V Congreso de Ingeniería de Organización
Valladolid-Burgos, 4-5 Septiembre 2003

Índice

El Reglamento de Medidas de Seguridad para ficheros de carácter personal como norma de Seguridad Informática

Carlos Alonso de Armiño, Lourdes Sáiz Bárcena, Ignacio Fontaneda González y Mª Rosario González Dieste
Universidad de Burgos, Escuela Politécnica Superior (Edificio C) C/ Francisco de Vitoria s/n 09006 Burgos
caap@ ubu.es
Universidad de Burgos, Escuela Politécnica Superior (Edificio C) C/ Francisco de Vitoria s/n 09006 Burgos
lsaiz@ubu.es
Universidad de Burgos, Escuela Politécnica Superior (Edificio A) C/ Cantabria s/n 09006 Burgos
ifontane@ubu.es
Universidad de Burgos, Escuela Politécnica Superior (Edificio Milanera) C/ Villadiego s/n 09001 Burgos
mrgonzalez@ubu.es

RESUMEN

El objetivo de este trabajo es profundizar en el estudio del Reglamento de Medidas de Seguridad para ficheros de carácter personal como norma de Seguridad Informática. Así se analizan los niveles de seguridad que establece este Reglamento, según la naturaleza de los datos que contengan los ficheros, sus características, lo que hemos denominado Cuadrante del Reglamento, de utilidad para la implantación y procesos de auditoría, y sus aspectos principales. Este Reglamento es una herramienta especialmente útil en un área prácticamente desabastecida de normas y reglas, dado que su intención es velar por la seguridad interna y externa de los datos que maneja cualquier organización y, por esta razón, su aplicación no debería limitarse en exclusiva a datos de carácter personal, sino al Sistema de Información en su conjunto, como un primer paso para la consecución de una Metodología de Seguridad en materia informática.

***Palabras clave**: Seguridad Informática, Ficheros de carácter personal.*

1. Introducción

- Fruto del **artículo 18.4 de la Constitución Española**, que emplaza al Legislador a limitar el uso de la informática para garantizar el honor, la intimidad, y el legítimo ejercicio de los derechos de los ciudadanos, así como de posteriores directivas europeas, surge la Ley Orgánica 5/1992 de Regulación de Tratamiento Automatizado de Datos de carácter personal (**LORTAD**), que posteriormente es perfeccionada y derogada por la **Ley Orgánica 15/99** de **Protección de Datos de Carácter Personal** (**LOPD**).
- Dicha Ley, en paralelismo a su antecesora, establece en su Artículo 9.- Seguridad de los datos que: "El responsable del fichero, y, en su caso, el encargado del tratamiento, deben **adoptar las medidas de índole técnica y organizativas necesarias** que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural". Ordenando además que no se registren datos en ficheros que no reúnan las condiciones, y estableciendo que **se reglamentarán dichas condiciones y requisitos.**

- Fruto de este emplazamiento de Ley surge el **R.D. 994/1999 Reglamento de Medidas de Seguridad para Ficheros con Datos de Carácter Personal** (**Reglamento de Seguridad**), que es nuestro objeto de análisis.

2. El Reglamento de Medidas de Seguridad

2.1 Niveles de Seguridad

El Reglamento de Seguridad, inicia su desarrollo estableciendo **tres niveles de seguridad, según sea la naturaleza de los datos** de carácter personal que contengan los ficheros:

NIVEL DE NATURALEZA LOS DATOS	BASICO	MEDIO	ALTO
	• Nombre • Apellidos • Direcciones de contacto (Físicas o electrónicas) • Teléfono (fijo o móvil) • Otros	• Comisión infracciones penales • Comisión infracciones administrativas • Información de Hacienda Pública • Información de servicios financieros	• Ideología • Religión/Creencias • Origen racial • Salud • Vida sexual • Datos reunidos para fines policiales (sin consentimiento)

Es decir, y siempre bajo la perspectiva de datos de personas físicas, se establece una **jerarquía de protección**:

- El nivel superior corresponde a los datos especialmente **protegidos** según la LOPD, ósea; los ideológicos, religiosos, raciales, de salud, vida sexual e investigación policial.
- A un nivel medio están los datos que aportan **perfiles delictivos o financieros**
- En la base se encuentran los datos pura y simplemente **identificativos**

2.2. Características

A partir de aquí se establece el Reglamento, con las siguientes características:

- Como una **estructura Acumulativa**. Estableciendo una serie de requisitos para el Nivel Básico, que se mantendrán y ampliarán en el Nivel Medio que, a su vez se mantendrán y ampliarán en el Nivel Alto.
- Con **espíritu de Norma adaptable**. El Reglamento se elabora con evidente colaboración de expertos en la materia, y adquiere un espíritu de Norma Abierta a interpretación, y a adaptación dentro de cada organización. De igual forma que una Norma de Calidad, exige el cumplimiento de una serie de requisitos, pero deja libre la forma de implantación de los

mismos. Y no puede ser de otra forma, puesto que a partir del Nivel Medio, exige la realización de Auditorías.

- Con filosofía de **herramienta Empresarial**. Los requisitos que establece el Reglamento, no se limitan a establecer un marco de seguridad para los datos de carácter personal ante terceros malintencionados. Se establecen requisitos para:
- Garantizar la **seguridad e integridad** de los datos dentro de la empresa.
- Establecer una **estructura organizativa** adecuada en su tratamiento.
- Establecer un **sistema documental** de utilidad inherente a la empresa.

2.3. Cuadrante del Reglamento

Antes de entrar a desarrollar algunos puntos del Reglamento, aportaremos **un Cuadrante Resumen** del mismo que, sin duda, será de utilidad para procesos de implantación y auditoría:

CONCEPTO	NIVEL BASICO	NIVEL MEDIO	NIVEL ALTO
1.- Documento de Seguridad	Procedimiento **Documentado**. Estructura. Ámbito definido. Revisión y **actualización**.	**Responsable** de Seguridad. **Auditorías**.	
2.- Funciones y Obligaciones	**Definidas** y documentadas. Personal **debe conocer** normas que le afecten.		
3.- Incidencias	**Registro** incidencias; tipo, momento, personas, efectos.	**Recuperación** es incidencia.	
4.- Identificación y Autenticación	**Relación** usuarios con accesos permitidos, actualizada. Contraseñas procedimiento, cambio periódico, cifradas.	Forma **inequívoca** y **personalizada**. **Limitar intentos** de acceso fallidos.	**Registrar** accesos: usuario, momento, fichero, tipo, autorizado, y registro accedido. **Guardar** 2 años. **Revisión** periódica. **Informe** mensual.
5.- Control de Acceso	Usuarios acceden **sólo a recursos precisos**. Existe responsable asignación.	Control **acceso físico.**	
6.- Gestión de Soportes	**Identificar** tipo de información que contienen. Inventariables/almacenables. Salida soportes autorizada.	Medidas soporte **desechado** o reutilizado. **Registro** entradas y salidas.	Distribución soportes **cifrada**.
7.- Copias Respaldo y Recuperación	**Verificar** correcta definición y aplicación. Garantizar **reconstrucción**. Copia al menos **semanal.**		Copia en **lugar diferente** (garantía seguridad).
8.- Pruebas Aplicaciones		**No datos reales**, salvo garantía seguridad.	
9.- Ficheros Temporales	Deben **garantizar misma seguridad y borrarse** tras su uso.		
10.-Telecomunicaciones	Deben **garantizar misma seguridad.**		**Cifradas**

= es de aplicación lo del nivel inferior.

2.4. Puntos Principales

Documento de Seguridad

Esta Norma (Reglamento de Seguridad), deberá ser implantada por la organización responsable del fichero a través de un **Documento de Seguridad de obligado cumplimiento**, para el personal con acceso a los Sistemas de Información que manejan los ficheros con datos de carácter personal.

Con espíritu paralelo al grupo de procedimientos que surge, dentro del **sistema documental**, en la implantación de Sistemas de Calidad, el documento o (podemos interpretar), grupo de procedimientos, **deberán contener**:

- ✓ **Ámbito de Aplicación**. Especificando de manera detallada los Recursos protegidos, y la parte de la organización afectada por dicha implantación.

- ✓ **Medidas, normas, procedimientos, reglas y estándares** para garantizar lo requerido en el Reglamento.
  Dichas herramientas habrán podido ser **adoptadas por la organización o elaboradas por ella misma**. De nuevo queda clara la viabilidad y la lógica de implantación de un sistema documental, que pueda integrar distintos procedimientos o instrucciones de trabajo bajo el documento de seguridad, de una forma paralela a como se integran las normas externas e internas bajo un manual de calidad, en un sistema de calidad normalizado.

- ✓ **Funciones y obligaciones del personal**. Que será objeto de un punto posterior.

- ✓ **Estructura de los ficheros** con datos de carácter personal y **descripción de los sistemas de información** que los tratan.
  Entramos en este apartado, en un **mayor nivel de detalle del ámbito de aplicación** del Documento de Seguridad, aportando una estructura concreta a los ficheros objeto de protección, y una mayor definición de los Sistemas de Información **(*)** que operan sobre ellos.
  (*) "Conjunto de ficheros automatizados, programas, soportes y equipos empleados", según la propia definición del Reglamento de Seguridad.

- ✓ Procedimiento de notificación, gestión y respuesta ante las **incidencias**. Que será objeto de un punto posterior.

- ✓ Los procedimientos de realización de **copias de respaldo y de recuperación** de los datos. Que será objeto de un punto posterior.

Dicho Documento debe mantenerse en todo momento **actualizado y debe ser revisado** cuando se produzcan cambios relevantes en el sistema de información o en la organización.
De nuevo se produce un absoluto paralelismo hacia sistemas documentales con vías de revisión y aprobación.

Para **Nivel Medio** y (por extensión acumulativa) para **Nivel Alto** se exige que el documento recoja:

- ✓ El nombramiento de un **Responsable de Seguridad (*)**. El Reglamento especifica expresamente que en ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero.
  (*) "Persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables", según la propia definición del Reglamento de Seguridad.

- ✓ La realización de **Auditorías al menos cada dos años**.

  - El **objeto** de dichas auditorías serán los sistemas de información e instalaciones de tratamiento de datos, para verificar el cumplimiento del Reglamento y de los procedimientos e instrucciones vigentes en materia de seguridad de datos. Es obvio, como en cualquier sistema normalizado, que si el documento de seguridad cumple con el Reglamento y las instrucciones vigentes, la auditoría se centrará sobre el cumplimiento de este último.
  - Dicha auditoría podrá ser **interna o externa**. Realizada por tanto por personal de la propia organización - para el que parece lógico exigir cierto grado de independencia -, o por empresas o profesionales especializados en este tipo de servicio.
  - El **informe de auditoría** (auditoría documentada por tanto), deberá dictaminar sobre la adecuación de las medidas y controles, identificar deficiencias y proponer las medidas correctoras o complementarias necesarias. Incluyendo los datos, hechos y observaciones en que se basen los dictámenes y recomendaciones. Será **analizado** por el responsable de seguridad, que elevará las conclusiones al responsable del fichero para la adopción de **medidas correctoras** y quedará a **disposición de la Agencia de Protección de Datos** (Organismo inspector y sancionador en materia de cumplimiento de protección de datos de carácter personal).

- ✓ Las **medidas** que sea necesario adoptar cuando un **soporte vaya a ser desechado o reutilizado**. Que será objeto de un punto posterior.

Funciones y Obligaciones del Personal

En este punto el Reglamento establece una **clara vinculación entre la organización y la seguridad**, condicionando la existencia de esta última, al hecho de que se establezca, registre y transmita una estructura de **funciones y responsabilidades** al personal implicado en el tratamiento. Estas deberán:

- ✓ Quedar claramente **definidas y documentadas** en el Documento de Seguridad.

- ✓ Ser **transmitidas y conocidas** por el personal, así como las consecuencias que les acarrearía el caso de su incumplimiento.

Registro de Incidencias

Entendiendo por tal a "cualquier **anomalía que afecte o pudiera afectar a la seguridad de los datos**", las Incidencias:

- ✓ Deberán quedar registradas documentalmente en el llamado **Registro de incidencias**, detallando; tipo de incidencia, momento en que se produjo, personas implicadas (la que notifica y a la que se comunica) y efectos que se derivan de ella.

En este apartado queda especialmente latente el **espíritu de integridad interna** de los datos, es decir, el Reglamento no sólo articula medidas con el fin de asegurar que los datos de carácter personal lleguen a manos de terceros, si no que también se centra en que prevalezca la integridad y validez de dichos datos dentro de la organización que legalmente los utiliza.

Y dicho espíritu de integridad interna queda especialmente claro cuando se establece que para **Nivel Medio** y (por extensión acumulativa) para **Nivel Alto:**

- ✓ La **Recuperación de datos**, se entiende de soportes de copia de seguridad (respaldo y recuperación o backup), se considerará como una incidencia.

Identificación y Autenticación (*)

(*) "**Identificación**: Procedimiento de reconocimiento de la identidad de un usuario. / **Autenticación**: Procedimiento de comprobación de la identidad de un usuario", según la propia definición del Reglamento de Seguridad.

Al respecto de las medidas que se establecen para que los usuarios, del sistema de información afecto a Reglamento, se identifiquen y autentifiquen su personalidad, la norma se centra en el mecanismo más extendido; el correspondiente a nombre de usuario/contraseña. Para ello se establece que:

- ✓ El responsable del fichero debe asegurar la **existencia y actualización** de una **relación de usuarios autorizados y recursos a los que tienen acceso**. Identificando, por tanto el "quién" y el "a qué" documentalmente.

- ✓ Debe de establecer **procedimientos de identificación y autenticación**. Es decir debe definir el "cómo".

- ✓ Si el mecanismo de autenticación **se basa en contraseñas** (lo que responde a la práctica más habitual), debe existir un **procedimiento de asignación, distribución y almacenamiento** - en forma ininteligible - de estas que garantice su confidencialidad e integridad. Además, el documento de seguridad, debe establecer **cambios periódicos** de las mismas.

Para **Nivel Medio** y (por extensión acumulativa) para **Nivel Alto** se exige que:

- ✓ Cada usuario tenga un **acceso inequívoco y personalizado**, y se verifique que está autorizado. La implementación exacta de este requisito va a depender de la interpretación que se haga individualmente, pero en todo caso, invita a la articulación de procesos más sofisticados. Deja incluso entrever la vía de que un usuario deba identificarse y/o autentificarse a través de varios datos.

- ✓ Se **limite el número de intentos de acceso fallidos**. Es decir que se tomen medidas contra intentos reiterados, que podrían ser ejecutados por procedimientos automáticos, con el fin de encontrar la clave o contraseña de acceso.

Para **Nivel Alto** se exige además que, tras el proceso de identificación y autenticación se **abra la traza para gestionar un Registro de Accesos** que será objeto de desarrollo en el siguiente punto.

Control de Acceso

Tras haber reglamentado, en el apartado anterior, con especial detalle, los mecanismo de control para que sea "quién" debe de ser, el usuario que acceda a los datos, y el "cómo" dicho usuario autentifica su identidad; en este apartado lo que se pretende asegurar es que, dicho usuario no acceda más que a los recursos, "a los qué" le es preciso acceder.

- ✓ Que los usuarios **sólo puedan acceder a los recursos que les sean precisos**, para el desarrollo de su función.
- ✓ El Responsable del fichero debe establecer **mecanismos para accesos no deseados**.
- ✓ La **Relación de Usuarios** contendrá los accesos autorizados para cada uno de ellos.
- ✓ Sólo **personal autorizado** para ello podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos.

Para **Nivel Medio** y (por extensión acumulativa) para **Nivel Alto** se exige que:

- ✓ Deberá establecerse un **control de acceso físico a las instalaciones** donde se encuentren ubicados los datos objeto de protección, para impedir el acceso a las personas que no se autorice expresamente a través del Documento de Seguridad.

Para **Nivel Alto** se debe **gestionar un Registro de Accesos**(se entiende informatizado), que:

- ✓ **Recoja al menos los datos** de; qué usuario, en qué momento, y sobre qué fichero intentó un acceso, de qué tipo fue el acceso y si fue autorizado o no.
- ✓ Si fue autorizado que recoja **a qué registro** se accedió.
- ✓ Los **mecanismos para dicho registro estarán bajo el control del responsable de seguridad**, que no debe permitir en ningún caso su desactivación.
- ✓ Dicho registro **se guardará al menos durante dos años**.
- ✓ El responsable de seguridad le someterá a **revisiones periódicas** sobre las que elaborará **informes**, al menos **mensuales**.

En descarga de lo gravoso de este punto, con lo que supone para el Sistema Informático el mantenimiento del tradicionalmente conocido como *"printlog" o "diario de abordo",*

debemos considerar la gran cantidad de **herramientas y utilidades de auditoría** que integran hoy en día la mayoría de los sistemas operativos y sistemas de gestión de bases de datos.

Gestión de Soportes

Entendidos los soportes como los **medios físicos donde se almacenan los datos** (discos duros, extraíbles, cintas, listados…), deberán:

- ✓ **Identificar** el tipo de información que contienen.
- ✓ Ser **inventariables y almacenables** en lugares de acceso restringido.
- ✓ Estar sometidos a un sistema de **autorización de salida** de las instalaciones.

Para **Nivel Medio** y (por extensión acumulativa) para **Nivel Alto** se exige que:

- ✓ Se tomen medidas para que los **soportes reutilizados** o desechados sean irrecuperables.
- ✓ Se establezca un **registro de Entradas/Salidas** autorizadas.

Para **Nivel Alto**:

- ✓ Los soportes se **distribuirán cifrados**.

Copias de Respaldo y Recuperación

Los popularmente conocidos como backup o copias de segurirdad, deberán:

- ✓ Establecerse mediante procedimiento de **definición y aplicación verificada** (que funcione y que se haga)
- ✓ **Garantizar la reconstrucción** de los datos *"en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción"* **(*)**
  (*) En este sentido el Reglamento establece lo que entendemos como una exigencia de difícil cumplimiento. Cualquier solución técnica para la observancia estricta de este párrafo, acarreará excesivos costes, recursos y sobrecargas al sistema. Nuestro criterio es limitar esta capacidad a objetivos racionales.
- ✓ Periodicidad **al menos semanal**.

Para **Nivel Alto**:

- ✓ Debe **conservarse una copia en un lugar diferente** al de los soportes.

En todo este apartado vuelve a quedar especialmente claro el **espíritu de integridad interna** de los datos, buscando la integridad y validez de los datos sólo dentro de la organización.

Pruebas de Aplicaciones

Para **Nivel Medio** y (por extensión acumulativa) para **Nivel Alto** se exige que, a la hora de probar nuevos programas o nuevas versiones de estos:

✓ Los **ficheros de prueba no deben contener datos reales**.

Ficheros Temporales

Los ficheros temporales, que habitualmente utilizan las aplicaciones como una herramienta para cálculos intermedios, y que suelen contener parte de los datos de los ficheros permanentes (pudiendo darse el caso de que estos fueran datos personales), deben:

✓ Garantizar la **seguridad, y ser borrados** tras su uso.

Telecomunicaciones

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones deberán **garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.**

Para **Nivel Alto** **las comunicaciones**:

✓ Deben **ser cifradas**.

3. Sistema Documental Propuesto

A lo largo de todo este escrito, se viene reflexionando entre el **paralelismo** que puede y, a nuestro juicio, debe existir, entre la implantación de un **sistema documental para la implantación del Reglamento de Medidas de Seguridad**, y lo que es más conocido; un sistema documental normalizado para la gestión de la calidad. Basándonos en dicha reflexión, vamos a proponer un esquema de implantación del citado Sistema Documental.

3.1. Nivel Manual. Documento de Seguridad

Al igual que en los sistemas de gestión de calidad encontramos como tronco el llamado "Manual de Calidad", aquí nos encontraremos con el **Documento de Seguridad**.

El **cometido** de dicho documento es múltiple:

- Describir **ámbito de aplicación y responsabilidades**, con expresa aceptación por parte del responsable del fichero (Dirección de Organismo).
- **Justificar punto por punto el cumplimiento** integro de las obligaciones que impone el Reglamento de Medidas de Seguridad.
- **Integrar los otros niveles** de documentos, internos o externos, referenciando a cada uno en el punto concreto de aplicación conforme a Reglamento.

3.2. Nivel Documentación Externa Integrada

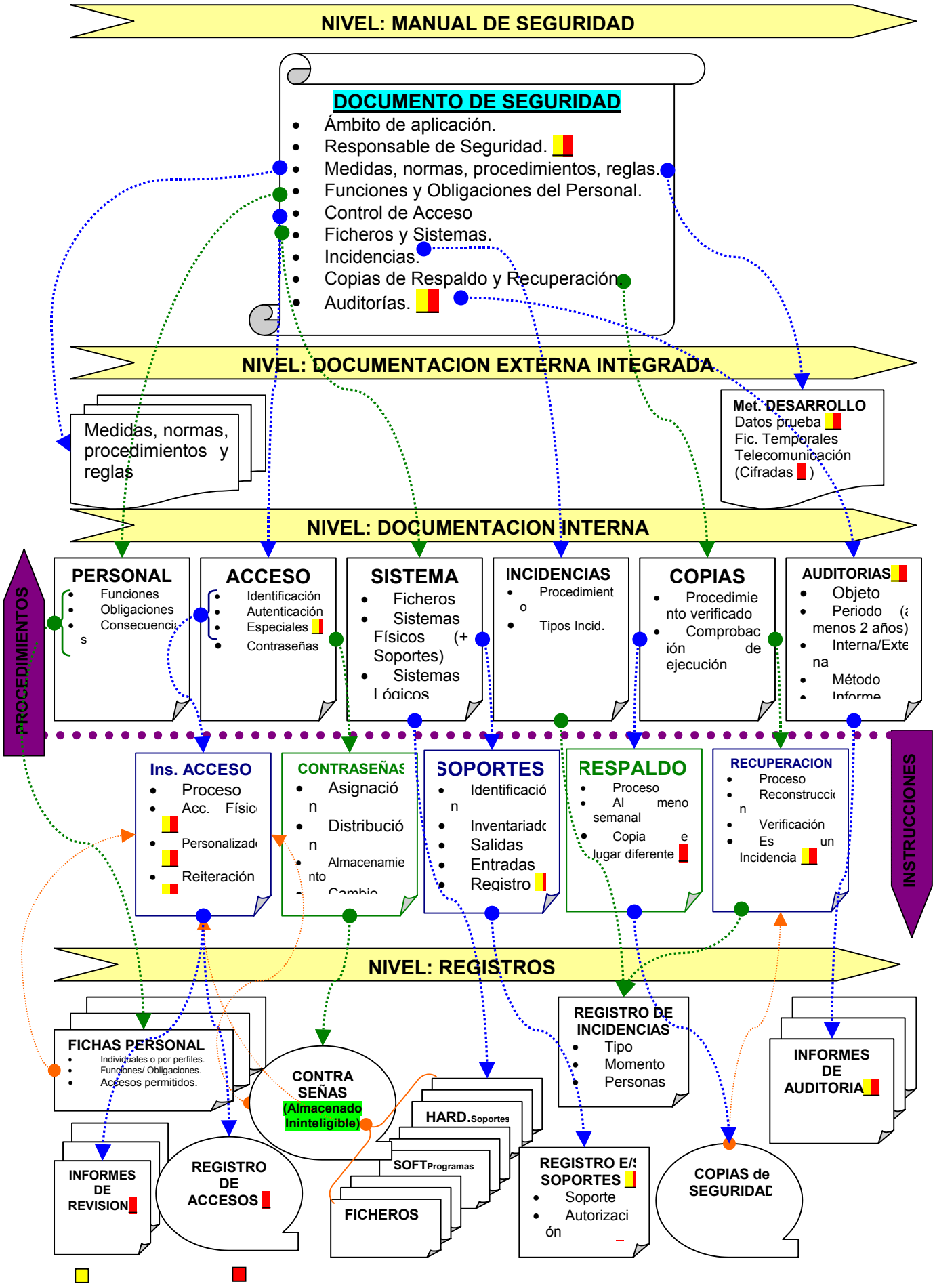
Aquí se integrará **otra documentación**, no propiamente generada dentro del Sistema Documental, pero que de alguna forma integra parte de los cometidos del mismo.

A nuestro juicio se deberá referenciar a:

- **Medidas, normas, procedimientos y reglas** internas (preexistentes o paralelas) o externas, que se adoptan a fin de reforzar los cumplimientos en materia de seguridad.
- **Metodologías de Desarrollo de aplicaciones**, en las que se deberán contemplar apartados concretos del Reglamento como son: los datos de prueba, los ficheros temporales y las telecomunicaciones.

3.3. Nivel Documentación Interna

Este nivel estará constituido por los **Procedimientos e Instrucciones de trabajo** que se desarrollan de manera expresa para el cumplimiento del Reglamento.


NIVEL: MANUAL DE SEGURIDAD
DOCUMENTO DE SEGURIDAD
Ámbito de aplicación.
Responsable de Seguridad.
Medidas, normas, procedimientos, reglas.
Funciones y Obligaciones del Personal.
Control de Acceso
Ficheros y Sistemas.
Incidencias.
Copias de Respaldo y Recuperación
Auditorías.
NIVEL: DOCUMENTACION EXTERNA INTEGRADA
Medidas, normas, procedimientos y reglas
Met. DESARROLLO
Datos prueba
Fic. Temporales
Telecomunicación (Cifradas)
NIVEL: DOCUMENTACION INTERNA
PROCEDIMIENTOS
PERSONAL
Funciones
Obligaciones
Consecuencias
ACCESO
Identificación
Autenticación
Especiales
Contraseñas
SISTEMA
Ficheros
Sistemas Físicos (+ Soportes)
Sistemas Lógicos
INCIDENCIAS
Procedimiento
Tipos Incid.
COPIAS
Procedimiento verificado
Comprobación de ejecución
AUDITORIAS
Objeto
Periodo (a menos 2 años)
Interna/Externa
Método
Informe
INSTRUCCIONES
Ins. ACCESO
Proceso
Acc. Físic
Personalizad
Reiteración
CONTRASEÑAS
Asignación
Distribución
Almacenamiento
Cambio
SOPORTES
Identificación
Inventariado
Salidas
Entradas
Registro
RESPALDO
Proceso
Al menos semanal
Copia e lugar diferente
RECUPERACION
Proceso
Reconstrucción
Verificación
Es un Incidencia
NIVEL: REGISTROS
FICHAS PERSONAL
Individuales o por perfiles.
Funciones/ Obligaciones.
Accesos permitidos.
CONTRA SEÑAS (Almacenado Ininteligible)
REGISTRO DE INCIDENCIAS
Tipo
Momento
Personas
INFORMES DE AUDITORIA
INFORMES DE REVISION
REGISTRO DE ACCESOS
HARD.Soportes
SOFTProgramas
FICHEROS
REGISTRO E/S SOPORTES
Soporte
Autorización
COPIAS de SEGURIDAD

En cuanto a los **Procedimientos** creemos que deberán aparecer al menos:

- **Personal.** Relativo a sus funciones y obligaciones.
- **Acceso.** Relativo a Identificación y Autenticación, Accesos especiales (con posible registro de accesos), y Contraseñas.
- **Sistema.** Detalle de Ficheros protegidos, Sistemas Físicos (incluidos los soportes), y Sistemas Lógicos incluyendo en ellos los programas y sus operativas de acceso.
- **Incidencias.** Procedimiento de actuación y clasificaciones de estas.
- **Copias.** Procedimiento de copias de Respaldo y Recuperación.
- **Auditorías.** (Sólo niveles medio y alto). Procedimiento de auditorías.

En cuanto a las **Instrucciones de Trabajo,** como ampliación o mejor detalle de los Procedimientos, creemos que podrían aparecer:

- **Instrucción de Acceso.** Proceso detallado, y personalizado, de acceso de los usuarios a las aplicaciones y los datos. Posible Registro de Acceso.
- **Contraseñas.** Detalle de gestión de contraseñas.
- **Soportes.** Gestión de soportes y posible control de Entrada y Salida.
- **Respaldo.** Realización de copias de seguridad y almacenamiento de estas.
- **Recuperación.** Reconstrucción de los datos a partir de las copias de seguridad

3.4. Nivel Registros

Soportes **informatizados o informatizables** donde se **recogen los datos a los que obliga el Reglamento**.

Podemos extraer del reglamento que estos serán al menos:

- **Fichas y Relación de Personal.** Pudiendo ser individuales o por perfiles de usuarios, y recogiendo sus cometidos, funciones y permisos particulares.
- **Registro de accesos.** (Sólo para nivel alto). Registro detallado de accesos al sistema y a los datos.
- **Informes de Revisión del Registro de accesos.** (Sólo para nivel alto). Informes de revisión de dichos fichero, al menos mensuales.
- **Contraseñas.** Fichero de contraseñas almacenado de forma ininteligible.
- **Ficheros.** Relación y descripción de ficheros objeto del régimen de seguridad.
- **Software.** Relación y descripción de aplicaciones objeto del régimen de seguridad.
- **Hardware.** Relación y descripción de los sistemas, incluidos los soportes, objeto del régimen de seguridad.
- **Registro de Entrada y Salida de Soportes.** (Sólo para nivel medio y alto). Registro de Entradas y Salidas, con Autorizaciones y Cifrados (Nivel alto).
- **Registro de Incidencias.** Relación detallada de incidencias registradas.
- **Copias de Seguridad.** Soportes y ficheros relativos a las copias de respaldo y recuperación.
- **Informes de Auditoría.** (Sólo para nivel medio y alto). Informes fruto de la realización de las auditorías, al menos bianuales.

4. Conclusiones

- Al aprobar este Real Decreto el 11 de Junio de 1.999, se establecieron plazos máximos de aplicación, el más amplio de ellos es de 3 años. Por eso, desde el **11 de Junio de 2.002,** es de **obligado** cumplimiento para organizaciones con ficheros de Datos de Carácter Personal.

- En un área especialmente desabastecida de normas y reglas, como es inherente a la continua evolución de los sistemas informáticos, el Reglamento de Seguridad, como norma abierta y adaptable, que vela por la seguridad interna y externa de los datos que maneja cualquier organización, nos parece una herramienta útil. Y su aplicación no debería limitarse en exclusiva a Datos de Carácter Personal, sino al Sistema de Información en su conjunto, como un **primer paso en la consecución de una Metodología de Seguridad Informática**.