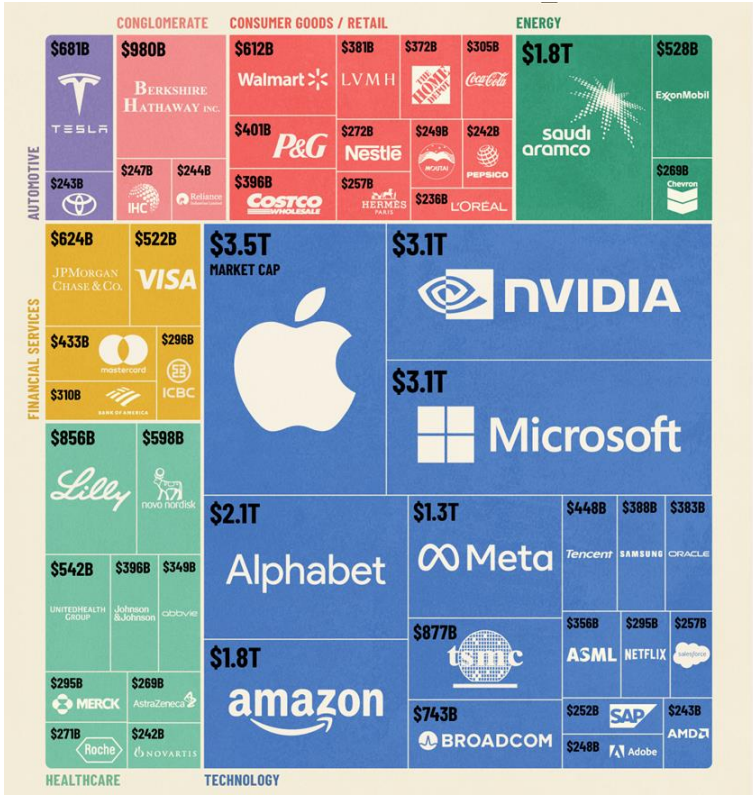
Data Management Fundamentals
Módulo 11 – Data Security

Óscar Alonso Llombart
Data & AI Strategy and Governance Lead at T-Systems Iberia
oscar.alonso-llombart@t-systems.com
https://www.linkedin.com/in/oscar-alonso-llombart/

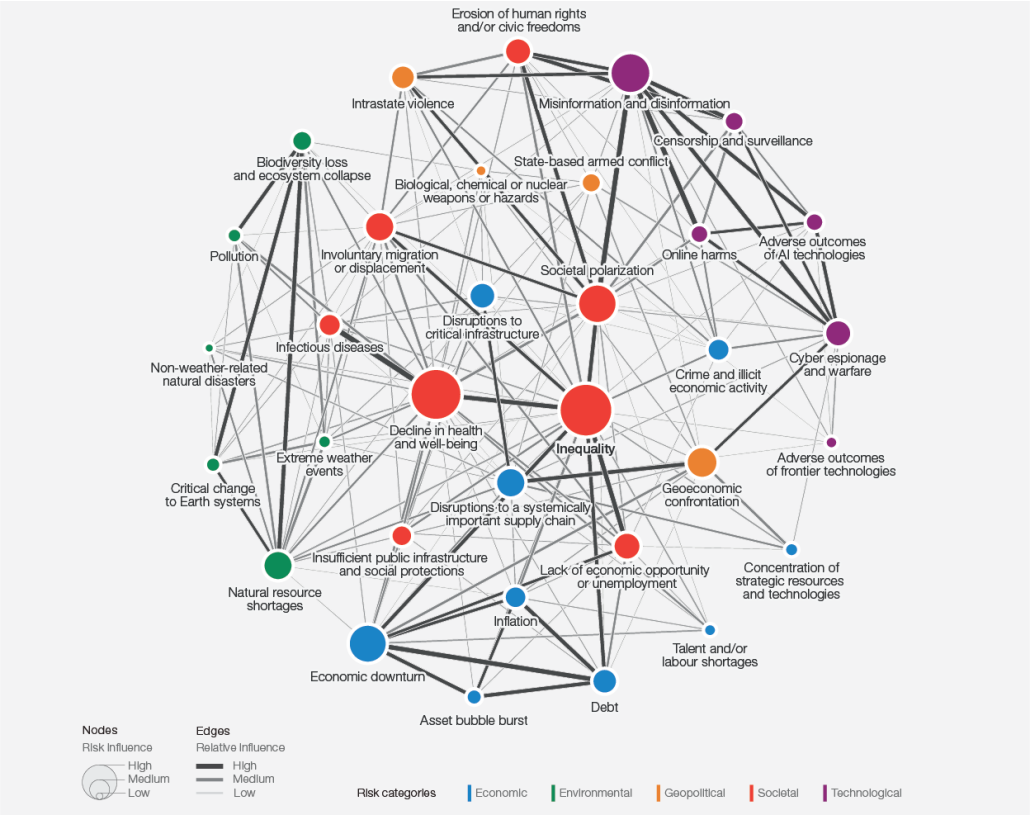
The 50 Most Valuable Companies in the World in 2024



Rank	Company	Industry	Market Cap ($B)
1	Apple	Technology	$3,454
2	NVIDIA	Technology	$3,111
3	Microsoft	Technology	$3,073
4	Alphabet	Technology	$2,055
5	Amazon	Technology	$1,842
6	Saudi Aramco	Energy	$1,803
7	Meta	Technology	$1,318
8	Berkshire Hathaway	Conglomerate	$980
9	TSMC	Technology	$877
10	Eli Lilly	Healthcare	$856

Fuente: https://www.visualcapitalist.com/ranked-the-50-most-valuable-companies-in-the-world-in-2024/

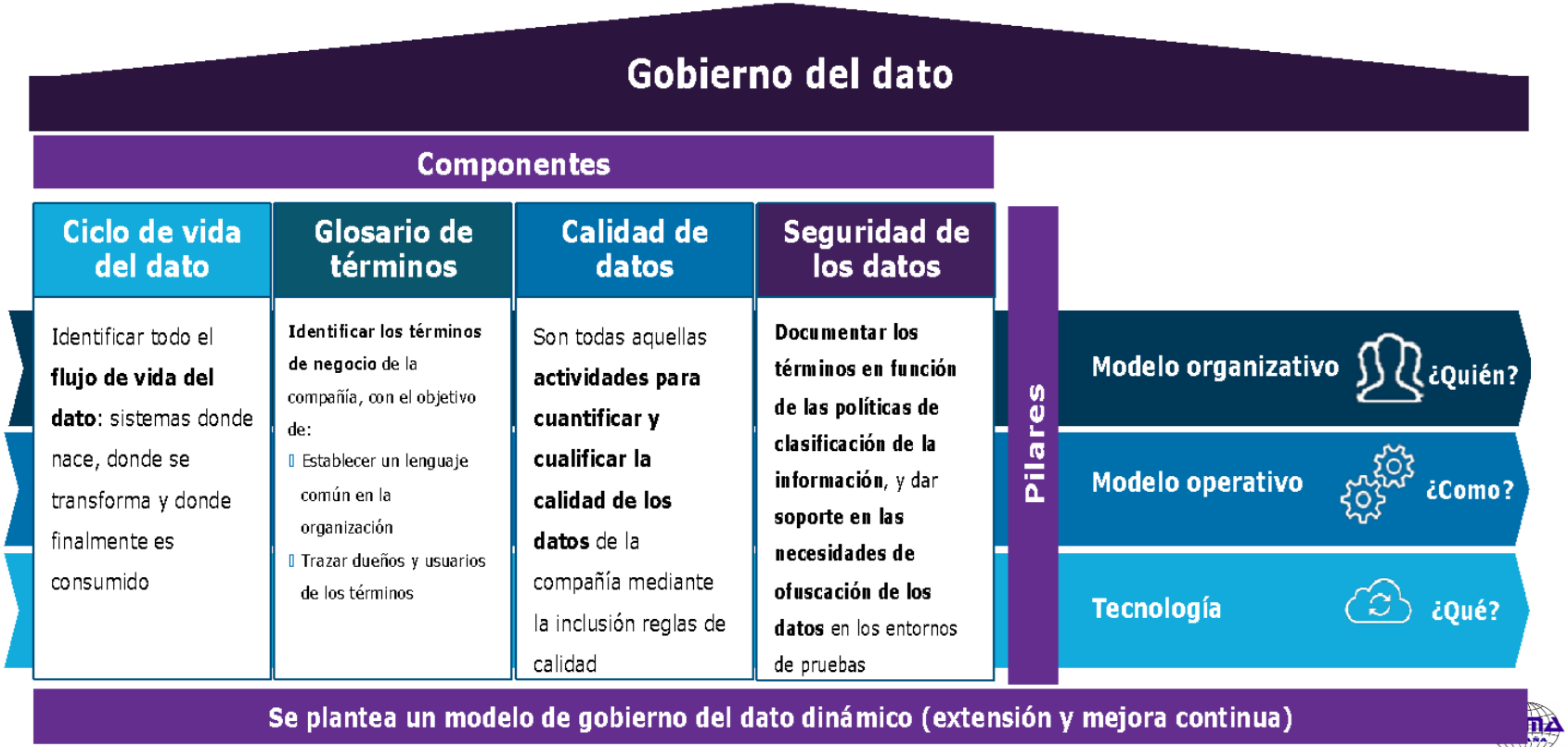
Los datos son un activo a ser protegido y cuidado



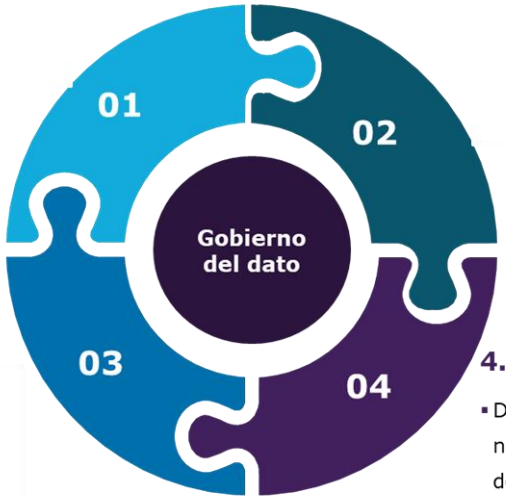
Fuente: https://es.weforum.org/publications/global-risks-report-2025/digest/

Los 5 “must” que deben cumplir los datos

Componentes tipo de gobierno de los datos



Componentes tipo de gobierno de los datos



4. Seguridad de los datos

- Documentar los términos de negocio en función de las políticas de clasificación de la información
- Dar soporte en relación a las necesidades de ofuscación de los datos en los entornos de pruebas

Actividades

- Identificar los requisitos de seguridad de datos pertinentes: clasificación de los distintos términos de negocio en función de si es información sensible, confidencial o de GDPR, en función de la política de seguridad de la Compañía.
- Incluir en la herramienta tecnológica la clasificación de seguridad de los términos de negocio.
- Asegurar el cumplimiento de la normativa vigente en relación a protección de datos
- Evaluar los riesgos de seguridad actuales e identificar iniciativas para solventar las posibles deficiencias.
- Aplicar controles y procedimientos para garantizar el cumplimiento de las políticas definidas.
- Identificar responsables y procesos para la correcta gestión.

Resultados esperados

- Garantizar el cumplimiento normativo en relación al tratamiento de los datos personales (GDPR)
- Asegurar el cumplimiento de las políticas de seguridad y de clasificación de la información establecidas por la Dirección

Aspectos clave de la seguridad y privacidad de datos

Data classification

Another key aspect is to ensure the quality and accuracy of the data, as poor data quality can compromise the security and privacy of the data and its users

Data quality can also enhance the security and privacy of the data by reducing the risk of errors, fraud, identity theft, or breaches that may result from inaccurate, outdated, or duplicate data

Data quality

Another key aspect is to ensure the quality and accuracy of the data, as poor data quality can compromise the security and privacy of the data and its users

Data quality can also enhance the security and privacy of the data by reducing the risk of errors, fraud, identity theft, or breaches that may result from inaccurate, outdated, or duplicate data

Data ownership

Defining and assigning roles and responsibilities for data owners, digital support, and stewards is a crucial aspect of ensuring the security and privacy of data

1. Data ownership refers to the responsibility for the respective data in a particular data domain
2. Digital support manages data storage, backup, recovery, and archiving
3. Data stewards oversee data quality, consistency, and compliance

This trio of roles collectively plays a vital role in shaping policies, procedures, and standards for safeguarding and preserving data

Data access

Control and monitor the access and usage of the data, as unauthorized or inappropriate access can jeopardize the security and privacy of the data and its subjects

Data access refers to the ability and permission of the users or applications to view, modify, or transfer the data

Data access can be regulated by implementing data encryption, authentication, authorization, auditing, and logging mechanisms

Data lifecycle

Data lifecycle refers to the stages and transitions that the data goes through from its creation to its disposal, such as collection, storage, processing, distribution, retention, and deletion

We can manage the data lifecycle by defining and applying the policies, rules, and schedules for each stage of the data lifecycle, as well as by evaluating and optimizing the performance, efficiency, and cost-effectiveness of the data lifecycle

The data lifecycle can also support data security and privacy by ensuring that the data is stored securely, processed lawfully, distributed securely, retained appropriately, and deleted securely

Data culture

Foster and maintain a culture of security and privacy awareness and accountability among the data users, producers, and managers

Data culture refers to the values, beliefs, attitudes, and behaviors that influence how the data is perceived, handled, and utilized in an organization

We can cultivate data culture by providing regular training, education, and communication on the best practices, standards, and regulations for security and privacy of the data, as well as by promoting a culture of trust, transparency, and responsibility for the data

¿Qué, quién y cómo?

Propiedad

La propiedad de los datos (quién) identificando a las personas y posiciones que participan en la gestión de datos dentro de la organización y asegurando la definición formal de sus responsabilidades y rendición de cuentas

Gestión

La gestión de los datos (qué) permitiendo aprovechar al máximo los activos de los datos con el apoyo de los procesos y herramientas adecuadas

Gobierno

El gobierno de los datos (cómo) de los datos proporcionando dirección y estructura a las actividades de propiedad y de gestión de los datos

Data Security

La seguridad de los datos incluye la planificación, el desarrollo y la ejecución de políticas y procedimientos de seguridad para proporcionar una autenticación, autorización, acceso y auditoría adecuados de los datos y los activos de información.

Los aspectos clave de Data Security son:

- **Los Stakeholders (Grupo de Interés):** Las organizaciones deben reconocer las necesidades de privacidad y confidencialidad de sus interesados, incluidos los clientes, pacientes, estudiantes, ciudadanos, proveedores o socios comerciales. Todos los integrantes de una organización deben ser fideicomisarios responsables de los datos sobre las partes interesadas.
- **Regulaciones gubernamentales:** Se han establecido reglamentos gubernamentales para proteger los intereses de algunos interesados. Los reglamentos tienen diferentes objetivos. Algunos restringen el acceso a la información, mientras que otros garantizan la apertura, la transparencia y la responsabilidad. (GDPR, Basilea, Solvency)

Data Security

- **Assets que son parte de la ventaja competitiva de la empresa:** Cada organización tiene datos de propiedad exclusiva que debe proteger. Los datos de una organización permiten conocer a sus clientes y, cuando se aprovechan eficazmente, pueden proporcionar una ventaja competitiva. Si los datos confidenciales son robados o violados, una organización puede perder la ventaja competitiva.
- **Necesidades de acceso legítimo:** Al proteger los datos, las organizaciones también deben permitir el acceso legítimo. Los procesos empresariales requieren que las personas que desempeñan determinadas funciones puedan acceder a los datos, utilizarlos y mantenerlos.
- **Obligaciones contractuales:** Los acuerdos contractuales y de no divulgación también influyen en los requisitos de seguridad de los datos. Por ejemplo, la norma PCI, un acuerdo entre las empresas de tarjetas de crédito y las empresas comerciales individuales, exige que se protejan determinados tipos de datos de maneras definidas (por ejemplo, la codificación obligatoria de las contraseñas de los clientes).

Distinciones en materia de seguridad

IMPORTANTE EXAMEN

Vulnerabilidad de la inyección SQL

En un ataque de inyección SQL, el autor inserta (o "inyecta") declaraciones de bases de datos no autorizadas en un canal de datos SQL vulnerable, como procedimientos almacenados y espacios de entrada de aplicaciones Web.

- Estas sentencias SQL inyectadas se pasan a la base de datos, donde a menudo se ejecutan como comandos legítimos.

- Mediante la inyección SQL, los atacantes pueden obtener acceso sin restricciones a toda una base de datos.

Rol clave en ciberseguridad: CISO (Chief Information Security Officer)

Un jefe de seguridad de la información (CISO) es el ejecutivo de nivel superior de una organización responsable de establecer y mantener la visión, la estrategia y el programa de la empresa para garantizar que los activos y las tecnologías de la información estén adecuadamente protegidos.

- El CISO dirige al personal en la identificación, desarrollo, implementación y mantenimiento de procesos en toda la empresa para reducir los riesgos de la información y la tecnología de la información (TI).

- Responde a los incidentes, establecen normas y controles adecuados, gestiona las tecnologías de seguridad y dirige el establecimiento y la aplicación de políticas y procedimientos.

- El CISO también suele encargarse del cumplimiento de las normas relativas a la información (por ejemplo ISO/CEI 27001).

¿De quién es la responsabilidad?

Chief Information Security Officer (CISO)

- Asegurar la información desde el punto de vista de seguridad y protección de los datos
- Definir y mantener procesos para garantizar el correcto uso de los datos
- Asegurar la confidencialidad de los mismos
- Determinar las medidas de protección de datos
- Definir criterios de confidencialidad a nivel de metadatos

Chief Data Officer (CDO)

- Gestionar el movimiento y consolidación de datos
- Velar por la aplicación de los requisitos y criterios de seguridad y protección de los datos
- Definir y mantener atributos para la clasificación de confidencialidad
- Conocer la definición y aplicación de los requerimientos regulatorios relativos a los datos
- Implantar las políticas, regulaciones y normativas referentes a los datos

Data Protection Officer (DPO)

- Definir y mantener procesos y estándares para garantizar la clasificación de los datos sensibles y asegurar la privacidad de los mismos
- Definir los criterios de privacidad de los metadatos asociados
- Coordinar con la data office la implantación de las políticas, regulaciones y normativas referentes a los datos

El enfoque de DAMA DMBOK

- La seguridad de los datos incluye la planificación, el desarrollo y la ejecución de políticas y procedimientos de seguridad para proporcionar una autenticación, autorización, acceso y auditoría adecuados de los datos y los activos de información.
- Los aspectos específicos de la seguridad de los datos (qué datos deben protegerse, por ejemplo) difieren entre las industrias y los países.
- El objetivo de las prácticas de seguridad de los datos es el mismo: proteger los bienes de información en consonancia con las reglamentaciones de privacidad y confidencialidad, los acuerdos contractuales y los requisitos comerciales.

El enfoque de DAMA DMBOK

La seguridad de la información comienza por clasificar los datos de una organización a fin de identificar qué datos requieren protección. El proceso general incluye los siguientes pasos:

- **Identificar y clasificar los activos de datos sensibles:** Dependiendo de la industria y la organización, puede haber pocos o muchos activos y una gama de datos sensibles (incluyendo la identificación personal, médica, financiera y más).
- **Localizar los datos sensibles en toda la empresa:** Los requisitos de seguridad pueden ser diferentes, dependiendo de dónde se almacenen los datos. Una cantidad significativa de datos sensibles en una sola ubicación supone un alto riesgo debido al daño posible de una sola brecha.
- **Determinar cómo se debe proteger cada activo:** Las medidas necesarias para garantizar la seguridad pueden variar entre los bienes, según el contenido de los datos y el tipo de tecnología.
- **Identificar la forma en que esta información interactúa con los procesos comerciales:** Es necesario analizar los procesos comerciales para determinar qué acceso se permite y en qué condiciones.

IMPORTANTE EXAMEN

Repositorio de metadatos

Desarrollo de un repositorio de metadatos con las características de los datos significa que todas las partes de la empresa pueden saber con precisión qué nivel de protección requiere la información sensible.

- Este enfoque permite que varios departamentos, unidades de negocio y proveedores utilicen los mismos metadatos.

- Los metadatos de seguridad estándar pueden optimizar la protección de datos y guiar el uso de la empresa y los procesos de soporte técnico, lo que permite reducir los costos.

- Esta capa de seguridad de la información puede ayudar a prevenir el acceso no autorizado y el uso indebido de los activos de datos.

- Cuando los datos confidenciales se identifican correctamente como tales, las organizaciones construyen la confianza con sus clientes y socios.

- **Los metadatos relacionados con la seguridad se convierten por sí mismos en un activo** estratégico, aumentando la calidad de las transacciones, la presentación de informes y el análisis empresarial, al tiempo que se reduce el costo de la protección y los riesgos asociados que causa la pérdida o el robo de información.

La seguridad de los datos en una organización sigue estos principios rectores

- **Colaboración:** La seguridad de los datos es un esfuerzo de colaboración en el que participan los administradores de seguridad de la tecnología de la información, los administradores de datos/gobierno de datos, los equipos de auditoría interna y externa y el departamento jurídico.
- **Enfoque de negocio:** Los estándares y políticas de Seguridad de Datos deben ser aplicados de manera consistente en toda la organización.
- **Gestión proactiva:** El éxito en la gestión de la seguridad de los datos depende de ser proactivo y dinámico, de la participación de todos los interesados, de la gestión del cambio y de la superación de los cuellos de botella organizativos o culturales, como la tradicional separación de responsabilidades entre la seguridad de la información, la tecnología de la información, la administración de datos y los interesados comerciales.
- **Rendición de cuentas clara (accountability):** Las funciones y responsabilidades deben definirse claramente, incluida la "cadena de custodia" de los datos en todas las organizaciones y funciones.
- **Impulsada por los metadatos:** La clasificación de seguridad de los elementos de los datos es una parte esencial de las definiciones de los datos.
- **Reducción del riesgo mediante la disminución de la exposición:** Se debe minimizar la proliferación de datos sensibles/confidenciales, especialmente en entornos no productivos.

Las 4 As de la seguridad de los datos

1. **Autenticación:** Validar el acceso de los usuarios. Cuando un usuario intenta acceder a un sistema, el sistema necesita verificar que la persona es quien dice ser.
   - **Ejemplo:** Uso de contraseñas, biometría (huellas dactilares, reconocimiento facial), tarjetas inteligentes, autenticación de dos factores (2FA).
2. **Autorización:** Proceso que determina qué recursos y acciones están permitidos para un usuario autenticado.
   - **Ejemplo:** Un usuario con privilegios de administrador puede acceder a todos los archivos del sistema, mientras que un usuario estándar solo puede acceder a sus propios archivos.
3. **Auditoría:** Proceso de registrar y revisar actividades y eventos para asegurar que se cumplen las políticas de seguridad y para identificar actividades sospechosas o no autorizadas.
   - **Ejemplo:** Registros de acceso, registros de cambios en los sistemas, análisis de logs para detectar intentos de intrusión.
4. **Administración:** Gestión y mantenimiento continuo de las políticas, procedimientos y herramientas de seguridad para garantizar que el sistema de seguridad funcione correctamente.
   - **Ejemplo:** Configuración de controles de seguridad, actualización de software de seguridad, capacitación de usuarios sobre buenas prácticas de seguridad, gestión de usuarios y permisos.

IMPORTANTE EXAMEN

CRUDE Matrix, Metadata Tracking, Data Masking - Pseudo Anonymization

El framework de DAMA DMBOK 2 enfoca el riesgo de datos con esta fórmula:

- Vulnerabilidad
- Amenaza
- Riesgo
  - Critical Risk Data (CRD)
  - High Risk Data (HRD)
  - Moderate Risk Data (MDR)

IMPORTANTE EXAMEN

CRUDE Matrix

Esta matriz se utiliza en Data Security para vigilar los procesos de relación **(CRUD–Create,Read, Update, Delete**) ayuda a mapear las necesidades de acceso a los datos y orientan la definición de los grupos de funciones de seguridad de los datos, los parámetros y los permisos.

Algunas versiones añaden una E para “Ejecutar” y se transforma en “CRUDE.”

CRUD MATRIX

Calling Item	Item Type	COUNTER	CUSTOMER	EMPLOYEE	PRODUCT	SALES_ORDER_ITEMS	SALES_ORDER
ALL_SALES_ORDER_ITEMS_DETAILS	View			R	R	R	R
ALL_PRODUCTS	View				R		
ALL_ORDERS_BY_EMPLOYEE	View						R
EMPLOYEE_COUNT	Trigger			R			
TRG_ORDER	Trigger				R		
CUSTOMERS.InsertCustomer	Procedure		C				
CUSTOMERS.UpdateCustomerName	Procedure		U				
CUSTOMERS.DeleteCustomerById	Procedure		D				
EMPLOYEES.OrdersByEmployee	Procedure		R	R		R	R
PRODUCTS.ProductsByCustomer	Procedure		R		R	R	R
PRODUCTSBYCUSTOMER	Procedure		R		R	R	R
pfc_updateprep	Event	RU					
itemchanged	Event				R		
demopfc.pbl.d_tab_customer	Datawindow Object		RU				
demopfc.pbl.d_tab_sales_order	Datawindow Object		R	R	R	R	R
demopfc.pbl.d_ff_sales_order	Datawindow Object		R	R			RU
demopfc.pbl.d_tab_employee	Datawindow Object			RU			

Table or Column Accessed

Components Accessing the table/column

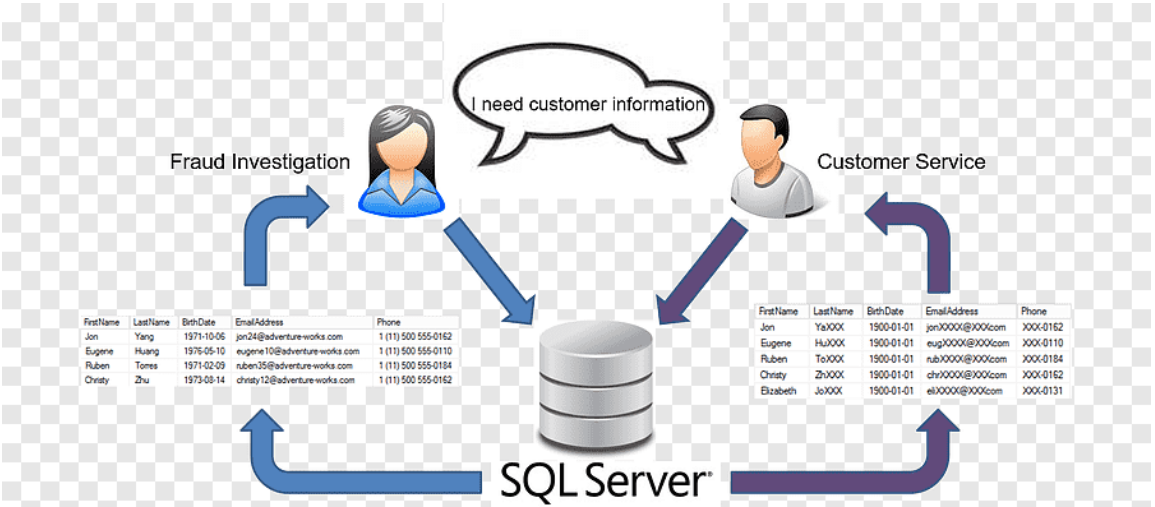
Type of Access (Create, Read, Update, Delete)

IMPORTANTE EXAMEN

Data Masking

El enmascaramiento de datos o la ofuscación de datos es el proceso de ocultar los datos originales con contenido modificado (caracteres u otros datos).

La razón principal para aplicar el enmascaramiento a un campo de datos es proteger los datos clasificados como información de identificación personal.



Data Masking

El enmascaramiento de datos es un tipo de seguridad centrada en los datos. Hay dos tipos de enmascaramiento de datos, el persistente y el dinámico. El enmascaramiento persistente puede ejecutarse en vuelo o en el lugar.

Enmascaramiento de datos persistente

El enmascaramiento persistente de los datos altera de forma permanente e irreversible los datos. Este tipo de enmascaramiento no suele utilizarse en entornos de producción, sino más bien entre un entorno de producción y entornos de desarrollo o de prueba. El enmascaramiento persistente altera los datos, pero éstos deben seguir siendo viables para su uso en procesos de prueba, aplicación, informe, etc.

Data Masking

Enmascaramiento dinámico de datos

El enmascaramiento dinámico de datos cambia la apariencia de los datos al usuario final o al sistema sin cambiar los datos subyacentes. Esto puede ser extremadamente útil cuando los usuarios necesitan acceder a algunos datos de producción sensibles, pero no a todos.

Métodos de enmascaramiento

Existen varios métodos para enmascarar u ofuscar los datos. Entre ellos contamos con:

- **Sustitución:** Reemplazar caracteres o valores enteros con los de una búsqueda o como un patrón estándar. Por ejemplo, los nombres de pila pueden ser sustituidos por valores aleatorios de una lista.
- **Barajado:** Intercambiar elementos de datos del mismo tipo dentro de un registro, o intercambiar elementos de datos de un atributo entre filas. Por ejemplo, mezclar los nombres de los proveedores entre las facturas de los proveedores, de manera que el proveedor original sea reemplazado por un proveedor válido diferente en una factura.

Data Masking

Métodos de enmascaramiento (continuación)

- **Desviación temporal:** Mover las fechas +/- un número de días - lo suficientemente pequeño como para preservar las tendencias, pero lo suficientemente significativo como para hacerlas no identificables.

- **Desviación del valor:** Aplicar un factor aleatorio +/- un por ciento, nuevamente lo suficientemente pequeño como para preservar las tendencias, pero lo suficientemente significativo como para hacerlas no identificables.

- **Anulación o eliminación:** Eliminar los datos que no deberían estar presentes en un sistema de prueba.

- **Aleatorización:** Sustituir parte o la totalidad de los elementos de datos por caracteres aleatorios o una serie de un solo carácter.

Data Masking

Métodos de enmascaramiento (continuación)

- **Enmascaramiento de la expresión:** Cambiar todos los valores al resultado de una expresión. Por ejemplo, una expresión simple codificaría de manera rígida todos los valores en un gran campo de base de datos de forma libre (que podría contener potencialmente datos confidenciales) para que sea "Este es un campo de comentario".

- **Enmascaramiento de claves:** Designa que el resultado del algoritmo/proceso de enmascaramiento debe ser único y repetible porque se está utilizando para enmascarar un campo clave de la base de datos (o similar). Este tipo de enmascaramiento es extremadamente importante para comprobar que se mantiene la integridad en torno a la organización.

Data Masking

Pseudoanonimización es un procedimiento de gestión de datos donde se reemplazan campos de información personal dentro de un registro de datos por uno o más identificadores artificiales o pseudónimos.

Un pseudónimo único por cada campo reemplazado, o grupo de campos reemplazados, hace cada registro de datos menos identificable mientras se queda apto para análisis de datos y procesamiento de datos.

El Reglamento General de Protección de Datos de la Unión Europea se refiere a pseudonimización como algo demandado para cualquier almacenaje de datos personales sobre personas dentro del UE como alternativa a la otra opción de anonimización de datos.

Data Masking

Information (name)	Anonymized	Pseudonymized
Peter	*****	4We8Kd
Annabelle	******	L8Fg447bA
Mark	*****	KJDe23
Elizabeth	******	Aq18zRe87
Mark	******	KJDe23
Annabelle	******	L8Fg447bA

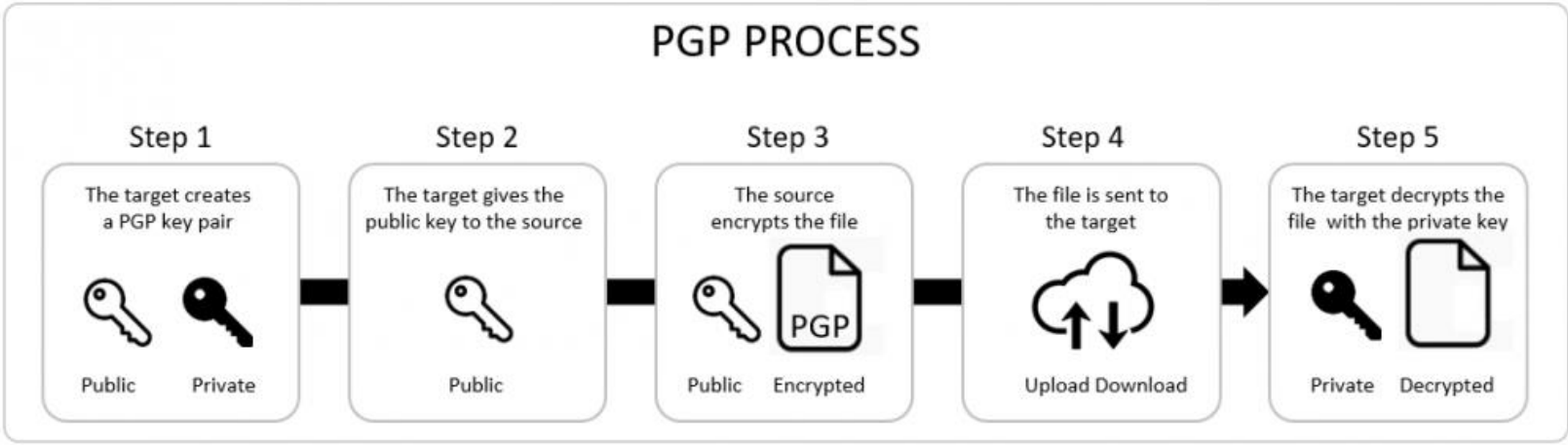
Cómo proteger los datos

Cifrado: La encriptación es el proceso de traducir un texto simple en códigos complejos para ocultar información privilegiada, verificar la transmisión completa o verificar la identidad del remitente. Los datos cifrados no pueden ser leídos sin la clave o el algoritmo de descifrado, que se almacena por separado y no puede ser calculado sobre la base de otros elementos de datos del mismo conjunto de datos.

- **Hash:** La encriptación Hash utiliza algoritmos para convertir los datos en una representación matemática. Los algoritmos exactos utilizados y el orden de aplicación deben conocerse para invertir el proceso de cifrado y revelar los datos originales.
- **Clave privada:** La encriptación de la clave privada utiliza una clave para cifrar los datos. Tanto el remitente como el destinatario deben tener la clave para leer los datos originales. Los datos pueden ser encriptados un carácter a la vez (como en una corriente) o en bloques.

Cómo proteger los datos

Clave pública: En la encriptación de clave pública, el emisor y el receptor tienen diferentes claves. El emisor utiliza una clave pública de libre acceso, y el receptor utiliza una clave privada para revelar los datos originales.



Nivel de garantías aportado por cada técnica de anonimización

Categoría	Técnica	Riesgo de singularización	Riesgo de vinculabilidad	Riesgo de inferencia
Aleatorización	Adición del ruido	Sí	A veces	A veces
	Permutación	Sí	A veces	A veces
	Privacidad Diferencial	A veces	A veces	A veces
Generalización	Anonimato-K	No	Sí	Sí
	Diversidad-L	No	Sí	A veces
	Proximidad-T	No	Sí	A veces
Seudonimización	Cifrado por Hash	Sí	Sí	A veces
	Tokenización	Sí	Sí	Sí

Fuente: Introducción a la anonimización de datos: técnicas y casos prácticos. Datos.gob.es

Principios de Zero Trust aplicado a los datos

1.Acceso mínimo necesario (Principio de menor privilegio)

1. Solo los usuarios, dispositivos y aplicaciones con una **necesidad legítima** pueden acceder a los datos.
2. Se usa **gestión de identidad y acceso (IAM)** y **autenticación multifactor (MFA)** para validar cada acceso.

2.Segmentación y clasificación de datos

1. Los datos se dividen en diferentes niveles según su sensibilidad (**público, interno, confidencial, secreto**).
2. Se aplican **controles de acceso específicos** a cada tipo de dato.

3.Verificación continua de acceso y comportamiento

1. Se supervisa **quién accede, desde dónde y con qué frecuencia**.
2. Se usan técnicas de **detección de anomalías** para identificar accesos sospechosos.

Principios de Zero Trust aplicado a los datos

4. Cifrado y protección de datos en todo momento

1. Los datos deben estar cifrados **en reposo, en tránsito y en uso**.
2. Se implementan soluciones como **Data Loss Prevention (DLP)** y **tokenización**.

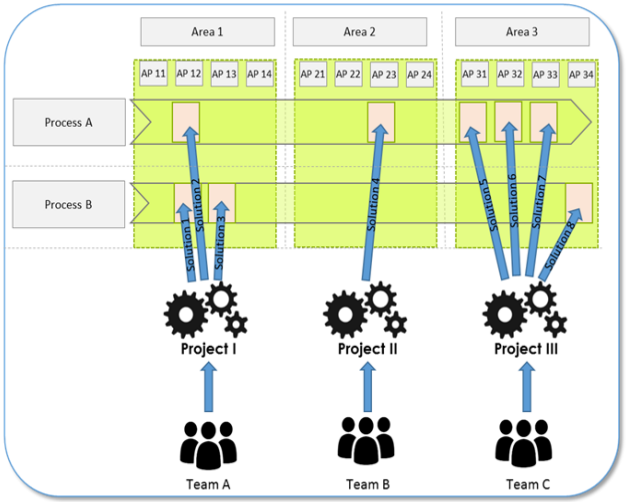
5.Auditoría y trazabilidad constante

1. Todo acceso y modificación de datos se registra en **logs de auditoría**.
2. Se aplican herramientas de **SIEM (Security Information and Event Management)** para detectar incidentes.

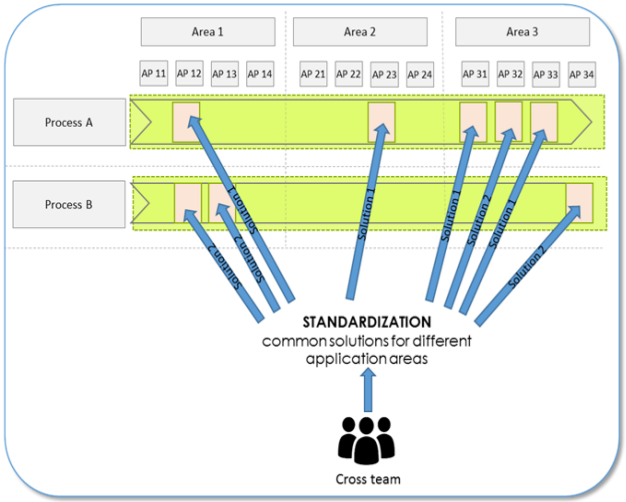
Data Security and Data Compliance Framework

¿Cómo es un proyecto de data security y data compliance?

Por proyectos – Quick Wins



Estandarización



+

- Orientado a Quick Wins
- Simplicidad en la gestión y coordinación de equipos
- Coste inicial más bajo
- Adaptación inicial más rápida

-

- Mayor riesgo de desalineamiento entre las diferentes aplicaciones
- Posible sobrecoste a posteriori al no homogeneizar procesos y/o tareas
- Mayor riesgo de errores por la falta de especialización de los equipos en seguridad/GDPR

+

- Economías de escala
- Mejor transferencia de conocimiento; creación de una base común de conocimiento
- Creación de aceleradores para la adopción de GDPR y control de los problemas comunes
- Facilita la responsabilidad proactiva y las tareas del DPO

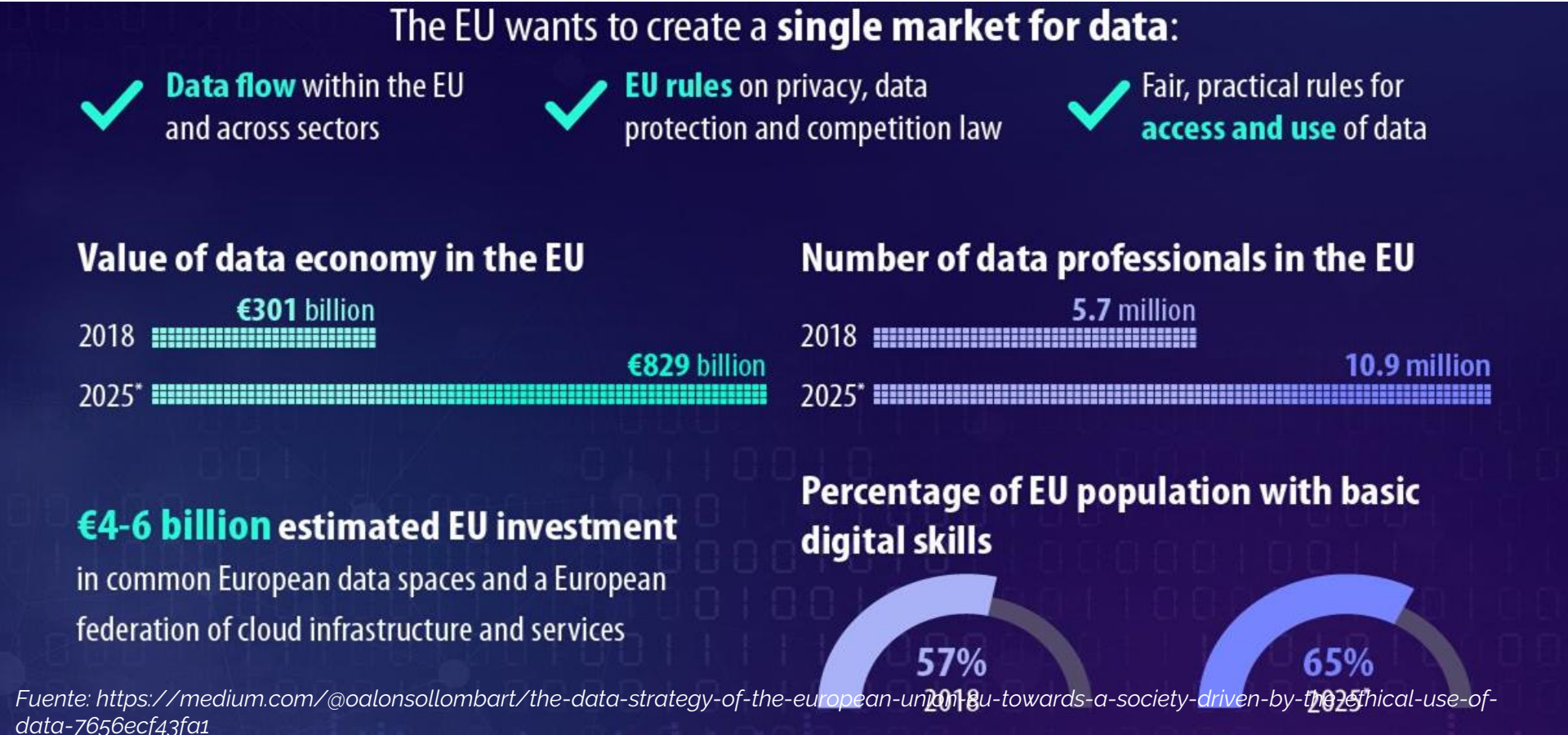
-

- Coste inicial más elevado
- Compleja coordinación de actividades de cumplimiento
- Posibles bloqueos en la ejecución por sobrecarga del equipo dedicado
- Los resultados no son tan visibles en el corte plazo

¿Cómo es un proyecto de data security y data compliance?

1. Conoce la organización e identifica los puntos débiles en el tratamiento de datos personales
2. Crea un inventario de datos personales y tratamientos si no existe e identifica a las personas clave que se deben involucrar en el proceso
3. Define las medidas técnicas y organizativas a aplicar en la organización así como el enfoque metodológico
4. Implanta las medidas definidas para la adaptación a la nueva regulación
5. Forma y conciencia a todo el personal en la organización

La estrategia europea de datos



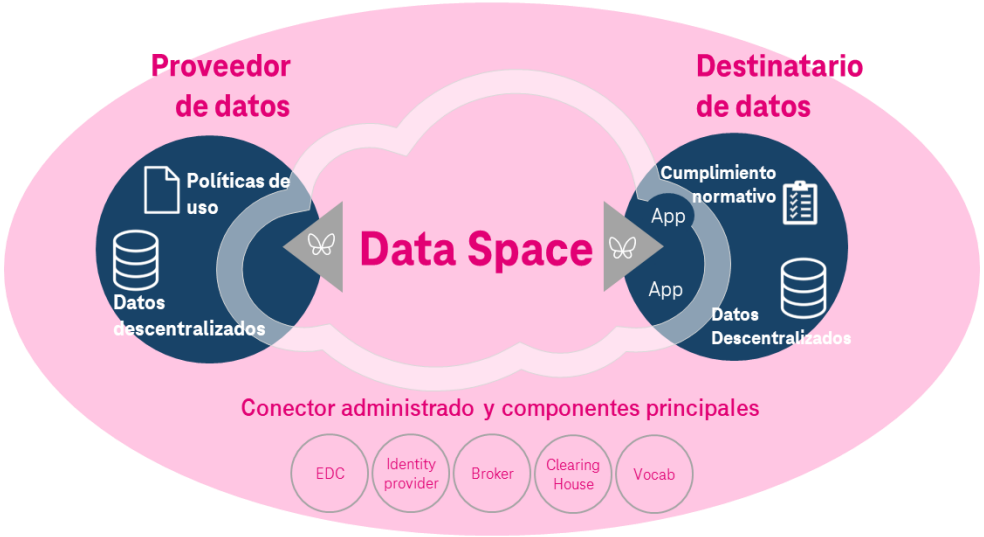
Fuente: https://medium.com/@oalonsollombart/the-data-strategy-of-the-european-union-eu-towards-a-society-driven-by-the-ethical-use-of-data-7656ecf43fa1

¿Qué es un espacio de datos?

NO únicamente datasets

Los Data Spaces son **ecosistemas** para compartir **productos de datos** en una **red descentralizada**:

los datos **permanecen en su origen**



NO es un datalake ni un sitio donde "subir datos"

KEY FEATURES

- **Marketplace central** para el intercambio de **productos** de datos **seguro** y **confiable** entre empresas y/o consumidores.
- Permiten la **armonización** y **accesibilidad** de productos de datos enriquecidos (**comerciales y públicos**)
- Sirven como habilitador de análisis/IA al ofrecer aplicaciones líderes en la industria en un **workspace colaborativo**.
- El propietario de los datos conserva el control sobre el flujo y el uso de los datos (**soberanía de los datos**).

Fuente: T-Systems

¿Qué es un espacio de datos?

Nuevos requerimientos legales

Las nuevas regulaciones exigen transparencia e intercambio de datos al tiempo que defienden la privacidad de los datos y la soberanía digital.

Valores de la UE - Sostenibilidad

La responsabilidad ambiental y social es solicitada por las partes interesadas y los clientes y se aplica mediante leyes climáticas. La sostenibilidad no se puede alcanzar sola.

Nuevos modelos de negocio

Los mercados requieren estrategias innovadoras para reducir costos y crear nuevos modelos de negocios basados en datos. Las cadenas de datos aumentan la transparencia. Los mercados hacen que los productos sean visibles.

Fuente: T-Systems

La estrategia europea de datos

Data Act

Elementos principales

¿Cuál es el propósito?

Regula el acceso y uso de datos generados por dispositivos conectados y otros tipos de datos no personales para fomentar la economía de datos, la innovación y la competitividad.

¿Qué está protegido?

Datos personales y no personales, secretos comerciales y derechos de propiedad intelectual.

¿Quiénes son los destinatarios?
El sector público, para acceder a datos en poder del sector privado.

Objetivos principales

- ✓ **Garantizar la equidad en la asignación del valor de los datos entre los agentes del mundo digital.**
- ✓ Estimular un mercado de datos competitivo.
- ✓ Generar posibilidades para la innovación basada en los datos.
- ✓ Hacer que los datos sean más accesibles para todos.

Data Governance Act

Elementos principales

¿Cuál es el propósito?

Establecer un marco regulador para la gestión de datos en la Unión Europea, **promoviendo el intercambio seguro y confiable de datos** entre entidades públicas y privadas

¿Qué está protegido?

Se pretende facilitar a las empresas el acceso a datos de forma fiable, minimizando el riesgo de uso indebido.

¿Quiénes son los destinatarios?
Empresas que trabajan con grandes cantidades de datos.

Objetivos principales

- ✓ Fortalecer los mecanismos para aumentar la disponibilidad de datos para su reutilización.
- ✓ Aumentar la confianza en el intercambio de datos.
- ✓ Superar los obstáculos técnicos para la reutilización de los datos.
- ✓ **Crear espacios comunes europeos de datos en ámbitos estratégicos.**

Directrices éticas para una IA confiable de la UE

El enfoque de la ética en la IA está **basado en los derechos fundamentales consagrados en los Tratados de la UE, la "Carta de la UE" y la legislación internacional de derechos humanos. En 2019,** la Comisión Europea establece las directrices éticas para una IA fiable, un **total de 4 principios éticos y 7 requerimientos**

Principios éticos:

1. Respecto de la autonomía humana
2. Prevención del daño
3. Equidad
4. Explicabilidad

Vínculo de los 7 requerimientos:

Todos tienen la **misma importancia**, se apoyan mutuamente y **deben implementarse** y **evaluarse** durante todo el **ciclo de vida completo** del **modelo** de **IA**

Fuente: https://digital-strategy.ec.europa.eu/es/library/ethics-guidelines-trustworthy-ai

Fuente: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN

La AI ACT de la UE

En 21 de abril de 2021, la Comisión Europea publicó un Proyecto de ley para regular la IA en la Unión Europea.

La IA Act (AIA) es importante por su definición expansiva de los sistemas de IA, y la imposición de una amplia **documentación**, **capacitación** y requisitos de **monitorización** de las herramientas de IA que caen bajo su competencia.

Cualquier empresa con exposición al mercado de la UE que **desarrolle o desee adoptar** un software basado en algoritmos de Inteligencia Artificial será afectada por la AIA.


EUROPEAN COMMISSION

Brussels, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

EN EN

Fuente: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN

It’s not about privacy, it’s about power

TED Ideas worth spreading WATCH DI

It's not about privacy -- it's about power

144,558 views | Carole Cadwalladr | TEDSummit 2019 • July 2019

Data Management Fundamentals
Módulo 11 – Data Security

Óscar Alonso Llombart
Data & AI Strategy and Governance Lead at T-Systems Iberia
oscar.alonso-llombart@t-systems.com
https://www.linkedin.com/in/oscar-alonso-llombart/