TEMA 7: NORMATIVA DE SEGURIDAD DE DATOS

7.1 Normativa de Seguridad de datos

Ley Orgánica de Protección de Datos de Carácter Personal (LOPD 15/1999): Deroga y sustituye a la antigua LORTAD.

Subsisten las normas reglamentarias existentes, en especial:

- Real Decreto 428/1993 (Estatutos Agencia Protección de Datos)
- Real Decreto 1332/1994 (Notificación e inscripción, ejercicio de derechos, procedimiento sancionador, etc.)
- Real Decreto 994/1999 (Medidas de seguridad)

7.2 Seguridad de Datos: Definiciones

Datos de carácter personal:

Cualquier información concerniente a personas físicas identificadas o identificables.

Cualquier información que pueda ser atribuida y que identifique a una persona física.

También habremos de considerar datos de carácter personal toda aquella información ligada a un contrato, siempre y cuando dicho contrato pueda ser relacionado con una persona física concreta.

Los datos de tipo económico o financiero y, en la medida en que dichos datos puedan asociarse a una persona física en particular, como podría ser el número de cuenta bancaria, se consideran asimismo como datos de carácter personal.

Una excepción la constituyen los datos que son de dominio público, como los obtenidos a partir del censo, por ejemplo, que no se consideran datos de carácter personal y pueden ser utilizados libremente.

Dato de persona o de identificación personal:

Son el subconjunto más importante y más pequeño de los datos de carácter personal (por ejemplo el nombre, DNI, etc.)

Con frecuencia se confunde lo que es un dato de carácter personal con un dato de persona o de identificación personal

Datos no considerados de carácter personal:

De la definición de dato de carácter personal de desprende que aquellos datos, a través de los cuales no sea posible identificar a una persona física concreta, no serán considerados de carácter personal.

Asimismo, toda la información relativa a personas **jurídicas** o información no asociada a personas físicas (por ejemplo información agregada o estadística) no será tampoco información de carácter personal.

Fichero:

Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Por lo tanto, cualquier fichero que, entre otros datos, contenga DNI/NIF o nombre y apellidos de una persona física será considerado de carácter personal.

7.3 *Derechos*

Consentimiento del afectado:

- El tratamiento de datos de carácter personal requerirá el consentimiento inequívoco del afectado

- No será necesario cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa.

- Nadie podrá ser obligado a declarar datos de ideología, religión o creencias.

Derecho de Acceso:

Toda persona cuyos datos personales sean tratados tiene derecho a solicitar y obtener información sobre éstos. El ejercicio de este derecho es gratuito

El responsable del fichero o tratamiento debe resolver la petición de acceso en un plazo de un mes.

Derecho de Rectificación:

Toda persona física tiene derecho a rectificar y corregir los errores o incorrecciones, en todo o en parte, que presentan sus datos personales.

El responsable del fichero o tratamiento, en el plazo de 10 días, tiene la obligación de hacer efectivo el derecho de rectificación y notificarlo al interesado y a los terceros que dispongan de los datos, que también los han de rectificar. El ejercicio de este derecho es gratuito.

Derecho de Cancelación (derecho al olvido)

Toda persona física tiene derecho a que sean cancelados sus datos personales cuando dejen de ser necesarios o pertinentes para la finalidad para la que se obtuvieron y a que no se conserven sus datos por un período de tiempo superior al necesario. El ejercicio de este derecho es gratuito.

El responsable del fichero o tratamiento tiene la obligación de hacer efectivo este derecho de cancelación en el plazo de diez días y de notificarlo al interesado y a los terceros que dispongan de los datos, que también los han de cancelar.

La cancelación dará lugar al bloqueo de los datos; únicamente se conservarán a disposición de la Administración pública, jueces y tribunales para atender posibles responsabilidades nacidas del tratamiento, durante el plazo de su prescripción. Una vez transcurrido este plazo se tendrán que suprimir.

Derecho de Oposición:

Toda persona tiene derecho a oponerse al tratamiento de sus datos personales cuando existan motivos fundamentados y legítimos relativos a una concreta situación personal. El ejercicio de este derecho es gratuito.

Derecho de Información

- Al solicitar datos personales se deberá informar de modo expreso, preciso e inequívoco:
  - Existencia del fichero o tratamiento, finalidad y destinatarios
  - Carácter obligatorio o facultativo de las respuestas
  - Posibilidad del ejercicio de los derechos de acceso, rectificación, cancelación y oposición (Arts. 6.4, 15, 16 y 17, LOPD)
  - Identidad y dirección del responsable del tratamiento

Derecho a ser Informado

- Derecho que tienen todas las personas físicas de las cuales se soliciten u obtengan datos de carácter personal a ser informadas sobre el destino y la finalidad que tendrán los datos y los responsables ante los que podrán ejercer sus derechos. (Art. 5, LOPD)

Derecho de Consulta al Registro de Protección de Datos

- Toda persona física puede conocer la existencia de tratamientos de datos personales, sus finalidades y la identidad del responsable del fichero o tratamiento mediante consulta pública y gratuita en el Registro de Protección de Datos. (Art. 14, LOPD)

7.4 Real Decreto 994/1999

Contempla:

- Reglamento de Medidas de Seguridad

- Ámbito de aplicación:
  - Ficheros
  - Centros de tratamiento
  - Locales
  - Equipos
  - Sistemas
  - Programas
  - Personas

7.5 Niveles de seguridad

Tres tipos de datos:

- Datos de Nivel Básico
- Datos de Nivel Medio
- Datos de Nivel Alto

- Nivel Básico
  - Todos los ficheros con datos personales

- Nivel Medio
  - Servicios Financieros
  - Que se rijan por el artículo 28 de la LORTAD (Morosidad)
  - Infracciones administrativas o penales
  - Hacienda Pública
  - Datos suficientes que permitan evaluar la personalidad del individuo

- Nivel Alto (*)

- Ideología
- Religión
- Creencias
- Origen racial
- Salud
- Vida sexual
- Fines policiales

(*) La Ley Orgánica 15/1999 concreta los datos "especialmente protegidos"

7.6 Datos especialmente protegidos

- Nadie podrá ser obligado a declarar datos de ideología, religión o creencias

- Se necesita consentimiento expreso y por escrito para ficheros que revelen ideología, afiliación sindical, religión o creencias

- Prohibidos los creados con la finalidad exclusiva de almacenar ideología, afiliación sindical, religión, creencias, origen racial o étnico o vida sexual

- Excepción de los datos de salud utilizados por profesionales sanitarios

7.7 Medidas de seguridad: Nivel Básico

- Existencia de un Documento de Seguridad, actualizado y adecuado, en todo momento, a las disposiciones vigentes

- Contenido:

  1. Ámbito de aplicación

  2. Funciones y obligaciones del personal

  3. Procedimiento de notificación, gestión y respuesta ante incidencias

  4. Procedimientos de realización de copias de respaldo y recuperación

- Funciones y obligaciones del personal

  ✓ Claramente definidas y documentadas

- ✓ Conocimiento de las normas de seguridad que afecten al desarrollo de sus funciones, así como de las consecuencias del incumplimiento

- Registro de incidencias

  - ❖ Tipo de incidencia
  - ❖ Momento en que se ha producido
  - ❖ Persona que realiza la notificación
  - ❖ A quién se le comunica
  - ❖ Efectos que se hubieran derivado

- Identificación y autenticación

  - ❖ Existencia de una relación actualizada de usuarios con acceso al Sistema Operativo
  - ❖ Procedimientos de identificación y autenticación
  - ❖ Procedimiento de asignación, distribución y almacenamiento de contraseñas que garantice confidencialidad e integridad
  - ❖ Cambio de contraseñas con la periodicidad que establezca el Documento de Seguridad

- Control de acceso

  - ❖ Los usuarios tendrán acceso autorizado únicamente a los recursos necesarios para el desempeño de su función
  - ❖ Existirán mecanismos que impidan acceder a recursos diferentes a los autorizados
  - ❖ Sólo el personal autorizado en el Documento de Seguridad podrá administrar los permisos

- Gestión de soportes

  - ❖ Identificación del tipo de información que contienen
  - ❖ Inventariados
  - ❖ Almacenaje en lugar con acceso restringido
  - ❖ Salida fuera de los locales de ubicación: únicamente autorizada por el responsable del fichero

- Copias de respaldo y recuperación

  ✓ Verificación de la correcta aplicación de los procedimientos

  ✓ Garantía de reconstrucción al estado anterior a la pérdida o destrucción

  ✓ Deberán realizarse, al menos, copias de respaldo semanales

7.8 Medidas de seguridad: Nivel Medio

- Documento de Seguridad

  - Identificación del responsable de seguridad
  - Controles periódicos
  - Medidas a adoptar cuando se desechen o reutilicen soportes

- Auditoría

  - Interna o externa, cada dos años
  - Adopción de medidas correctoras
  - A disposición de la APD

- Identificación y autenticación

  - Identificación inequívoca y personalizada de todo usuario y verificación de que está autorizado

  - Limitación de la posibilidad de intentar reiteradamente el acceso no autorizado

- Control de acceso físico

  "Exclusivamente el personal autorizado en el Documento de Seguridad podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal" (Art. 19, Real Decreto 994/1999)

- Gestión de soportes

  – Registro de entrada

    - Tipo de soporte
    - Fecha y hora
    - Emisor
    - Número de soportes

- Tipo de información contenida
- Forma de envío
- Persona responsable de la recepción (debidamente autorizada)

– Registro de salida

- Tipo de soporte
- Fecha y hora
- Destinatario
- Número de soportes
- Tipo de información contenida
- Forma de envío
- Persona responsable de la entrega (debidamente autorizada)

– Impedir cualquier recuperación en soportes desechados

– Adopción de medidas que impidan la recuperación de datos, cuando salgan fuera de los locales de ubicación

Registro de incidencias

– Procedimientos de recuperación realizados
– Persona que ejecutó el proceso
– Datos restaurados
– Qué datos ha sido necesario grabar manualmente
– Autorización por escrito para la ejecución de los procedimientos de recuperación

- Pruebas con datos reales

"Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado"

(Art. 22, Real Decreto 994/1999)

7.9 Medidas de seguridad: Nivel Alto

- Distribución de soportes

❖ Cifrado de datos

❖ Impedir que la información sea inteligible o manipulable durante su transporte

- Registro de accesos
  - Identificación del usuario, fecha y hora, fichero accedido, tipo de acceso y si ha sido autorizado o denegado
  - Identificación del registro accedido
  - Mecanismos de control bajo el control directo del responsable de seguridad
  - Dos años de conservación
  - Informe mensual de revisiones y problemas detectados

- Copias de respaldo y recuperación
  - En un lugar diferente al de los equipos
  - Mismas medidas de seguridad

- Transmisión de Datos
  - Cifrado o similar

7.10 Datos de carácter personal: Consecuencias prácticas

- No podrán almacenarse en directorios de red o equipos con acceso "universal"
- Los listados en papel tienen que cumplir los mismos niveles de seguridad que los ficheros
- Se evitará el uso indiscriminado de disquetes
- Atención al uso de ordenadores portátiles
- Lectura obligatoria del Documento de Seguridad

7.11 Ficheros temporales

- Deberán de cumplir el nivel de seguridad que les corresponda
- Serán borrados, una vez que hayan dejado de ser necesarios para los fines que motivaron su creación

7.12 Infracciones y sanciones

- Leves: 600€ a 60.000€
  - No atender a los derechos del interesado
  - No proporcionar información a la APD
  - No inscribir ficheros
  - Recoger datos sin proporcionar información al interesado (Art. 5: Derecho a ser informado)
  - Incumplir el deber del secreto
- Graves: 60.000€ a 300.000€
  - Finalidad distinta al objeto de la empresa
  - No recabar consentimiento del afectado
  - Conculcación de los principios de la Ley
  - Impedimento u obstaculización del ejercicio de los derechos del interesado
  - Mantener datos inexactos
  - Vulneración del secreto en datos relativos a infracciones, solvencia, personalidad, etc.
  - Mantener ficheros, locales, programas o equipos sin las debidas condiciones de seguridad
  - No remitir a la APD las notificaciones previstas en la Ley
  - Obstrucción al ejercicio de la APD
  - No inscribir ficheros habiendo sido requerido por el Director de la APD

    - Incumplir el deber de información en datos recabados de persona distinta al interesado

- Muy graves: 300.000€ a 600.000€
    - Recogida en forma engañosa y fraudulenta
    - Comunicación o cesión fuera de los casos permitidos
    - Recabar o tratar datos sin consentimiento expreso
    - No cesar en el uso una vez requerido por la APD o por el interesado
    - Transferencia a países que no proporcionen un nivel de seguridad equiparable
    - Tratar datos de forma ilegítima o con menosprecio de principios y garantías aplicables
    - Vulneración del secreto de datos especialmente protegidos o recabados con fines policiales
    - No atender u obstaculizar sistemáticamente el ejercicio de los derechos del interesado
    - No atender sistemáticamente el deber de notificación