

# Seguridad Informática y la LOPD

Rev 4.0 20/05/2010



**José Juan Cerpa Ortega**  
Ingeniero en Informática

Network & Computer Technologies SL  
NCT Informática

# Índice

- Antecedentes
- Desarrollo normativo actual
- Objeto y ámbito de aplicación
- Principios fundamentales
- Definiciones importantes y Actores
- Movimiento internacional de datos
- Clasificación de los activos
- Metodología de trabajo
- Medidas de seguridad
- Infracciones y Sanciones
- Conclusiones

## Información

Casi **7 de cada 10** empresas sufre algún tipo de ataque informático. Si según el INE hay más 3 millones de empresas/ empresarios supone más de 2 millones.

Entre los más frecuentes en las pymes son: la **denegación de servicios** (89,9%), los **virus** del tipo troyano (77,3), la recepción de correo no deseado o **spam** (58,7%), otros virus informáticos (42,7), la instalación de **software espía** (19,5%), las **intrusiones** remotas en el ordenador (13,4%) y las intrusiones en el correo electrónico (9,7%).

Kaspersky Labs 2009

Según Symantec en EEUU es el 75% de las empresas y las pérdidas anuales superan los 2 millones de dolares.

Fuente:

[http://www.symantec.com/content/es/mx/enterprise/white\\_papers/Symantec\\_DataCenter\\_10\\_Report\\_Global.pdf](http://www.symantec.com/content/es/mx/enterprise/white_papers/Symantec_DataCenter_10_Report_Global.pdf)

## ***Antecedentes***

---

Estudia el pasado si quieres pronosticar el futuro.  
(Confucio)

## ***Antecedentes***

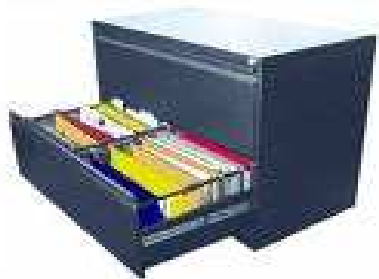
- La **Constitución Española** de 1978: En el artículo 18.4 se dispone: "La Ley **limitará el uso de la INFORMÁTICA para garantizar** el honor y **la intimidad** personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"

# ¿Por qué?

## INFORMACIÓN-AUTOMATIZADA

# Antecedentes

- Los **avances tecnológicos** en la informática y las comunicaciones proporcionan **beneficios e inconvenientes** (fundamentalmente en el derecho a la intimidad de las personas).



**ANTES**

**=**



**AHORA**



**AL INSTANTE  
SIN COSTE**

**¿Microsoft vs Google?**  
**¿Y Facebook?**

# Antecedentes



## **Antecedentes**

- La **Ley Orgánica 5/1992** de Regulación del Tratamiento Automatizado de Datos de Carácter Personal de 29 de Octubre (**LORTAD**). Regula el tratamiento en ficheros automatizados.
- El **Real Decreto 994/1999** de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal, de 11 de Junio, (**RMS**)
  - Desarrolla la LORTAD, y regula las **medidas técnicas y organizativas** que deben aplicarse a los sistemas de información en los cuales se traten datos de carácter personal de forma automatizada.
  - Este reglamento se encuentra actualmente **derogado**.

## Desarrollo normativo

- La **Ley Orgánica 15/1999** de Protección de Datos de Carácter Personal (**LOPD**) que amplía el ámbito de aplicación a todo tipo de ficheros, independiente del soporte en el que sean tratados.
- El **Real Decreto 1720/2007**, de 21 de Diciembre de desarrollo de la LOPD (Aprobado en Consejo de Ministros de 21/12/2007, publicado en el BOE el 19/01/2008, entró en vigor el 19/04/2008).
  - Conocido como RLOPD.
  - Desarrolla tanto los principios de la ley, como las **medidas de seguridad** a aplicar.
  - Se aplica a **ficheros en cualquier otro tipo de soportes**.

## ***Objeto y ámbito de aplicación***

- Garantizar y **proteger**, EN LO QUE CONCIERNE AL TRATAMIENTO DE LOS DATOS PERSONALES, las libertades públicas y **los derechos fundamentales de las personas físicas**, y especialmente de su honor, intimidad y privacidad personal y familiar.
- La ley será de aplicación a los **datos de carácter personal registrados en soporte físico**, que los haga **susceptibles de tratamiento**, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.
  - Excepciones:
    - Actividades exclusivamente personales o **domésticas**
    - Ficheros sometidos a la normativa de **Materias clasificadas**
    - Ficheros para la investigación del **terrorismo** y formas graves de **delincuencia** organizada.

## ***Principios fundamentales***

- Calidad de los datos
- Derecho de información
- Solicitud de consentimiento
- Datos especialmente protegidos (no obligado a declarar)
- Datos relativos a la salud (autorización expresa)
- Seguridad de los datos
- Deber de secreto
- Comunicación de los datos
- Cesión de los datos para la prestación de servicios

## ***Definiciones***

---

.

**Definid y no discutireis. (Aristóteles)**

## Definiciones

- Un **dato de carácter personal** es cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas **cuya identidad pueda determinarse, directa o indirectamente**, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social.
- **Fichero** (lógico): Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso

# Actores

- Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento.
- Responsable del fichero o tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros **decida sobre la finalidad, contenido y uso del tratamiento**, aunque no lo realizase materialmente.
- Encargado del tratamiento: La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, **trate datos personales por cuenta del responsable** del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la **prestación de un servicio**.

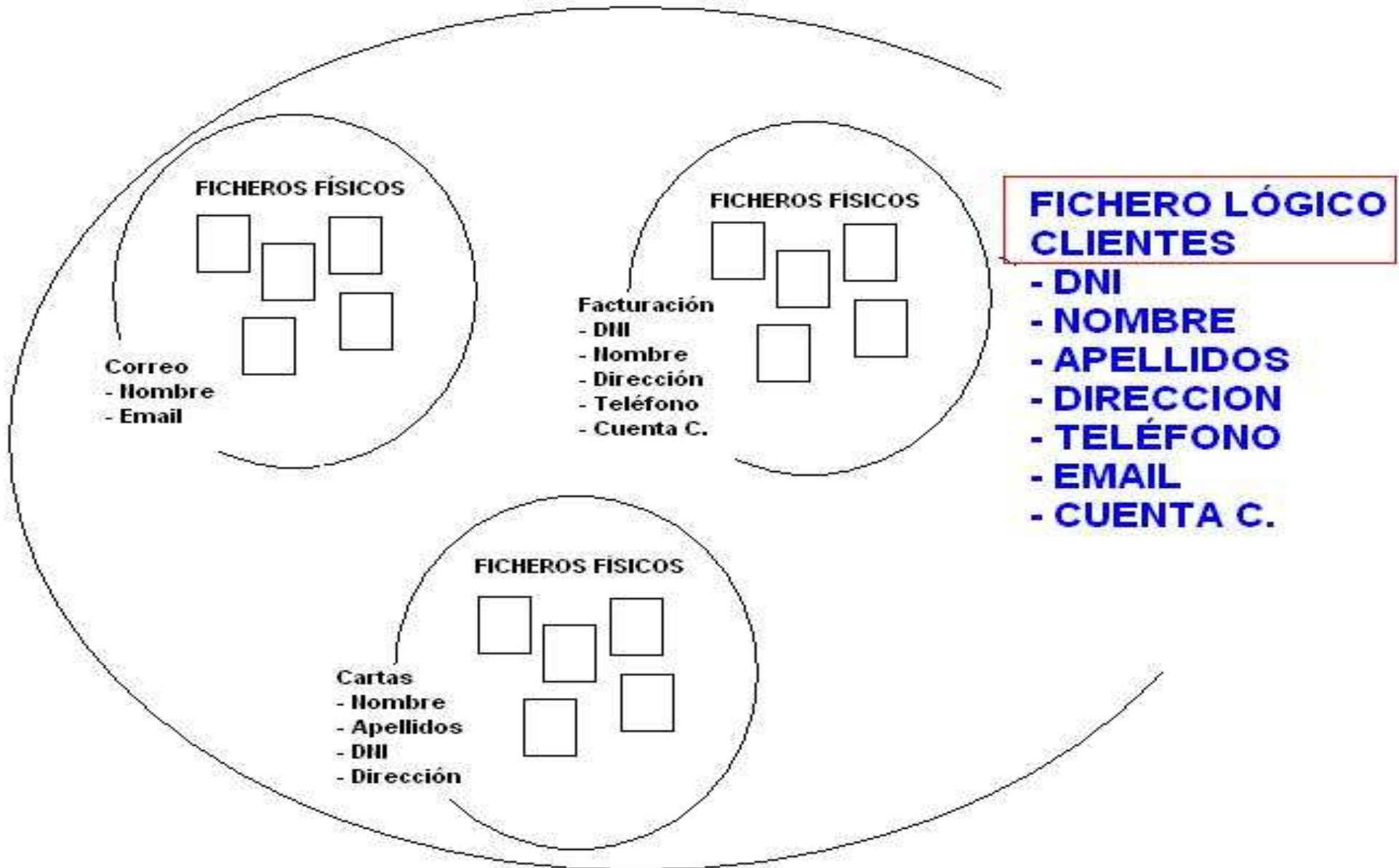
# Actores

- Relación entre responsable y encargado deberá estar regulada a través de **CONTRATO** si hay acceso a datos. El dicho es vital cuando se elabora un contrato.
  - A qué datos se accede
  - Con que nivel de seguridad
  - Para que se utilizarán dichos datos
  - Responsabilidad en caso de uso indebido
  - Otros:
    - En caso de software enunciar cada uno de las funciones que el software realizará.
    - En caso de hardware identificar las máquinas sobre las que se dará servicio.
    - Limitar la responsabilidad y/o contratar un seguro de RC
    - Ej. <http://www.contratosinformaticos.com>

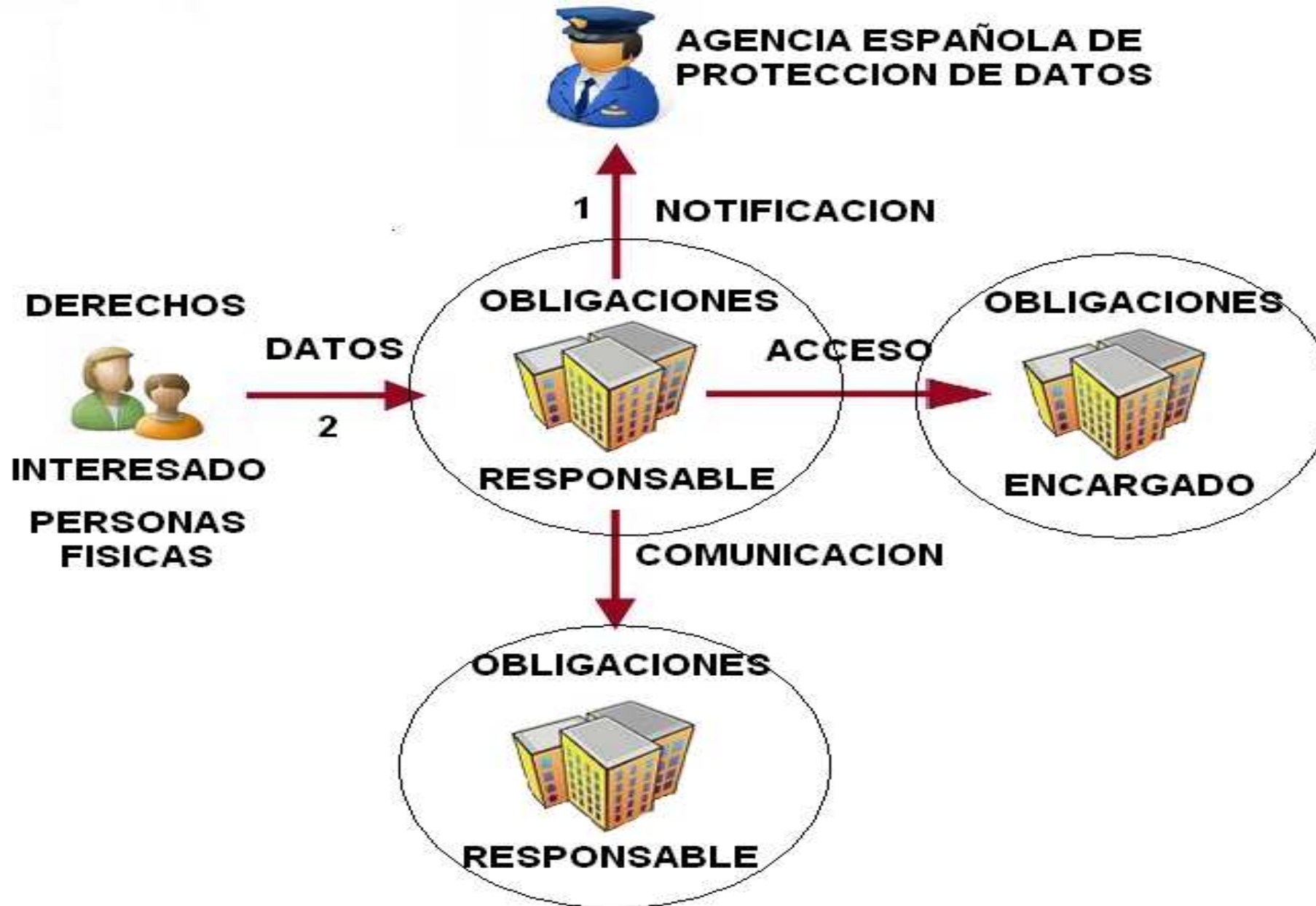
# Actores

- **La Agencia de Protección de Datos**: órgano encargado de **velar por el cumplimiento de la legislación** sobre protección de datos y controlar su aplicación
  - Será **dirigida y representada por el director** de la APD.
  - Integrado a la APD existe el órgano de **Registro General de Protección de datos** donde se inscribirán los ficheros tanto de titularidad pública como privada.
  - Las **comunidades autónomas** podrán crear y mantener sus propios registros de ficheros.
  - Las autoridades de control (funcionarios considerados autoridad pública) en el ejercicio de sus funciones podrán **inspeccionar** los ficheros, documentos, y equipos físicos y lógicos usados para el tratamiento. Normalmente actúan previa denuncia de un interesado/afectado.

# Definiciones – Ejemplo Fichero Lógico



# Normativa actual

































## ***Movimiento internacional de datos***

- Queda **prohibida la transferencia internacional (países fuera del Espacio Económico Europeo)** de datos de carácter personal a países que no cumplan los mínimos de seguridad exigidos (equiparable a la presente ley) **sin la autorización PREVIA del director de la AEPD**, que sólo la otorgará si se obtienen las garantías adecuadas.
  - Lo dispuesto en el párrafo anterior no será de aplicación cuando el afectado haya dado su **consentimiento inequívoco** a la transferencia prevista.
  - En países como Argentina la AEPD ha declarado positivamente sobre su nivel de protección.
  - En los **EEUU** sólo los países adheridos a los principios de **puerto seguro (safe harbor)**
  - **EEE = EU + Islandia, Noruega y Liechtenstein.**

# Movimiento internacional de datos - Hosting



	Austria		Grecia
	Bélgica		Hungría
	Bulgaria		Islandia
	Chipre		Irlanda
	República Checa		Italia
	Dinamarca		Liechtenstein
	Estonia		Letonia
	Finlandia		Lituania
	Francia		Luxemburgo
	Alemania		Malta
	Países Bajos		Eslovaquia
	Noruega		Eslovenia
	Polonia		España
	Portugal		Suecia
	Rumania		Reino Unido

## Otros Países:

Suiza  
EEUU-Puerto Seg.  
Canada  
Argentina  
Bailia de Jersey  
Isla de Man  
Guernsey

## ***Clasificación de los activos – La información***

---

**Si no sabemos dónde vamos difícilmente llegaremos.**

## ***Clasificación de los activos – La información***

- **Muy importante inventariar y clasificar los activos. (hardware, software, información, procesos, personas...)**
- **La Ley clasifica los datos en: Nivel alto:**
  - Se aplicará a los ficheros o tratamientos de datos que hagan referencia a la **ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual** de las personas y respecto de los que no se prevea la posibilidad de adoptar el nivel básico;

## ***Clasificación de los activos – La información II***

- ***Nivel medio:*** Se aplicará a los ficheros o tratamientos de datos relativos a:
  - aquellos que se rijan por el artículo 29 de la LOPD referente a la prestación de servicios de **solvencia patrimonial y crédito**,
  - los de **entidades financieras** para las finalidades relacionadas con la prestación de **servicios financieros**;
  - los de **mutuas de accidentes de trabajo y enfermedades profesionales** de la Seguridad Social;
  - los que ofrezcan una **definición de la personalidad** y permitan evaluar determinados aspectos de la misma o del comportamiento de personas;
  - y los de los **operadores de comunicaciones** electrónicas, respecto de los datos de tráfico y localización.

## **Clasificación de los activos – La información III**

- **Nivel básico:** Se aplicará a **cualquier otro fichero** que contenga datos de carácter personal. También a ficheros que contengan **datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando:**
  - los datos se utilicen con la única finalidad de realizar una **transferencia dineraria** a entidades de las que los afectados sean asociados o miembros.
  - Se trate de ficheros o tratamientos no automatizados o sean tratamientos manuales de estos tipos de datos de **forma incidental o accesoria**, que no guarden relación con la finalidad del fichero;
  - y en los ficheros o tratamientos que contengan datos de **salud**, que se refieran exclusivamente al **grado de discapacidad** o la simple declaración de invalidez, con motivo del **cumplimiento de deberes públicos**.Ej Rentas.

## ***Clasificación de los activos – La información IV***

- **Disposición adicional (RD 1720/2007)**
  - Los productos de software destinados al tratamiento automatizado de datos personales deberán incluir en su descripción técnica el nivel de seguridad, básico, medio o alto, que permitan alcanzar.
  - **Ejemplo software para un dentista.**
    - Una simple agenda para control de citas. DNI, nombre y apellidos, dirección, teléfono, fecha y hora.
    - Añadimos un campo observaciones para posibles inconvenientes. Ej. Cambios o retrasos.
    - ¿Qué pasa si el dentista incluye otros datos?

**Toda batalla es ganada antes de ser librada.  
(Sun Tzu)**

**Hazlo simple.**

# Metodología PHVA



## METODOLOGÍA

<i>*Planificar*</i>	establecer los objetivos y procesos necesarios para conseguir resultados de acuerdo con los requisitos del cliente y las políticas de la organización;
<i>*Hacer*</i>	implementar los procesos;
<i>*Verificar*</i>	realizar el seguimiento y la medición de los procesos y los productos respecto a las políticas, los objetivos y los requisitos para el producto, e informar sobre los resultados.
<i>*Actuar*</i>	tomar acciones para mejorar continuamente el desempeño de los procesos.

## ***Metodología***

- Documentar Procedimiento de copias de seguridad y restauración de datos
  - ¿Qué quiere/necesita realmente y cuanto cuesta?
  - Quién/es son los responsables?
  - ¿Origen?
  - ¿Destino? ¿Local? ¿Remoto?
  - ¿Espacio necesario?
  - ¿Soporte?
  - ¿Horario?
  - ¿Revisiones de las copias? ¿Medición?
  - Pruebas de restauración
  - Comprobación de los procedimientos

## *Metodología*

- ROI. Return of investment (Retorno de la inversión)
- $ROI = (\text{Beneficio} - \text{coste}) / \text{coste}$
- ¿Es rentable lo que vamos a implantar?
- Si no es rentable hay que descartarlo por otra opción
- Ej. 1 - Cadenas de seguridad en portátiles
- Ej. 2 – Sistema backup vs alta disponibilidad (replicado)

## ***Medidas de seguridad***

---

**Una cadena es tan fuerte como su eslabón más débil.  
(Anónimo)**

**Más vale prevenir que curar.**

## ***Medidas de seguridad***

- Seguridad se basa en 3 principios: disponibilidad, confidencialidad e integridad.
- El eslabón más débil suele ser casi siempre “un ser humano”. Hay que conocer los riesgos/amenazas a los activos para saber como protegerlos.
- Es de vital importancia formar y concienciar al personal.
- Se dan por supuestas la implementación de medidas genéricas:
  - Antivirus, Antispyware, Antispam, Firewall
  - Actualizaciones de sistema operativo y software
  - Cambio de contraseñas por defecto
  - etc.

# Medidas de seguridad I

- **Nivel básico:**
  - **Elaborar documento de seguridad e implementar**
    - **Funciones y obligaciones del personal**, delegaciones y medidas para darlas a conocer y consecuencias del incumplimiento. Ej. Formación, manual de buen uso.
    - **Procedimiento de notificación y gestión. Registro de incidencias.** Ej registro manual o automatizado.
    - **Control de acceso lógico** (sólo automatizados). **Relación actualizada de usuarios y accesos autorizados.** Personal encargado de autorizar/denegar accesos. Mecanismos para evitar accesos indebidos. Ej NTFS Windows.
    - Gestión de **soportes y documentos (inventario, identificación, salida autorizada incluso por email, traslado seguro, destrucción o borrado antes de deshecho...)**. Ej sistema etiquetado EAN código de barras. Software eraser.

## ***Medidas de seguridad II***

- **Nivel básico:**
  - **Elaborar documento de seguridad e implementar (mixto)**
    - Identificación y autenticación. (sólo automatizados). Medidas que garanticen **identificación inequívoca y personalizada. Procedimientos de asignación, distribución y almacenamiento de contraseñas. Administración de usuarios y directivas.**
    - **Copias de respaldo y recuperación.** (sólo automatizados) Al menos una vez **semanal. Procedimientos detallados de copia y recuperación. Verificación semestral** de los procedimientos. Se **evitaran pruebas con datos reales** si no se garantiza el nivel de seguridad adecuado haciendo previamente copia de seguridad. Software de backup de windows.

## ***Medidas de seguridad III***

- **Medidas de seguridad para nivel medio:**
  - **Todas las de nivel básico y además**
    - **Responsable de seguridad** encargado de coordinar y controlar el cumplimiento.
    - **Auditoría bienal** elaborando **informe con deficiencias y medidas correctoras** y complementarias. Se analizará por el responsable de seguridad y elevará conclusiones al responsable que tomará las medidas oportunas y quede a disposición de la AEPD. Cuestionarios y observación.
    - Gestión de **soportes** y documentos (**registro de entrada y salida**). Registro manual o automatizado.
    - Identificación y autenticación (sólo automatizados). **Se limita el intento de accesos fallidos**. Directivas.
    - **Control de acceso físico a las instalaciones** donde estén los sistemas. (sólo automatizados)
    - **Registro de incidencias (recuperación de datos autorizada)**

## *Medidas de seguridad IV*

- Medidas de seguridad para nivel alto:
  - Todas las de nivel básico, medio y además
    - Gestión y **distribución de soportes cifrado.**
    - **Copias de respaldo** y procedimiento de recuperación **fuera de los locales.** Backup online.
    - **Registro de acceso a los datos** (¿Quién? ¿Cuándo? ¿A qué información?). **Logs** del sistema, directivas de auditoría.
    - Telecomunicaciones. **Comunicaciones** por redes públicas e inalámbricas de forma **cifrada.** Protocolos seguros IPSec.

# Medidas de seguridad V - Resumen

CUADRO RESUMEN

SOLO FICHEROS AUTOMATIZADOS

	Nivel Básico	Nivel Medio	Nivel Alto
<b>RESPONSABLE DE SEGURIDAD</b>		El responsable del fichero tiene que designar a uno o varios responsables de seguridad (no es una delegación de responsabilidad). El responsable de seguridad es el encargado de coordinar y controlar las medidas del documento.	
<b>PERSONAL</b>	<p>Funciones y obligaciones de los diferentes usuarios o de los perfiles de usuarios claramente definidas y documentadas.</p> <p>Definición de las funciones de control y las autorizaciones delegadas por el responsable.</p> <p>Difusión entre el personal, de las normas que les afecten y de las consecuencias por su incumplimiento.</p>		
<b>INCIDENCIAS</b>	<p>Registro de incidencias: tipo, momento de su detección, persona que la notifica, efectos y medidas correctoras.</p> <p>Procedimiento de notificación y gestión de las incidencias.</p>	<p>Anotar los procedimientos de recuperación, persona que lo ejecuta, datos restaurados, y en su caso, datos grabados manualmente.</p> <p>Autorización del responsable del fichero para la recuperación de datos.</p>	

# Medidas de seguridad VII - Resumen

CUADRO RESUMEN

SOLO FICHEROS AUTOMATIZADOS

	Nivel Básico	Nivel Medio	Nivel Alto
<b>CONTROL DE ACCESO</b>	<p>Relación actualizada de usuarios y accesos autorizados.</p> <p>Control de accesos permitidos a cada usuario según las funciones asignadas.</p> <p>Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados.</p> <p>Concesión de permisos de acceso sólo por personal autorizado.</p> <p>Mismas condiciones para personal ajeno con acceso a los recursos de datos.</p>	<p>Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información.</p>	<p>Registro de accesos: usuario, hora, fichero, tipo de acceso, autorizado o denegado.</p> <p>Revisión mensual del registro por el responsable de seguridad.</p> <p>Conservación 2 años.</p> <p>No es necesario este registro si el responsable del fichero es una persona física y es el único usuario.</p>
<b>IDENTIFICACIÓN Y AUTENTICACIÓN</b>	<p>Identificación y autenticación personalizada.</p> <p>Procedimiento de asignación y distribución de contraseñas.</p> <p>Almacenamiento ininteligible de las contraseñas.</p> <p>Periodicidad del cambio de contraseñas (&lt;1 año).</p>	<p>Límite de intentos reiterados de acceso no autorizado.</p>	<p>Sistema de etiquetado confidencial.</p> <p>Cifrado de datos en la distribución de soportes.</p> <p>Cifrado de información en dispositivos portátiles fuera de las instalaciones (evitar el uso de dispositivos que no permitan cifrado, o adoptar medidas alternativas).</p>
<b>GESTIÓN DE SOPORTES</b>	<p>Inventario de soportes.</p> <p>Identificación del tipo de información que contienen, o sistema de etiquetado.</p> <p>Acceso restringido al lugar de almacenamiento.</p> <p>Autorización de las salidas de soportes (incluidas a través de e-mail) Medidas para el transporte y el desecho de soportes.</p>	<p>Registro de entrada y salida de soportes: documento o soporte, fecha, emisor/destinatario, número, tipo de información, forma de envío, responsable autorizado para recepción/entrega.</p>	

# Medidas de seguridad VII - Resumen

CUADRO RESUMEN

SOLO FICHEROS AUTOMATIZADOS

	Nivel Básico	Nivel Medio	Nivel Alto
COPIAS DE RESPALDO	<p>Copia de respaldo semanal.</p> <p>Procedimientos de generación de copias de respaldo y recuperación de datos.</p> <p>Verificación semestral de los procedimientos.</p> <p>Reconstrucción de los datos a partir de la última copia. Grabación manual en su caso, si existe documentación que lo permita.</p> <p>Pruebas con datos reales. Copia de seguridad y aplicación del nivel de seguridad correspondiente.</p>		<p>Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos.</p>
AUDITORIA		<p>Al menos cada dos años, interna o externa.</p> <p>Debe realizarse ante modificaciones sustanciales en los sistemas de información con repercusiones en seguridad.</p> <p>Verificación y control de la adecuación de las medidas.</p> <p>Informe de detección de deficiencias y propuestas correctoras.</p> <p>Análisis del responsable de seguridad y conclusiones elevadas al responsable del fichero.</p>	
TELECOMUNICACIONES			<p>Transmisión de datos a través de redes electrónicas cifradas.</p>

## ***Infracciones y Sanciones I***

**El desconocimiento de la Ley no exime de su cumplimiento. (Principio general del derecho)**

**El conocimiento disminuye el riesgo. Formación continua.**

# *Infracciones y Sanciones I*

- Los responsables de los ficheros y los encargados de tratamiento estarán sujetos al régimen sancionador establecido en la presente Ley. Han aumentado un 45%.
- Tipos de infracciones
  - Leves. Sanciones entre 601,01 a 60101,21 €
    - **No atender a la solicitud del interesado** de rectificación o cancelación de sus datos
    - No proporcionar información que solicite la AEPD en el ejercicio de sus competencias
    - **No solicitar la inscripción de ficheros** de carácter personal en el Registro General
    - **Recoger datos de carácter personal sin proporcionarles información** (art. 5)
    - **Incumplir el deber de secreto (nivel básico)**

# *Infracciones y Sanciones II*

- **Tipos de infracciones**

- **Graves**

- Crear ficheros de titularidad privada o **iniciar la recogida de datos con una finalidad distinta al objeto legítimo de la empresa**
- **Recabar datos sin el consentimiento expreso** de las personas afectadas
- **Tratar los datos** de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente ley o con **incumplimiento de los preceptos de protección** que impongan las disposiciones reglamentarias de desarrollo
- **Impedir u obstaculizar el ejercicio de los derechos** de acceso y oposición

## ***Infracciones y Sanciones III***

- **Tipos de infracciones**
  - **Graves. Sanciones entre 60101,21 a 300506,05 €**
    - **Mantener datos** de carácter personal **inexactos** o no rectificarlos o cancelarlos cuando proceda
    - **Vulnerar el deber de secreto** en ficheros con datos de nivel medio o alto
    - **Mantener los ficheros**, locales, programas o equipos que contengan datos de carácter personal **sin las debidas condiciones de seguridad**
    - No remitir a la AEPD las notificaciones previstas en la ley
    - La **obstrucción** al ejercicio de la **función inspectora**
    - **No inscribir un fichero** de datos de carácter personal **cuando haya sido requerido** por el director de la AEPD

# Infracciones y Sanciones IV

- **Tipos de infracciones**

- **Graves**

- **Incumplir el deber de información** que se establece en los artículos 5, 28 y 29 cuando los **datos hayan sido recabados de persona distinta del afectado.**

- **Muy Graves. Sanciones entre 300506,05 a 601012,10 €**

- **Recogida de datos de forma engañosa** o fraudulenta
- **Comunicación** o cesión de **datos** de carácter personal, **fuera de los casos en que estén permitidas**
- **Recabar y tratar** datos de carácter personal a los que se refiere el artículo 7.2 y 7.3 (**datos protegidos**) cuando no medie **consentimiento expreso del afectado**
- No cesar en el uso ilegítimo de los tratamientos cuando sea requerido por el director de la AEPD

# Infracciones y Sanciones V

- **Tipos de infracciones**

- **Muy Graves**

- **Transferencia de datos** de carácter personal **con destino a países que no proporcionen un nivel de protección** equiparable sin autorización del director de la AEPD
    - **Tratar datos de forma ilegítima** o con menosprecio cuando se atente contra el ejercicio de los derechos fundamentales
    - **Vulneración del deber de guardar secreto** referente a datos protegidos
    - **No atender u obstaculizar** de forma sistemática los **derechos** de acceso, rectificación, cancelación u oposición.
    - **No atender de forma sistemática** el deber legal de notificación de la inclusión de datos en un **fichero**

## *Ejemplos de Infracciones y Sanciones*

- **Procedimiento PS/00317/2007 (art. 9)**
  - Multa de 60101,21 € rebajada a 3000 €.A un abogado por tener **compartida en el emule una base de datos** con información de 1500 clientes.
  
- **Procedimiento PS/00288/2007 (art. 9)**
  - Multa de 60101,21 € rebajada a 6000 € al BBVA por **dejar depositado en la basura 7 cajas con información** de clientes.

# CONCLUSIONES

- “El único sistema seguro es aquél que está apagado en el interior de un bloque de hormigón protegido en una habitación sellada rodeada por guardias armados”. **(Gene Spafford)**
- **La seguridad es un proceso** no un producto. Revisión continua.
- La **información** es uno de los **activos más importantes** protégela independientemente de si tiene datos personales o no. Perderla podría llevar a la “muerte” de un negocio.
- El conocimiento disminuye el riesgo. Formación continua.
- Los informáticos tenemos la responsabilidad (obligación) de reducir los daños. SEAMOS PROFESIONALES.

# • **Gracias por la atención**

- Resolución de dudas
- Más información en mi blog [www.josejuancerpa.com](http://www.josejuancerpa.com)
  - En facebook. [www.facebook.com/jose.j.cerpa](http://www.facebook.com/jose.j.cerpa)
  - Empresa. [www.nct-informatica.es](http://www.nct-informatica.es)
  - Teléfono 928931807