# LAS MEDIDAS DE SEGURIDAD

**Vicente M. González Camacho**
**Vocal Asesor- Jefe Gabinete Director**
**(Antigua – 25-29 / 02 / 2008)**

# REFLEXIONES PREVIAS

# REFLEXIONES PREVIAS

- La práctica exige actualización de normas.
- Desde RD 994/1999 no se regulaban con detalle.
- La sistematización aporta seguridad y orden.
- Surge la necesidad de aclarar casos concretos.
- Al mismo tiempo se requiere flexibilidad.
- Aplicación a ficheros no automatizados.
- Cumplimiento dentro del sentido común.
- Principios de conservación y seguridad afectados con la implantación de las medidas.
- Objetivo: garantizar y proteger datos personales.

# DEFINICIONES
## (RD 1720/2007)

# DEFINICIONES

- VIGENTES:
  - Accesos autorizados, autenticación, contraseña, control de acceso, copia de respaldo, identificación, incidencia, recurso, responsable de seguridad, soporte, sistema de información y usuario.

- NUEVOS:
  - Documento: escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.
  - Ficheros temporales: creados por usuarios o procesos, necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

# DEFINICIONES (II)

- Perfil de usuario: accesos autorizados a un grupo de usuarios.
- Sistema de tratamiento: modo en que se organiza o utiliza un sist. de información (automatizados, no automatizados o parcialmente automatizados).
- Transmisión de documentos: traslado, entrega, envío, comunicación o divulgación de la información contenida en el mismo.

# MEDIDAS DE SEGURIDAD

## (RD 1720/2007)

# MEDIDAS DE SEGURIDAD

## I. D.T. SEGUNDA: PLAZOS DE IMPLANTACIÓN MS.

- **Ficheros existentes**
  - **Automatizados:**
    - Seguridad Social, Mutuas, Perfiles → 1 año ( Nivel Medio).
    - Violencia de género → 1 año (Nivel Medio) → 18 meses (Nivel Alto).
    - Teleco (tráfico, localizac.) → 1 año (N. Med.) → 18 mes (Rgtro accesos)
    - Adaptación resto de ficheros → 1 año (arts. 93, 94, 101, 104).
  - **No automatizados:**
    - Nivel Básico (1 año)
    - Nivel Medio (18 meses)
    - Nivel Alto ( 2 años)

- **Ficheros nuevos manuales y/o automatizados:**
  Aplicación del nivel correspondiente desde su creación.

# MEDIDAS DE SEGURIDAD (II)

## II. DISPOSICIONES GENERALES

– Los responsables de ficheros o tratamientos y encargados implantarán las medidas de seguridad que se clasifican en tres niveles: Básico, Medio y Alto.

**ALTO** **Datos especialmente protegidos**
**Fines policiales sin consentimiento de las personas afectada**
**Violencia de género**

**MEDIO** **Infracciones administrativas o penales**
**Servicios de información sobre solvencia patrimonial y crédito**
**Administraciones Tributarias - potestades tributarias**
**Entidades financieras - servicios financieros**
**Seguridad Social, Mutuas accidentes laborales y enfermedades profes.**
**Elaboración de perfiles**

**MEDIO (+ registro de accesos)** **Operadores TELECO – tráfico y localización-**

# MEDIDAS DE SEGURIDAD (III)

**BÁSICO**

**- Cualquier otro fichero o tratamiento de DP.**

**- Ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando:**

**1.- transferencia dineraria -entidades de las que los afectados sean asociados o miembros-.**

**2.- tratamiento manual de forma incidental o accesoria, sin guardar relación con la finalidad.**

**- Datos de Salud - grado o condición de discapacidad o invalidez - cumplimiento de deberes públicos.**

# MEDIDAS DE SEGURIDAD (IV)

- Se aplicarán a ficheros o tratamientos de DP independientemente:

- **de quién realice el tratamiento**
  - Encargado del tratamiento
    - Diferentes modos de prestación del servicio (art. 82)
  - Prestación de servicios sin acceso a datos personales
    - Cláusula informativa en el contrato (art. 83)

- **desde dónde se realice**
  - Acceso a DP a través de redes de comunicaciones (públicas o no -art. 85-)
  - Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento
    - Dispositivos portátiles (art. 86)

- **cómo se realice**
  - Ficheros temporales o copias de trabajo de documentos (art. 87)

# MEDIDAS DE SEGURIDAD (V)

## III. DOCUMENTO DE SEGURIDAD

- Obligación del responsable del fichero o tratamiento.
- Interno (medidas técnicas y organizativas).
- Único y general o individualizado(según fichº o tratmto).
- Contenido en función del nivel de seguridad implantado.
- Actualizado (cambios relevantes: afecten a MS).
- Recogerá delegaciones de autorizaciones.
- Recogerá las situaciones especiales
  - Prestaciones de servicios, uso de portátiles.
  - Medidas compensatorias en lugar de previstas.

# MEDIDAS DE SEGURIDAD (VI)

## IV. FICHEROS Y TRATAMIENTOS AUTOMATIZADOS

### A) Nivel Básico:

- Funciones y obligaciones de usuarios, funciones de control y delegaciones del responsable.
- Procedimiento de notificación y gestión de incidencias (registro).
- Actualizac. de usuarios, perfiles y autorizaciones.
- Identificar información de documentos, ser inventariados y sólo accesibles por autorizados.
- Autorización salida de soportes y documentos (incluidos los anejos a un correo electrónico).
- Mecanismo identificación usuarios que accedan.
- Procedimientos realización semanal de copias de respaldo.

# MEDIDAS DE SEGURIDAD (VII)

**B) Nivel Medio:**

- **Designación responsables de seguridad.**
- **Auditoría interna o externa (cada 2 años mínimo).**
- **Sistema de registro de entrada y salida soportes.**
- **Mecanismo que limite acceso reiterado sin autorización.**
- **Sólo autorización acceso instalaciones equipos.**
- **Registro de incidencias.**

# MEDIDAS DE SEGURIDAD (VIII)

**C) Nivel Alto:**

- **Sistema identificación de soportes.**
- **Cifrado DP de portátiles utilizados en exterior.**
- **Realización copias de respaldo y procedimiento recuperación DP en lugar distinto de equipos.**
- **Registro de accesos (2 años conservación), salvo que responsable fichero sea persona física y garantice que sólo él accede a DP.**

**V. D.A. ÚNICA:**

**Productos de software deben incluir en descripción técnica, nivel de seguridad alcanzable.**

# MEDIDAS DE SEGURIDAD (IX)

## VI. FICHEROS Y TRATAMIENTOS NO AUTOMATIZADOS

A) Nivel Básico:

- Obligaciones comunes.
- Archivo soportes y documents (legislac. especfca).
- Mecanismos que impidan abrir dispositivos de almacenamiento.
- Custodia soportes y documentos por una persona si no hay dispositivos de almacenamiento.

B) Nivel Medio:

- Designación resp. seguridad (doc. segdad).
- Auditoría interna o externa (cada 2 años mínimo).

# MEDIDAS DE SEGURIDAD (X)

**C) Nivel Alto:**

- **Almacenamiento información en los elementos y lugares establecidos.**
- **Copias de documentos bajo control del personal autorizado y evitando acceso al destruirlos.**
- **Acceso información por personal autorizado.**
- **Traslado de documentación impidiendo acceso y manipulación de información.**

# INFORMES GABINETE JURÍDICO AEPD

# INFORMES GABINETE JURÍDICO AEPD

- **A) FACULTATIVO QUE CESA EN EJERCICIO PROFESIÓN**

➢ ***Informe 136839/2007:***

- **Aplicación LOPD a facultativo que cesa en ejercicio de funciones respecto ficheros HC de pacientes.**
- **Ámbito aplicación LOPD (art. 2 LOPD).**
- **Responsabilidad gestión y custodia doc. facultativos que ejerzan individualmente (art. 17.5 LAP).**
- **Independientemente de cesación, sometimiento normas de custodia y conservación HC durante plazos establecidos (art. 8 LOPD).**
- **Obligación de notificación creación ficheros a AEPD.**
- **Aplicación medidas técnicas y organizativas (art. 17.6 LAP y art. 9 LOPD).**
- **Aplicación LOPD a ficheros manuales (RD 1720/2007).**
- **Posible contratación encargado (art. 12 LOPD).**

# INFORMES GABINETE JURÍDICO AEPD (II)

- **B) DATOS INCLUIDOS EN CURRICULUM**

➢ ***Informe 95916/2007:***

  - **MS aplicables a ficheros con datos de currículum.**
  - **Aplicación MS según información (art. 4 RD 994/1999).**
  - **Minusvalía física o psíquica es dato salud (porcentaje discapacidad es DS: art. 1 g) RD 1720/2007).**
  - **Aplicación medidas de nivel alto (art. 4.3 RD 994/1999).**

# INFORMES GABINETE JURÍDICO AEPD (III)

- **C) TRATAMIENTO DATOS ALUMNOS DISCAPACITADOS**

➢ ***Informe 57676/2007:***

  - **Tratamiento datos alumnos discapacitados para asignatura de educación física.**
  - **Tratamiento datos salud (art. 7.3 LOPD).**
  - **Consentimiento expreso padres o tutores.**
  - **Consentimiento libre, específico, informado e inequívoco (art. 3 h) LOPD).**
  - **Salvo ley que habilite tratamiento (LOCE 10/2002)**
  - **Deber de información siempre (art. 5 LOPD).**
  - **Aplicación medidas técnicas y organizativas (art. 17.6 LAP y art. 9 LOPD).**
  - **Aplicación medidas de nivel alto (art. 4.3 RD 994/1999).**

# INFORMES GABINETE JURÍDICO AEPD (IV)

- **D) ACCESO FICHEROS LABORATORIO**

➢ ***Informe 19881/2007:***

- **MS exigidas sistema acceso de pacientes a resultados analíticos del laboratorio vía telemática.**
- **Aplicación medidas técnicas y organizativas (art. 17.6 LAP y art. 9 LOPD).**
- **Aplicación medidas de nivel alto (art. 4.3 RD 994/1999).**
- **Tratamiento datos salud (art. 7.3 LOPD).**
- **Imposibilitar interceptación y accesos indebidos.**
- **Sistema de contraseñas acorde con LOPD si asegura carácter personalísimo de la consulta.**
- **Conocimiento de DP supone cesión (art. 11.1 LOPD).**

# INFORMES GABINETE JURÍDICO AEPD (V)

- **E) CESIÓN DATOS DISCAPACITADOS A EMPRESAS**

➢ ***Informe 33158/2006:***

- **MS que debe implantar Asociación Discapacitados.**
- **Posible cesión de DPS a empresas contratantes.**
- **Minusvalía física o psíquica es dato salud (porcentaje discapacidad es DS: art. 1 g) RD 1720/2007).**
- **Tratamiento datos salud (art. 7.3 LOPD).**
- **Aplicación medidas técnicas y organizativas (art. 17.6 LAP y art. 9 LOPD).**
- **Aplicación medidas de nivel alto (art. 4.3 RD 994/1999).**
- **Comunicación DP a empresas (art. 11.1 LOPD).**
- **Consentimiento expreso padres o tutores.**
- **Deber de información siempre (art. 5 LOPD).**

# ¡ MUCHAS GRACIAS !

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS