UD1A: Legislación y normativa legal en materia de seguridad informática

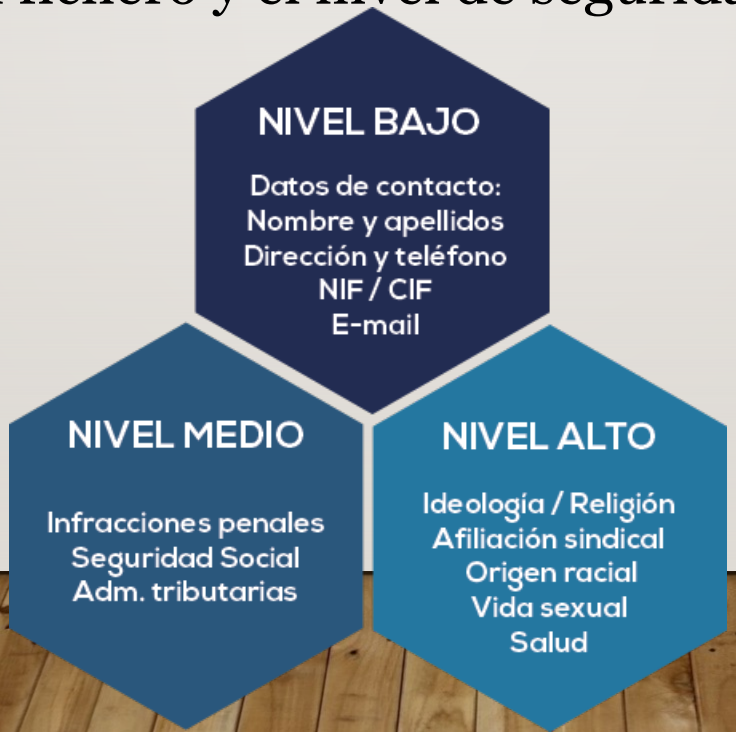
Seguridad y Alta disponibilidad
2º ASIX

Ley de protección de datos

- La normativa que regula la gestión de los datos personales es la Ley de Protección de Datos de Carácter Personal (LO 15/1999) más conocida como LOPD. El objetivo de esta ley es garantizar y proteger los derechos fundamentales y la intimidad de las personas físicas. Especifica para qué se pueden usar, cómo deber ser el procedimiento de recogida y los derechos que tienen las personas a las que se refieren entre otros aspectos.

Medidas de seguridad

- Siempre que se vaya a crear un fichero de datos personales se debe solicitar la aprobación de la Agencia de protección de datos. En esta solicitud se deben especificar los datos que contendrá el fichero y el nivel de seguridad que se aplicará al fichero.



Nivel de seguridad	Definición	Medidas de seguridad aplicadas a este nivel
Básico	Todos los datos personales tienen como mínimo este nivel.	◦ Debe existir un documento donde estén reflejadas las funciones y obligaciones de cada usuario del fichero. El responsable del fichero debe almacenar a su vez una lista de los usuarios con sus accesos y las contraseñas deben ser cambiadas en un periodo no superior a un año. ◦ Debe crearse un registro de incidencias del fichero de datos. ◦ Cualquier documento que se deseche y que contenga datos de carácter personal tendrá que ser borrado o destruido. ◦ Las copias de seguridad deberán ser como mínimo una a la semana.
Medio	Referidos a infracciones, gestión tributaria, datos fiscales y financieros. Datos sobre las características y personalidad de los afectados.	◦ Al menos una vez cada dos años se realizará un auditoría que verificará los procedimientos de seguridad aplicados. ◦ Se deben establecer mecanismos para evitar el acceso reiterado no autorizado a los datos y sistemas de control de acceso a los lugares donde se encuentren los equipos con los datos.
Alto	Referidos a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.	◦ Los datos deben cifrarse para su transporte tanto físico (en un portátil) como por redes públicas o inalámbricas. ◦ Las copias de seguridad se deben almacenar en un lugar físico distinto al de los datos. ◦ Se deben registrar todos los intentos de acceso de los últimos dos años como mínimo.

Nuevas obligaciones

- **Rendición de cuentas**

- Se amplia la información que se les debe dar a los interesados en relación con el tratamiento de sus datos así como a sus derechos en esta materia.

- Se incorpora el concepto de privacidad desde el diseño, lo cual se traduce en que la elaboración de los procedimientos empresariales se tiene que realizar teniendo en cuenta la protección de datos desde un primer momento.

Nuevas obligaciones

- **Notificación de violaciones de seguridad**

- La nueva normativa exige que las violaciones en la seguridad que puedan afectar a los datos personales sean notificadas en un plazo máximo de 72 horas a la Autoridad de Control correspondiente (Agencia Española de Protección de Datos).

- Si además si en esa violación se pueden ver afectado datos de carácter sensible y con gran repercusión a los afectados, también se lo deberá notificar a estos mismos.

Nuevas obligaciones

- **Registro de las actividades de tratamiento**

- La nueva normativa, elimina la obligación de registrar los ficheros ante la Autoridad de Control correspondiente.

- No obstante obliga a llevar un registro interno de todos los tratamientos de datos personales que lleva a cabo la entidad, siempre que esta tenga más de 250 empleados o cuando se traten, no de forma ocasional, datos sensibles..

Nuevas obligaciones

- **Responsabilidad proactiva**
- También llamado Accountability.
- Esta responsabilidad activa se refiere a la necesidad de prevención por parte de las organizaciones que manejan datos personales.
- Las empresas y entidades deben adoptar medidas que garanticen de manera suficiente que están en condiciones de cumplir con las reglas, derechos y garantías que el Reglamento establece.
- El RGPD entiende que actuar únicamente cuando ya ha tenido lugar la infracción no es suficiente como estrategia, debido a que esa infracción puede ocasionar daños a los interesados que puede ser muy complicado compensar o reparar.
- Para ello todas las organizaciones que tratan datos deben efectuar un análisis de riesgo de sus tratamientos para poder establecer qué medidas han de aplicar y cómo hacerlo.
- Estos análisis pueden ser procedimientos sencillos en entidades que no llevan a cabo más que unos pocos tratamientos elementales que no supongan, por ejemplo, datos especialmente protegidos, o trabajos más complejos, en entidades que desarrollen muchos tratamientos, que afecten a gran número de personas o que por sus características requieren de una valoración cuidadosa de sus riesgos..

Nuevas obligaciones

- **Delegado de Protección de Datos**

- Se trata de una nueva figura de responsabilidad dentro de la entidad.

- El DPO, se encargará de la planificación de las medidas de seguridad aplicables a los tratamientos de datos. así como la gestión de los mismos.
- Hay que destacar que servirá de enlace entre la empresa y la autoridad de control.

- Solo será obligatorio en determinados casos, los cuales encontremos regulados en la nueva LOPD cuando está definitivamente se apruebe.

NUEVOS CAMBIOS EN LA NORMATIVA

LOPD 1999 - 2018		LOPD - RGPD A PARTIR DE 2018
FICHEROS		REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO
REGISTRO DE INCIDENCIAS		NOTIFICACIÓN BRECHAS A LA AEPD
DERECHOS ARCO		AMPLIADO A DERECHO AL OLVIDO Y PORTABILIDAD
RESPONSABLE DE SEGURIDAD		DELEGADO DE PROTECCIÓN DE DATOS
INFORME DE AUDITORIA		EVALUACIÓN DE IMPACTO
900 - 600.000€		2 - 4% FACTURACIÓN ANUAL 10 - 20 MILLONES €
CONSENTIMIENTO TÁCITO		CONSENTIMIENTO INEQUÍVOCO
FIRMA CONTRATO ENCARGADO DE TRATAMIENTO DE TERCEROS		SOLICITAR CERTIFICADO AL TERCERO PARA VERIFICAR QUE CUMPLE LA NORMATIVA