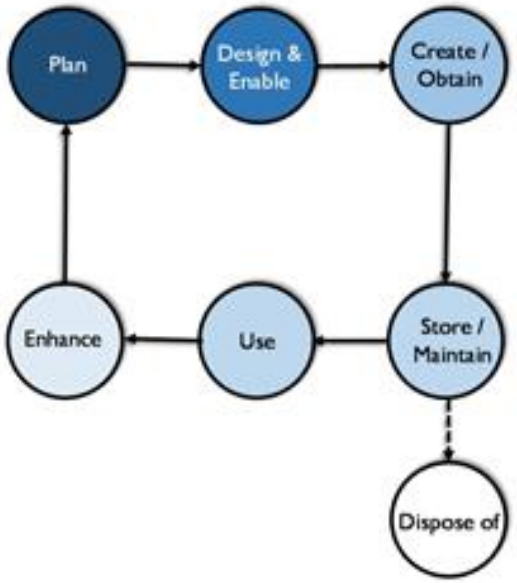
Conocimiento
- Aprendizaje
- Comprensión
- Aplicación

¿Los datos poseen un ciclo de vida?



https://online.hbs.edu/blog/post/data-life-cycle

Visión de Negocios



DAMA – DMBook 2.0
Visión General

RGPD – Marco de Protección de Datos
Visión de Privacidad

Tipos de Datos

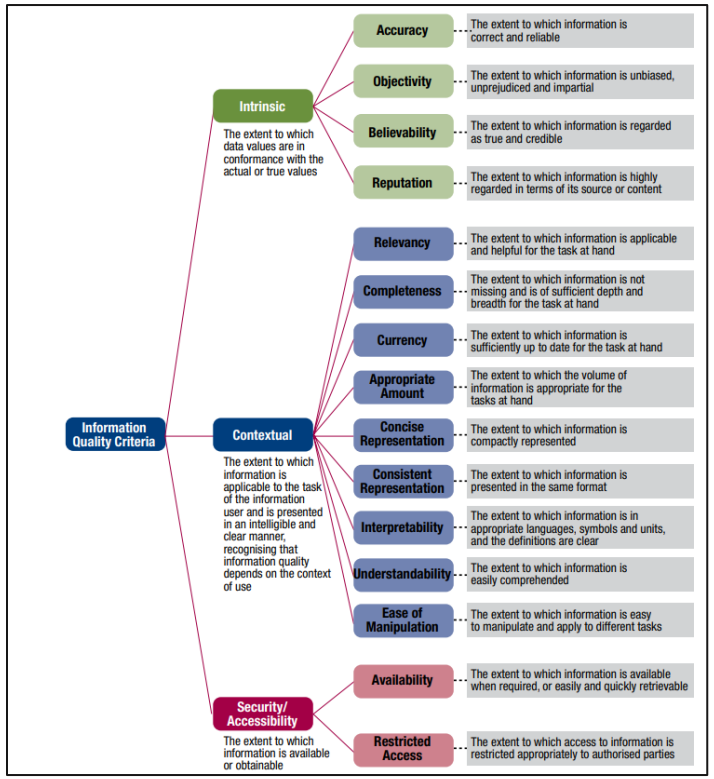
- Datos Personales. Cualquier información de una persona física identificada o identificable.
  - Poseen nivel de criticidad según la normativa que sea aplicable

- Datos Públicos. Datos que no están sujetos a restricciones de privacidad, seguridad o acceso, conforme a requisitos legales y definiciones propias de la organización. (caso especial en Chile Ley de Transparencia)

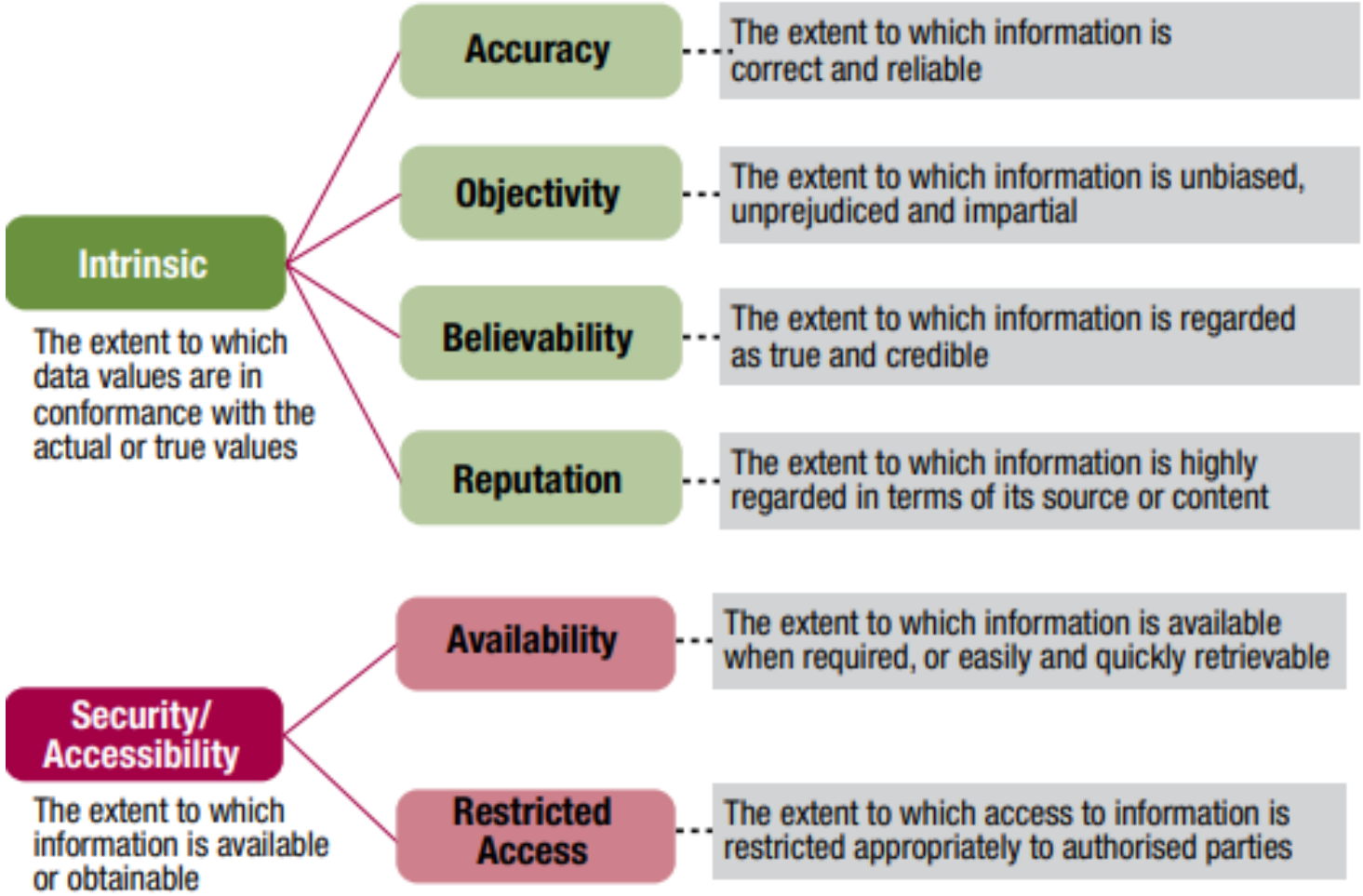
- Datos Abiertos. Datos a disposición de un uso masivo para que puedan ser usados, reutilizados y redistribuidos libremente.

- Datos Privados. Todo aquel dato que la organización quiera mantener un resguardo de su acceso y uso, siempre que cumpla con la legislación vigente vigente.

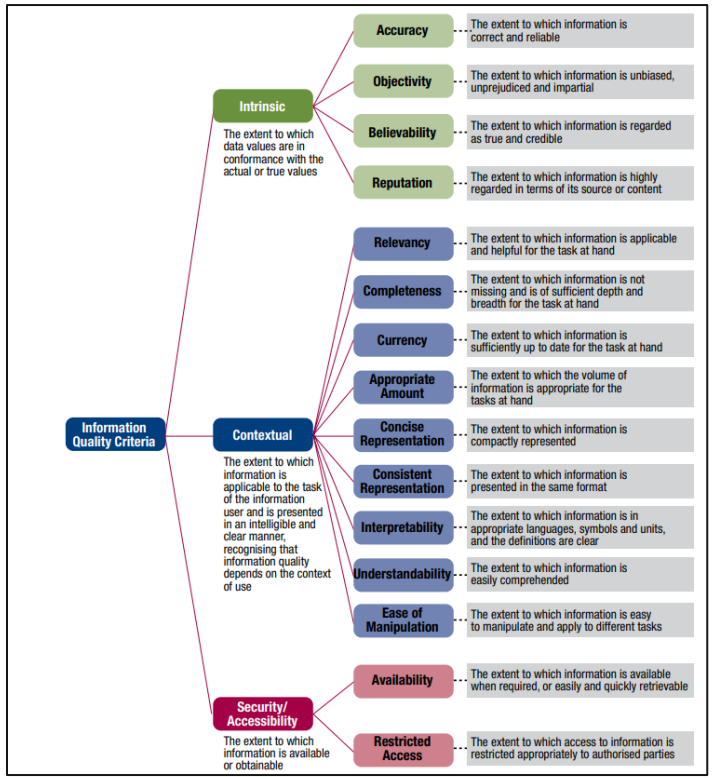
¿Qué elementos de calidad requieren los datos? (COBIT 5)



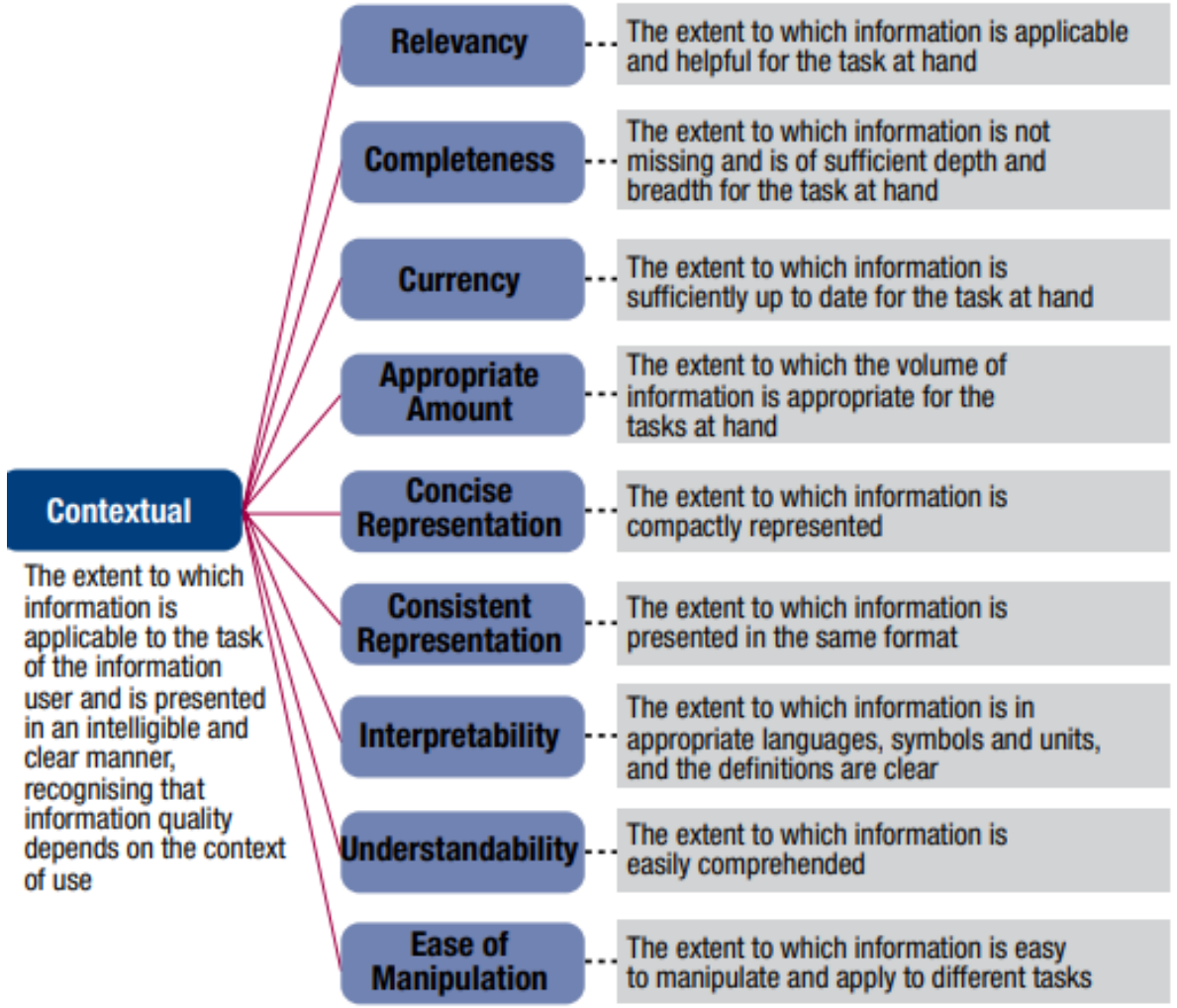
Cobit 5. Información Catalizadora



¿Qué elementos de calidad requieren los datos? (COBIT 5)



Cobit 5. Información Catalizadora



¿Qué elementos de calidad requieren los datos?

DQ DIMENSION	#	%
ACCESSIBILITY	37	52,11%
ACCURACY	61	85,92%
ACTIONABLE	1	1,41%
ADEQUATE	1	1,41%
ALIGNMENT	1	1,41%
APPLICABILITY	2	2,82%
APPROPRATENESS	4	5,63%
APPROPRIATE AMOUNT	18	25,35%
AUTHORIZATION	1	1,41%
AVAILABILITY	19	26,76%
BELIEVEABILITY	28	39,44%
CLARITY	5	7,04%
COHERENCE	1	1,41%
COMPAREABLITIY	2	2,82%
COMPLETENESS	64	90,14%
COMPLIANCE	3	4,23%
COMPREHENSIVENESS	4	5,63%
CONCISENESS	26	36,62%
CONCORDANCE	1	1,41%
CONFIDENTIALIITY	3	4,23%
CONSISTENCY	53	74,65%
CONTENT	1	1,41%
CONVENIENCE	1	1,41%
CORRECTNESS	9	12,68%
CREDIBILITY	8	11,27%
COST	5	7,04%
CURRENCY	13	18,31%
DATA COVERAGE	5	7,04%
DATA DECAY	3	4,23%
DATA SPECIFICATION	3	4,23%
DEFINITION	3	4,23%
DISTORTION	1	1,41%

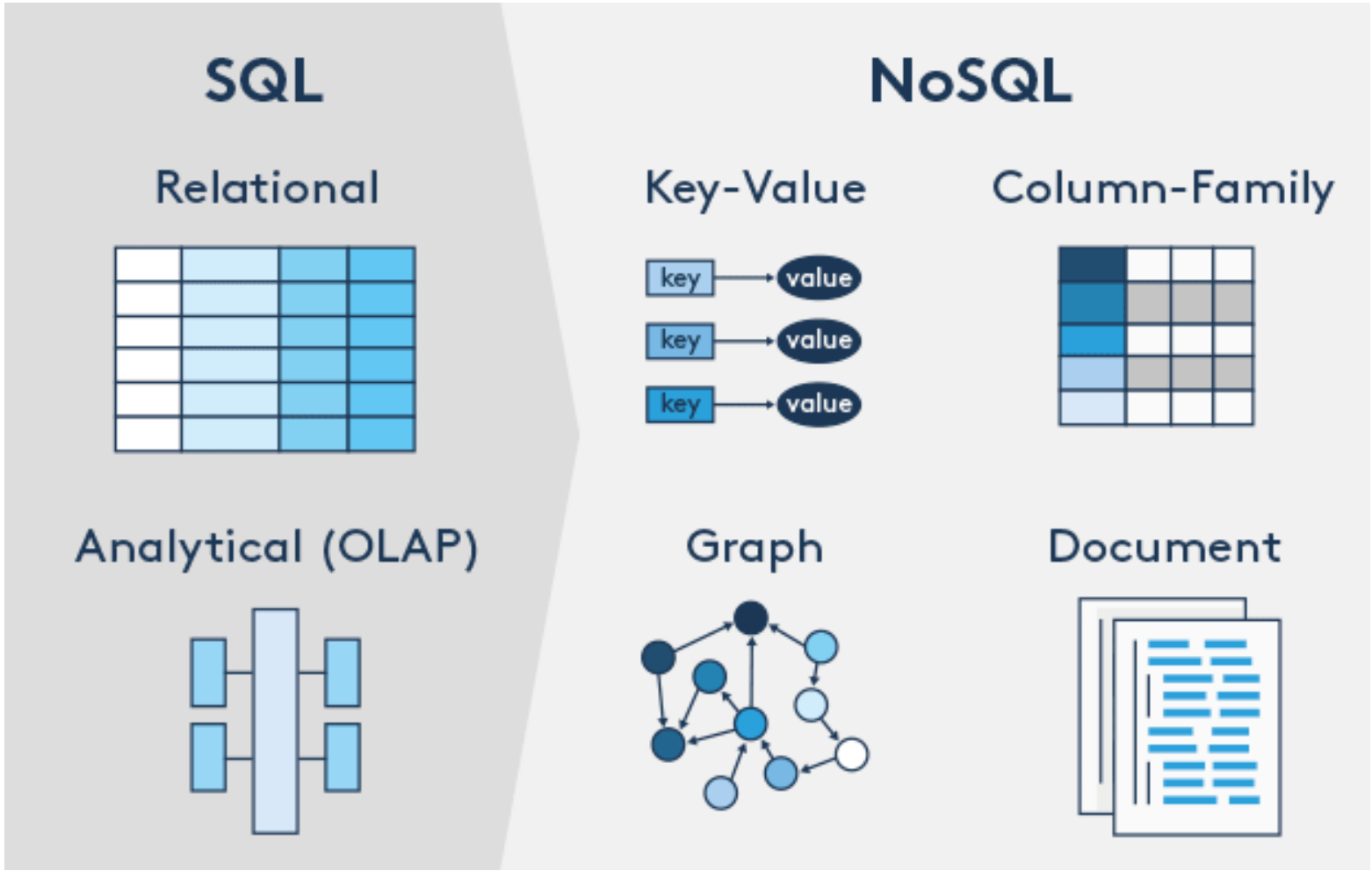
DQ DIMENSION	#	%
DUPLICATION	6	8,45%
EASE OF MANIPULATION	10	14,08%
EASE OF OPERATION	5	7,04%
EFFECTIVENESS	1	1,41%
EFFICIENCY	7	9,86%
EXISTENCE	1	1,41%
FLEXIBILITY	3	4,23%
FORMAT	4	5,63%
FREE OF ERROR	12	16,90%
FREEDOM FROM BIAS	2	2,82%
FRESHNESS	1	1,41%
GRANULARITY	2	2,82%
IMPORTANCE	2	2,82%
INFORMATIVENESS	2	2,82%
INTEGRITY	10	14,08%
INTERACTIVITY	1	1,41%
INTERPRETABILITY	23	32,39%
LEVEL OF DETAIL	1	1,41%
MAINTAINABILITY	5	7,04%
MANIPULABILITY	1	1,41%
MEANINGFULNESS	2	2,82%
METADATA	4	5,63%
MINIMALITY	2	2,82%
NAVIGATION	2	2,82%
OBJECTIVITY	20	28,17%
PLAUSABILITY	1	1,41%
PORTABILITY	2	2,82%
PRECISION	11	15,49%
PRESENTATION	4	5,63%
PRIVACY	3	4,23%
QUANTITY	4	5,63%
READABLE	3	4,23%

DQ DIMENSION	#	%
RECOVERABILITY	1	1,41%
REDUNDANCY	5	7,04%
RELEVANCY	27	38,03%
RELIABILITY	11	15,49%
REPEATABILITY	1	1,41%
REPUTATION	20	28,17%
RESPONSIVENESS	1	1,41%
SAFETY	2	2,82%
SCOPE	1	1,41%
SECURITY	24	33,80%
SOURCE	2	2,82%
SPEED	1	1,41%
STEWARDSHIP	1	1,41%
SUFFICIENCY	1	1,41%
TIMELINESS	53	74,65%
TRACEABILITY	7	9,86%
TRANSACTABILITY	3	4,23%
TRANSPARANCY	1	1,41%
UPDATE	1	1,41%
UNAMBIGUOUS	3	4,23%
UNDERSTANDABILITY	25	35,21%
UNIQUENESS	3	4,23%
USABILITY	15	21,13%
VALIDITY	9	12,68%
VALUE ADDED	17	23,94%
VOLATILITY	7	9,86%

Revisión de 71 papers científicos y las principales buenas prácticas.

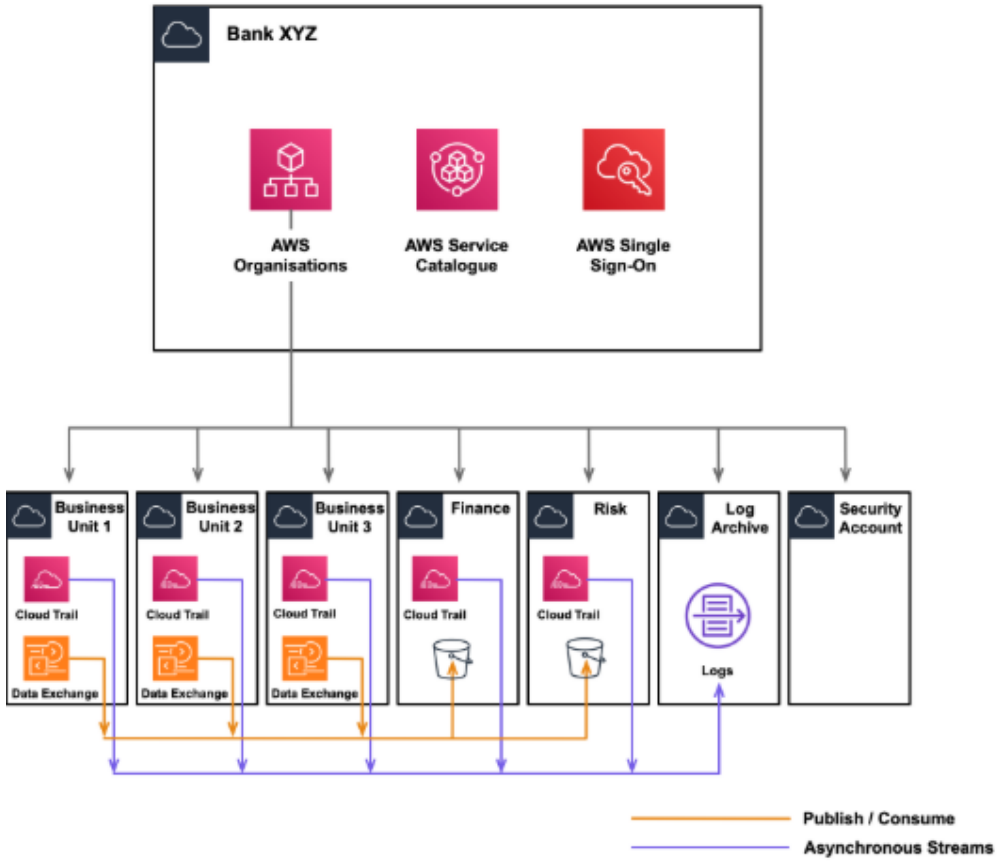
https://libstore.ugent.be/fulltxt/RUG01/002/783/884/RUG01-002783884_2019_0001_AC.pdf

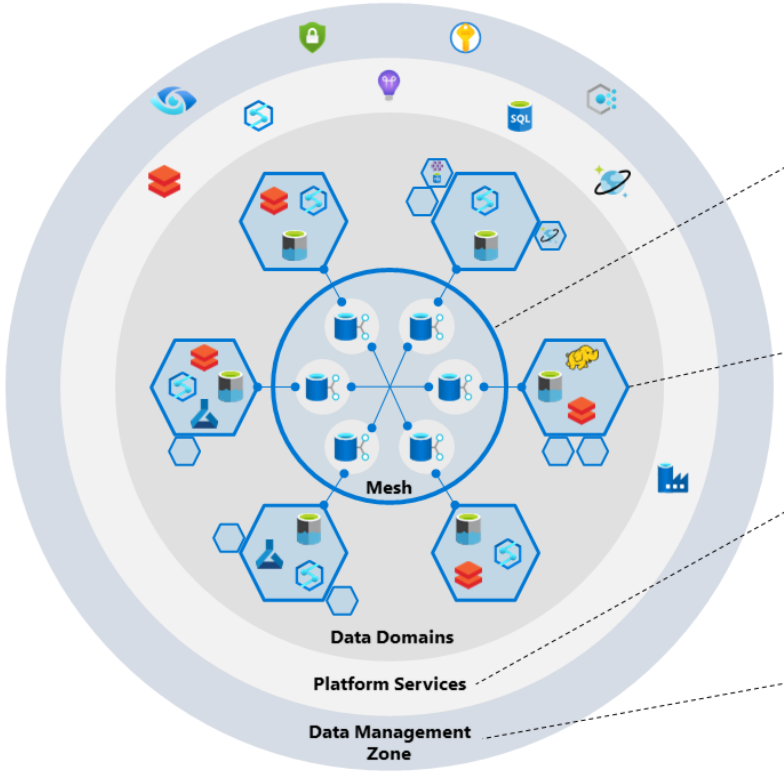
¿Dónde se almacenan los datos?



ORACLE DATABASE
MySQL
PostgreSQL
Microsoft SQL Server
Redis
APACHE HBASE
mongoDB
Cassandra
riak
CouchDB relax
Neo4j

¿Dónde se almacenan los datos? (visión nube)





The **data mesh** intelligently distributes data products between data domains. Read data stores share compute resources. This reduces costs, solves interoperability concerns, and better addresses time-variant and non-volatile concerns of large data consumers.

Data domains operate their own applications or analytics platforms, whilst adhering to common policies and standards.

The central **platform services** defines blueprints that encompass baseline security, policies, capabilities, and standards.

A key concept for every enterprise-scale analytics and AI implementation is having one **data management zone**. This subscription, which is required for data management, contains resources that'll be shared across all landing zones.

Introducción al Gobierno de Datos

¿Qué es el Gobierno de Datos? (Microsoft)

- El gobierno de datos es el sistema de directivas internas que utilizan las organizaciones para proteger y administrar los datos empresariales y acceder a ellos.

- Aunque los sistemas pueden variar en complejidad de una organización a otra, siempre tienen algunas características comunes: procesos internos, directivas, roles definidos, métricas y estándares de conformidad.

- El objetivo del sistema es ayudar a las personas a utilizar de manera segura y eficaz las grandes cantidades de datos generados por las empresas hoy en día.

https://www.microsoft.com/es-cl/security/business/security-101/what-is-data-governance-for-enterprise

Definiciones claves del Gobierno de Datos - Microsoft

- Marco de gobierno de datos
- Protección de la información
- Prevención de pérdida de datos
- Catalogación y detección de datos
- Clasificación de los datos
- Propiedad de los datos
- Seguridad de datos
- Soberanía de los datos y uso compartido de datos transfronterizo
- Calidad de los datos
- Administración del ciclo de vida de los datos
- Seguimiento del acceso y los derechos relativos a los datos
- Linaje de datos
- Privacidad de los datos
- Contratos de datos y administración de fuentes de confianza
- Propósito y uso ético
- Administración de datos maestros

https://www.microsoft.com/es-cl/security/business/security-101/what-is-data-governance-for-enterprise

¿Qué es el Gobierno de Datos? (Google)

- El gobierno de datos abarca todas las medidas adoptadas para que los datos sean seguros, privados y precisos y, además, estén disponibles y se puedan usar. Incluye todas las acciones que deben realizar los usuarios, los procedimientos que deben seguir y la tecnología que utilizan durante todo el ciclo de vida de los datos.

- El gobierno de datos significa fijar estándares internos (es decir, políticas de datos) que regulen cómo se recopilan, almacenan, procesan y eliminan los datos. Rige quiénes pueden acceder a qué tipos de datos y cuáles de estos están sometidos al gobierno. También implica cumplir los estándares externos que fijan las asociaciones del sector, los organismos públicos y otras partes interesadas.

https://cloud.google.com/learn/what-is-data-governance?hl=es

¿Qué es el Gobierno de Datos? (IBM)

- El gobierno de datos promueve la disponibilidad, calidad y seguridad de los datos de una organización a través de diferentes políticas y normas. Estos procesos determinan los propietarios de los datos, las medidas de seguridad de los datos y los usos previstos de los datos.El objetivo del gobierno de datos es mantener datos de alta calidad que sean seguros y de fácil acceso para obtener información empresarial más profunda.

- Los esfuerzos del big data y la transformación digital son los principales impulsores de los programas de gobierno de datos. A medida que aumenta el volumen de datos de nuevas fuentes de datos, como las tecnologías de Internet de las cosas (IoT), las organizaciones deben reconsiderar sus prácticas de gestión de datos para escalar su inteligencia empresarial. Los programas eficaces de gobierno de datos buscan mejorar la calidad de los datos, reducir los silos de datos, garantizar el cumplimiento y la seguridad, y distribuir el acceso a los datos de forma adecuada.

https://www.ibm.com/es-es/topics/data-governance

Gobernanza de Datos vs Gestión de Datos

Gobernanza de datos

Estrategia/Vinculación

La gobernanza de datos aporta un enfoque holístico para la estrategia, administración, seguridad y uso de la información.

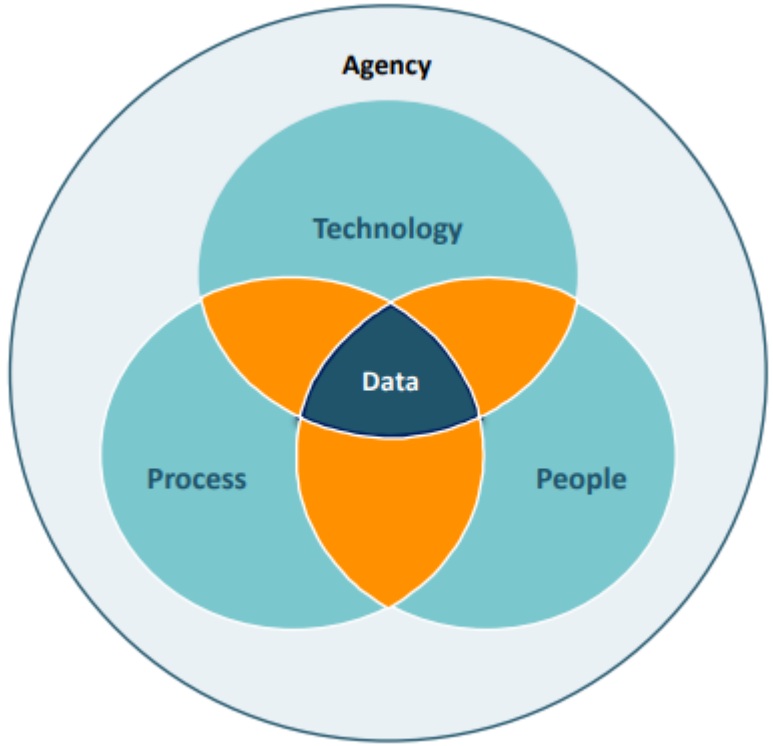
Gestión de Datos

Operación

La gestión de datos vigila todo el ciclo de vida del dato.

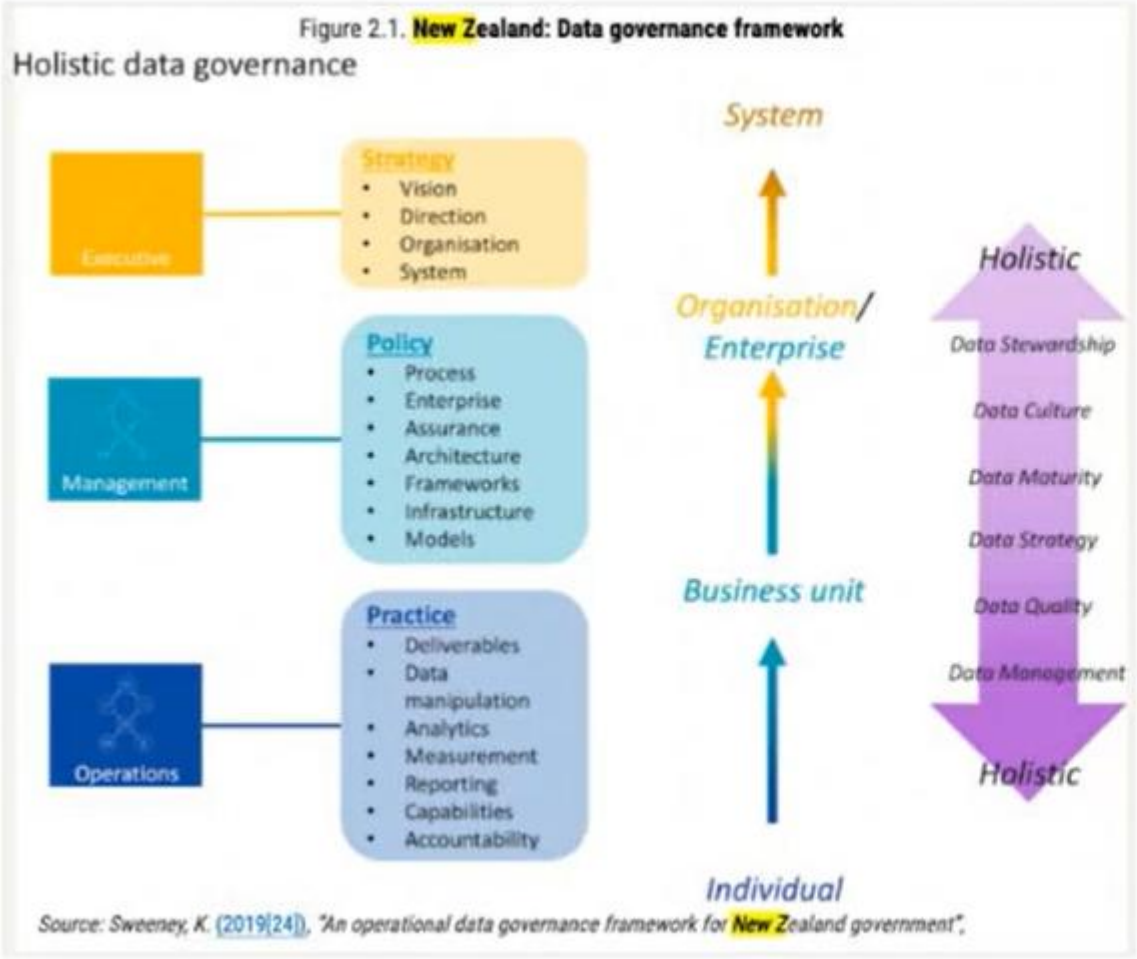
¿Por qué el Gobierno de Datos?

- Nos ayuda a Responder:
  - ¿Por qué? - Visión/Estrategia/Cumplimiento
  - ¿Qué? – Infraestructura de datos
  - ¿Quién? – Roles/Responsabilidades
  - ¿Cómo? – Buenas Prácticas/Procesos/Herramientas
  - ¿Dónde? – Procesos de Negocio/Tecnologías



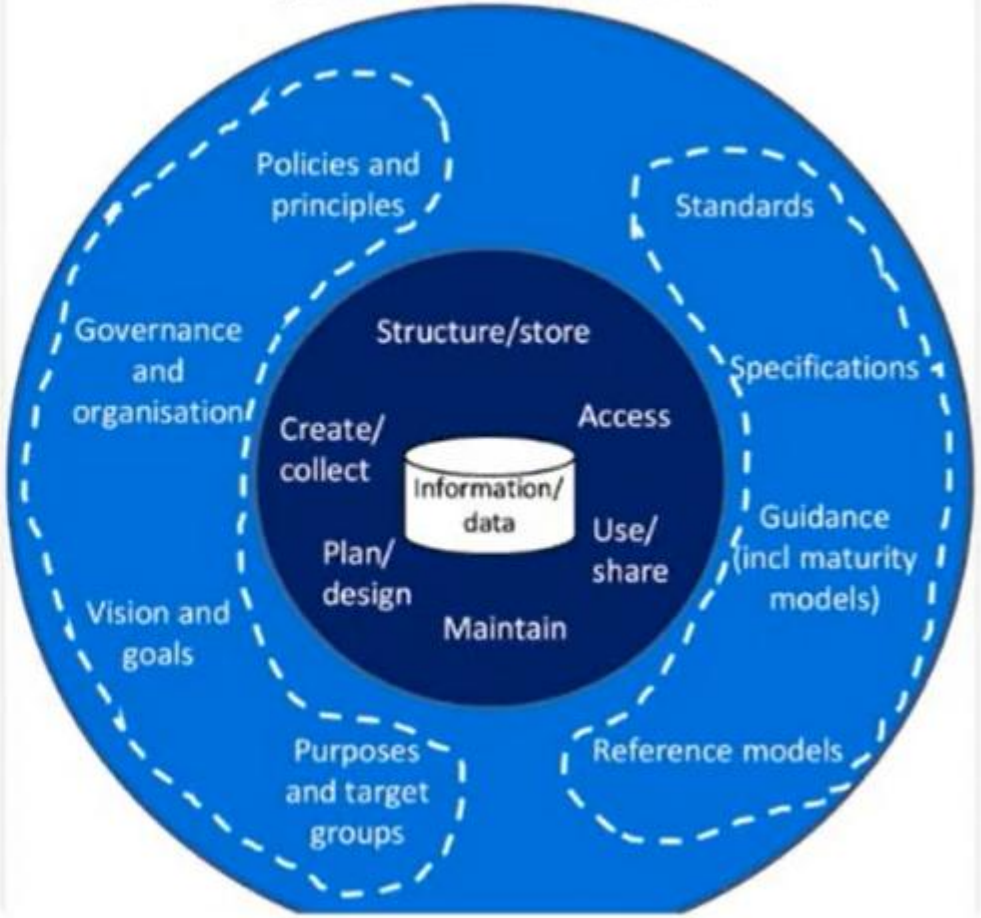
Estrategia de Datos – Gobierno de New Zeland & Norway

Figure 2.1. New Zealand: Data governance framework

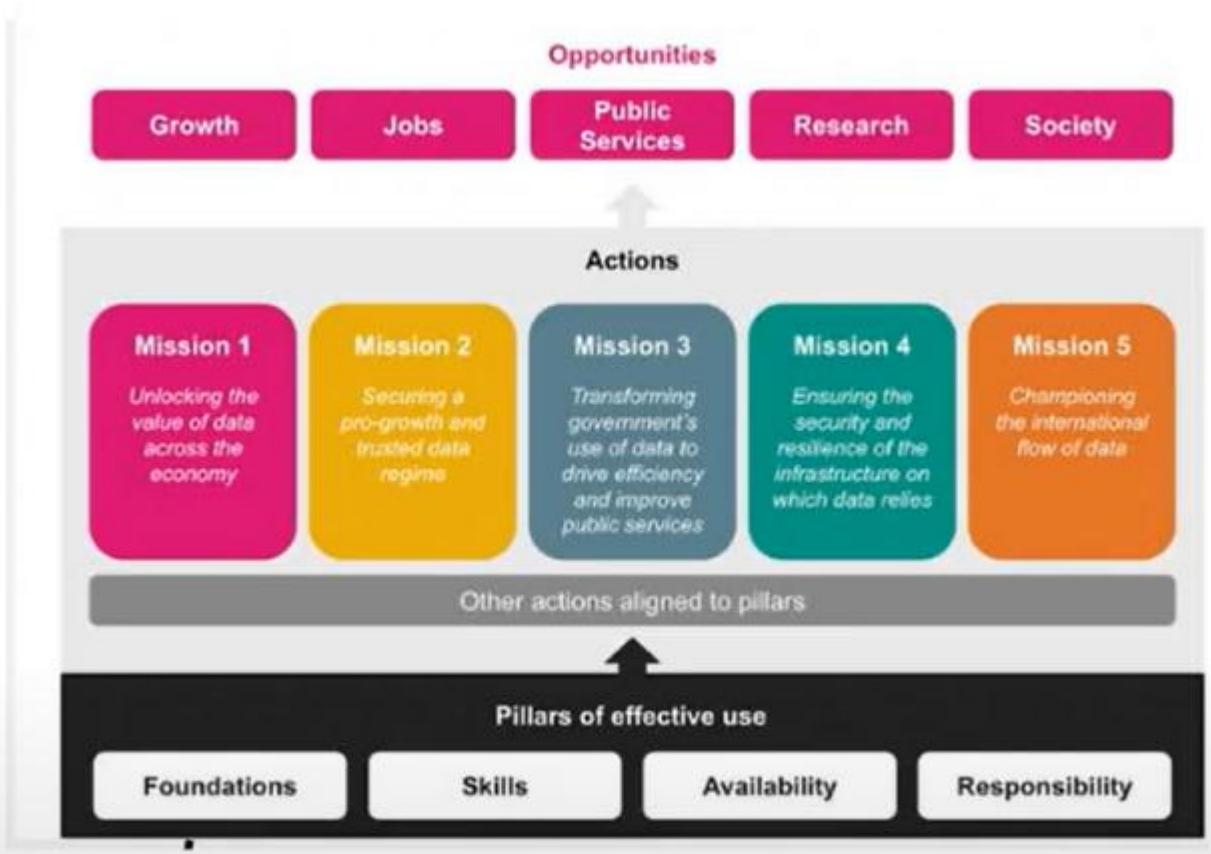


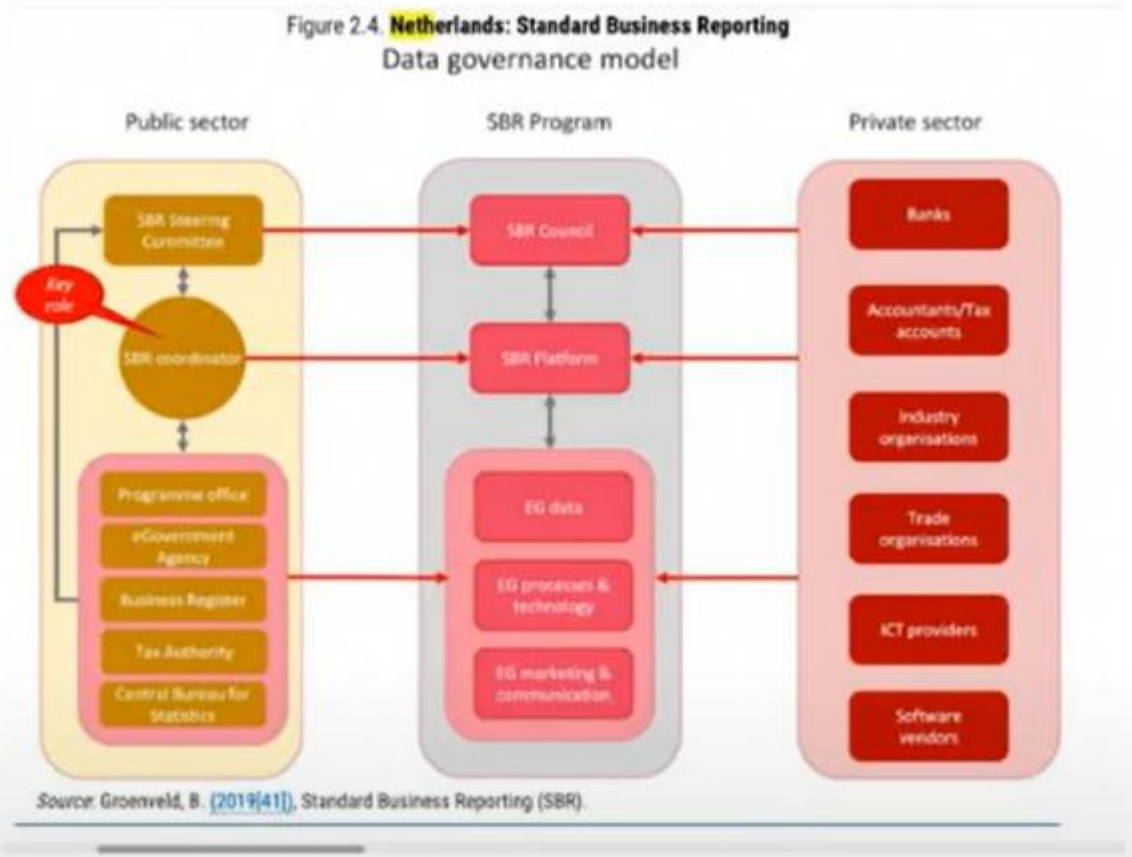
Source: Sweeney, K. (2019[24]), "An operational data governance framework for New Zealand government".

Figure 2.2. Norway: Information governance model

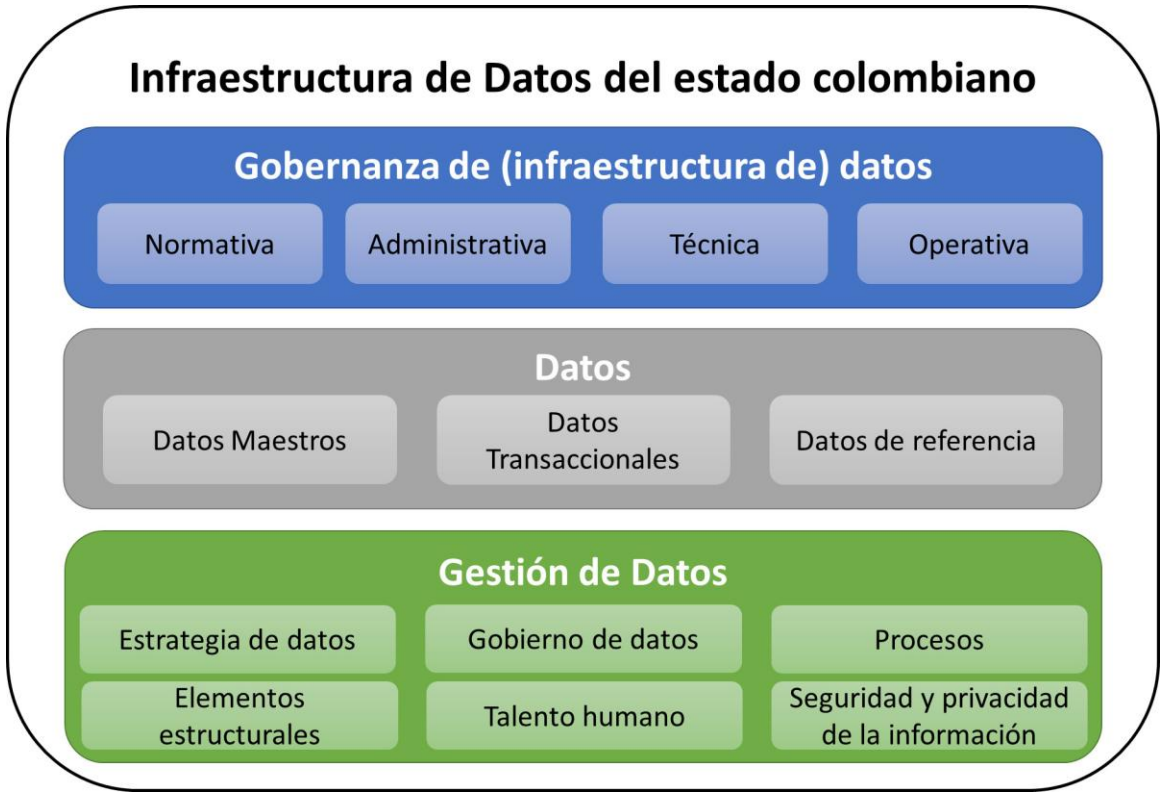


Estrategia de Datos – Gobierno de UK & Netherlands



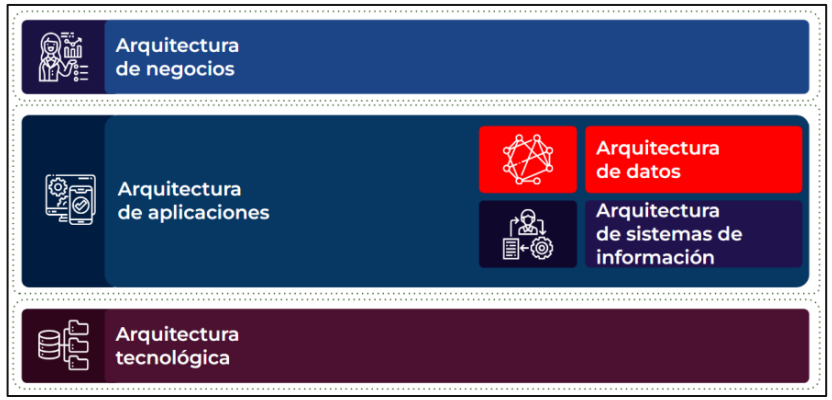


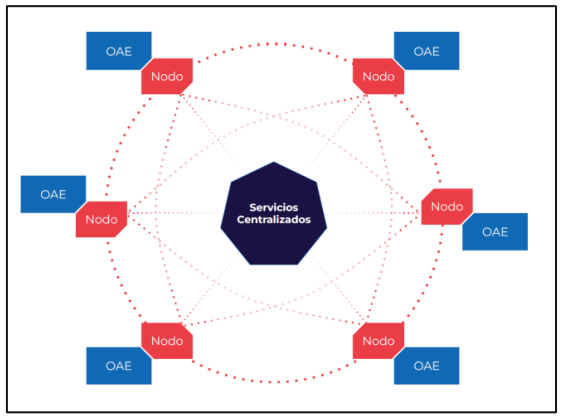
Estrategia de Datos – Gobierno de Colombia



https://infraestructuradatos.gov.co/798/w3-propertyvalue-378989.html

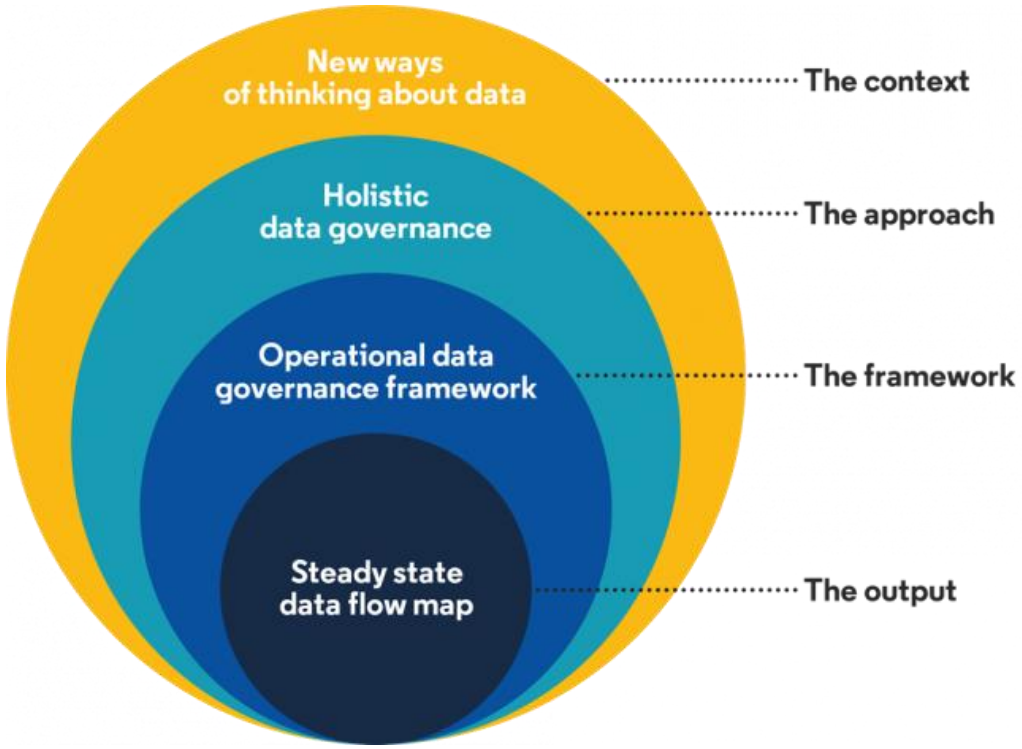
Estrategia de Datos – Gobierno de Chile

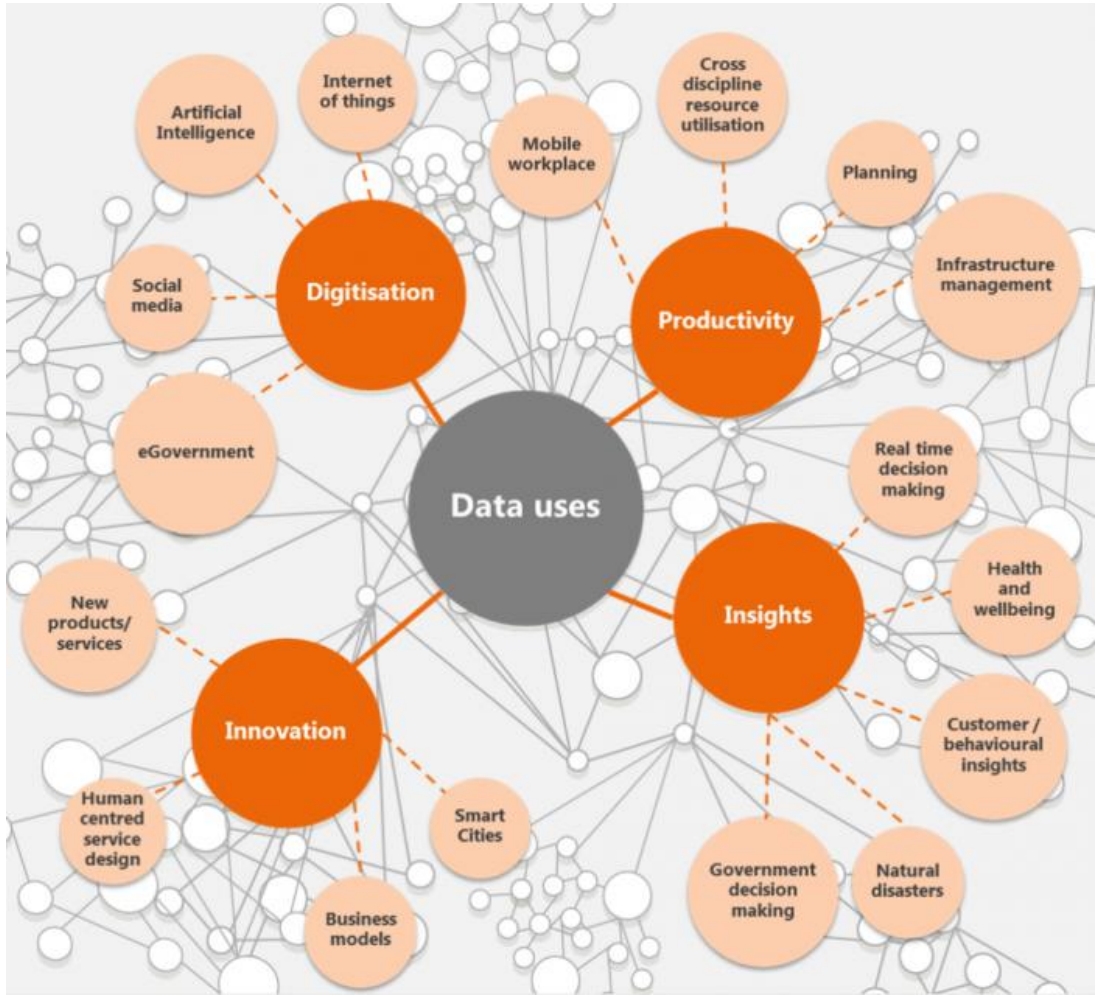




[Presentación gobierno de Datos . Chile]

La visión del Gobierno de New Zeland



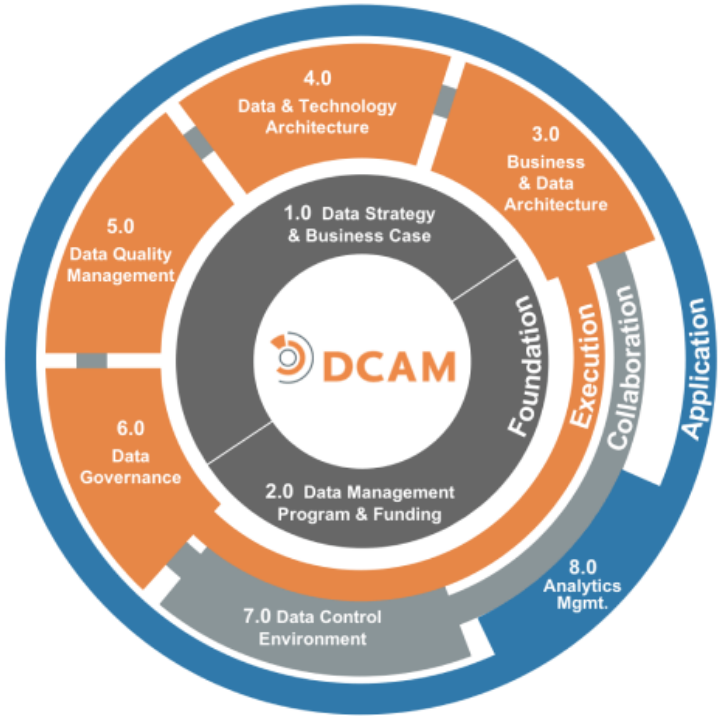


Componente y procesos claves

Modelo DAMA

ÁREA	PROCESO
DM	DM.1. Gestión de Requisitos de Datos
	DM.2. Gestión de la Infraestructura Tecnológica
	DM.3. Gestión de Datos Históricos
	DM.4. Gestión de la Seguridad de Datos
	DM.5. Gestión de la Configuración de Datos
	DM.6. Gestión de Datos Maestros y de Referencia
	DM.7. Arquitectura y Diseño de Datos
	DM.8. Establecimiento de Fuentes y Destinos de Datos
	DM.9. Integración de Datos
DQM	DQM.1. Planificación de Calidad de Datos
	DQM.2. Monitorización y Control de Calidad de Datos
	DQM.3. Aseguramiento de Calidad de datos
	DQM.4. Mejora de Calidad de Datos
DG	DG.1. Establecimiento de Estrategias de Datos
	DG.2. Gestión del Ciclo de Vida de los Datos
	DG.3. Gestión del Valor de los Datos
	DG.4. Establecimiento de Estándares, Políticas y Buenas Prácticas
	DG.5. Gestión de Recursos Humanos
	DG.6. Gestión de Recursos Financieros
	DG.7. Monitorización de las Estrategias Organizacionales de Datos
	DG.8. Gestión de Cambios en las Estrategias de Datos

Modelo MDMA



Modelo DCAM

Estándares de Gobierno de Datos

Estándares de Gobierno de Datos

- ✓DAMA – DMBook
- ✓Modelo Alarcos de Madurez de Datos (MAMD)
- ✓DCAM: Data Management Capability Assessment Model
- ✓COBIT 2019

DAMA - DMBook

https://www.dama.org/

Organismo internacional profesional con capítulos locales

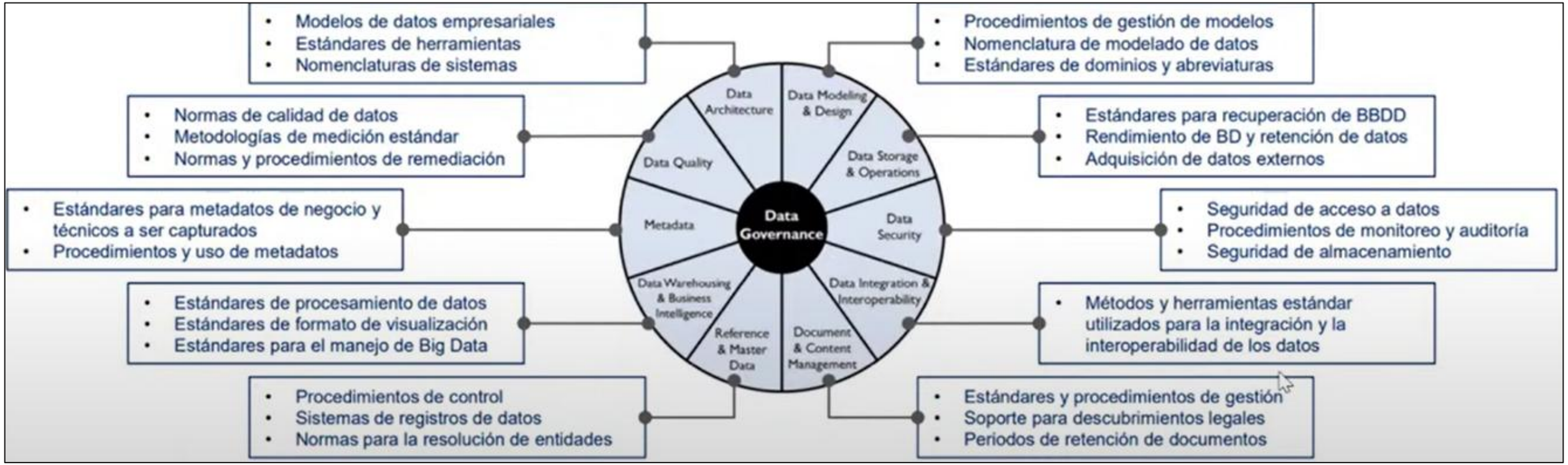
Modelo General de Referencia

Cada función se define en detalle en el libro de referencia DMBook 2 (2017)

Contexto general:

- El framework se define en DMBook 2.
- Ofrece certificaciones asociadas
- Se basa en la implementación de cada función del modelo
- Agnóstico tecnológicamente
- Requiere una adecuación a contextos de IA.
- Complejo de implementar en su completitud, pero funcional si toma las actividades claves.
- Es el más importante modelo de referencia en uso y aplicación actualmente.

DAMA - DMBook



✓Una visión más detallada del marco de referencia.

Metodología MAMD: El Modelo Alarcos de mejora de datos

MAMD
Modelo Alarcos de Mejora Datos v.3.0

https://dqteam.es/mamd/

Spin off de Universidad de la Mancha y grupo Alarcos

Modelo General de Referencia

ÁREA	PROCESO
DM	DM.1. Gestión de Requisitos de Datos
	DM.2. Gestión de la Infraestructura Tecnológica
	DM.3. Gestión de Datos Históricos
	DM.4. Gestión de la Seguridad de Datos
	DM.5. Gestión de la Configuración de Datos
	DM.6. Gestión de Datos Maestros y de Referencia
	DM.7. Arquitectura y Diseño de Datos
	DM.8. Establecimiento de Fuentes y Destinos de Datos
	DM.9. Integración de Datos
DQM	DQM.1. Planificación de Calidad de Datos
	DQM.2. Monitorización y Control de Calidad de Datos
	DQM.3. Aseguramiento de Calidad de datos
	DQM.4. Mejora de Calidad de Datos
DG	DG.1. Establecimiento de Estrategias de Datos
	DG.2. Gestión del Ciclo de Vida de los Datos
	DG.3. Gestión del Valor de los Datos
	DG.4. Establecimiento de Estándares, Políticas y Buenas Prácticas
	DG.5. Gestión de Recursos Humanos
	DG.6. Gestión de Recursos Financieros
	DG.7. Monitorización de las Estrategias Organizacionales de Datos
	DG.8. Gestión de Cambios en las Estrategias de Datos

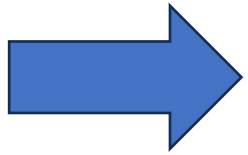
Cada función se define en detalle en metodología de referencia

Contexto general:

- Es muy funcional
- Se integra con conjunto de normas ISO de calidad de datos y gobierno de datos
- Agnóstico tecnológicamente
- La estructura de procesos es muy lógica.
- Posee la clasificación de madurez de los procesos en torno a capacidades
- Posee mucha investigación científica
- Carece de un alto nivel de adopción

Metodología MAMD: El Modelo Alarcos de mejora de datos

ÁREA	PROCESO
DM	DM.1. Gestión de Requisitos de Datos
	DM.2. Gestión de la Infraestructura Tecnológica
	DM.3. Gestión de Datos Históricos
	DM.4. Gestión de la Seguridad de Datos
	DM.5. Gestión de la Configuración de Datos
	DM.6. Gestión de Datos Maestros y de Referencia
	DM.7. Arquitectura y Diseño de Datos
	DM.8. Establecimiento de Fuentes y Destinos de Datos
	DM.9. Integración de Datos
DQM	DQM.1. Planificación de Calidad de Datos
	DQM.2. Monitorización y Control de Calidad de Datos
	DQM.3. Aseguramiento de Calidad de datos
	DQM.4. Mejora de Calidad de Datos
DG	DG.1. Establecimiento de Estrategias de Datos
	DG.2. Gestión del Ciclo de Vida de los Datos
	DG.3. Gestión del Valor de los Datos
	DG.4. Establecimiento de Estándares, Políticas y Buenas Prácticas
	DG.5. Gestión de Recursos Humanos
	DG.6. Gestión de Recursos Financieros
	DG.7. Monitorización de las Estrategias Organizacionales de Datos
	DG.8. Gestión de Cambios en las Estrategias de Datos



Nivel de Madurez	Proceso
1	DM.01. Procesamiento de datos
	DM.02. Gestión de infraestructura tecnológica
2	DM.03. Gestión de requisitos de datos
	DM.04. Gestión de requisitos de datos
	DM.05. Gestión de seguridad de datos
	DM.06. Gestión de datos históricos
	DQM.02. Control y monitorización de calidad de datos
	DG.01. Establecimiento de estándares, políticas, buenas prácticas y procedimientos
3	DM.07. Gestión de arquitectura y diseño de datos
	DM.08. Gestión de fuentes y destinos de datos
	DM.09. Gestión de integración de datos
	DM.10. Gestión de datos maestros
	DQM.01. Planificación de calidad de datos
	DG.02. Establecimiento de estrategias de datos
	DG.03. Establecimiento del ciclo de vida de los datos
	DG.04. Gestión de recursos humanos
	DG.05. Establecimiento de estructuras organizacionales
4	DQM.3. Aseguramiento de calidad de datos
	DG.6. Gestión de recursos financieros
5	DQM.4. Mejora de calidad de datos

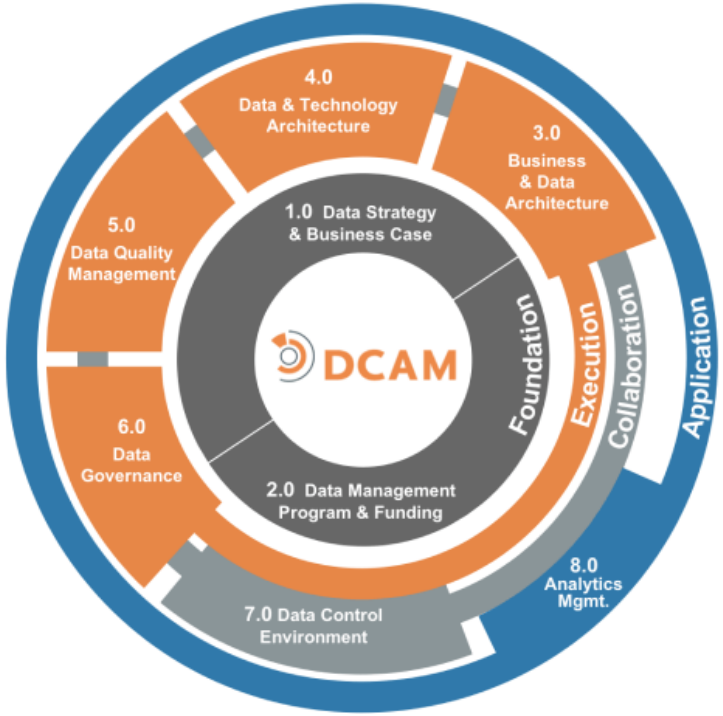
DCAM: Data Management Capability Assessment Model

EDMCouncil

https://edmcouncil.org/

Organismos privado que propia y fortalece el desarrollo del modelo y sus capacidades asociadas.

Modelo General de Referencia



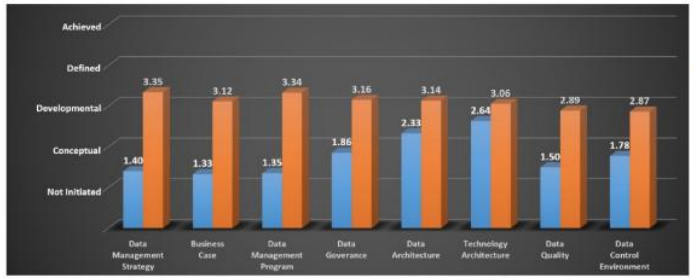
Cada función se define en detalle en metodología de referencia

Contexto general:

- Es muy funcional y práctico
- Incorpora el uso de casos de negocio
- Facilita el patrocinio del programa
- Define menos funciones que DAMA
- Evalúa la madurez de los procesos de manera detallada (instrumentos asociados)
- Incluye el gobierno de algoritmos, analítica, entre otros.
- Alto potencial de aumento en se uso
- La versión es español es reciente.

DCAM: Data Management Capability Assessment Model

1	2	3	4	5	6
No iniciado	**Conceptual**	**En Desarrollo**	**Definido**	**Logrado**	**Mejorado**
No ejecutado	Pasos iniciales de planificación	Compromiso continuo	Definido y verificado	Adoptado y aplicado	Integrado y optimizado
Actividades ad hoc llevadas a cabo por voluntarios No hay formalización No hay conciencia de la necesidad o existencia de esta competencia.	Se reconoce la necesidad de competencia Se discuten los problemas Existe una cierta conciencia de que en alguna estructura podrían existir habilidades.	Se definen los principales grupos de interés Los flujos de trabajo están definidos y las reuniones están en curso El progreso es visible a partir de los artefactos producidos	Totalmente verificado por todas las partes interesadas (negocio, tecnología y datos) Responsabilidades definidas y asignadas Políticas y normas definidas	La competencia es operativa y está respaldada por evidencia La competencia es ejecutiva, verificable y medible Se reconocen los beneficios y se mide su valor añadido	La experiencia está totalmente integrada en la cultura operativa de la empresa La competencia se evalúa y verifica regularmente La competencia está sujeta a un proceso de mejora continua avalado por la evidencia
No está en los objetivos del negocio. A nivel general, la gestión de datos no se ha pensado realmente, pero alguna actividad podría ser llevada a cabo por el negocio de forma aleatoria.	No hay fondos o recursos disponibles para la gestión de datos, pero se está empezando a pensar en el tema. Se organizan talleres y reuniones de lluvia de ideas para pensar en cómo seguir la Gestión de Datos.	Las actividades están en curso. Hay un compromiso con el desarrollo de la capacidad. Se definen proyectos y objetivos. Todavía queda mucho trabajo por hacer, pero hay un camino por recorrer para implementar la Gestión de Datos.	La capacidad percibida como necesaria está completamente desarrollada. Se ha definido el modelo futuro y cómo se implementará. Existe la aprobación de todas las partes interesadas principales.	La capacidad es operativa. Toda la organización es consciente de ello. Las actividades relacionadas con la Gestión de Datos se llevan a cabo y se integran en los procesos de negocio. No hay mucho trabajo por hacer con respecto a esta capacidad.	La capacidad es una buena práctica que puede ser un modelo a seguir para otras empresas. La capacidad se comprueba periódicamente con el objetivo de mejorarla sistemáticamente.



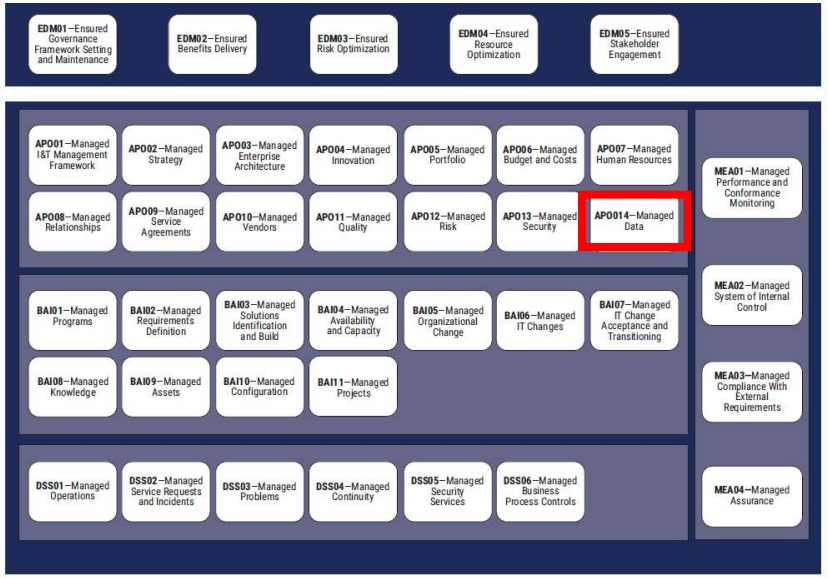
COBIT 2019: Proceso de Datos Gestionados (APO 14)

Modelo General de Referencia

COBIT 2019

https://isaca.org/

Framework creado por el Organismo internacional profesional ISACA el cual posee capítulos locales
.



Dentro de sus 40 procesos define el Proceso de Gobierno de Datos.

Contexto general:

- Solo define un proceso relacionado
- Se basa en las mejores prácticas
- Posibilita una integración con otros procesos claves de gobierno y gestión de IT
- Define muy bien que hacer (los objetivo), pero no el como.
- Permite evaluar la madurez del proceso, pero de manera muy atómica.
- Buen punto de referencia para saber que hacer, el cual se debe complementar con otros marcos para su implementación

COBIT 2019: Proceso de Datos Gestionados (APO 14)

B. Componente: Estructuras organizativas								
Práctica clave de gestión	Director de riesgos	Director de TI	Director de tecnologías digitales	Comité de riesgos empresariales	Director de seguridad de la información	Función de gestión de datos	Asesor legal	
APO14.01 Definir y comunicar la estrategia y los roles y responsabilidades de la gestión de datos de la organización.	R	A	R		R	R		
APO14.02 Definir y mantener un glosario empresarial consistente.	R	A	R		R	R		
APO14.03 Establecer los procesos y la infraestructura para la gestión de metadatos.	R	A	R		R	R		
APO14.04 Definir una estrategia de calidad de los datos.	R	A	R		R	R		
APO14.05 Establecer las metodologías, procesos y herramientas para la creación de perfiles de datos.	R	A	R		R	R		
APO14.06 Asegurar un enfoque de evaluación de la calidad de los datos.	R	A	R		R	R		
APO14.07 Definir la estrategia de depuración de datos.	R	A	R		R	R		
APO14.08 Gestionar el ciclo de vida de los activos de datos.	R	A	R	R	R	R	R	
APO14.09 Soportar el archivado y retención de datos.	R	A	R	R	R	R	R	
APO14.10 Gestionar los acuerdos de toma de copias de seguridad y restauración de datos.	R	A	R		R	R	R	

A. Componente: Proceso *(cont.)*	
Práctica de gestión	**Métricas modelo**
APO14.04 Definir una estrategia de calidad de los datos. Definir una estrategia integrada en toda la organización para lograr y mantener el nivel de calidad de datos (como la complejidad, integridad, precisión, integridad, exactitud, completitud, validez, trazabilidad y oportunidad) requerido para respaldar las metas y objetivos empresariales.	a. Número de esfuerzos de mejora de la calidad de los datos identificados y registrados en un plan secuencial b. Porcentaje de partes interesadas satisfechas con la calidad de los datos

Actividades	Nivel de capacidad
1. Definir una estrategia de calidad de los datos en colaboración con las partes interesadas empresariales y tecnológicas, aprobada y gestionada por la dirección ejecutiva. La estrategia debería favorecer pasar del estado actual al objetivo. También debe alinearse de forma explícita con los objetivos empresariales y la estrategia de gestión de datos de la organización.	3
2. Asegurar que la estrategia de calidad de los datos se respete en toda la organización y venga acompañada de las políticas, procesos y directrices correspondientes.	
3. Afianzar las políticas, procesos y gobierno de la estrategia de calidad de los datos durante todo el ciclo de vida de los datos. Exigir los procesos correspondientes en la metodología del ciclo de vida de desarrollo del sistema.	
4. Desarrollar, monitorizar y mantener un plan secuencial para el esfuerzo de mejora de la calidad de los datos en toda la organización.	
5. Para evaluar el progreso, supervisar los planes a fin de cumplir las metas y objetivos de la estrategia de calidad de los datos.	4
6. Recopilar sistemáticamente los informes de las partes interesadas sobre problemas de calidad de los datos. Incluir sus expectativas para mejorar la calidad de los datos en la estrategia de calidad de los datos. Medirlos y monitorizarlos.	

Integración del GD con Privacidad y Seguridad

Pilares de Integración – Mirada Estrategica

1. 🧩 **Consolidación del gobierno corporativo digital**

   Integrar estas tres disciplinas eleva la gestión de datos a un **nivel de gobernanza estratégica**, donde la información se administra con criterios de **valor, riesgo y cumplimiento**, como cualquier otro activo crítico del negocio.

   → Se convierte en una **función de gobierno corporativo**, no solo tecnológica.

2. 🔷 **Base para la toma de decisiones confiables y sostenibles**

   El Gobierno de Datos garantiza **integridad y calidad**; la Seguridad y la Privacidad garantizan **legitimidad y protección**.

   Su articulación asegura que las **decisiones estratégicas se basen en datos confiables, verificables y éticamente gestionados**, evitando errores regulatorios o reputacionales.

3. 🧠 **Gestión integral del riesgo digital y reputacional**

   Al alinear riesgos de información, cumplimiento y privacidad, la organización obtiene una **visión 360° del riesgo**, permitiendo priorizar inversiones, anticipar contingencias y fortalecer su **resiliencia institucional** ante incidentes o fiscalizaciones.

4. 🏗️ **Arquitectura organizacional basada en confianza**

   La convergencia entre gobierno, seguridad y privacidad crea un marco de **"confianza por diseño"** (trust by design), donde cada proceso, tecnología o dato opera dentro de **límites definidos y auditables**, fortaleciendo la relación con clientes, reguladores y socios estratégicos.

5. 📈 **Alineamiento entre estrategia digital y cumplimiento regulatorio**

   La integración permite que la **innovación tecnológica y la adopción de IA, cloud o big data** avancen bajo control y trazabilidad.

   Así, el crecimiento digital no compromete el cumplimiento: lo **potencia y legitima** ante reguladores y stakeholders.

6. ⚖️ **Sinergia entre eficiencia operativa y control**

   Articular los tres sistemas evita duplicidades, mejora la coordinación interdepartamental (TI, Legal, Riesgos, Cumplimiento) y habilita **modelos de gestión más ágiles**, con control embebido en los procesos.

   → La eficiencia no se opone al control, **se convierte en su resultado natural.**

7. 🌎 **Reputación y liderazgo institucional en confianza digital**

   En mercados donde la confianza es un activo, una organización con un gobierno de datos alineado a seguridad y privacidad **proyecta credibilidad, transparencia y madurez.**

   Esto fortalece su posicionamiento ante clientes, autoridades y socios internacionales.

8. 🚀 **Fundamento para la innovación ética y la inteligencia artificial responsable**

   La integración de estas disciplinas proporciona las **condiciones habilitantes** para el uso responsable de tecnologías emergentes, asegurando **ética algorítmica, gobernanza de datos y cumplimiento proactivo.**

   → Es la **plataforma estratégica de la economía basada en datos.**

Pilares de Integración – Mirada Táctica

1. 🧱 **Estandarización de políticas y marcos de control**

   Integrar los tres sistemas permite desarrollar un **marco normativo unificado**, donde las políticas de datos, seguridad y privacidad compartan lenguaje, estructura y objetivos.

   → Resultado: documentos coherentes, sin contradicciones, más fáciles de auditar y comunicar.

2. 🧩 **Matriz integrada de riesgos y controles**

   Se consolida una **única matriz de riesgos del dato**, donde cada amenaza tiene su correlato en controles de gobernanza (DAMA), seguridad (ISO 27001) y privacidad (ISO 27701).

   → Resultado: priorización clara, mitigaciones coordinadas y trazabilidad total.

3. 🔍 **Catálogo maestro de datos y activos de información**

   Un **inventario común** que identifica los datos, sus dueños, ubicaciones, niveles de criticidad y requisitos de protección.

   → Resultado: control granular sobre qué se protege, quién lo usa y bajo qué regulación.

4. 🔒 **Procesos sincronizados de gestión de acceso y privilegios**

   Se alinea el **rol del Data Owner** con los procesos de control de acceso del SGSI y las exigencias de minimización del PIMS.

   → Resultado: asignación de accesos basada en necesidad y legitimidad del tratamiento, con evidencias auditables.

5. 🧠 **Integración del ciclo de vida del dato en procesos operativos**

   Cada área aplica el mismo ciclo: **creación → clasificación → uso → retención → eliminación**, acompañado de registros automáticos.

   → Resultado: trazabilidad operativa, cumplimiento automático y reducción de fuga o retención indebida de información.

6. 📈 **Tablero de gestión integrado (Data–Security–Privacy Dashboard)**

   Indicadores comunes: incidentes, brechas, calidad de datos, cumplimiento de derechos, cumplimiento ISO.

   → Resultado: visibilidad en tiempo real para el Comité de Riesgos y toma de decisiones basada en evidencia.

7. 🤝 **Coordinación entre roles clave**

   Establecer un **Comité de Gobierno de Datos, Seguridad y Privacidad**, con representantes del CISO, DPO, Data Owner y Riesgos.

   → Resultado: decisiones conjuntas, priorización de inversiones, gestión proactiva de incidentes y cumplimiento integrado.

8. 🧭 **Integración en auditorías y evaluaciones de madurez**

   Los programas de auditoría y autoevaluación combinan los controles de **DAMA, ISO 27001 y 27701**, evaluando madurez en gestión de datos, seguridad y privacidad de forma conjunta.

   → Resultado: visión completa del nivel de madurez institucional y roadmap de mejora coherente.

Pilares de Integración – Mirada Operativa

1. 🧱 **Estandarización de políticas y marcos de control**

   Integrar los tres sistemas permite desarrollar un **marco normativo unificado**, donde las políticas de datos, seguridad y privacidad compartan lenguaje, estructura y objetivos.

   → Resultado: documentos coherentes, sin contradicciones, más fáciles de auditar y comunicar.

2. 🧩 **Matriz integrada de riesgos y controles**

   Se consolida una **única matriz de riesgos del dato**, donde cada amenaza tiene su correlato en controles de gobernanza (DAMA), seguridad (ISO 27001) y privacidad (ISO 27701).

   → Resultado: priorización clara, mitigaciones coordinadas y trazabilidad total.

3. 🔍 **Catálogo maestro de datos y activos de información**

   Un **inventario común** que identifica los datos, sus dueños, ubicaciones, niveles de criticidad y requisitos de protección.

   → Resultado: control granular sobre qué se protege, quién lo usa y bajo qué regulación.

4. 🔒 **Procesos sincronizados de gestión de acceso y privilegios**

   Se alinea el **rol del Data Owner** con los procesos de control de acceso del SGSI y las exigencias de minimización del PIMS.

   → Resultado: asignación de accesos basada en necesidad y legitimidad del tratamiento, con evidencias auditables.

5. 🧠 **Integración del ciclo de vida del dato en procesos operativos**

   Cada área aplica el mismo ciclo: **creación → clasificación → uso → retención → eliminación**, acompañado de registros automáticos.

   → Resultado: trazabilidad operativa, cumplimiento automático y reducción de fuga o retención indebida de información.

6. 📈 **Tablero de gestión integrado (Data–Security–Privacy Dashboard)**

   Indicadores comunes: incidentes, brechas, calidad de datos, cumplimiento de derechos, cumplimiento ISO.

   → Resultado: visibilidad en tiempo real para el Comité de Riesgos y toma de decisiones basada en evidencia.

7. 🤝 **Coordinación entre roles clave**

   Establecer un **Comité de Gobierno de Datos, Seguridad y Privacidad**, con representantes del CISO, DPO, Data Owner y Riesgos.

   → Resultado: decisiones conjuntas, priorización de inversiones, gestión proactiva de incidentes y cumplimiento integrado.

8. 🧭 **Integración en auditorías y evaluaciones de madurez**

   Los programas de auditoría y autoevaluación combinan los controles de **DAMA, ISO 27001 y 27701**, evaluando madurez en gestión de datos, seguridad y privacidad de forma conjunta.

   → Resultado: visión completa del nivel de madurez institucional y roadmap de mejora coherente.

Pilares de Integración del Gobierno de Datos.

Pilar / Dimensión	Gobierno de Datos (DAMA-DMBOK 2)	Seguridad de la Información (ISO 27001 / 27002)	Privacidad y Protección de Datos (ISO 27701 / RGPD)	Similitudes y Puntos de Integración
🏛 **Marco y estructura de gestión**	Define un **Data Governance Framework** con dominios (arquitectura, metadatos, calidad, seguridad, datos maestros) y componentes de gobierno, gestión y valor.	Establece un **SGSI (Sistema de Gestión de Seguridad de la Información)** basado en PDCA y la estructura HLS de las normas ISO.	Extiende el SGSI hacia un **PIMS (Privacy Information Management System)** incorporando controles de privacidad y cumplimiento RGPD.	Los tres son **sistemas de gestión certificables**, compatibles y basados en **mejora continua**. Pueden coexistir bajo un marco único de gobernanza digital.
👥 **Roles y responsabilidades**	Define **Data Owner, Data Steward, Data Custodian, Data Architect**, con funciones sobre calidad, uso y linaje.	Define **CISO**, responsables de activos, custodios y comité de seguridad.	Define **DPO**, responsables y encargados del tratamiento, y titulares de datos.	Comparten el principio de **propiedad, custodia y rendición de cuentas (accountability)**. Los roles se complementan: el Data Owner y el DPO coinciden en la responsabilidad sobre el ciclo de vida del dato.
🎯 **Gestión de riesgos**	Analiza riesgos de calidad, disponibilidad e integridad de los datos, y su uso indebido.	Evalúa riesgos sobre **confidencialidad, integridad y disponibilidad (CIA)**.	Evalúa riesgos sobre **derechos y libertades** de las personas (DPIA).	Todos siguen un **modelo sistemático de análisis y tratamiento de riesgos** con base en impacto y probabilidad. Permite construir una **matriz de riesgos unificada** entre datos, seguridad y privacidad.
🧱 **Políticas y procedimientos**	Políticas de gobierno, calidad, arquitectura y seguridad del dato.	Políticas de seguridad: control de acceso, gestión de activos, continuidad, criptografía.	Políticas de privacidad: consentimiento, minimización, retención, transparencia.	Los tres requieren **documentos formales aprobados por la alta dirección**, difundidos y revisados periódicamente. Pueden integrarse en una **Política Corporativa de Gobierno, Seguridad y Privacidad de Datos**.
🔄 **Ciclo de vida del dato**	Establece fases: **creación → uso → almacenamiento → retención → eliminación**, con linaje y trazabilidad.	Protege la información en todas las etapas del ciclo de vida.	Aplica principios de **finalidad, limitación y minimización** del tratamiento.	Comparten un enfoque **basado en procesos y trazabilidad**, garantizando control de acceso, registro y eliminación segura.
🔍 **Clasificación y etiquetado**	Clasifica datos según **dominio, criticidad y contexto**.	Clasifica información según **nivel de confidencialidad** (pública, interna, restringida, confidencial).	Clasifica por **categorías de datos personales** (sensibles, financieros, biométricos).	Todos requieren **inventarios y catálogos de datos** como base de controles. El catálogo de activos del SGSI puede actuar como **catálogo maestro de Gobierno de Datos**.
🌐 **Integración con la estrategia corporativa**	Alinea el uso del dato con la **estrategia organizacional** y la **toma de decisiones basada en datos**.	Integra la seguridad con la **continuidad de negocio**, gestión de proveedores y gobierno corporativo.	Vincula la privacidad con la **confianza digital**, reputación y cumplimiento global.	Todos buscan **crear valor a partir del dato seguro y confiable**. COBIT 2019 (APO14) sirve como **marco de gobernanza común** para articular los tres sistemas.

Integración General

1. Inventario y clasificación de datos

Principio: Mantener un registro exhaustivo de activos de datos, categorizándolos según tipo, sensibilidad y uso legítimo.

Controles asociados:

DAMA: *Data Architecture, Metadata Management*

ISO 27001: A.5.9, A.5.12

ISO 27701: A.7.2.4 Inventario de datos personales y A.7.3.2 Identificación de categorías de PII

ISO 29100: Minimización y limitación de propósito

Ley de Protección de Datos: arts. 5–6 (finalidad y proporcionalidad)

Ley de Ciberseguridad: gestión de activos críticos

Resultado: control de exposición y trazabilidad completa de los conjuntos de datos.

2. Propiedad, custodia y responsabilidad

Principio: Designar responsables y custodios para cada dominio de datos.

Controles asociados:

DAMA: *Data Stewardship, Governance Oversight*

ISO 27001: Cl. 5.3 Roles y responsabilidades

ISO 27701: A.7.3.1 Responsabilidad del responsable y encargado del tratamiento

ISO 29100: Responsabilidad (accountability)

Ley de Protección de Datos: art. 4

Ley de Ciberseguridad: responsables institucionales de seguridad

Resultado: cadena de rendición de cuentas documentada y verificable.

3. Política integrada de gobierno, seguridad y privacidad

Principio: Consolidar una política corporativa que alinee los objetivos de valor, riesgo y cumplimiento.

Controles asociados:

DAMA: *Governance Framework*

ISO 27001: Cl. 5.2 Política de Seguridad

ISO 27701: Cl. 5.2 Política de Privacidad

ISO 29100: Transparencia y responsabilidad

Ley de Ciberseguridad: art. 15 (Política de Seguridad Organizacional)

Resultado: coherencia normativa y dirección única de gobernanza.

4. Ciclo de vida del dato

Principio: Gestionar la creación, uso, retención y eliminación segura de datos.

Controles asociados:

DAMA: *Data Lifecycle Management*

ISO 27001: A.8.10 Eliminación de información

ISO 27701: A.7.4.9 Retención y supresión de datos personales

ISO 29100: Limitación de retención

Ley de Protección de Datos: art. 11

Resultado: cumplimiento verificable del principio de finalidad y vida útil del dato.

Integración General

1. Inventario y clasificación de datos

Principio: Mantener un registro exhaustivo de activos de datos, categorizándolos según tipo, sensibilidad y uso legítimo.

Controles asociados:

DAMA: *Data Architecture, Metadata Management*

ISO 27001: A.5.9, A.5.12

ISO 27701: A.7.2.4 Inventario de datos personales y A.7.3.2 Identificación de categorías de PII

ISO 29100: Minimización y limitación de propósito

Ley de Protección de Datos: arts. 5–6 (finalidad y proporcionalidad)

Ley de Ciberseguridad: gestión de activos críticos

Resultado: control de exposición y trazabilidad completa de los conjuntos de datos.

2. Propiedad, custodia y responsabilidad

Principio: Designar responsables y custodios para cada dominio de datos.

Controles asociados:

DAMA: *Data Stewardship, Governance Oversight*

ISO 27001: Cl. 5.3 Roles y responsabilidades

ISO 27701: A.7.3.1 Responsabilidad del responsable y encargado del tratamiento

ISO 29100: Responsabilidad (accountability)

Ley de Protección de Datos: art. 4

Ley de Ciberseguridad: responsables institucionales de seguridad

Resultado: cadena de rendición de cuentas documentada y verificable.

3. Política integrada de gobierno, seguridad y privacidad

Principio: Consolidar una política corporativa que alinee los objetivos de valor, riesgo y cumplimiento.

Controles asociados:

DAMA: *Governance Framework*

ISO 27001: Cl. 5.2 Política de Seguridad

ISO 27701: Cl. 5.2 Política de Privacidad

ISO 29100: Transparencia y responsabilidad

Ley de Ciberseguridad: art. 15 (Política de Seguridad Organizacional)

Resultado: coherencia normativa y dirección única de gobernanza.

4. Ciclo de vida del dato

Principio: Gestionar la creación, uso, retención y eliminación segura de datos.

Controles asociados:

DAMA: *Data Lifecycle Management*

ISO 27001: A.8.10 Eliminación de información

ISO 27701: A.7.4.9 Retención y supresión de datos personales

ISO 29100: Limitación de retención

Ley de Protección de Datos: art. 11

Resultado: cumplimiento verificable del principio de finalidad y vida útil del dato.

Integración General

5. Calidad, exactitud y completitud de los datos

Principio: Asegurar que los datos sean exactos, actualizados y aptos para su propósito.

Controles asociados:

DAMA: *Data Quality Management*

ISO 27001: A.5.13 Integridad de la información

ISO 27701: A.7.4.8 Exactitud y actualización de los datos personales

ISO 29100: Calidad de datos

Ley de Protección de Datos: art. 9

Resultado: datos fiables que respaldan decisiones y cumplen requisitos legales.

6. Control de acceso basado en roles

Principio: Garantizar acceso solo a quienes lo necesitan por rol y función.

Controles asociados:

DAMA: *Security & Access Management*

ISO 27001: A.5.15–A.5.18

ISO 27701: A.7.4.6 Gestión de acceso a PII

ISO 29100: Seguridad

Ley de Ciberseguridad: art. 14

Resultado: principio de mínimo privilegio y reducción de riesgos de fuga.

7. Gestión de identidades y autenticación

Principio: Verificar identidades y asegurar la autenticación múltiple.

Controles asociados:

DAMA: *Security Operations*

ISO 27001: A.5.16 Gestión de identidades

ISO 27701: extensión de seguridad en tratamientos de PII

Ley de Ciberseguridad: autenticación robusta y multifactor

Resultado: accesos seguros y trazables a activos de datos.

8. Integridad y coherencia de la información

Principio: Evitar alteraciones no autorizadas y garantizar consistencia entre fuentes.

Controles asociados:

DAMA: *Data Quality Assurance*

ISO 27001: A.8.12

ISO 27701: A.7.4.8

Ley de Ciberseguridad: principio de integridad de los datos críticos

Resultado: datos coherentes y verificables en procesos auditor.

Integración General

9. Trazabilidad y linaje de datos

Principio: Registrar y monitorear el flujo de los datos a lo largo de su vida.

Controles asociados:

DAMA: *Metadata Management, Data Lineage*

ISO 27001: A.5.23 Registro de eventos

ISO 27701: A.7.4.10 Registro de actividades de tratamiento

ISO 29100: Transparencia

Ley de Ciberseguridad: registro obligatorio de logs e incidentes

Resultado: evidencia completa de procesos y decisiones sobre datos.

10. Gestión de incidentes y brechas

Principio: Responder a eventos que comprometan la seguridad o privacidad del dato.

Controles asociados:

DAMA: *Security Operations*

ISO 27001: A.5.24 Gestión de incidentes de seguridad

ISO 27701: A.7.5.1 Gestión de incidentes de privacidad y notificación

Ley de Protección de Datos: art. 30

Ley de Ciberseguridad: art. 21

Resultado: respuesta rápida y cumplimiento de deber de notificación.

11. Transferencia y compartición segura de información

Principio: Garantizar que toda transferencia mantenga protección equivalente.

Controles asociados:

DAMA: *Integration & Interoperability*

ISO 27001: A.5.14 Transferencia de información

ISO 27701: A.7.4.7 Transferencia internacional de PII

ISO 29100: Transparencia y consentimiento

Ley de Protección de Datos: art. 20

Resultado: intercambio seguro y auditable de información entre organizaciones.

12. Gestión de proveedores y terceros

Principio: Asegurar que los proveedores cumplan los mismos estándares de protección.

Controles asociados:

DAMA: *Governance Oversight*

ISO 27001: A.5.19

ISO 27701: A.7.2.6 Relaciones entre responsables y encargados

Ley de Ciberseguridad: evaluación de riesgos de proveedores

Resultado: contratos con obligaciones y controles alineados a riesgos.

Integración General

13. Protección criptográfica

Principio: Aplicar cifrado a datos en tránsito y reposo.

Controles asociados:

DAMA: *Security Management*

ISO 27001: A.8.24–A.8.25

ISO 27701: extensión técnica de seguridad en PII

Ley de Ciberseguridad: uso obligatorio de criptografía en información crítica

Resultado: confidencialidad garantizada en todo entorno.

14. Respaldo y recuperación

Principio: Proteger la disponibilidad de los datos mediante copias seguras.

Controles asociados:

DAMA: *Data Operations*

ISO 27001: A.8.13

ISO 27701: A.7.4.11 Restauración y respaldo de datos personales

Ley de Ciberseguridad: continuidad de servicios esenciales

Resultado: recuperación controlada y resiliencia operativa.

15. Gestión de vulnerabilidades

Principio: Identificar y corregir vulnerabilidades que puedan exponer datos.

Controles asociados:

DAMA: *Security Management*

ISO 27001: A.8.8 Gestión de vulnerabilidades

Ley de Ciberseguridad: monitoreo y reportes al CSIRT

Resultado: mitigación preventiva y menor superficie de ataque.

16. Seguridad por diseño y por defecto

Principio: Incorporar privacidad y seguridad desde la concepción del proceso.

Controles asociados:

DAMA: *Architecture Management*

ISO 27001: A.8.9 Seguridad en el desarrollo

ISO 27701: A.7.4.2 Privacidad por diseño y por defecto

ISO 29100: Privacy by Design

Ley de Protección de Datos: art. 8

Resultado: cumplimiento proactivo y reducción de riesgos en innovación digital.

Integración General

17. Gestión de configuraciones seguras

Principio: Asegurar que las plataformas de datos mantengan configuraciones controladas.

Controles asociados:

DAMA: *Operations Management*

ISO 27001: A.8.9

Ley de Ciberseguridad: normas de configuración segura de infraestructuras

Resultado: entornos robustos y sin exposición innecesaria.

18. Evaluaciones de impacto en privacidad (DPIA)

Principio: Evaluar los riesgos de tratamientos de datos personales antes de su inicio.

Controles asociados:

DAMA: *Risk Management*

ISO 27001: Cl. 6.1

ISO 27701: A.7.2.5 Evaluaciones de impacto en privacidad

ISO 29100: Evaluación de riesgos de privacidad

Ley de Protección de Datos: art. 32

Resultado: tratamientos legítimos y proporcionales al riesgo.

19. Gestión de derechos de los titulares

Principio: Implementar procesos para ejercer derechos de acceso, rectificación, oposición y supresión.

Controles asociados:

DAMA: *Data Stewardship*

ISO 27701: A.7.4.1–A.7.4.5

ISO 29100: Participación individual

Ley de Protección de Datos: arts. 14–16

Resultado: procesos trazables y automatizados de respuesta a solicitudes.

20. Minimización, enmascaramiento y anonimización

Principio: Limitar el tratamiento a la cantidad mínima necesaria de datos.

Controles asociados:

DAMA: *Privacy & Security Domain*

ISO 27001: A.8.11 Enmascaramiento de datos

ISO 27701: A.7.4.3 Minimización y pseudonimización

ISO 29100: Minimización de datos

Ley de Protección de Datos: art. 6

Resultado: reducción de exposición y cumplimiento de proporcionalidad.

Integración General

21. Supervisión y monitoreo continuo

Principio: Vigilar el cumplimiento y detectar comportamientos anómalos en el uso de datos.

Controles asociados:

DAMA: *Security Monitoring*

ISO 27001: A.5.23, A.5.24

ISO 27701: Cl. 9 Evaluación del desempeño

Ley de Ciberseguridad: art. 20

Resultado: detección temprana de brechas y mejora continua del sistema.

22. Capacitación y concienciación

Principio: Asegurar que todo el personal comprenda sus deberes respecto al dato.

Controles asociados:

DAMA: *Governance Culture*

ISO 27001: Cl. 7.3 Concienciación y formación

ISO 27701: A.7.2.2 Capacitación en privacidad

Ley de Ciberseguridad: art. 25

Resultado: cultura organizacional orientada a la protección del dato.

23. Gestión de continuidad y resiliencia

Principio: Mantener la disponibilidad de los datos frente a interrupciones.

Controles asociados:

DAMA: *Data Operations*

ISO 27001: A.5.30–A.5.32

ISO 27701: A.7.4.11

Ley de Ciberseguridad: art. 19

Resultado: operación resiliente y protección de servicios críticos.

24. Revisión y mejora continua

Principio: Evaluar y actualizar periódicamente el sistema de gobierno de datos.

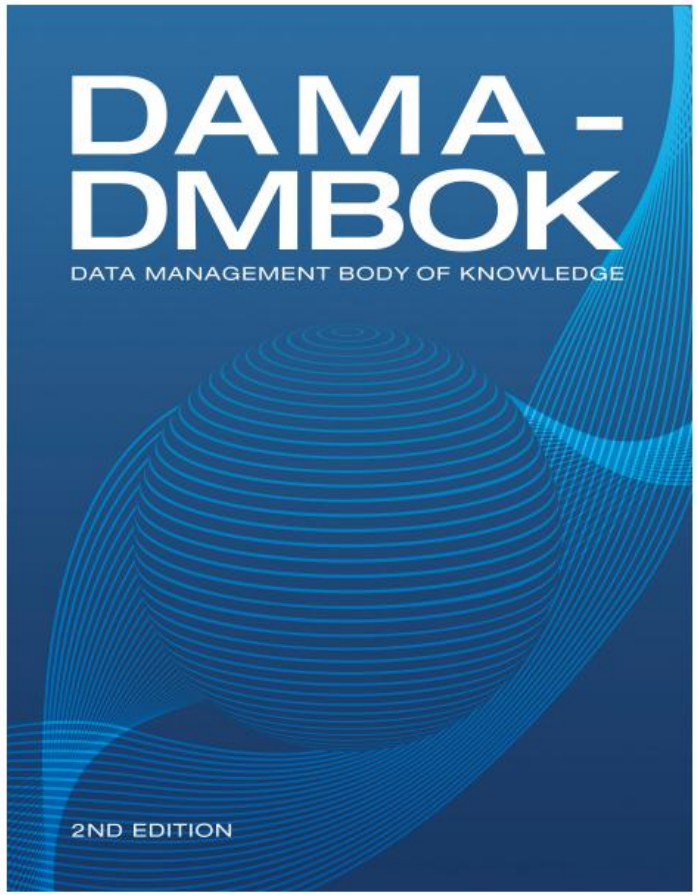
Controles asociados:

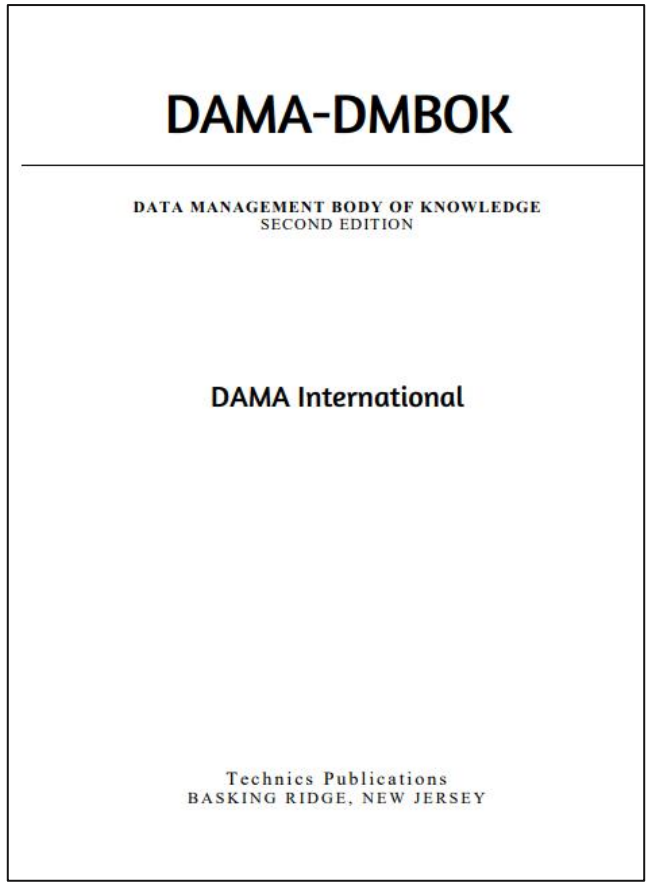
DAMA: *Governance Oversight*

ISO 27001: Cl. 9.1–9.3

Componentes de DMBOK 2.0

Referencias





Referencias:

- Todo el contenido de esta sesión esta basado en el libro de referencia DMBok 2 (2017)

DAMA - DMBok

https://www.dama.org/

Organismo internacional profesional con capítulos locales

Modelo General de Referencia

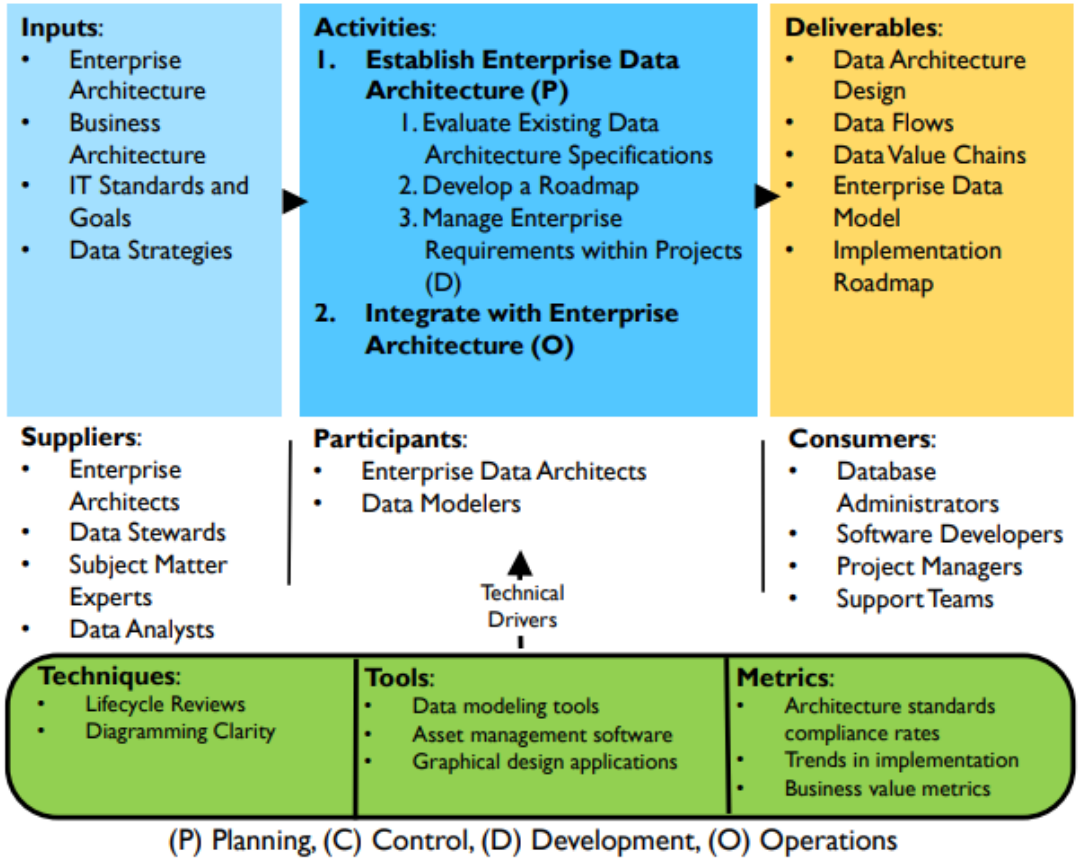
Cada función se define en detalle en el libro de referencia DMBok 2 (2017)

Contexto general:

- El framework se define en DMBOK 2.
- Ofrece certificaciones asociadas
- Se basa en la implementación de cada función del modelo
- Agnóstico tecnológicamente
- Requiere una adecuación a contextos de IA.
- Complejo de implementar en su completitud, pero funcional si toma las actividades claves.
- Es el más importante modelo de referencia en uso y aplicación actualmente.

I.- Arquitectura de Datos

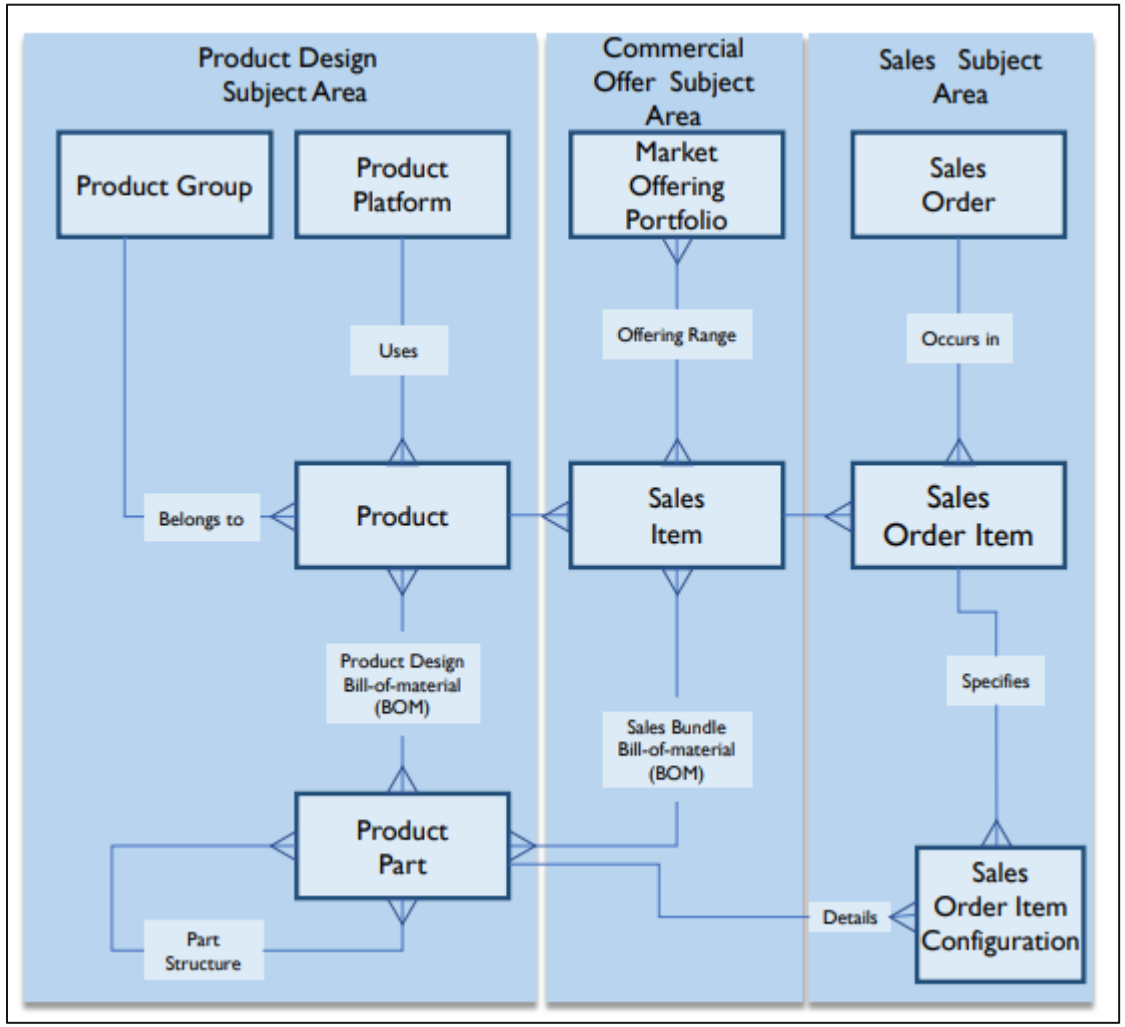
- Propósito: Identificar las necesidades de datos de la empresa (independientemente de su estructura) y diseñar y mantener los planes maestros para satisfacerlas. Utilizar los planes maestros para guiar la integración de datos, controlar los activos de datos y alinear las inversiones en datos con la estrategia empresarial.
- Objetivos:
  1. Identificar los requisitos de almacenamiento y procesamiento de datos
  2. Diseñar estructuras y planes para satisfacer las necesidades de datos actuales y a largo plazo de la empresa.
  3. Preparar estratégicamente a las organizaciones para que evolucionen rápidamente sus productos, servicios y datos y aprovechen las oportunidades de negocio inherentes a las tecnologías emergentes.

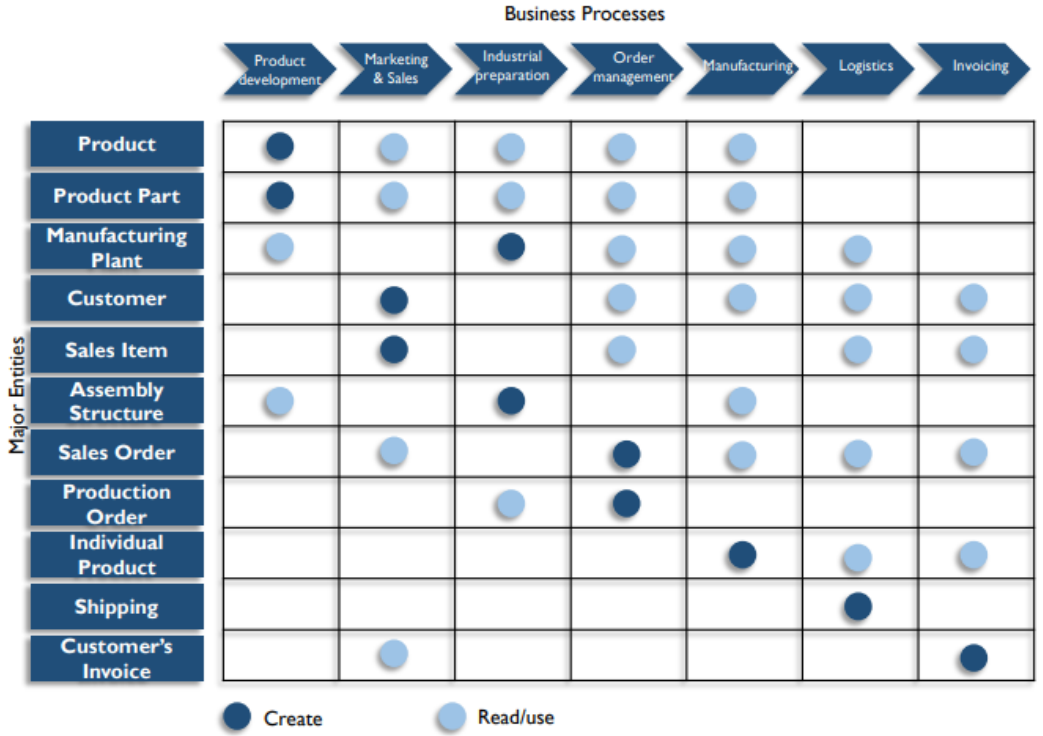


Framework Zachman

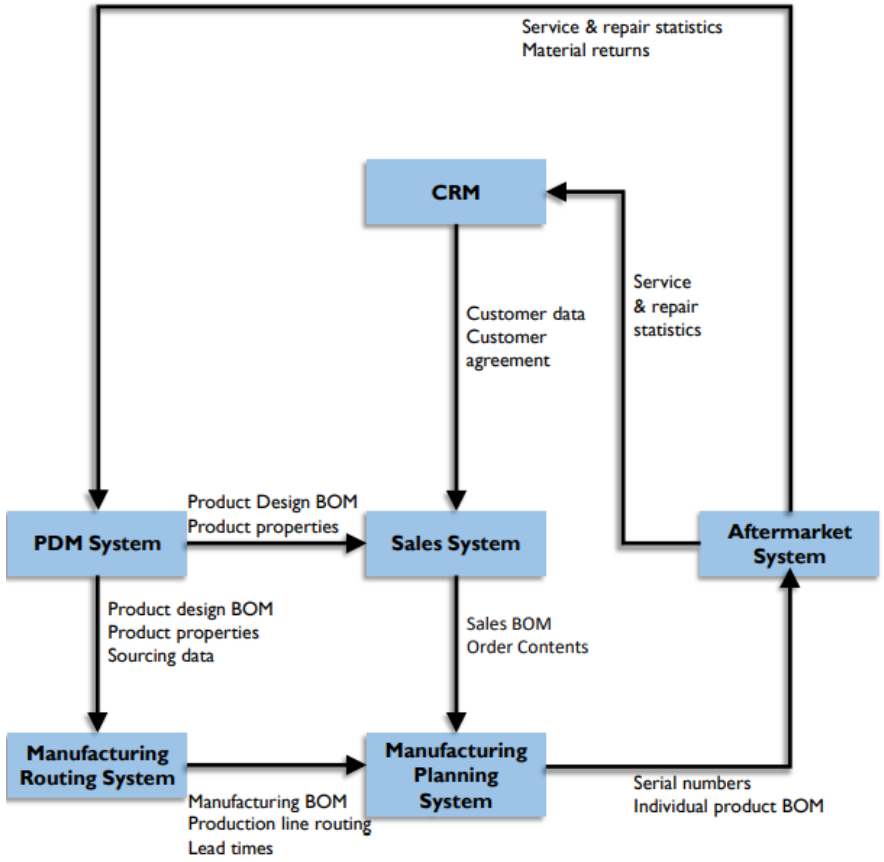
	What	How	Where	Who	When	Why	
Executive	Inventory Identification	Process Identification	Distribution Identification	Responsibility Identification	Timing Identification	Motivation Identification	Scope Context
Business Management	Inventory definition	Process Definition	Distribution Definition	Responsibility Definition	Timing Definition	Motivation Definition	Business Concepts
Architect	Inventory Representation	Process Representation	Distribution Representation	Responsibility Representation	Timing Representation	Motivation Representation	System Logic
Engineer	Inventory Specification	Process Specification	Distribution Specification	Responsibility Specification	Timing Specification	Motivation Specification	Technology Physics
Technician	Inventory Configuration	Process Configuration	Distribution Configuration	Responsibility Configuration	Timing Configuration	Motivation Configuration	Tool Components
Enterprise	Inventory Instantiations	Process Instantiations	Distribution Instantiations	Responsibility Instantiations	Timing Instantiations	Motivation Instantiations	Operational Instances
	Inventory Sets	Process Flows	Distribution Networks	Responsibility Assignments	Timing Cycles	Motivation Intentions	

La Arquitectura de Datos – Desde los procesos

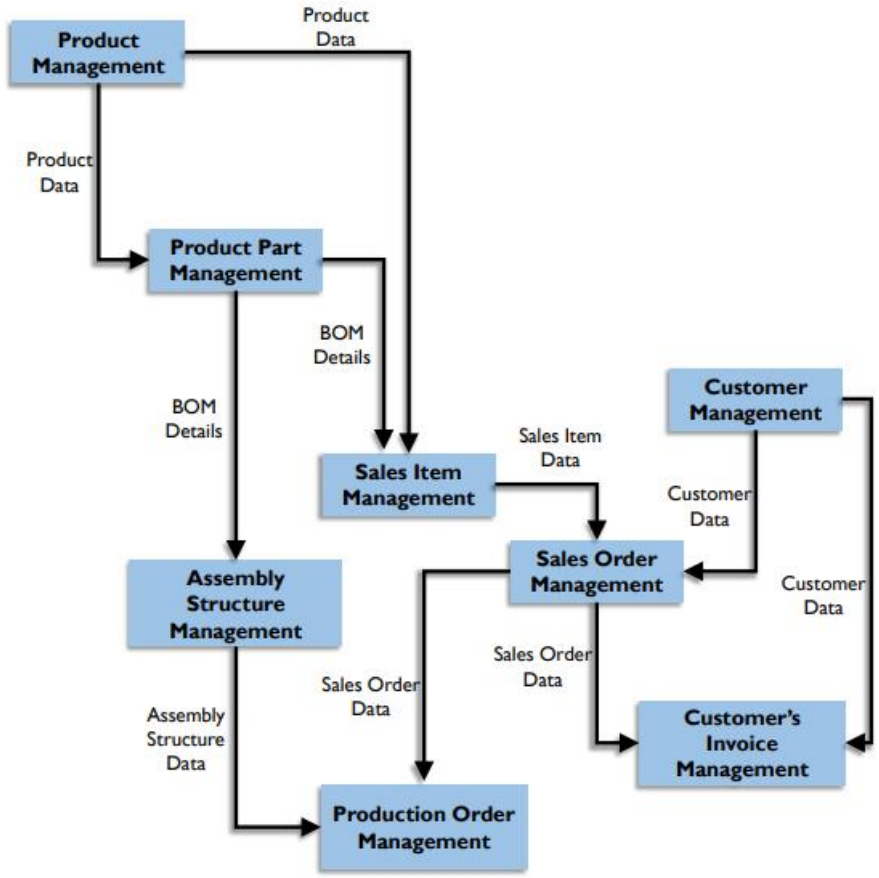




La Arquitectura de Datos – Desde los procesos



Diagramas de Flujo



Dependencias de Datos

Seguridad y Privacidad Asociada

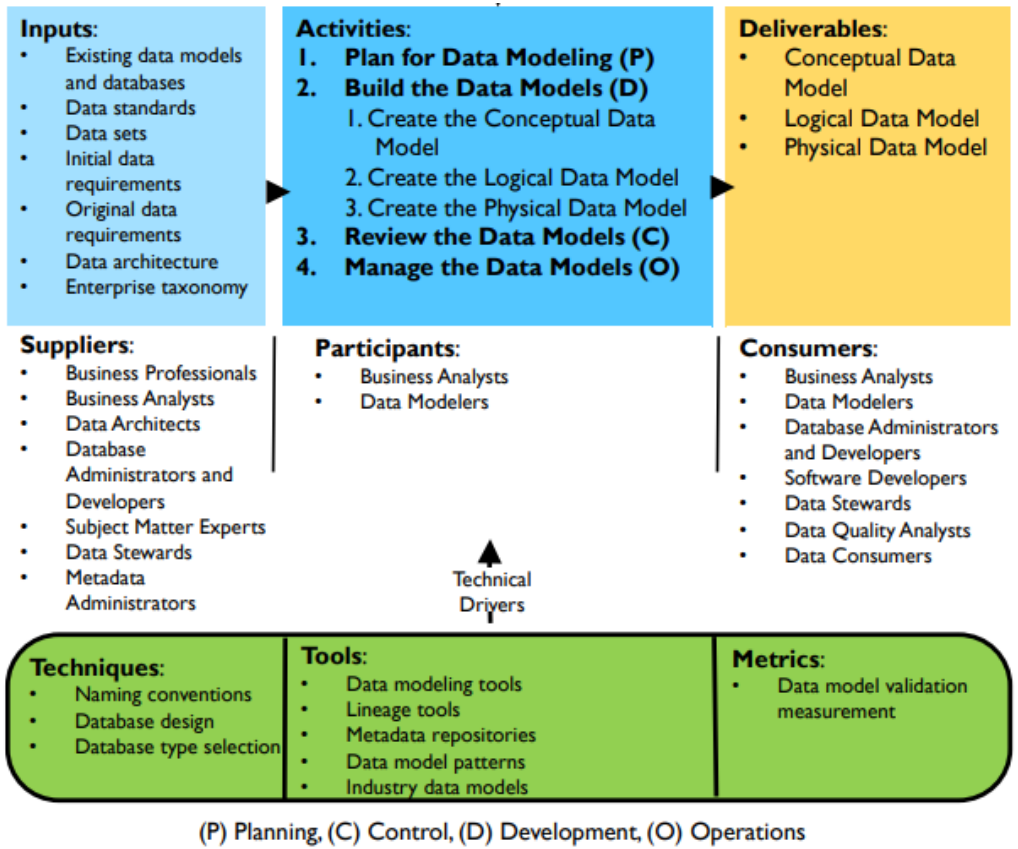
1. **Identificación y modelado de activos de información críticos**
   - La arquitectura permite mapear las fuentes, repositorios y flujos de datos, lo que facilita su clasificación dentro del inventario de activos del SGSI (control A.5.9).
   - Este modelo apoya el enfoque de protección basada en riesgo (Cláusula 6.1) y la gestión de la continuidad de información crítica (A.5.30–A.5.32).
2. **Diseño de dominios y zonas seguras de información**
   - La arquitectura define límites lógicos y físicos de los datos según su nivel de sensibilidad.
   - Seguridad aplica controles de acceso (A.5.15–A.5.18) y segmentación de redes o entornos para proteger dominios específicos (por ejemplo, datos financieros o personales).
3. **Gobierno de arquitectura con seguridad por diseño**
   - Cada componente arquitectónico incorpora controles de seguridad desde su concepción (A.8.9 "Seguridad en el desarrollo").
   - La arquitectura se convierte en la "matriz de control" que permite verificar que los sistemas nuevos cumplan los requisitos del SGSI y la Ley Marco de Ciberseguridad (art. 10 y 15).
4. **Trazabilidad y dependencias de datos para detección de incidentes**
   - El linaje de datos dentro de la arquitectura facilita el monitoreo de flujos y puntos de vulnerabilidad.
   - Los registros de eventos (A.5.23) se asocian a los objetos y relaciones definidas en la arquitectura, permitiendo correlación forense ante incidentes.

1. **Mapeo de flujos de datos personales y categorías de PII**
   - La arquitectura de datos documenta el recorrido de la información personal desde su origen hasta su destino (control A.7.2.4 de 27701).
   - Este mapeo es requisito base para aplicar el principio de *transparencia y control del titular* de ISO 29100 y para cumplir el deber de información al usuario (art. 5 y 6 de la Ley chilena).
2. **Privacidad por diseño en la estructura y los flujos de información**
   - Cada capa o dominio de la arquitectura incorpora salvaguardas de privacidad desde su definición (A.7.4.2 "Privacidad por diseño y por defecto").
   - Se definen controles automáticos de minimización, enmascaramiento y anonimización según el tipo de dato (A.7.4.3).
3. **Definición de metadatos y taxonomías de datos personales**
   - La arquitectura establece el catálogo maestro de tipos de datos y su correspondencia con bases, aplicaciones y procesos (A.7.3.2).
   - Permite ejecutar derechos ARCO de forma trazable y mantener evidencias de cumplimiento (accountability).
4. **Segmentación lógica y retención diferenciada**
   - A través del modelo arquitectónico se definen zonas de almacenamiento con distintas políticas de conservación, en línea con el principio de *limitación de retención* (ISO 29100) y el control A.7.4.9 de 27701.
   - Apoya la eliminación o anonimización automática cuando la finalidad expira (art. 11 de la Ley de Protección de Datos).

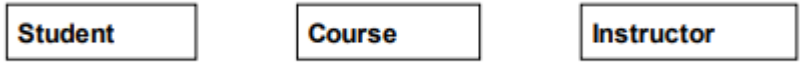
II.- Diseño y Modelamiento

- El modelado de datos es el proceso de descubrir, analizar y definir el alcance de los requisitos de datos, para luego representarlos y comunicarlos de forma precisa, denominada modelo de datos. Este proceso es iterativo y puede incluir un modelo conceptual, uno lógico y uno físico.

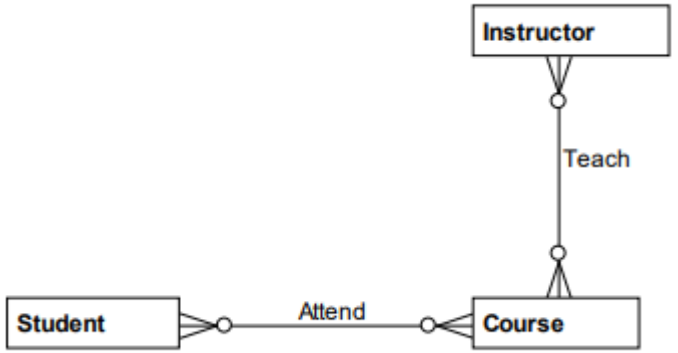
- Objetivo:
  1. Confirmar y documentar la comprensión de diferentes perspectivas, lo que resulta en aplicaciones que se alinean mejor con los requisitos empresariales actuales y futuros, y sienta las bases para completar con éxito iniciativas de amplio alcance, como la gestión de datos maestros y los programas de gobernanza de datos.



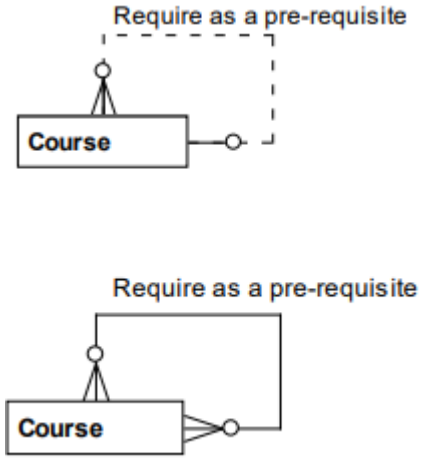
Componentes Modelo Relacional



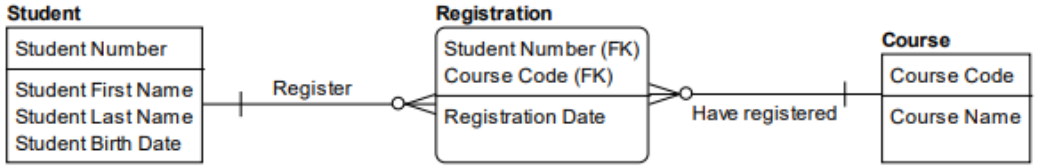
Entidades



Relaciones

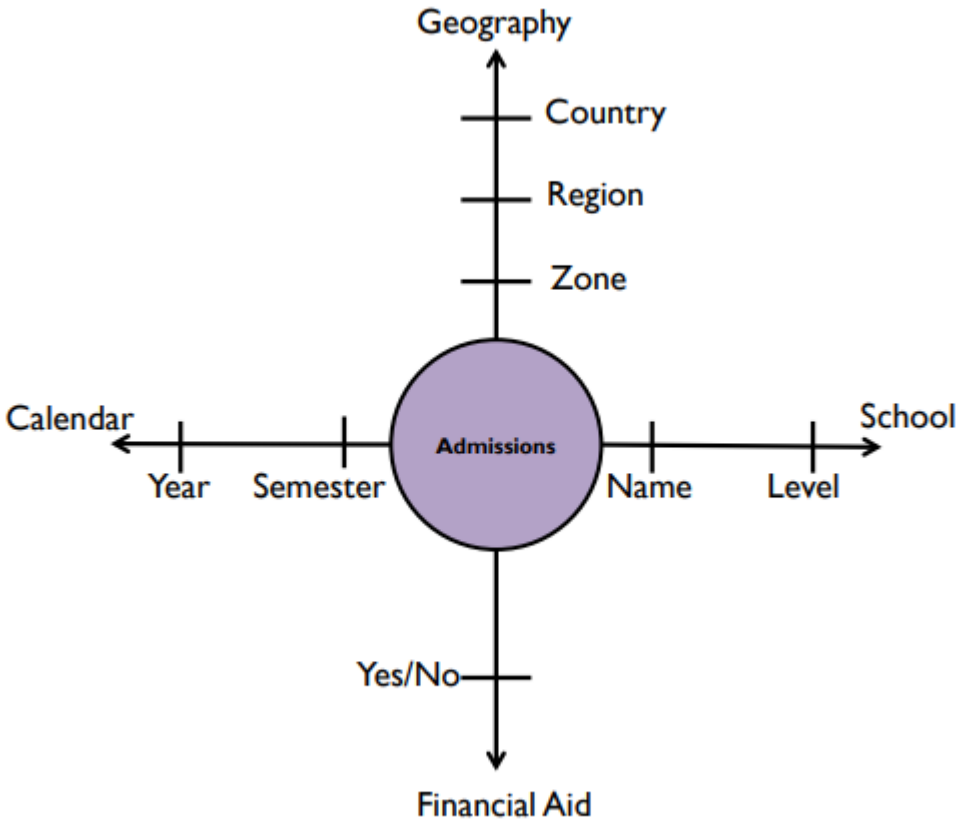


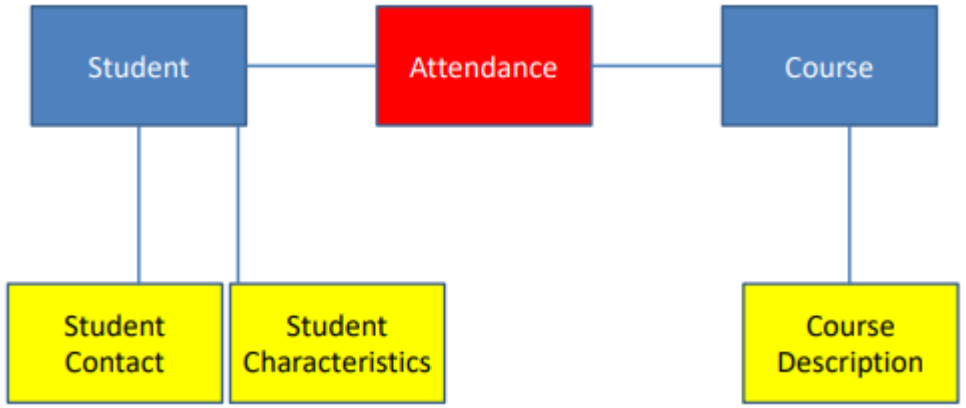
Relaciones Jerárquicas

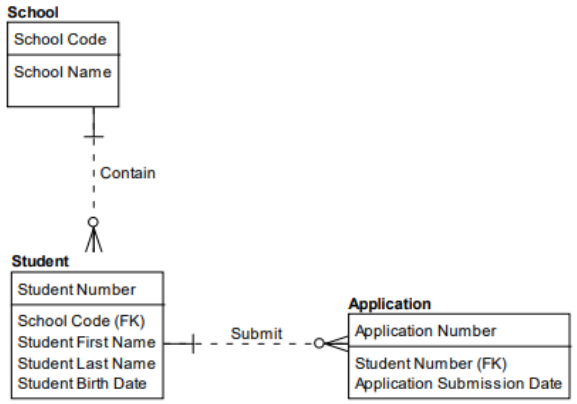


Relaciones Normalizadas
(Claves primarias)

Contexto de Información







Normalización

Types of Normalization in SQL

1NF

First Normal Form

- Ensures that each column contains only atomic values

2NF

Second Normal Form

- Eliminates partial dependencies.

3NF

Third Normal Form

- Eliminates transitive dependencies.

BCNF

Boyce-Codd Normal Form

- Strict version of 3NF that addresses additional anomalies.

4NF

Fourth Normal Form

- Deals with multi-valued dependencies

5NF

Fifth Normal Form

- Addresses join dependencies

Seguridad y Privacidad Asociada

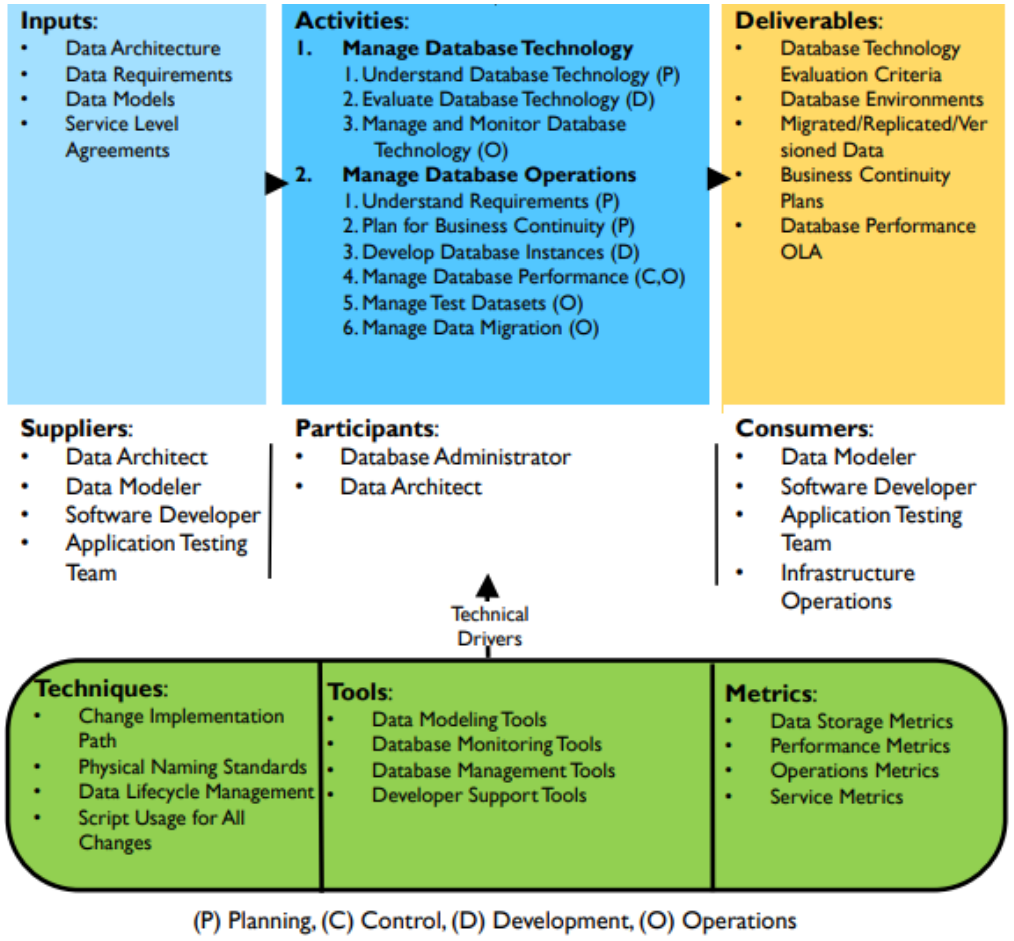
1. **Modelos de datos alineados al inventario de activos de información**
   - Cada entidad y atributo del modelo de datos se vincula con el catálogo de activos definido en el SGSI (A.5.9).
   - Permite visualizar dependencias y priorizar la aplicación de controles de protección, continuidad y respaldo (A.5.30–A.5.32).
2. **Definición de controles de acceso en el modelo lógico**
   - El diseño de entidades incorpora las reglas de acceso y visibilidad de campos según rol o perfil.
   - Se articula con los controles A.5.15–A.5.18 de ISO 27001 y con la Ley de Ciberseguridad (art. 14) sobre segregación de funciones.
   - Resultado: control de privilegios embebido en el propio diseño de la base de datos.
3. **Integridad referencial y control de cambios seguros**
   - El modelamiento lógico y físico establece reglas de integridad que previenen alteraciones no autorizadas o pérdida de coherencia.
   - Se alinea con A.8.12 "Integridad de la información" y con A.8.9 "Gestión de la configuración y del cambio seguro".
   - Cada modificación en el modelo se registra como cambio controlado bajo el SGSI.
4. **Seguridad por diseño en estructuras y relaciones de datos**
   - Los modelos de datos deben incluir restricciones técnicas y de relación que mitiguen exposición o duplicación innecesaria.
   - Se articula con A.8.9 y A.8.10 (seguridad en desarrollo y eliminación de información).
   - Cumple la exigencia de la Ley de Ciberseguridad de incorporar medidas de seguridad en la fase de diseño (art. 10).

1. **Modelado de flujos de PII y mapeo de relaciones entre entidades**
   - El modelo de datos documenta cómo se relacionan las tablas y atributos que contienen datos personales.
   - Permite identificar los puntos donde se produce tratamiento, transferencia o almacenamiento (A.7.2.4 y A.7.3.2 de ISO 27701).
   - Satisface el principio de *transparencia* de ISO 29100 y el deber de información de la ley chilena (art. 5).
2. **Aplicación del principio de minimización en el modelamiento lógico**
   - En la etapa de diseño se define la cantidad mínima de atributos personales requeridos.
   - Control A.7.4.3 de 27701 y principio de *proporcionalidad* (ISO 29100, Ley art. 6).
   - Evita incluir información innecesaria o sensible que aumente el riesgo de exposición.
3. **Incorporación de anonimización y pseudonimización en los modelos físicos**
   - Los esquemas físicos integran campos o vistas anonimizadas para fines de análisis o pruebas.
   - Controles A.7.4.3 (minimización) y A.7.4.7 (transferencias seguras) de 27701.
   - Permite cumplimiento de privacidad por diseño y limita el acceso a información identificable.
4. **Modelos de retención y eliminación vinculados al ciclo de vida del dato**
   - El modelo físico incorpora indicadores de retención y fechas de eliminación programada.
   - Alineado con A.7.4.9 de 27701 y con el principio de *limitación de retención* (ISO 29100).
   - Apoya la eliminación automatizada de registros una vez cumplida la finalidad (Ley art. 11).

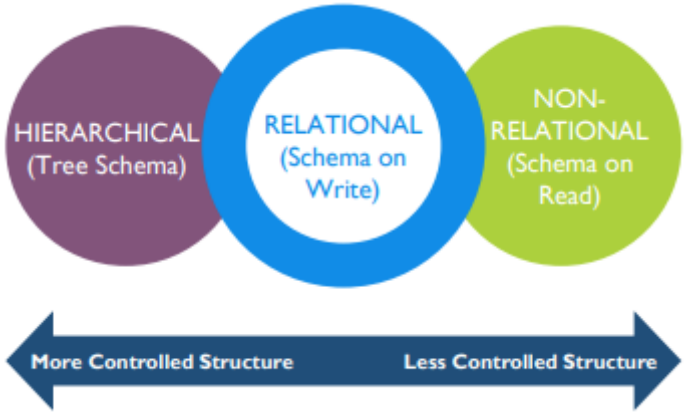
III.- Almacenamiento y Operación de Datos

- Diseño, implementación y soporte de los datos almacenados para maximizar su valor.

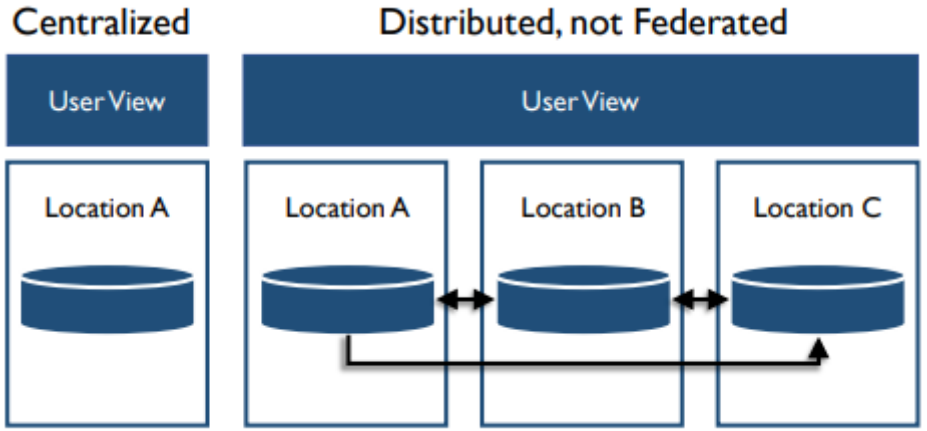
- Objetivos:
  1. Gestionar la disponibilidad de los datos durante todo su ciclo de vida.
  2. Garantizar la integridad de los activos de datos.
  3. Gestionar el rendimiento de las transacciones de datos.



Organización de la Base de Datos

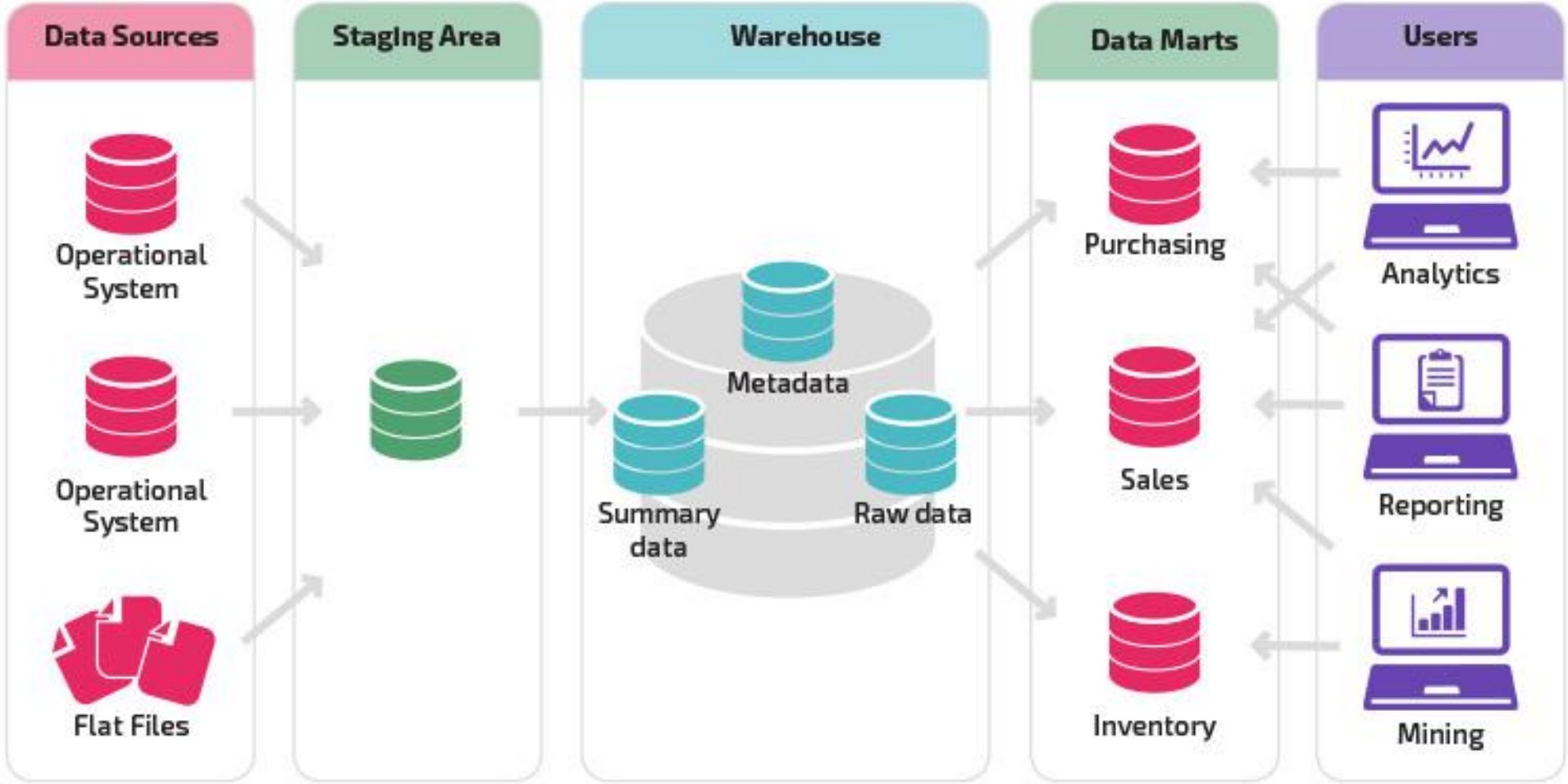


Alcance de las bases de datos

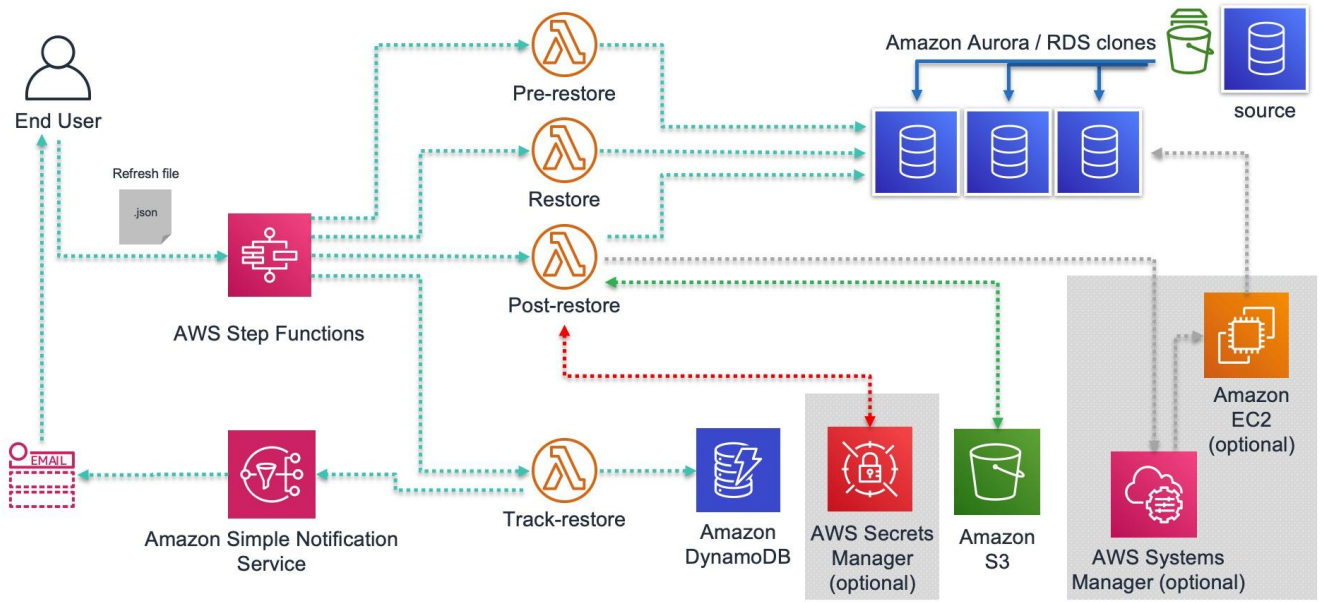


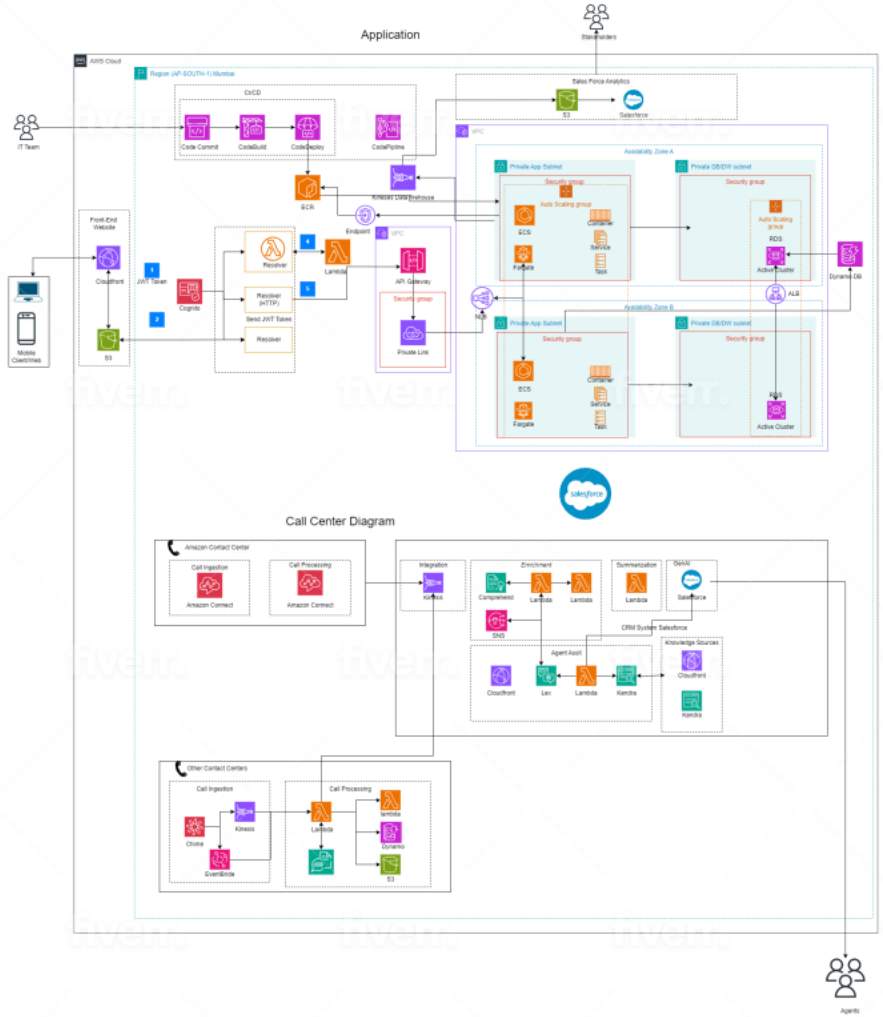
Centralizadas o Descentralizadas

Una concepción simple

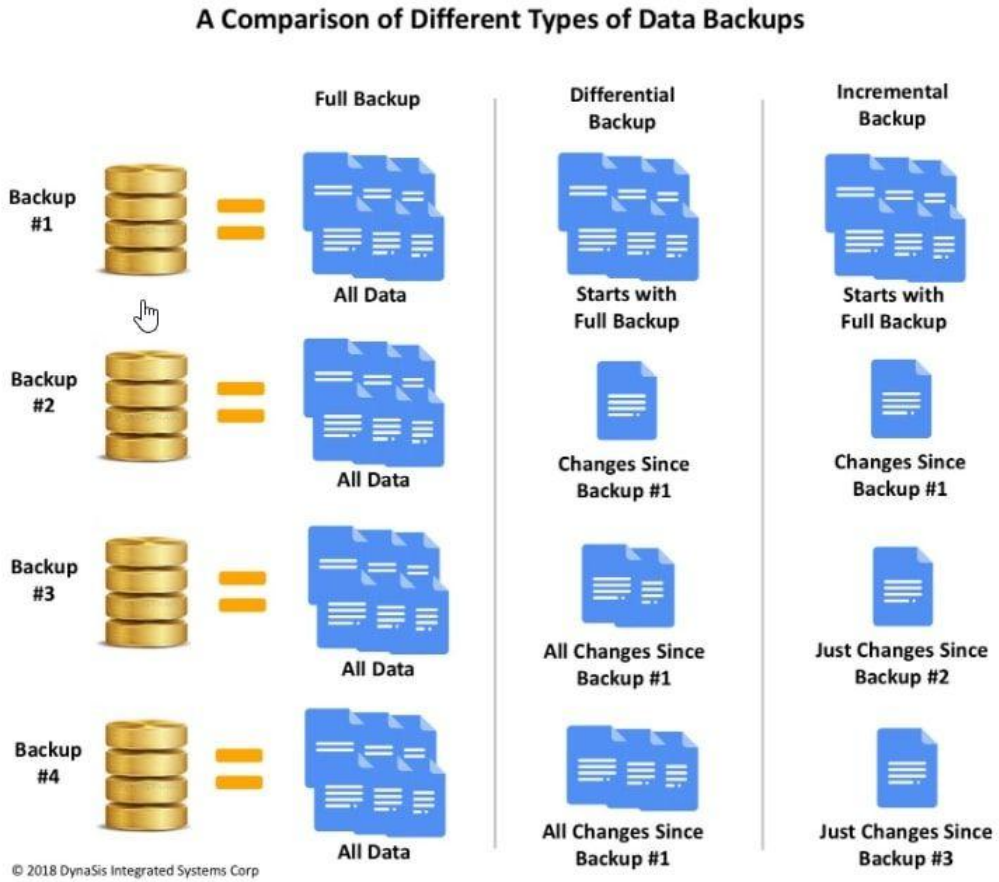


Una concepción más realista (AWS)

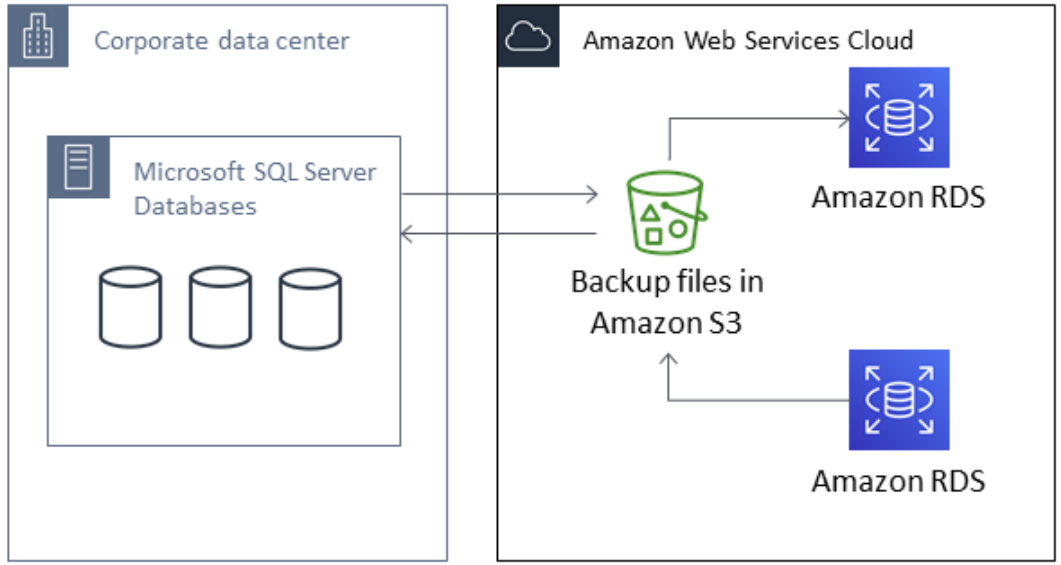




Estrategias de Respaldo

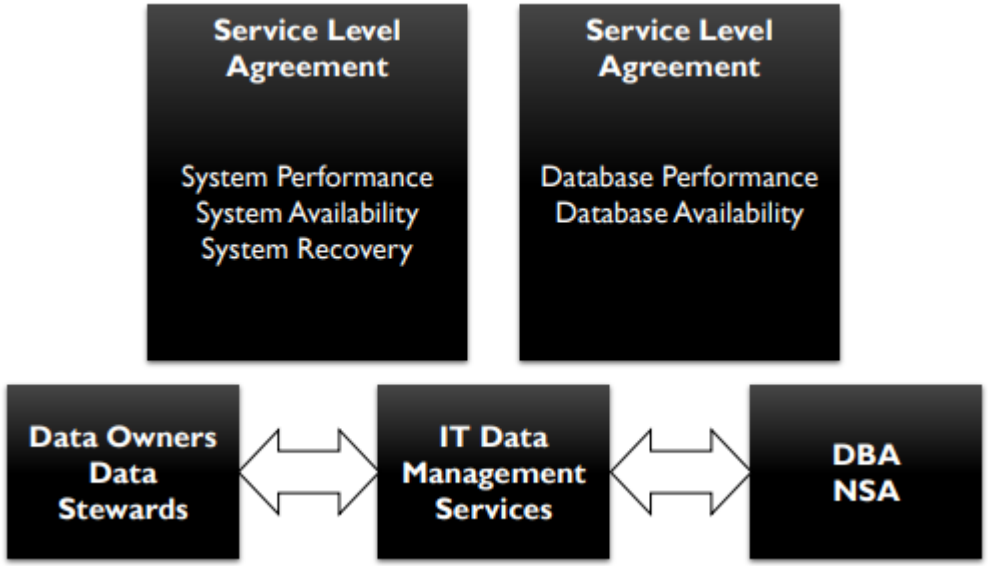


Tipos de Respaldo



Respaldo en la Nube

Organización de la Base de Datos



SLA Base de Datos

Factores Claves

Seguridad y Privacidad Asociada

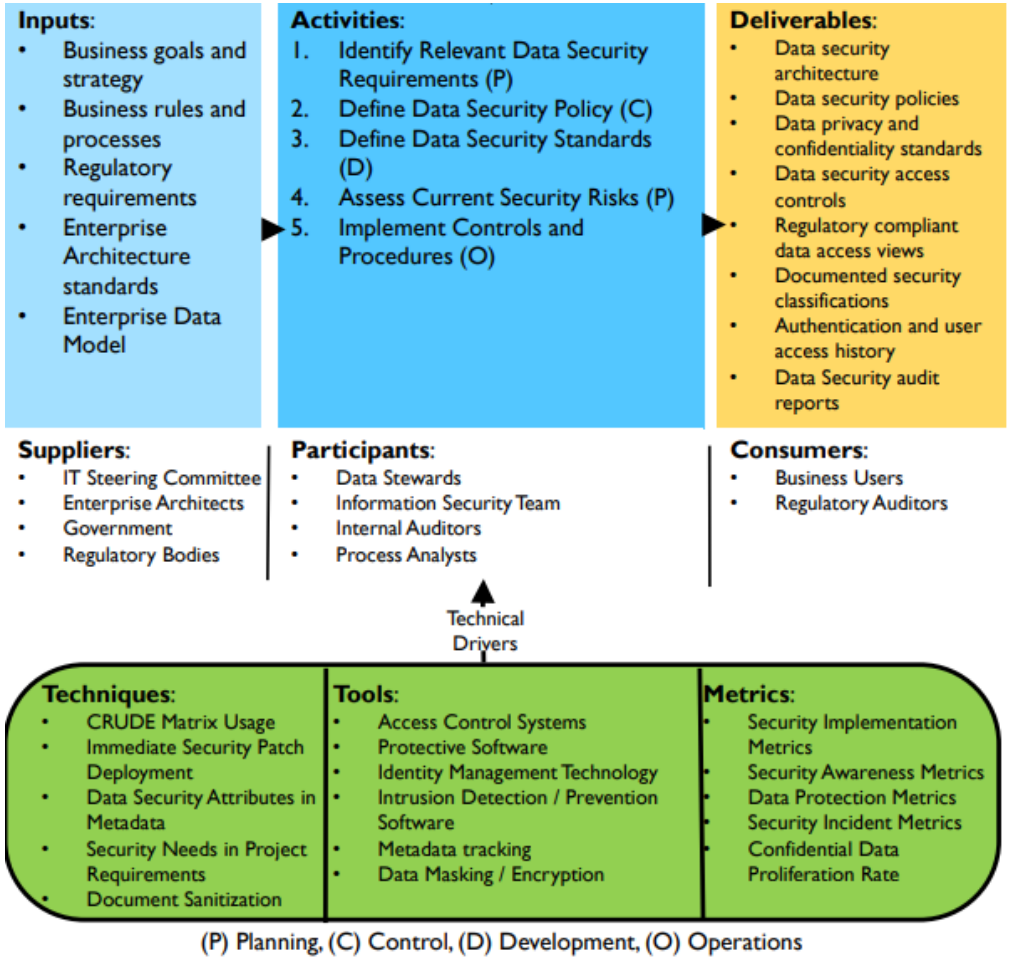
1. **Gestión segura de entornos de almacenamiento**
   - Los sistemas de bases de datos, repositorios cloud o físicos se administran bajo controles técnicos definidos en A.8.9 ("Configuración segura") y A.8.14 ("Separación de entornos").
   - La arquitectura operacional aplica políticas de endurecimiento y control de cambios bajo el SGSI.
   - Ley de Ciberseguridad: art. 10 exige proteger la infraestructura esencial mediante configuraciones seguras certificadas.
2. **Control de acceso a entornos operativos y de respaldo**
   - Cada repositorio de datos se asocia a permisos específicos según el principio de mínimo privilegio.
   - ISO 27001 A.5.15–A.5.18 (gestión de identidades, derechos y privilegios) y A.8.2 (acceso privilegiado).
   - Garantiza que las copias y entornos de respaldo no se conviertan en vectores de exposición.
3. **Disponibilidad y continuidad operacional**
   - Se integran políticas de respaldo y restauración (A.8.13) con los objetivos RTO/RPO definidos en el plan de continuidad del SGSI.
   - Los entornos de almacenamiento deben validarse regularmente mediante pruebas de restauración.
   - Ley de Ciberseguridad: art. 19 exige continuidad para servicios críticos y respaldo in situ o remoto certificado.
4. **Registro, monitoreo y trazabilidad de operaciones de almacenamiento**
   - Todo evento de lectura, escritura, eliminación o transferencia de datos en entornos productivos o de respaldo debe quedar trazado.
   - ISO 27001 A.5.23 ("Registro de eventos") y A.5.24 ("Gestión de incidentes").
   - Permite detección temprana de accesos anómalos o exfiltraciones desde entornos operacionales.

1. **Separación de datos personales en entornos productivos y de prueba**
   - A.7.4.3 de ISO 27701 establece la minimización y anonimización de datos personales en entornos de desarrollo y testeo.
   - El Gobierno de Datos define las reglas de extracción anonimizada para evitar uso indebido de PII fuera del entorno autorizado.
   - Ley de Protección de Datos: art. 6 y 11 (principio de proporcionalidad y finalidad).
2. **Gestión de retención y eliminación en sistemas de almacenamiento**
   - Cada base o sistema debe implementar rutinas automáticas de eliminación o bloqueo de datos una vez cumplida su finalidad.
   - ISO 27701 A.7.4.9 y principio de *limitación de retención* (ISO 29100).
   - Cumple el art. 11 de la Ley chilena sobre eliminación segura y definitiva de datos personales.
3. **Protección de datos personales en repositorios de respaldo**
   - Las copias de seguridad también deben incluir controles de acceso, cifrado y limitación de retención (A.7.4.11 de 27701).
   - Se define dentro del Gobierno de Datos un ciclo de vida del respaldo para evitar almacenamiento indefinido de PII.
   - ISO 29100 refuerza este principio bajo *Seguridad de la información y limitación de almacenamiento*.
4. **Privacidad por diseño en la operación de almacenamiento y servicios cloud**
   - Los contratos y configuraciones de servicios cloud o data center deben asegurar privacidad por diseño (A.7.4.2 de ISO 27701).
   - Esto incluye control de localización geográfica de los datos y validación de jurisdicciones seguras.
   - Ley de Protección de Datos: art. 20 regula transferencias y tratamiento transfronterizo.

IV.- Seguridad del Dato

- Propósito: Definición, planificación, desarrollo y ejecución de políticas y procedimientos de seguridad para garantizar la correcta autenticación, autorización, acceso y auditoría de los datos y activos de información.

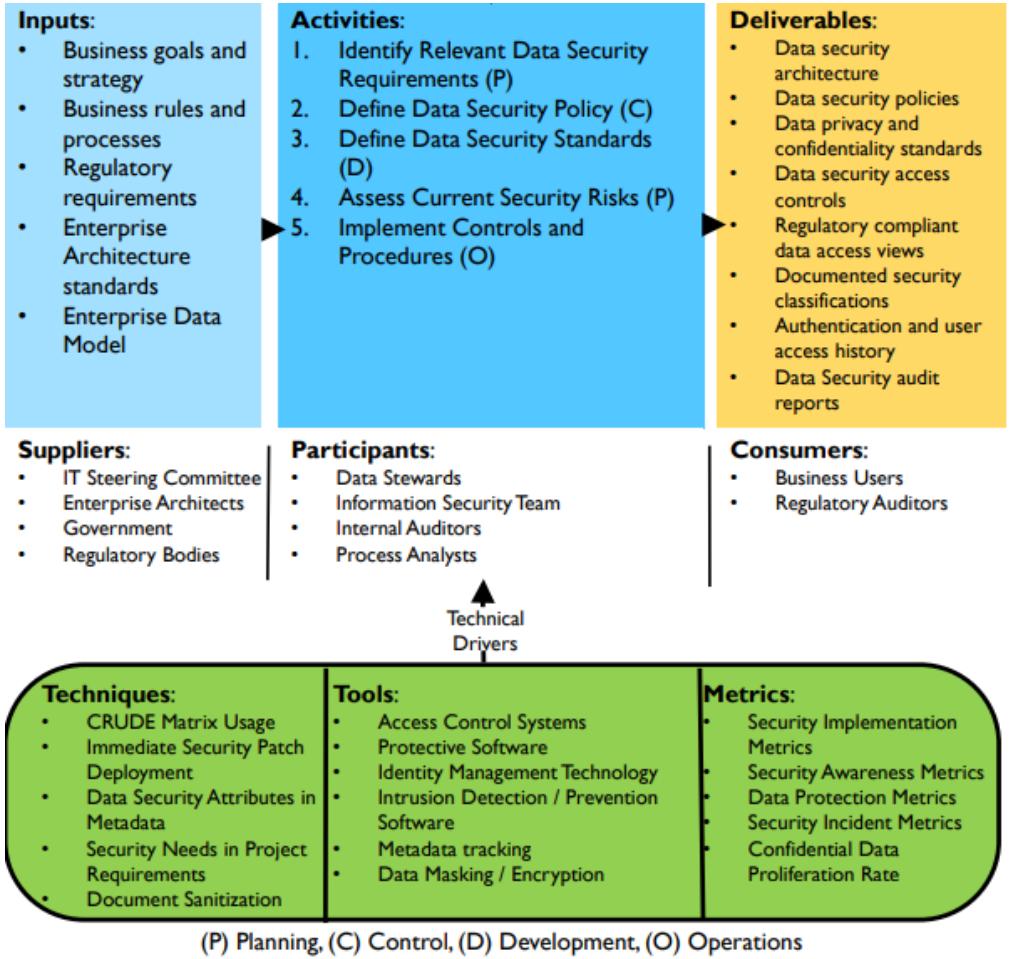
- Objetivos:
  1. Facilitar el acceso adecuado y prevenir el acceso inapropiado a los activos de datos empresariales.
  2. Comprender y cumplir con todas las normativas y políticas pertinentes en materia de privacidad, protección y confidencialidad.
  3. Garantizar el cumplimiento y la auditoría de las necesidades de privacidad y confidencialidad de todas las partes interesadas.



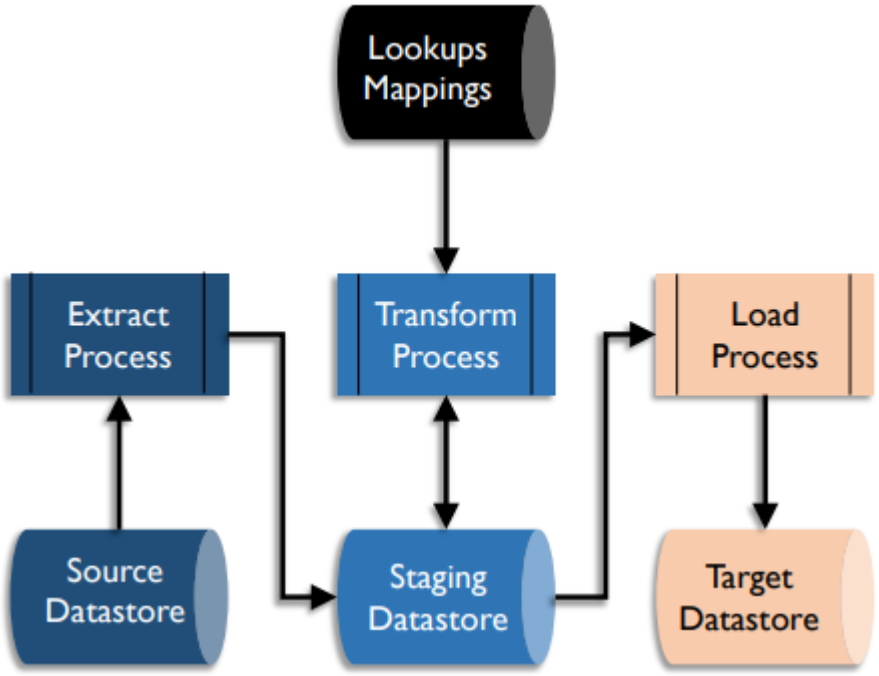
V.- Integración e Interoperabilidad

- Propósito: Gestionar la transferencia y consolidación de datos dentro y entre aplicaciones y organizaciones.

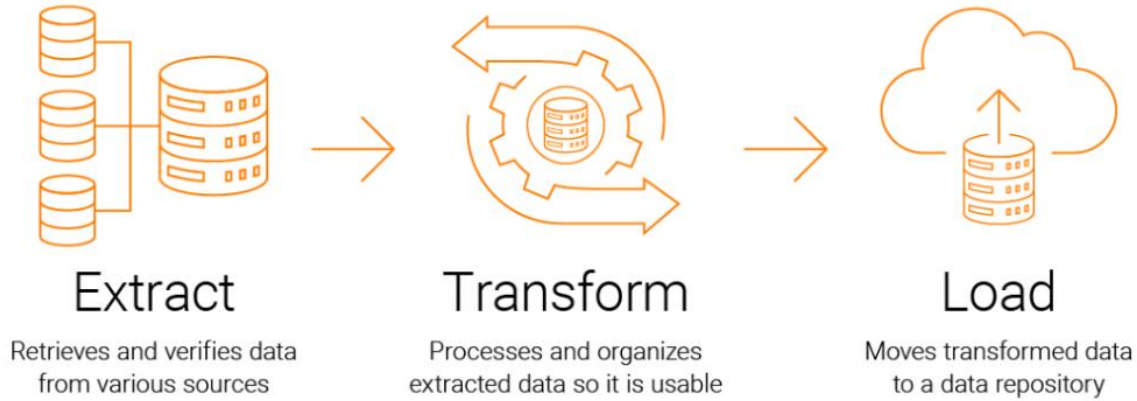
- Objetivos:
  1. Proporcionar datos de forma segura, cumpliendo con la normativa, en el formato y plazo necesarios.
  2. Reducir el coste y la complejidad de la gestión de soluciones mediante el desarrollo de modelos e interfaces compartidos.
  3. Identificar eventos significativos y activar alertas y acciones automáticamente.
  4. Apoyar las iniciativas de inteligencia empresarial, análisis, gestión de datos maestros y eficiencia operativa.



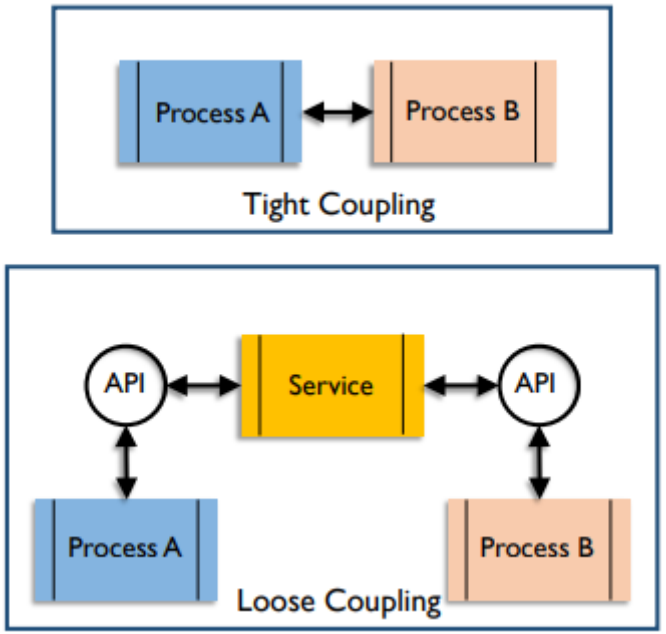
Herramientas de Carga de Datos



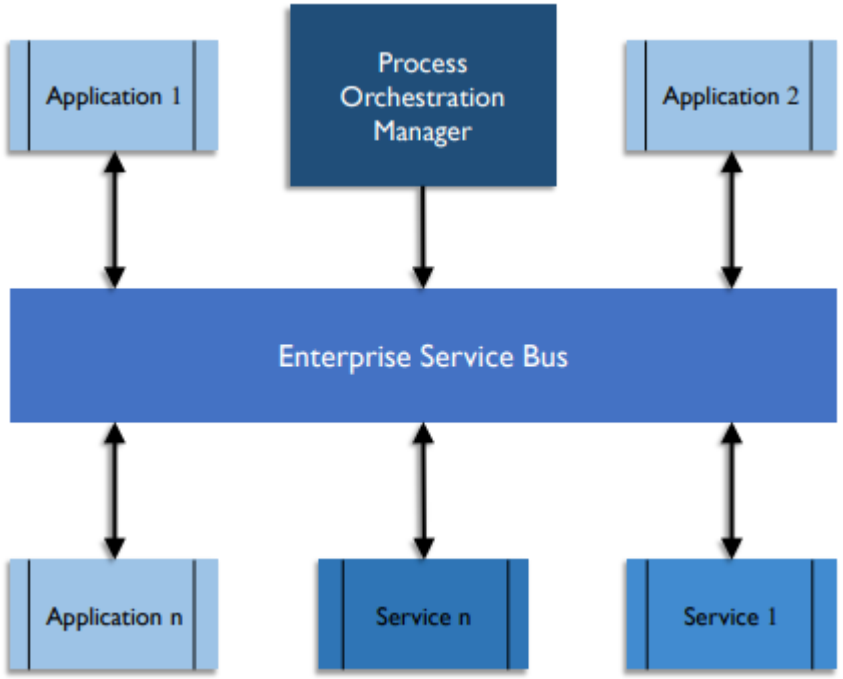
ETL – Visión General



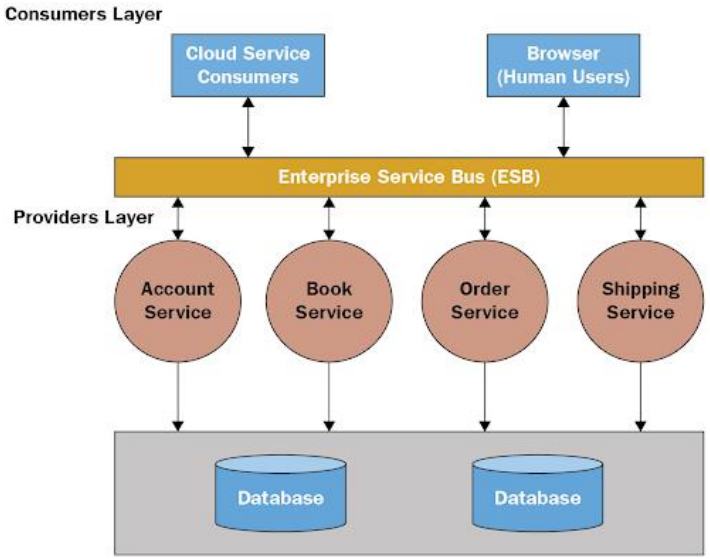
Herramientas de Intercambio de Datos



Web Service - API



Servicios de Bus



SOA – Servicios Orientados a la Arquitectura

Seguridad y Privacidad Asociada

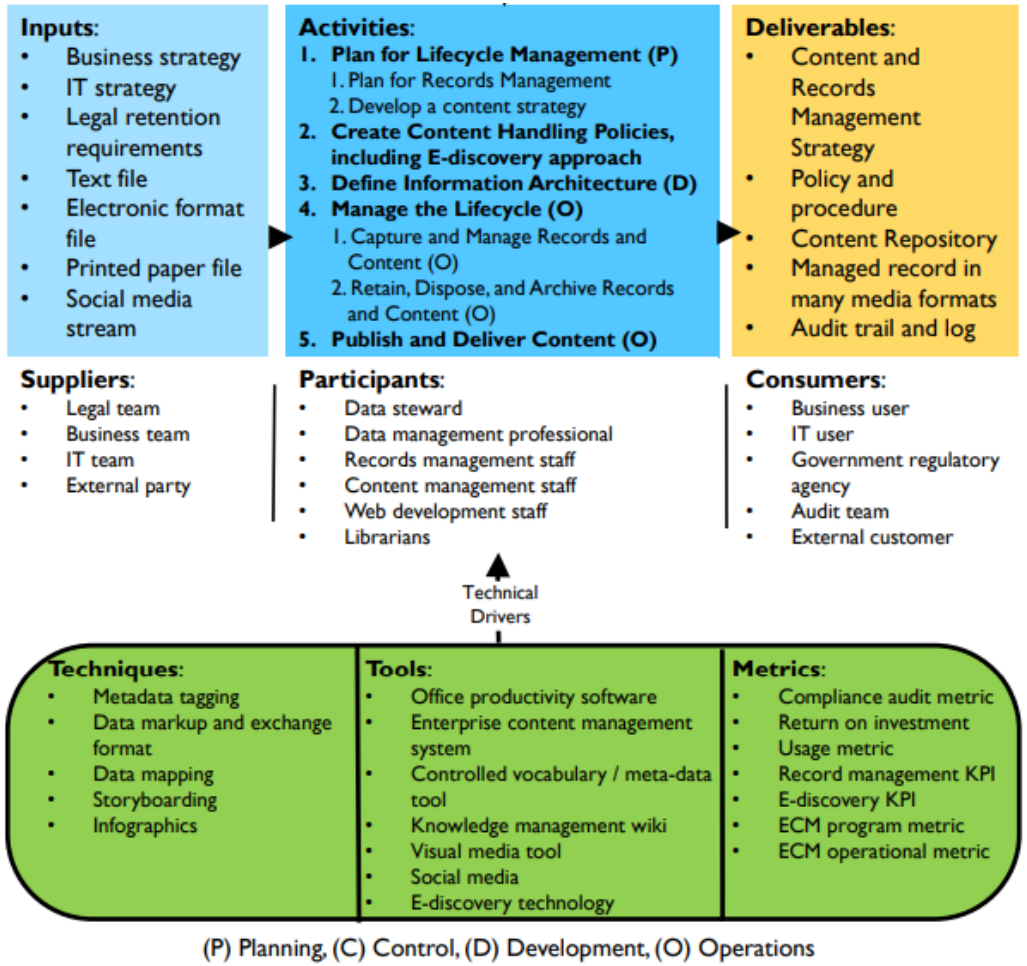
1. **Protección de los flujos de datos en tránsito**
   - Los mecanismos de integración (APIs, ETL, ESB, microservicios) deben garantizar cifrado punto a punto y autenticación mutua.
   - ISO 27001: A.8.24 "Uso de criptografía"
   - ISO 27001: A.5.14 "Transferencia de información"
   - Ley de Ciberseguridad: art. 10 y 12 (protección de redes y comunicaciones críticas).
   - **Resultado:** confidencialidad garantizada y mitigación de interceptaciones o fuga de información.
2. **Validación de origen, integridad y destino de los datos**
   - Los mecanismos de integración deben incorporar firmas digitales, checksum o validaciones automáticas para asegurar que los datos no se alteren en tránsito.
   - ISO 27001: A.8.12 "Integridad de la información"
   - Ley de Ciberseguridad: art. 19 (verificación y trazabilidad de transferencias).
   - **Resultado:** control técnico y legal sobre la autenticidad de las transmisiones.
3. **Gestión de interoperabilidad segura con terceros y proveedores**
   - Todo intercambio de datos con terceros debe sustentarse en contratos, SLAs y evaluaciones de seguridad.
   - ISO 27001: A.5.19 "Relaciones con proveedores"
   - Ley de Ciberseguridad: art. 22 (requisitos de seguridad para proveedores críticos).
   - **Resultado:** ecosistema de datos seguro y bajo gobernanza contractual.
4. **Monitoreo y auditoría de integraciones**
   - Registrar eventos y transferencias, detectando anomalías o patrones de extracción inusual.
   - ISO 27001: A.5.23 "Registro de eventos" y A.5.24 "Gestión de incidentes de seguridad".
   - Ley de Ciberseguridad: art. 21 (reporte obligatorio de incidentes al CSIRT Nacional).
   - **Resultado:** detección temprana y trazabilidad de incidentes en flujos de datos.

1. **Legitimidad y propósito del intercambio de datos personales**
   - Toda interoperabilidad debe estar justificada por una base legal o contractual.
   - ISO 27701: A.7.2.1 "Propósito del tratamiento de PII"
   - ISO 29100: Principio de *especificación de propósito*
   - Ley de Protección de Datos: art. 4–6 (licitud, finalidad y proporcionalidad).
   - **Resultado:** cada integración responde a un fin legítimo y documentado.
2. **Control de transferencias internacionales y cesiones a terceros**
   - Los flujos transfronterizos deben evaluarse según las garantías del país receptor o cláusulas contractuales.
   - ISO 27701: A.7.4.7 "Transferencia de datos personales a terceros"
   - ISO 29100: Transparencia y responsabilidad
   - Ley de Protección de Datos: art. 20 (transferencias internacionales).
   - **Resultado:** cumplimiento de soberanía y protección en la jurisdicción destino.
3. **Minimización y segmentación en la integración de datos personales**
   - En procesos de consolidación o interoperabilidad, deben transmitirse solo los atributos estrictamente necesarios.
   - ISO 27701: A.7.4.3 "Minimización"
   - ISO 29100: Principio de *minimización de datos*
   - Ley de Protección de Datos: art. 6 (proporcionalidad).
   - **Resultado:** menor exposición y alineamiento al principio de minimización.
4. **Transparencia y trazabilidad del flujo de datos personales**
   - Registrar y documentar todas las transferencias o integraciones que involucren PII.
   - ISO 27701: A.7.4.10 "Registro de actividades de tratamiento"
   - ISO 29100: *Transparencia y participación del titular*
   - Ley de Protección de Datos: art. 5 (deber de información al titular).
   - **Resultado:** el titular puede conocer cómo, dónde y con quién se comparten sus datos.

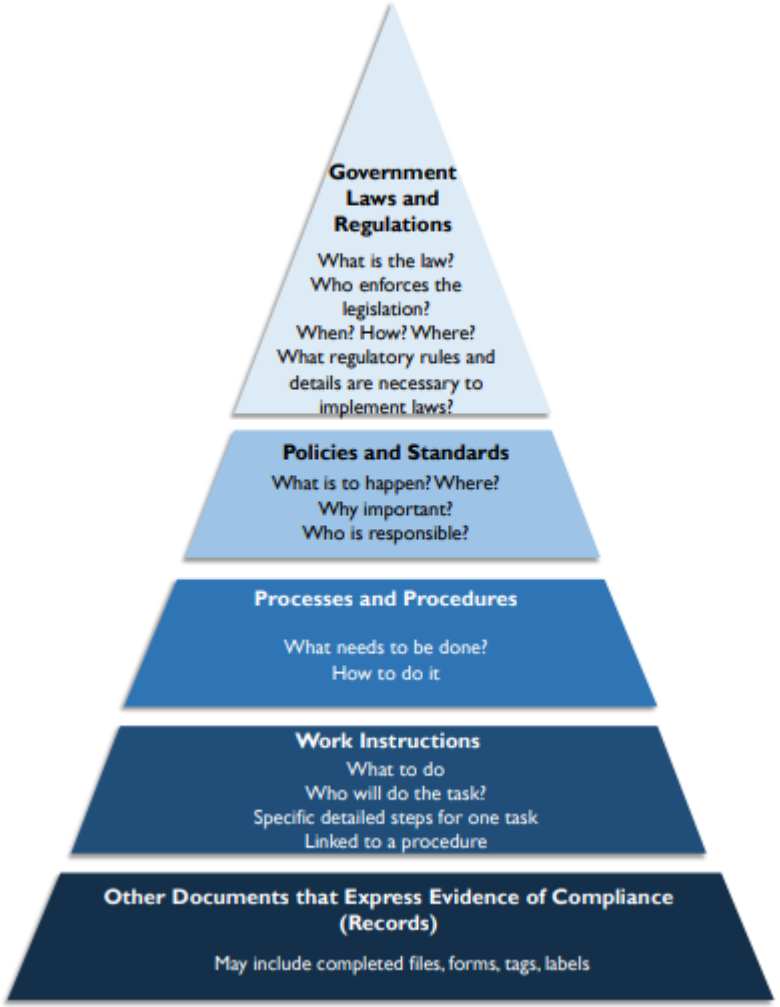
VI.- Gestión de Contenidos y Documentos

- Propósito: Actividades de planificación, implementación y control para la gestión del ciclo de vida de los datos y la información, presentes en cualquier formato o medio.

- Objetivos:
  1. Cumplir con las obligaciones legales y las expectativas del cliente en relación con la gestión de registros.
  2. Garantizar el almacenamiento, la recuperación y el uso eficaz y eficiente de los documentos y el contenido.
  3. Garantizar la integración del contenido estructurado y no estructurado.

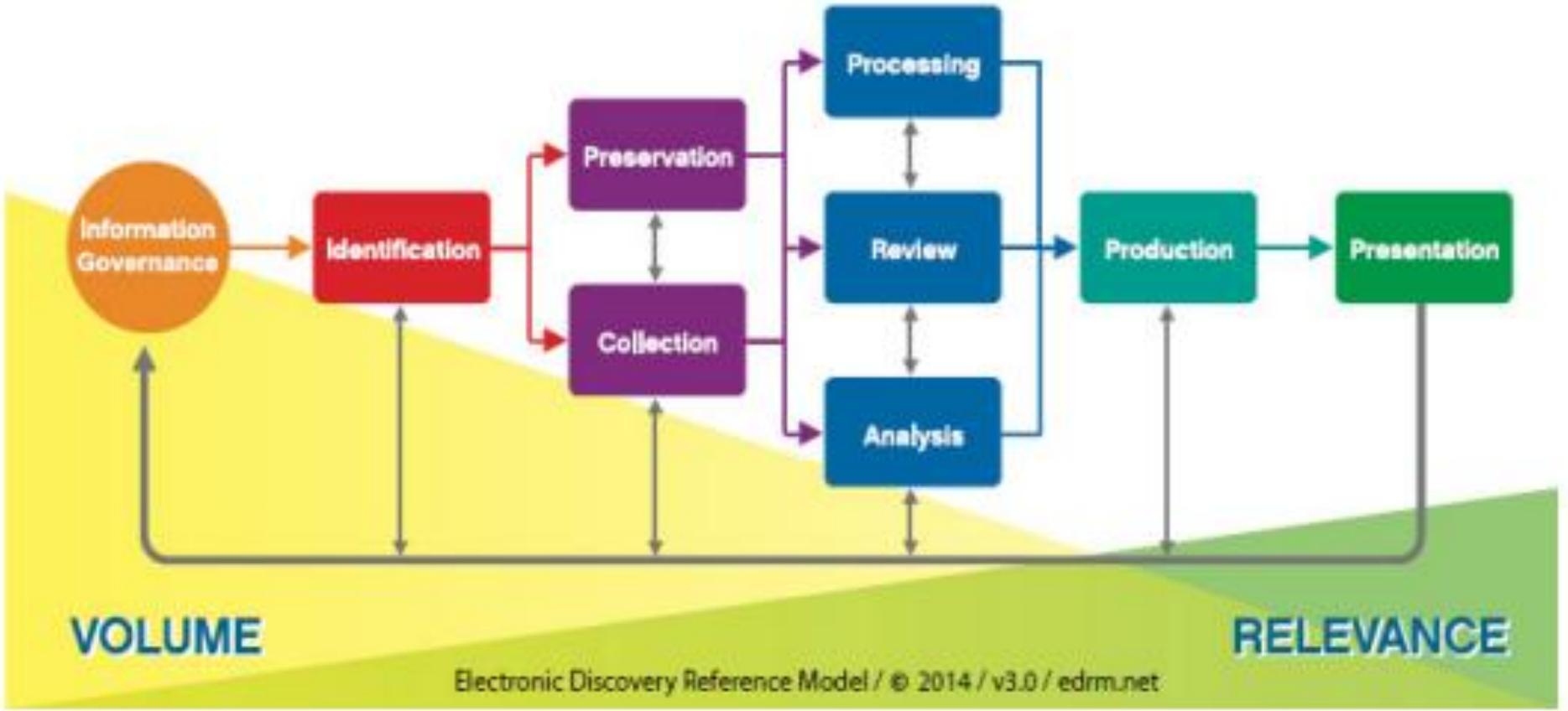


Jerarquía de Contenidos y Documentos



Data Asset	Formal	Revision	Custody
Action item lists		x	
Agendas			x
Audit findings		x	x
Budgets	x		
DD 250s			x
Final Proposal			x
Financial data and reports	x	x	x
Human Resources data		x	
Meeting minutes			x
Meeting notices and attendance lists		x	x
Project plans (including data management and configuration management plans)	x		
Proposal (in process)		x	
Schedules	x		
Statements of Work	x		
Trade studies		x	
Training material	x	x	
Working papers			x

Fases de la Gestión documental



Seguridad y Privacidad Asociada

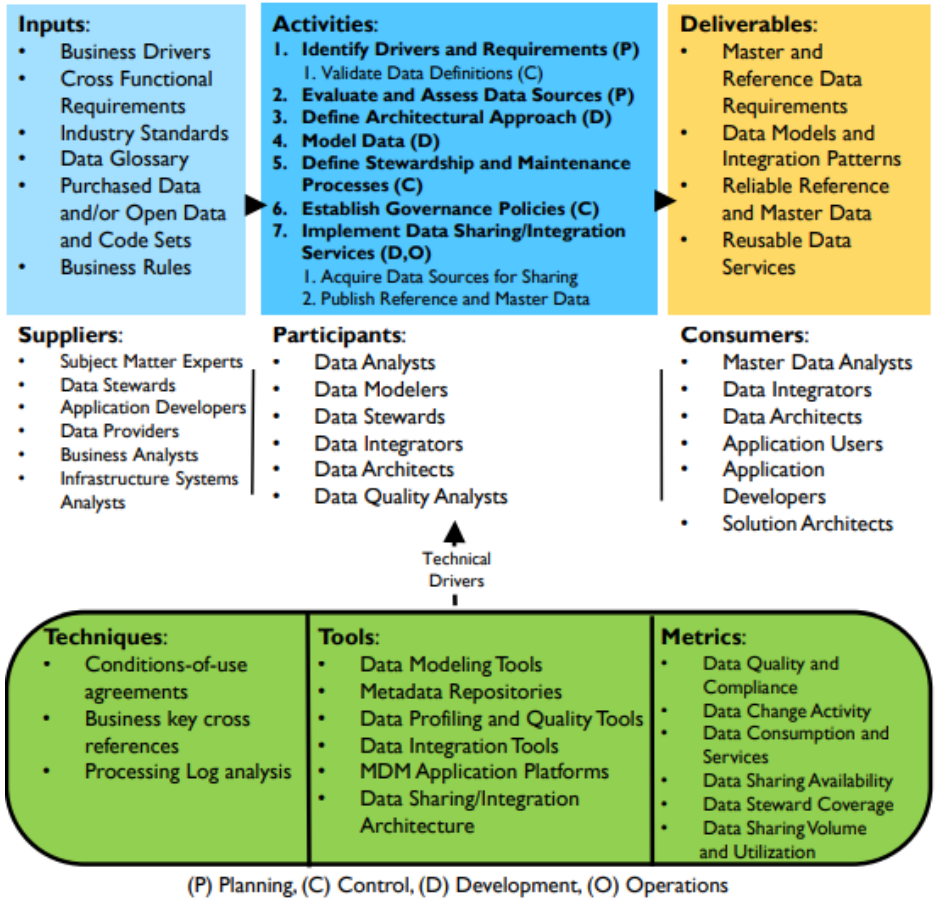
1. **Clasificación y etiquetado de documentos según criticidad**
   - Todo documento debe clasificarse según su nivel de confidencialidad y tipo de información contenida (corporativa, sensible, pública).
   - ISO 27001: A.5.12 "Clasificación de la información"
   - ISO 27001: A.5.9 "Inventario de activos"
   - Ley de Ciberseguridad: art. 10 (protección de información crítica).
   - **Resultado:** aplicación diferenciada de controles de seguridad física y lógica en la documentación.
2. **Control de acceso y custodia de documentos electrónicos**
   - Establecer permisos, auditoría de accesos y gestión de versiones en repositorios documentales (DMS, ECM, SharePoint, etc.).
   - ISO 27001: A.5.15–A.5.18 (gestión de accesos e identidades).
   - Ley de Ciberseguridad: art. 14 (segregación de funciones y protección de entornos).
   - **Resultado:** integridad documental asegurada y trazabilidad de responsables.
3. **Respaldo, recuperación y conservación de registros electrónicos**
   - Implementar copias de seguridad periódicas de archivos y repositorios críticos.
   - ISO 27001: A.8.13 "Copia de seguridad" y A.5.30–A.5.32 "Continuidad y disponibilidad".
   - Ley de Ciberseguridad: art. 19 (resiliencia y continuidad operativa).
   - **Resultado:** preservación de la evidencia documental ante incidentes o pérdida.
4. **Protección contra alteración o eliminación no autorizada**
   - Aplicar controles de integridad digital, checksum y auditoría para prevenir modificación o destrucción indebida.
   - ISO 27001: A.8.12 "Integridad de la información".
   - Ley de Ciberseguridad: art. 21 (registro y trazabilidad de eventos).
   - **Resultado:** conservación verificable de documentos oficiales y regulatorios.

1. **Identificación de documentos que contienen datos personales**
   - Catalogar los documentos (digitales o físicos) que incluyan PII o datos sensibles.
   - ISO 27701: A.7.3.2 "Identificación de categorías de datos personales".
   - ISO 29100: Principio de *transparencia y especificación de propósito*.
   - Ley de Protección de Datos: art. 5–6 (finalidad y proporcionalidad).
   - **Resultado:** control preciso sobre qué documentos están sujetos a obligaciones de privacidad.
2. **Gestión de retención y eliminación de documentos**
   - Establecer plazos diferenciados de conservación según tipo de documento y base legal.
   - ISO 27701: A.7.4.9 "Retención y supresión"
   - ISO 29100: Principio de *limitación de retención*
   - Ley de Protección de Datos: art. 11 (eliminación una vez cumplida la finalidad).
   - **Resultado:** cumplimiento del ciclo de vida del dato documental y reducción de riesgos regulatorios.
3. **Restricción de transferencia y circulación de documentos personales**
   - Controlar la distribución, copia o envío de documentos con información personal.
   - ISO 27701: A.7.4.7 "Transferencia de datos personales"
   - ISO 29100: Principio de *transparencia y consentimiento informado*.
   - Ley de Protección de Datos: art. 20 (transferencias internacionales).
   - **Resultado:** circulación documentada y conforme al principio de licitud.
4. **Privacidad por diseño en repositorios documentales**
   - Incorporar en los sistemas de gestión documental medidas como anonimización, control de metadatos y cifrado.
   - ISO 27701: A.7.4.2 "Privacidad por diseño y por defecto"
   - ISO 29100: *Privacy by Design*
   - Ley de Protección de Datos: art. 8 (protección proactiva de datos personales).
   - **Resultado:** cumplimiento de privacidad desde la tecnología y trazabilidad en todo el ciclo documental.

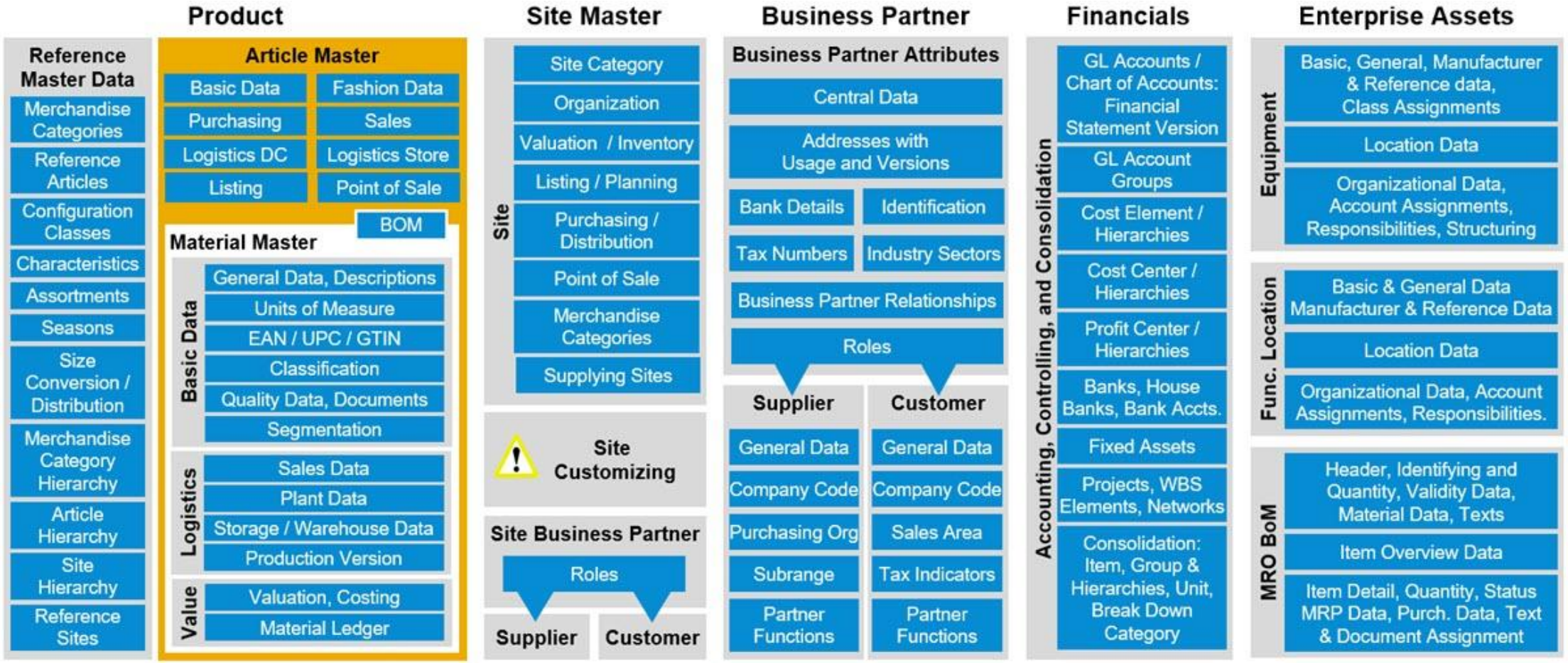
VII.- Datos Maestros

- Propósito: Gestionar datos compartidos para cumplir los objetivos organizacionales, reducir los riesgos asociados a la redundancia de datos, garantizar una mayor calidad y reducir los costos de integración de datos.

- Objetivos:
  1. Facilitar el intercambio de activos de información entre dominios y aplicaciones empresariales dentro de una organización.
  2. Proporcionar una fuente fiable de datos maestros y de referencia, conciliados y con calidad evaluada.
  3. Reducir los costos y la complejidad mediante el uso de estándares, modelos de datos comunes y patrones de integración.



Datos Maestros SAP



Seguridad y Privacidad Asociada

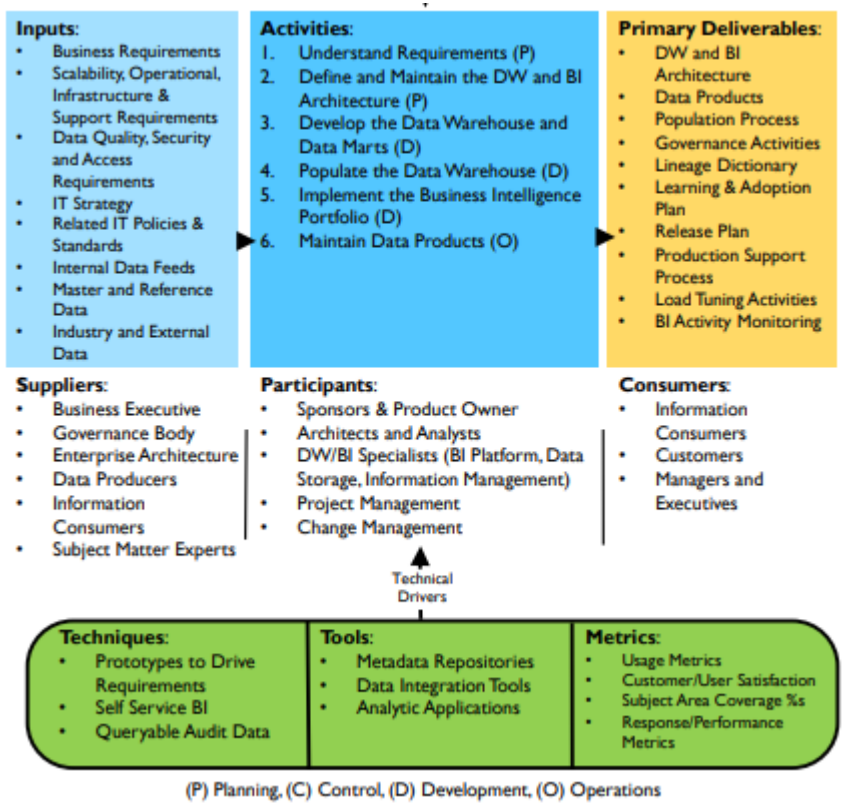
1. **Inventario y control de repositorios maestros**
   - Los sistemas que administran datos maestros (ERP, CRM, HRMS, directorios) deben estar inventariados como activos críticos.
   - ISO 27001: A.5.9 "Inventario de activos"
   - ISO 27001: A.5.12 "Clasificación de la información"
   - Ley de Ciberseguridad: art. 10 (protección de información crítica y servicios esenciales).
   - **Resultado:** identificación de las fuentes únicas de verdad (Single Source of Truth) bajo control SGSI.
2. **Gestión de acceso centralizada y segregada**
   - Los usuarios con privilegios sobre sistemas maestros deben tener acceso controlado y trazado.
   - ISO 27001: A.5.15–A.5.18 "Gestión de acceso e identidades"
   - ISO 27001: A.8.2 "Gestión de accesos privilegiados"
   - Ley de Ciberseguridad: art. 14 (segregación de funciones críticas).
   - **Resultado:** prevención de manipulación indebida o fuga desde fuentes maestras.
3. **Integridad y sincronización segura entre sistemas**
   - Toda réplica o sincronización de datos maestros debe garantizar integridad, autenticidad y cifrado del canal.
   - ISO 27001: A.8.12 "Integridad de la información"
   - ISO 27001: A.8.24 "Cifrado de datos en tránsito"
   - Ley de Ciberseguridad: art. 12 (protección de redes y canales).
   - **Resultado:** coherencia entre sistemas y mitigación de corrupción de datos.
4. **Monitoreo, registro y trazabilidad de actualizaciones**
   - Registrar quién crea, modifica o elimina datos maestros, y cuándo lo hace.
   - ISO 27001: A.5.23 "Registro de eventos"
   - ISO 27001: A.5.24 "Gestión de incidentes"
   - Ley de Ciberseguridad: art. 21 (registro y reporte obligatorio de incidentes).
   - **Resultado:** visibilidad completa de cambios y auditoría forense del dato maestro.

1. **Identificación de PII y categorías especiales en los datos maestros**
   - Los datos maestros deben clasificarse según contengan información personal o sensible (p. ej., nombre, RUT, salud, biometría).
   - ISO 27701: A.7.3.2 "Identificación de categorías de PII"
   - ISO 29100: Principio de *transparencia y especificación de propósito*
   - Ley de Protección de Datos: art. 5–6 (finalidad y proporcionalidad).
   - **Resultado:** segregación lógica entre datos personales y datos operacionales.
2. **Aplicación del principio de minimización en atributos maestros**
   - Los modelos MDM deben contener solo los atributos necesarios para los fines declarados.
   - ISO 27701: A.7.4.3 "Minimización y pseudonimización"
   - ISO 29100: Principio de *minimización de datos*
   - Ley de Protección de Datos: art. 6 (tratamiento proporcional).
   - **Resultado:** menor superficie de exposición y cumplimiento de privacidad por diseño.
3. **Sincronización responsable y control de transferencias de PII**
   - Los procesos de sincronización o integración entre sistemas deben incorporar controles sobre datos personales compartidos.
   - ISO 27701: A.7.4.7 "Transferencia de datos personales a terceros"
   - ISO 29100: Principio de *responsabilidad y consentimiento informado*
   - Ley de Protección de Datos: art. 20 (transferencias internacionales o interempresariales).
   - **Resultado:** gobernanza y trazabilidad de los flujos de PII a nivel organizacional.
4. **Gestión de derechos del titular desde el repositorio maestro**
   - Los sistemas MDM deben ser capaces de localizar, rectificar o eliminar registros personales a solicitud del titular.
   - ISO 27701: A.7.4.1–A.7.4.5 (derechos de los titulares)
   - ISO 29100: Principio de *participación individual*
   - Ley de Protección de Datos: arts. 14–16 (derechos ARCO y portabilidad).
   - **Resultado:** cumplimiento operativo de los derechos del titular en un único punto de control.

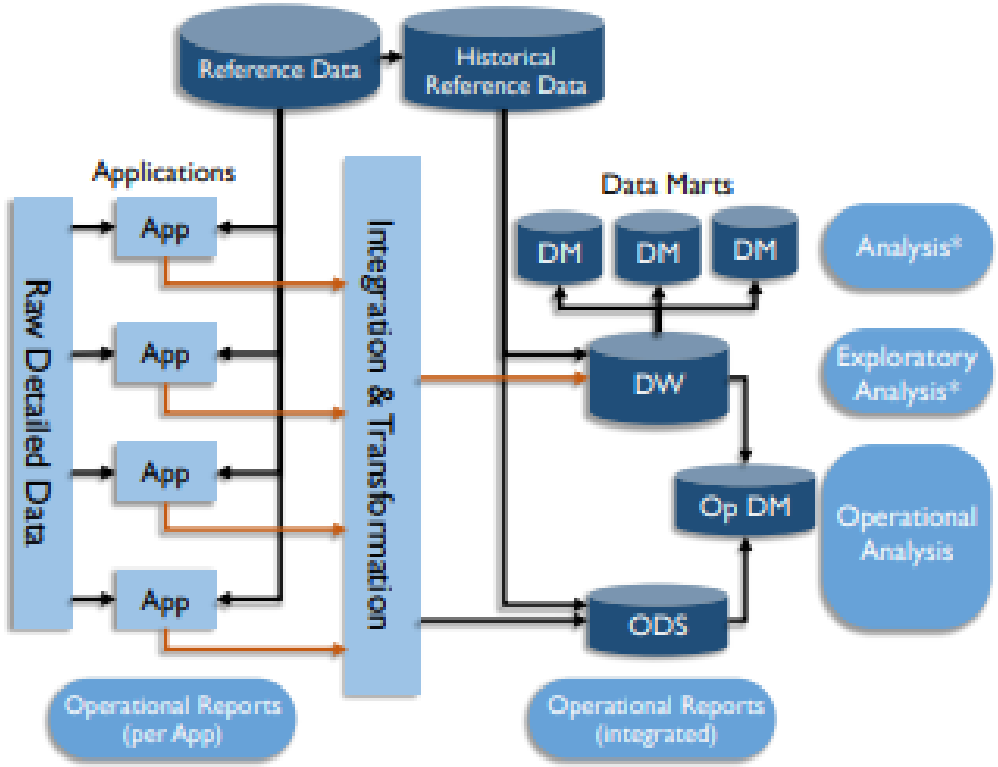
VIII.- Data Warehousing and Business Intelligence

- Propósito: Procesos de planificación, implementación y control para proporcionar datos de apoyo a la toma de decisiones y apoyar a los trabajadores del conocimiento que participan en informes, consultas y análisis.

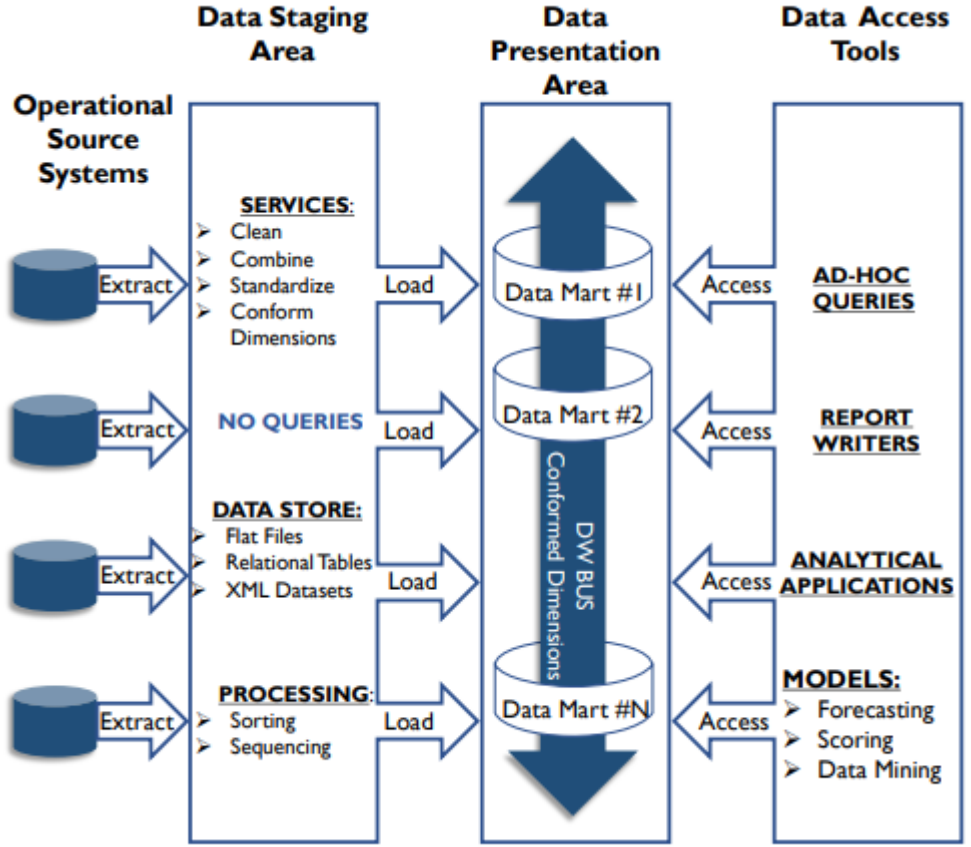
- Objetivos:
  1. Construir y mantener el entorno técnico y los procesos técnicos y comerciales necesarios para la entrega de datos integrados en apoyo de funciones operativas, requisitos de cumplimiento e inteligencia empresarial.
  2. Apoyar y posibilitar el análisis empresarial y la toma de decisiones eficaces por parte de los trabajadores de gestión del conocimiento.



Visión de Data Warehousing and Business Intelligence

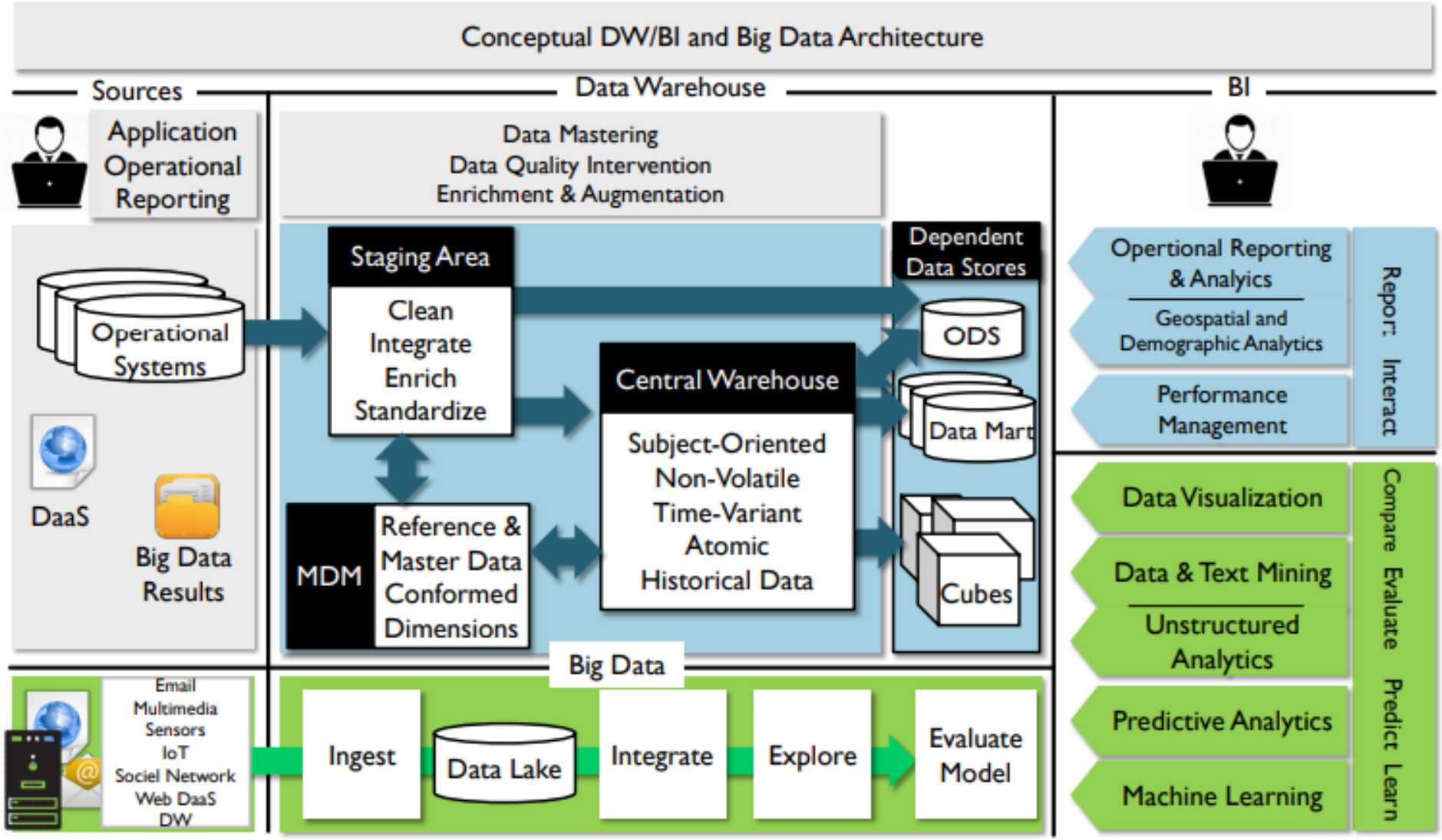


The Corporate Information Factory



Kimball's Data Warehouse

Conceptualización DW/BI and Arquitectura Big Data



Seguridad y Privacidad Asociada

1. **Segmentación y aislamiento del entorno analítico**
   - Los entornos DW/BI deben estar segregados de los sistemas operacionales y contener controles de acceso diferenciados.
   - ISO 27001: A.8.9 "Configuración segura" y A.8.14 "Separación de entornos".
   - Ley de Ciberseguridad: art. 10 (protección de infraestructuras críticas y segmentación de redes).
   - **Resultado:** menor exposición de datos sensibles y cumplimiento del principio de separación de dominios.
2. **Control de acceso granular en cubos, vistas y dashboards**
   - La visualización y análisis de información deben estar restringidos según el rol y la finalidad.
   - ISO 27001: A.5.15–A.5.18 "Control de acceso e identidades".
   - Ley de Ciberseguridad: art. 14 (principio de mínimo privilegio y segregación funcional).
   - **Resultado:** prevención de exposición no autorizada en entornos de análisis.
3. **Integridad y protección en los procesos ETL**
   - Los procesos de extracción, transformación y carga deben estar protegidos contra inyección, pérdida o alteración de datos.
   - ISO 27001: A.8.12 "Integridad de la información" y A.8.24 "Cifrado de datos en tránsito".
   - Ley de Ciberseguridad: art. 12 (protección de comunicaciones y procesamiento).
   - **Resultado:** datos consistentes y autenticados en el pipeline analítico.
4. **Registro y monitoreo de consultas analíticas**
   - Toda extracción, consulta o generación de reportes debe quedar registrada y auditada.
   - ISO 27001: A.5.23 "Registro de eventos" y A.5.24 "Gestión de incidentes de seguridad".
   - Ley de Ciberseguridad: art. 21 (monitoreo y reporte obligatorio de incidentes).
   - **Resultado:** trazabilidad total del uso de datos en inteligencia de negocios.

1. **Anonimización y minimización de datos personales en entornos analíticos**
   - Los procesos de carga hacia DW/BI deben eliminar identificadores personales directos.
   - ISO 27701: A.7.4.3 "Minimización y pseudonimización".
   - ISO 29100: Principio de *minimización de datos*.
   - Ley de Protección de Datos: art. 6 (principio de proporcionalidad).
   - **Resultado:** cumplimiento de privacidad por diseño y reducción de riesgo de reidentificación.
2. **Limitación de propósito y uso ético de la analítica**
   - Los análisis deben respetar el propósito original para el cual los datos fueron recolectados.
   - ISO 27701: A.7.2.1 "Propósito del tratamiento de PII".
   - ISO 29100: Principio de *especificación de propósito*.
   - Ley de Protección de Datos: art. 5 (finalidad legítima del tratamiento).
   - **Resultado:** análisis transparentes, alineados a las expectativas del titular y el marco legal.
3. **Evaluación de impacto en proyectos analíticos y de IA**
   - Cualquier uso de datos personales en modelos predictivos debe evaluarse mediante DPIA o Privacy Impact Assessment.
   - ISO 27701: A.7.2.5 "Evaluaciones de impacto en privacidad".
   - ISO 29100: Principio de *evaluación de riesgos de privacidad*.
   - Ley de Protección de Datos: art. 32 (evaluaciones de riesgo en tratamientos de alto impacto).
   - **Resultado:** detección temprana de riesgos éticos y regulatorios en proyectos de análisis avanzado.
4. **Transparencia y auditoría de procesos analíticos automatizados**
   - Los sistemas de BI deben conservar evidencia de reglas de negocio, algoritmos o modelos aplicados sobre datos personales.
   - ISO 27701: A.7.4.10 "Registro de actividades de tratamiento".
   - ISO 29100: Principio de *transparencia y participación del titular*.
   - Ley de Protección de Datos: art. 5 (derecho a conocer la lógica de decisiones automatizadas).
   - **Resultado:** trazabilidad y explicabilidad de decisiones analíticas basadas en datos.

IX.- Gestión de Metadatos

- Propósito: Actividades de planificación, implementación y control para permitir el acceso a servicios de alta calidad y metadatos integrados.

- Objetivos:
  1. Proporcionar comprensión organizacional de los términos y usos comerciales.
  2. Recopilar e integrar metadatos de diversas fuentes.
  3. Proporcionar una forma estándar de acceder a los metadatos.
  4. Garantizar la calidad y seguridad de los metadatos.

¿Que son los Metadato?

- Los metadatos describen qué datos posee una organización, qué representan, cómo se clasifican, de dónde provienen, cómo se mueven dentro de la organización, cómo evolucionan con el uso, quién puede y quién no puede usarlos, y si son de alta calidad. Los datos son abstractos. Las definiciones y otras descripciones del contexto facilitan su comprensión. Hacen comprensibles los datos, su ciclo de vida y los sistemas complejos que los contienen.

- El desafío radica en que los metadatos son un tipo de datos y deben gestionarse como tales. Las organizaciones que no gestionan bien sus datos generalmente no gestionan sus metadatos en absoluto. La gestión de metadatos a menudo proporciona un punto de partida para mejorar la gestión general de datos.

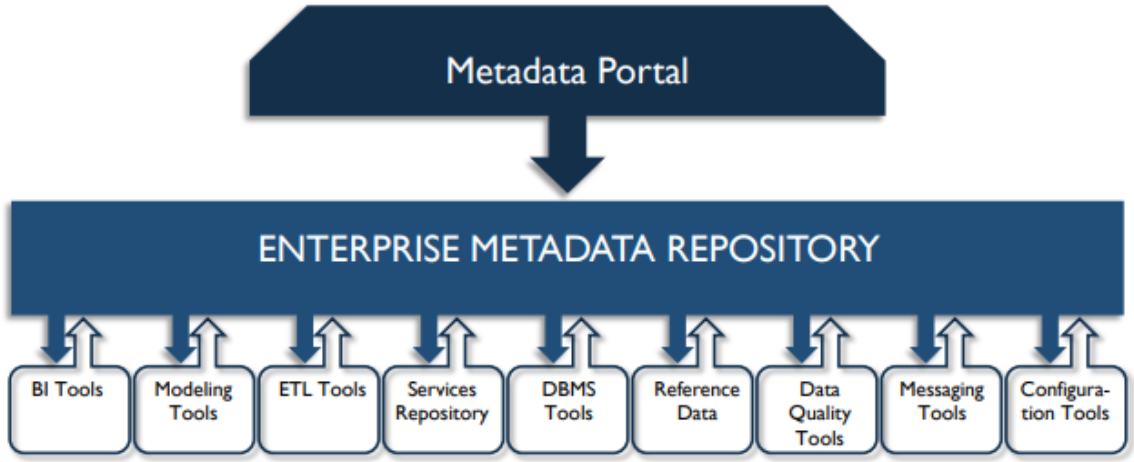
Metadatos de Negocio

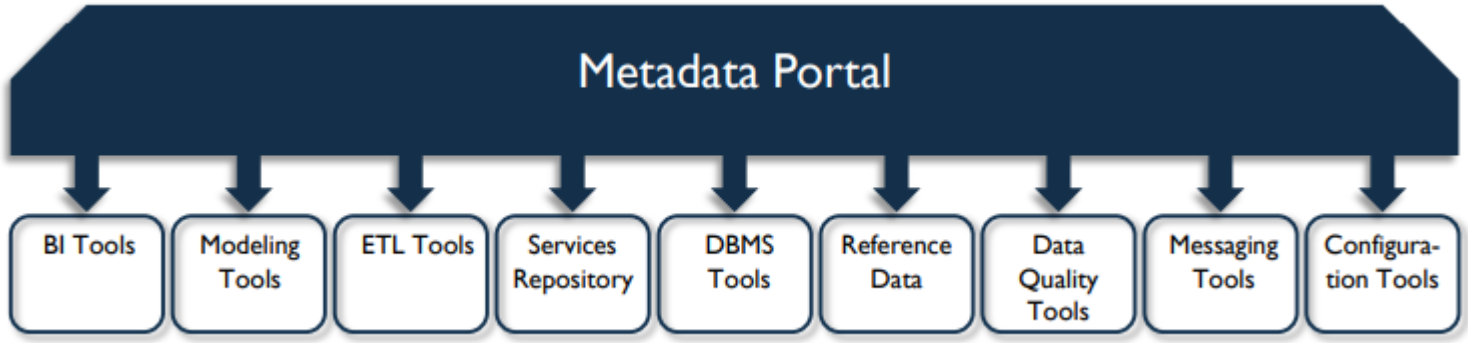
- Reglas de negocio, reglas de transformación, cálculos y derivaciones
- Modelos de datos
- Reglas de calidad de datos y resultados de medición
- Horarios según los cuales se actualizan los datos
- Verificación de datos y flujo de datos
- Estándares de datos
- Designaciones del sistema de registro de elementos de datos
- Restricciones de valor válido
- Información de contacto de las partes interesadas
- Problemas conocidos con los datos
- Notas de uso de datos

Metadatos Técnicos

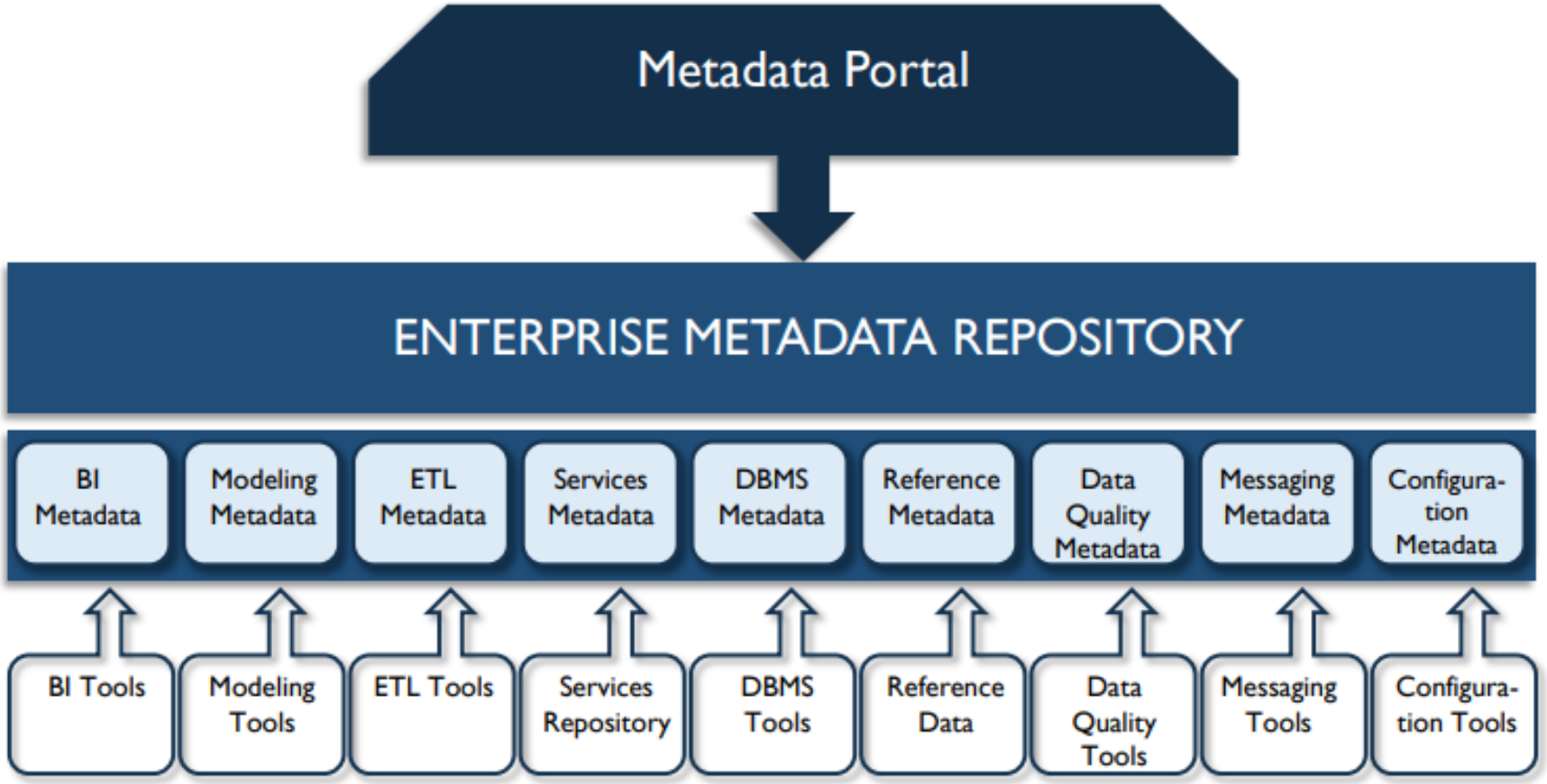
- Nombres de tablas y columnas de bases de datos físicas
- Propiedades de la columna
- Propiedades de los objetos de la base de datos
- Permisos de acceso
- Reglas CRUD de datos (crear, reemplazar, actualizar y eliminar)
- Modelos de datos físicos, incluidos nombres de tablas de datos, claves e índices
- Relaciones documentadas entre los modelos de datos y los activos físicos
- Detalles del trabajo ETL
- Definiciones de esquemas de formato de archivo
- Documentación de mapeo de origen a destino
- Documentación del flujo de datos
- Nombres y descripciones de programas y aplicaciones
- Programaciones y dependencias de trabajos del ciclo de actualización de contenido
- Reglas de recuperación y copia de seguridad
- Derechos de acceso a datos, grupos, roles

Arquitectura de Metadatos Centralizada v/s Distruibida

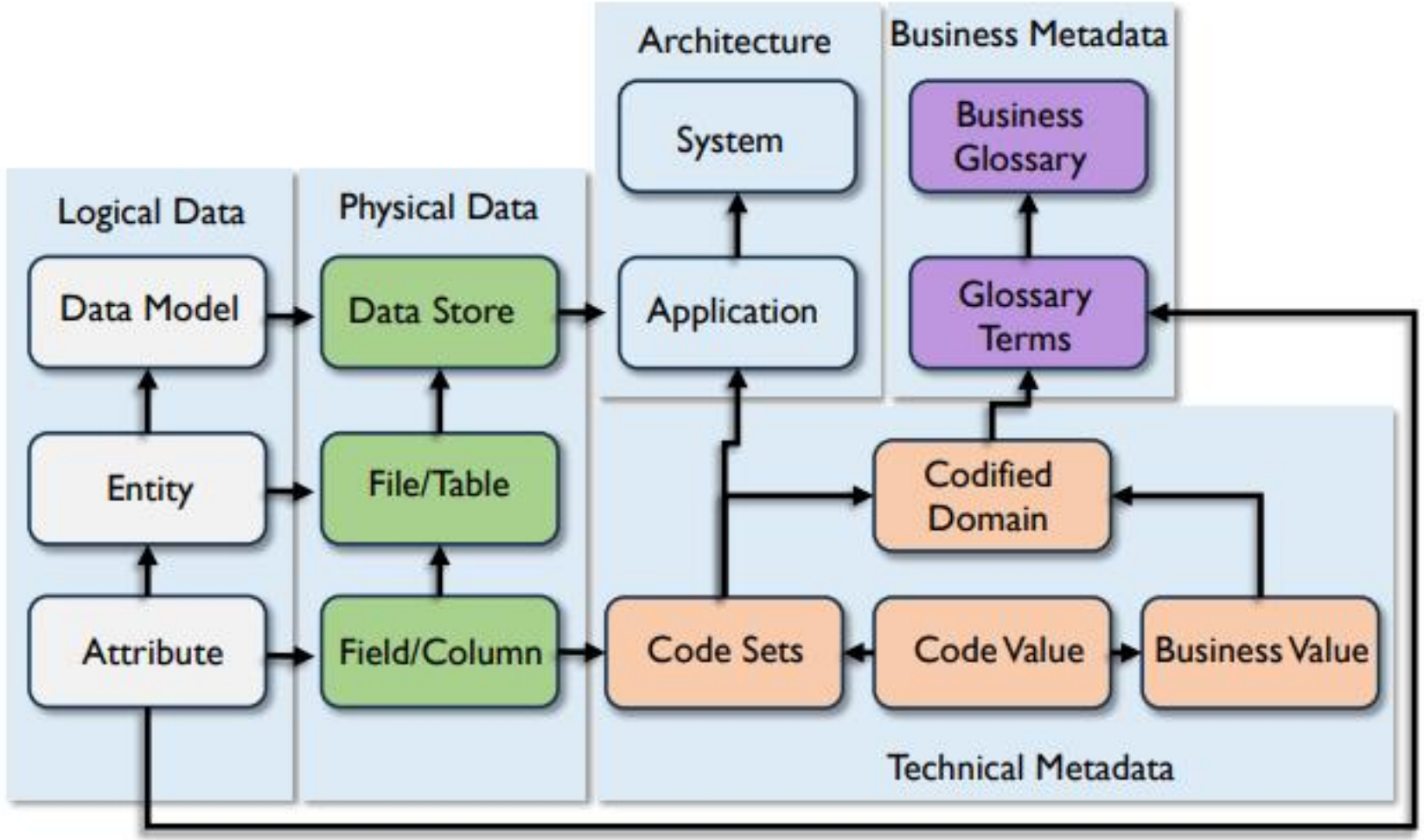




Arquitectura de Metadatos Hibrida



Ejemplo de Repositorio de Metadatos



Seguridad y Privacidad Asociada

1. **Inventario y clasificación extendida mediante metadatos**
   - Los metadatos documentan el nivel de criticidad, confidencialidad y propietario de cada activo de información.
   - ISO 27001: A.5.9 "Inventario de activos"
   - ISO 27001: A.5.12 "Clasificación de la información"
   - Ley de Ciberseguridad: art. 10 (protección de información crítica).
   - **Resultado:** visibilidad centralizada de los activos informacionales y su nivel de protección requerido.
2. **Metadatos de control de acceso y autorización**
   - Incluir en los metadatos las reglas de acceso, roles autorizados y restricciones de uso.
   - ISO 27001: A.5.15–A.5.18 "Gestión de acceso e identidades"
   - Ley de Ciberseguridad: art. 14 (principio de mínimo privilegio).
   - **Resultado:** alineación entre el modelo de acceso y el catálogo de datos, fortaleciendo el control de seguridad.
3. **Registro de eventos y trazabilidad automatizada**
   - Los metadatos deben contener información de cambios, consultas, transferencias y auditorías.
   - ISO 27001: A.5.23 "Registro de eventos"
   - ISO 27001: A.5.24 "Gestión de incidentes de seguridad"
   - Ley de Ciberseguridad: art. 21 (registro obligatorio y reporte de incidentes).
   - **Resultado:** trazabilidad completa de operaciones sobre datos, esencial para auditorías o respuesta a incidentes.
4. **Integración del linaje de datos con gestión de riesgos**
   - Vincular los metadatos de linaje (origen, transformación, destino) con el análisis de riesgo del SGSI.
   - ISO 27001: Cl. 6.1 "Acciones frente a riesgos y oportunidades"
   - Ley de Ciberseguridad: art. 9 (evaluación y gestión de riesgos cibernéticos).
   - **Resultado:** mapa de riesgos actualizado que permite proteger los flujos críticos de información.

1. **Identificación y catalogación de PII en los metadatos**
   - Los metadatos deben indicar si un activo contiene datos personales y su categoría (ordinarios o sensibles).
   - ISO 27701: A.7.3.2 "Identificación de categorías de datos personales"
   - ISO 29100: Principio de *transparencia y especificación de propósito*
   - Ley de Protección de Datos: art. 5–6 (licitud y finalidad).
   - **Resultado:** visibilidad clara de dónde residen los datos personales en la organización.
2. **Trazabilidad del tratamiento de datos personales**
   - Registrar en los metadatos qué procesos, áreas o terceros tratan la información personal.
   - ISO 27701: A.7.4.10 "Registro de actividades de tratamiento"
   - ISO 29100: Principio de *responsabilidad (accountability)*
   - Ley de Protección de Datos: art. 30 (registro de operaciones de tratamiento).
   - **Resultado:** cumplimiento del principio de responsabilidad demostrada y trazabilidad completa.
3. **Metadatos de retención y eliminación**
   - Incorporar en los metadatos la política de retención y las fechas de supresión de datos personales.
   - ISO 27701: A.7.4.9 "Retención y supresión"
   - ISO 29100: *Limitación de retención*
   - Ley de Protección de Datos: art. 11 (eliminación una vez cumplida la finalidad).
   - **Resultado:** automatización de la gestión del ciclo de vida de los datos personales.
4. **Metadatos sobre transferencias y consentimiento asociado**
   - Registrar los consentimientos, cláusulas contractuales y jurisdicciones aplicables a cada flujo de datos personales.
   - ISO 27701: A.7.4.7 "Transferencias internacionales"
   - ISO 29100: *Transparencia y consentimiento informado*
   - Ley de Protección de Datos: art. 20 (transferencias internacionales y consentimiento).
   - **Resultado:** evidencia documental de la legitimidad del tratamiento y trazabilidad del consentimiento.

X.- Calidad de Datos

- Propósito: Planificación, implementación y control de actividades que aplican técnicas de gestión de calidad a los datos, con el fin de garantizar que sean aptos para el consumo y satisfagan las necesidades de los consumidores.

- Objetivos:
  1. Desarrollar un enfoque gobernado para que los datos sean adecuados para su propósito, según los requisitos de los consumidores.
  2. Definir estándares, requisitos y especificaciones para los controles de calidad de los datos como parte de su ciclo de vida.
  3. Definir e implementar procesos para medir, supervisar e informar sobre los niveles de calidad de los datos.
  4. Identificar y promover oportunidades para mejorar la calidad de los datos mediante mejoras en los procesos y sistemas

Atributos de la Calidad de Datos

- Calidad de Datos Intrínseca
  - Precisión
  - Objetividad
  - Credibilidad
  - Reputación
- Calidad de Datos Contextual
  - Valor agregado
  - Relevancia
  - Oportunidad
  - Integridad
  - Cantidad Adecuada de Datos
- Calidad de Datos Representacional
  - Interpretabilidad
  - Facilidad de Comprensión
  - Consistencia Representacional
  - Representación Concisa
- Calidad de Datos
  - Accesibilidad
  - Seguridad de Acceso

Modelo de datos

- Contenido
  - Relevancia de los datos
  - Capacidad de obtener los valores
  - Claridad de las definiciones
- Nivel de detalle
  - Granularidad de los atributos
  - Precisión de los dominios de los atributos
- Composición
  - Naturalidad
  - Identificabilidad
  - Homogeneidad
  - Redundancia mínima necesaria
- Consistencia
  - Consistencia semántica
  - Consistencia estructural
- Reacción al cambio
  - Robustez
  - Flexibilidad

Valores de los datos

- Precisión
- Integridad
- Vigencia
- Coherencia

Representación

- Adecuación
- Interpretabilidad
- Portabilidad
- Precisión de formato
- Flexibilidad de formato
- Capacidad para representar valores nulos
- Uso eficiente del almacenamiento
- Instancias físicas de datos que cumplen con sus formatos

Seguridad y Privacidad Asociada

1. **Integridad y control de cambios en los datos**
   - Establecer mecanismos técnicos que garanticen que los datos no sean alterados, borrados o corrompidos de forma no autorizada.
   - ISO 27001: A.8.12 "Integridad de la información"
   - ISO 27001: A.5.23 "Registro de eventos"
   - Ley de Ciberseguridad: art. 21 (registro y trazabilidad de modificaciones).
   - **Resultado:** los datos mantienen su autenticidad y confiabilidad, auditables ante cualquier evento.
2. **Validación automatizada de entrada y procesamiento**
   - Aplicar controles automáticos que verifiquen la exactitud y coherencia de los datos al ser ingresados o procesados.
   - ISO 27001: A.8.9 "Gestión segura de configuraciones y procesos"
   - ISO 27001: A.5.13 "Gestión de la calidad de la información"
   - Ley de Ciberseguridad: art. 10 (integridad de operaciones en sistemas críticos).
   - **Resultado:** reducción de errores humanos y mayor consistencia de los registros.
3. **Monitoreo de calidad como parte del SGSI**
   - Incorporar la revisión de calidad en los controles del Sistema de Gestión de Seguridad de la Información (SGSI).
   - ISO 27001: Cl. 9.1–9.3 "Evaluación del desempeño y revisión por la dirección".
   - Ley de Ciberseguridad: art. 24 (auditorías periódicas).
   - **Resultado:** la calidad de datos se convierte en indicador de madurez del SGSI.
4. **Continuidad y restauración de datos íntegros**
   - Los respaldos deben preservar la estructura, precisión y completitud de los datos.
   - ISO 27001: A.8.13 "Copia de seguridad"
   - ISO 27001: A.5.30–A.5.32 "Continuidad y disponibilidad"
   - Ley de Ciberseguridad: art. 19 (resiliencia operativa y continuidad).
   - **Resultado:** restauraciones seguras, sin pérdida de integridad o contexto del dato.

1. **Exactitud y actualización de datos personales**
   - Garantizar que los datos personales sean precisos y estén actualizados de acuerdo con la finalidad del tratamiento.
   - ISO 27701: A.7.4.8 "Exactitud y actualización"
   - ISO 29100: Principio de *calidad de los datos*
   - Ley de Protección de Datos: art. 9 (exactitud y actualización).
   - **Resultado:** información veraz y actual, alineada al principio de legalidad del tratamiento.
2. **Minimización y pertinencia para el propósito**
   - Mantener solo los datos estrictamente necesarios para el objetivo declarado, eliminando redundancias o atributos irrelevantes.
   - ISO 27701: A.7.4.3 "Minimización"
   - ISO 29100: Principio de *proporcionalidad y limitación de propósito*
   - Ley de Protección de Datos: art. 6 (proporcionalidad).
   - **Resultado:** datos ajustados al propósito legítimo, reduciendo riesgo y exposición.
3. **Gestión de calidad y rectificación de datos personales**
   - Implementar procesos para detectar y corregir datos personales erróneos o desactualizados.
   - ISO 27701: A.7.4.1–A.7.4.5 (Derechos del titular: acceso, rectificación, supresión).
   - ISO 29100: *Participación individual.*
   - Ley de Protección de Datos: art. 14–16 (derechos ARCO y portabilidad).
   - **Resultado:** calidad sustentada en la participación del titular y cumplimiento del derecho de rectificación.
4. **Revisión de calidad antes de transferencia o uso analítico**
   - Antes de compartir o analizar información personal, debe verificarse la exactitud y pertinencia del dato.
   - ISO 27701: A.7.4.7 "Transferencia de datos personales a terceros"
   - ISO 29100: *Transparencia y responsabilidad*
   - Ley de Protección de Datos: art. 20 (transferencias seguras y fundadas).
   - **Resultado:** decisiones basadas en datos válidos, legítimos y verificables.

CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

Gobierno de Datos

Integración con Seguridad de la Información y Privacidad

ALIGNMENT
SOLUCIONES ESTRATÉGICAS

DIPLOMADO
CIBERSEGURIDAD