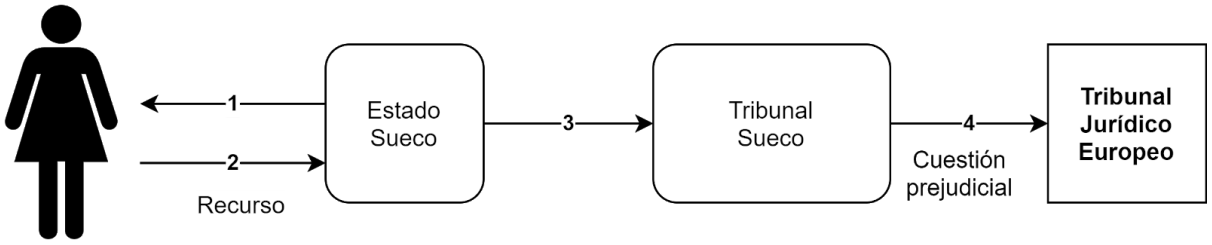
Protección de Datos

Tema 2

24/02/2020



Intimidad: derecho a proteger información íntima (enfermedad...).
Privacidad: derecho a proteger información privada (DNI, nombre, edad, residencia...).

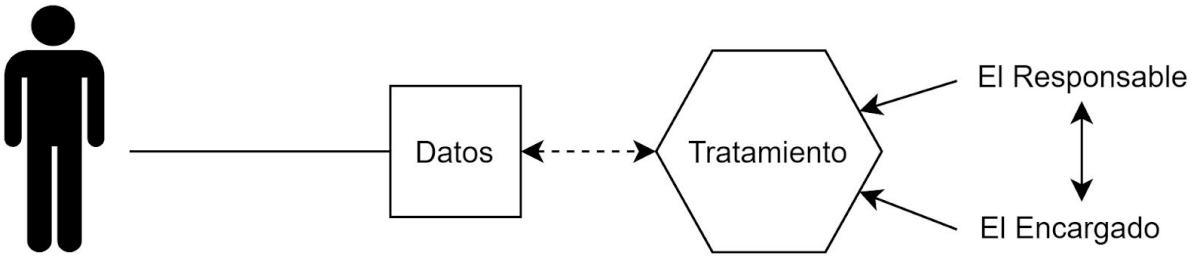
La **AEPD** (Agencia Española de Protección de Datos) es la que regula la gestión de datos.

- Apercibimiento (advertencia / aviso).
- Multa.
- Tratamiento de Datos.

RGPD: Reglamento General de Protección de Datos.
LOPDGDD: Ley Orgánica de Protección de Datos y de Garantía de Derechos Digitales.

Los **Tribunales ...**

- **... de Jurisdicción Civil** son los únicos que pueden **indemnizar** a una persona.
- **... de Jurisdicción Penal** son los únicos que pueden **encarcelar** a una persona.



26/02/2020

Principios de Tratamiento

Cuestión 2: *KKFashion, escuela de modelos*

a. *Interesados: Clientes, proveedores y alumnos (siempre que sean personas físicas).*
b. *Responsable(s): KKFashion, quien saca beneficio del tratamiento de datos.*
c. *Encargado: Quien procesa los datos, Estiquio Estíquez.*

Los **datos deben ser recogidos para un fin determinado y explícito**, en caso contrario se considera ilegal.

La recolección de datos con fines de archivo, estadísticos... y con fines públicos, se consideran incompatibles con la definición anterior.

Responsabilidad proactiva:

- Limitación de la finalidad.
- Minimización de datos.
- Exactitud.
- Limitación de conservación.

- *Integridad y confidencialidad*.
- Legitimación del tratamiento.

Responsabilidad práctica: hacer todo lo posible para no cometer ningún fallo evitable. En inglés «*accountability*», cuya traducción es «rendir cuentas».

Base de Legitimación:

- El consentimiento: clara acción afirmativa. El pseudo-consentimiento no es admitido por el reglamento.

- El interés legítimo del responsable: cualquier acción que no vaya contra la ley. Esto es muy difuso, lo que provoca un agujero legal. La solución de la UE es que «sobre dichos intereses no prevalezcan los los intereses, derechos y libertades fundamentales del interesado». Ejemplo: la mercadotecnia directa tiene interés legítimo.

- Otras componentes:
    - Ejecución del contrato.
    - Obligación penal.
    - Interés vital.
    - Interés y ejercicio de poderes públicos.

02/03/2020

Derechos ARCO:

- **Acceso**: Origen y uso de los datos (copia para el interesado).
- **Rectificación**: Corregir datos erróneos.
- **Cancelación**: Borrar datos (innecesidad o retiro del consentimiento).
- **Oposición**.

- Nuevos:
    - **Limitación**: No se borran los datos, pero tampoco se usan.
    - **Portabilidad**: Acceso a los datos. Se transmiten entre responsables.

04/02/2020

Deberes del responsable

Ejercer la Obligación de Información

Registro de Actividades de Tratamiento

Un nombre más adecuado sería el de *Declaración de Actividades de Tratamiento.*

Documento estático y simple que recoge qué datos van a registrarse y su finalidad. Declara el tratamiento que va a llevarse a cabo sobre ciertos datos.

Notificación de Violaciones de Seguridad

También llamado *brecha de seguridad*, se notificará con la mayor brevedad posible a la AEPD, sin dilación indebida y antes de 72 h.

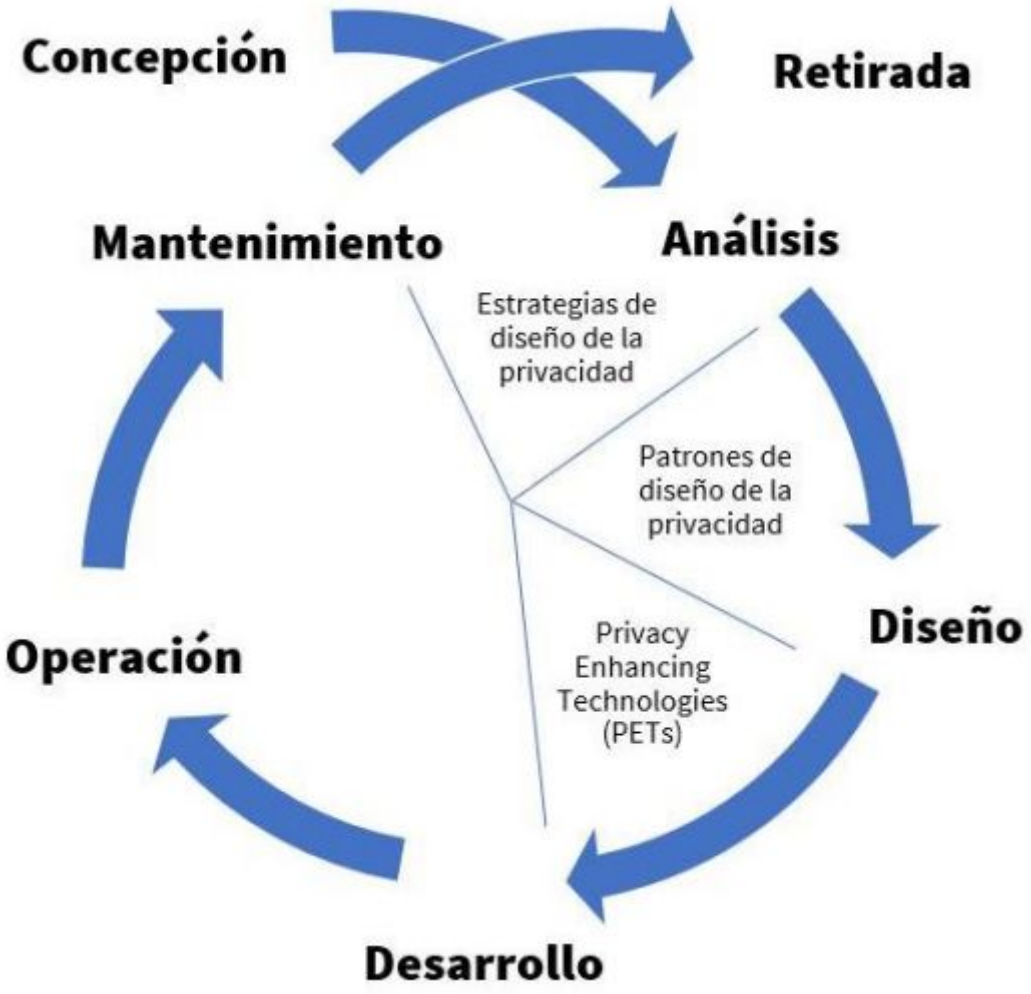
Elaboración de un Contrato de Encargo

Nombramiento del Delegado de Protección de Datos

Persona física / jurídica que tenga un perfil que implique conocimientos jurídicos y experiencia en el tratamiento de datos.

Seguridad

Seguridad, análisis de riesgos y evaluación de impacto



OBJETIVO DE PROTECCIÓN DE LA PRIVACIDAD	ESTRATEGIAS DE DISEÑO DE LA PRIVACIDAD ORIENTADAS A DATOS	ESTRATEGIAS DE DISEÑO DE LA PRIVACIDAD ORIENTADAS A PROCESOS
DESVINCULACIÓN	MINIMIZAR, ABSTRAER, SEPARAR, OCULTAR	
CONTROL		CONTROLAR, CUMPLIR, DEMOSTRAR
TRANSPARENCIA		INFORMAR

Tabla 3 – Asociación entre los objetivos de privacidad y las estrategias de diseño de la privacidad

ESTRATEGIA DE DISEÑO DE LA PRIVACIDAD		DESCRIPCIÓN Y TÁCTICAS	CONTROLES Y PATRONES DE DISEÑO
Estrategias orientadas a datos	Minimizar	Limitar al máximo posible el tratamiento de datos personales. TÁCTICAS: **seleccionar**, **excluir**, **podar** y **eliminar**	Anonimización Seudonimización Bloqueo de correlación en sistemas de gestión de identidad federada
	Ocultar	Evitar que los datos personales se hagan públicos o sean conocidos TÁCTICAS: **restringir**, **ofuscar**, **disociar** y **agregar**)	Cifrado Redes de mezcla Atributos basados en credenciales
	Separar	Mantener separados los conjuntos de datos personales. TÁCTICAS: **aislar** y **distribuir**	Listas negras anónimas Cifrado homomórfico Separación física y lógica
	Abstraer	Limitar al máximo el nivel de detalle utilizado en los tratamientos de datos personales. TÁCTICAS: **sumarizar**, **agrupar** y **perturbar**	Agregación en el tiempo K-anonimidad Ofuscación de medidas mediante agregación de ruido Granularidad dinámica de ubicación Privacidad diferencial

ESTRATEGIA DE DISEÑO DE LA PRIVACIDAD		DESCRIPCIÓN Y TÁCTICAS	CONTROLES Y PATRONES DE DISEÑO
Estrategias orientadas a procesos	Informar	Mantener informados a los sujetos de datos de la naturaleza y condiciones del tratamiento. TÁCTICAS: **facilitar**, **explicar** y **notificar**	Notificación de brechas de privacidad Visualización dinámica de la política de privacidad Iconos de privacidad Alertas de tratamiento
	Controlar	Proporcionar a los sujetos de datos un control efectivo sobre sus datos personales. TÁCTICAS: **consentir**, **alertar**, **elegir**, **actualizar**, **retirar**	Paneles de preferencias de privacidad Transmisión activa de presencia Selección de credenciales Consentimiento informado
	Cumplir	Respetar e impulsar el cumplimiento de las obligaciones impuestas en la normativa vigente y en la propia política de protección de datos. TÁCTICAS: **definir**, **mantener**, **defender**	Evaluación de impacto de privacidad en soluciones de gestión de identidad federada Control de acceso Gestión de obligaciones Políticas adheridas
	Demostrar	Poder demostrar que los tratamientos se realizan de una forma respetuosa con la privacidad. TÁCTICAS: **registrar**, **auditar** e **informar**.	Auditoría Registro

Deben establecerse varios perfiles distintos para el acceso a un sistema.

Medidas Organizativas

Deber de confidencialidad y secreto

Todo el personal que trate con datos personales deberá cumplir con el deber de confidencialidad y secreto.

No se pueden transmitir datos personales por teléfono, a menos que sean del y para el interesado.

Derechos de los titulares de los datos

Violaciones de seguridad de datos de carácter personal

Técnicas

Identificación

- Existencia de diferentes perfiles -con distintos permisos sobre el sistema-.
- Existencia de usuarios y contraseñas específicos para cada usuario.
- Confidencialidad de las contraseñas.

Deber de salvaguarda

- Actualización de dispositivos.
- Antivirus contra malware.
- Cortafuegos o firewall.

- Cifrado de datos.

- Copia de seguridad.

Si no puede establecerse un documento de Facilita, entonces debe realizarse un análisis explícito de riesgos.