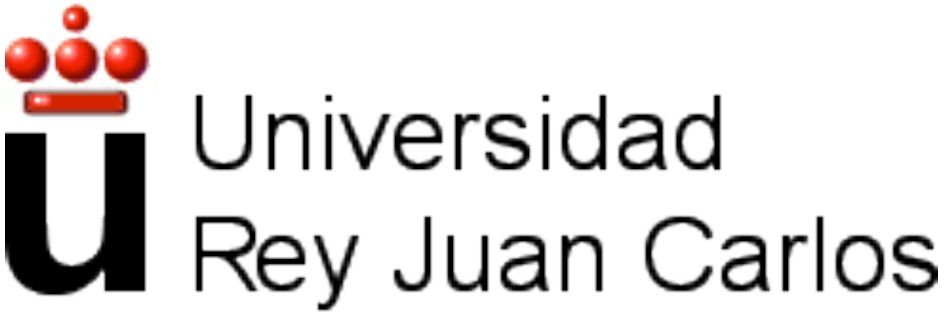


**ESCUELA SUPERIOR DE INGENIERÍA INFORMÁTICA**

**INGENIERÍA TÉCNICA EN INFORMÁTICA DE GESTIÓN**

**Curso Académico 2009/2010**

**PROYECTO DE FIN DE CARRERA**

# DOCUMENTO DE SEGURIDAD:

## REGLAMENTO DE MEDIDAS DE SEGURIDAD PARA EL TRATAMIENTO DE FICHEROS QUE CONTENGAN DATOS DE CARÁCTER PERSONAL

**AUTOR: Sergio Dombriz Espada**
**TUTOR: Javier Martínez Moguerza**

# Índice

# 1 | Resumen

Las empresas, tanto públicas como privadas, dependen hoy más que nunca de las Tecnologías de Información y Comunicación para su operatividad diaria. Por eso es muy importante hacer una gestión adecuada de los recursos de los que disponen.

El proceso de auditoría de Tecnologías de Información y Comunicación se puede definir como el examen objetivo, crítico, sistemático y selectivo de las políticas, normas, prácticas, procedimientos y procesos para dictaminar, respecto a la economía, eficiencia y eficacia de la utilización de los recursos de tecnologías de la información; la oportunidad, confiabilidad, validez de la información y la efectividad del sistema de control interno asociado a las tecnologías de la información y a la entidad en general, para lograr el desarrollo estratégico del negocio.

El proceso de auditoría de cumplimiento de La Ley Orgánica de Protección de Datos de Carácter Personal 15/1999, de 13 de Diciembre se estructura en:

- ✓ Análisis y evaluación de la entidad cliente
- ✓ Gestión de la Inscripción de Ficheros en la Agencia Española de Protección de Datos de Carácter Personal (en adelante AEPD).
- ✓ **Elaboración del Documento de Seguridad y procedimientos necesarios.**
- ✓ **Regularización de los Movimientos de Datos con Terceros.**
- ✓ **Implantación de Soluciones Técnicas Requeridas.**
- ✓ **Implantación de las Medidas de Seguridad Requeridas.**
- ✓ Plan de Formación específico.
- ✓ Auditoria Bienal.

En el este proyecto de fin de carrera está estructurado en dos puntos:

- ✓ Medidas de seguridad recomendadas por la Agencia Española de Protección de Datos para el cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal 15/1999, de 13 de Diciembre.
- ✓ Anexo: Recoge las políticas y procedimientos a modo de ejemplo que pueden utilizarse para cumplir con la Ley y con el Reglamento de la Ley Orgánica de Protección de Datos de Carácter Personal.

Los ejemplos propuestos nacen de la experiencia recibida en las auditorías de LOPD en la beca del Departamento de Seguridad Informática de una consultora de reconocido prestigio.

La Ley Orgánica de Protección de Datos de Carácter Personal 15/1999, de 13 de diciembre, nació con el objetivo de **garantizar la protección de nuestra intimidad frente a los abusos que se puedan producir en el tratamiento de los datos personales que estén en algún fichero digital o en papel**.

# 2 | Introducción

Este Proyecto de Fin de Carrera tiene como finalidad la elaboración de un documento que recoja las medidas de seguridad necesarias para el correcto cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal (en adelante LOPD).

Las medidas de seguridad propuestas son orientativas y sirven como ejemplo, pudiendo en cualquier caso, proponer otras que se adapten mejor a la Entidad a la que nos estemos refiriendo.

Los ficheros escogidos en los ejemplos han sido elegidos al azar de la web de la Agencia Española de Protección de Datos de Carácter Personal (en adelante AEPD), para exponer de forma clara la forma en la que tienen que ser declarados ante la AEPD.

Cabe resaltar que la AEPD sólo actúa en caso de denuncia.

La Ley Orgánica de Protección de Datos de Carácter Personal 15/1999, de 13 de diciembre, nació con el objetivo de **garantizar la protección de nuestra intimidad frente a los abusos que se puedan producir en el tratamiento de los datos personales que estén en algún fichero** (sea de titularidad pública o privada).

Esta Ley viene a ampliar el apartado 4º del artículo 18 de la Constitución Española: < y constituye la norma principal sobre la materia en nuestro país>.

La LOPD permanece vigente desde el 15 de enero de 2000, momento en el que quedó derogada la anterior LORTAD (Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de carácter personal) de 1992, que surgió a raíz de una recomendación de la Unión Europea.

La diferencia fundamental entre ambas es que el ámbito de la LORTAD únicamente abarcaba los ficheros que contuviesen datos de carácter personal que se almacenasen en soporte electrónico. La LOPD amplia este ámbito a cualquier tipo de soporte, es decir, los ficheros en formato papel también están sujetos a esta reglamentación.

## 2.1 Objeto de este documento

La actual Ley Orgánica 15/1999, de 13 de diciembre de Protección de datos de carácter personal adaptó nuestro ordenamiento a lo dispuesto por la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, derogando a su vez la hasta entonces vigente Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de datos de carácter personal.

El artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (LOPD), establece en su punto 1 que "el responsable del fichero, y, en su caso, el encargado del tratamiento, deberán 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".

El Reglamento de desarrollo de la LOPD, aprobado por el Real Decreto 1720/2007, de 21 de diciembre, fue publicado en el BOE número 17, de 19 de enero de 2008. El Título VIII de este reglamento desarrolla las medidas de seguridad en el tratamiento de datos de carácter personal y tiene por objeto establecer las medidas de índole técnica y organizativa necesarias para garantizar la seguridad que deben reunir los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos de carácter personal.

**Entre estas medidas, se encuentra la elaboración e implantación de la normativa de seguridad mediante un documento de seguridad de obligado cumplimiento para el personal con acceso a los datos de carácter personal.**

Este Documento deberá mantenerse permanente actualizado. Cualquier modificación relevante en los sistemas de información automatizados o no, en la organización de los mismos, o en las disposiciones vigentes en materia de seguridad de los datos de carácter personal conllevará la revisión de la normativa incluida y, si procede, su modificación total o parcial.

# 3 | Ámbito de aplicación

El documento será de aplicación a todos los ficheros que contienen datos de carácter personal bajo la responsabilidad del Responsable del Fichero *<Nombre del responsable>*, incluyendo los sistemas de información, soportes y equipos empleados para su tratamiento, las personas que intervienen en el tratamiento y los locales en los que se ubican o donde tienen lugar en el tratamiento.

Las Medidas de seguridad que afectan a los datos se clasifican en tres niveles acumulativos (básico, medio y alto), atendiendo a la naturaleza de la información tratada, en relación con la menor o mayor necesidad de garantizar la confidencialidad y la integridad de la información.

**NIVEL BÁSICO:** Se aplicará a cualquier otro fichero que contenga datos de carácter personal. También aquellos 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 o condición de discapacidad o la simple declaración de invalidez, con motivo del cumplimiento de deberes públicos.

**NIVEL MEDIO:** Se aplicará a los ficheros o tratamiento de datos: (En adelante #NIVEL MEDIO#)

- Relativos a la comisión de infracciones administrativas o penales;
- que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia patrimonial y crédito);
- de Administraciones Tributarias, y que se relacionen con el ejercicio de sus potestades tributarias;
- de entidades financieras para las finalidades relacionadas con la prestación de servicios financieros;
- de Entidades Gestoras y Servicios Comunes de Seguridad Social, que se relacionen con el ejercicio de sus competencias;

- de mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social;
- que ofrezcan una definición de la personalidad y permitan evaluar determinados aspectos de la misma o del comportamiento de las personas; y
- de los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización.

**NIVEL ALTO:** Se aplicarán a los ficheros o tratamientos de datos: (En adelante #NIVEL ALTO#)

- De ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, respecto de los que no se prevea la posibilidad de adoptar el nivel básico.
- Recabados con fines policiales sin consentimiento de las personas afectadas; y derivados de actos de violencia de género.

El Responsable de Seguridad se compromete a implantar y actualizar esta Normativa de Seguridad de obligado cumplimiento. Todas las personas que tengan acceso a los datos de los Ficheros, bien a través del sistema informático habilitado para acceder a los mismos, o bien a través de cualquier otro medio de acceso a los ficheros, se encuentran obligadas por ley a cumplir lo establecido en este documento, y sujetas a las consecuencias que pudieran incurrir en caso de incumplimiento.

El contenido del presente Documento de Seguridad se adecua a las disposiciones legales vigentes en esta materia, quedando bajo la custodia del Jefe de Seguridad de la Información de la Entidad (en adelante JSIE). Los distintos responsables dispondrán de la información de este documento que sea requerida para el desempeño de sus funciones.

Las medidas de seguridad contenidas en este Documento de Seguridad, afectan a toda la estructura organizativa, y deben ser cumplidas y observadas por todo el personal con acceso a los datos de carácter personal de la Entidad.

El presente Documento de Seguridad afecta a todos los ficheros declarados ante la Agencia Española de Protección de Datos (en adelante AEDP) con el alcance que se detalla en el mismo, cuya relación completa queda bajo la custodia del JSIE.

# 4 | Medidas y procedimientos encaminados a garantizar los niveles de seguridad

## 4.1 Identificación y autenticación del personal

**Según estipula el Reglamento en el art. 93 (Identificación y Autenticación):**

1. "El Responsable del Fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.
2. El Responsable del Fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que esté autorizado.
3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.
4. El Documento de Seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenaran de manera ininteligible."

**Según estipula el Reglamento en el art. 98 (Identificación y Autenticación):**

"El Responsable de Fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información."

Para todos los ficheros con tratamiento automatizado, los usuarios se identificaran en los sistemas de información mediante el sistema de credenciales usuario/contraseña. La asignación, distribución y almacenamiento de dichas contraseñas se realizan según los procedimientos desarrollados a tal efecto, y será responsabilidad de los administradores de los sistemas.

*<Las contraseñas deberán cumplir con la política de contraseñas definida por la Entidad. >*

Dicha política incluye con carácter general las siguientes obligaciones:

- Se usarán usuarios personalizados, no de grupo.
- Se cambiarán las contraseñas con periodicidad inferior a un año.
- Se almacenarán de forma ininteligible.
- Se limitará el máximo de intentos consecutivos de acceso no autorizado.

- Longitud mínima combinando letras, números y caracteres especiales:
    - Contener al menos siete caracteres.
    - Tener al menos un símbolo entre las posiciones segunda y sexta
    - Ser significativamente diferente de otras contraseñas anteriores
    - No contener el nombre de usuario ni una palabra o nombre común.

## 4.2 Control de acceso

El control de acceso se basará en el principio de mínimos privilegios, por lo que el personal sólo accederá a aquellos datos y recursos que precisa para el desarrollo de sus funciones. El Responsable del Fichero, a través de las personas a las que en cada caso se delegue esta función:

**Según estipula el Reglamento en el art. 91 (Encargado de Tratamiento):**

1. "Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.
2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.
5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio."

Dicha política incluye de con carácter general las siguientes obligaciones:

- Guardar cada acceso de forma individual.
- Identificar al usuario.
- Fecha y hora.
- Fichero al que se ha accedido.
- Tipo de acceso.
- Autorización o denegación de acceso.

- Si se autoriza, identificar el registro de acceso.

Los mecanismos deben estar protegidos contra su desactivación.

Los datos se han de conservar como máximo dos años.

La lista de acceso se debe actualizar periódicamente.

### 4.2.1 Control de acceso a los ficheros

- Al iniciar el proceso de arranque de cada ordenador conectado a la Entidad, se solicitará el identificador de usuario y la clave de acceso.
- Aquellos dispositivos que no disponen de conectividad en red, se identifican de manera local.
- Todos los usuarios tienen asignados los privilegios necesarios y suficientes para el correcto desarrollo de sus funciones.
- Los privilegios de acceso a los Ficheros están controlados por las aplicaciones y bases de datos donde están almacenados, donde se adjudican los permisos necesarios a cada usuario.
- Los procesos de alta y baja de usuarios incluyen de oficio la asignación y revocación de estos privilegios.
- Todos los sistemas que controlan la asignación de privilegios residen en determinadas ubicaciones físicas (CPD) a las que no se permite el acceso no autorizado (puerta cerrada con combinación conocida sólo por los administradores de sistemas autorizados).
- <Lista de personas autorizadas>

En el caso de tratamientos no automatizados (documentación y expedientes en papel) son de aplicación las siguientes medidas para limitar el acceso exclusivamente al personal autorizado.

- Se mantiene manualmente la lista de personas autorizadas para cada tratamiento, o ésta coincide con una división funcional de la organización, de forma que es posible identificar en todo momento las personas autorizadas. Se pueden identificar: (por ejemplo)
    - Área de RRHH

      Está en una zona dedicada y dispone de puerta con llave, que sólo permanece abierta en presencia del personal del área.

- Área de Administración

  Los documentos con datos de carácter personal se almacenan en armarios protegidos con llave.

- Área Financiera

  Contiene documentos de carácter personal y se almacenan en armarios protegidos con llave. Como medida de contingencia, se guarda una copia de cada llave en un lugar protegido.

- Los documentos utilizados por las dos áreas mencionadas sólo se sacan de la zona protegida el tiempo necesario para su tratamiento, no permaneciendo nunca fuera sin la supervisión de una persona autorizada. Sólo el personal autorizado tiene acceso a las llaves de los armarios o de las dependencias, en su caso.

### 4.2.2 Control de acceso a las instalaciones

**Según estipula el Reglamento en el art. 99 (Control de acceso físico):**

"Exclusivamente el personal autorizado en el Documento de Seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información."

El objetivo del control de acceso físico es controlar el acceso de personal y los recursos necesarios para la operación diaria, impedir el acceso accidental de terceros a datos de carácter personal en las instalaciones, así como prevenir riesgos de accidentes y daños a los sistemas de información e instalaciones.

**DOCUMENTO DE SEGURIDAD**

Los entornos a proteger serán el CPD, los despachos con ordenadores personales a nivel departamental y los armarios de las áreas de RRHH y Administración del Personal.

- Sólo el personal autorizado tendrá acceso permitido a los locales, instalaciones o despachos donde se encuentren los sistemas de información con datos de carácter personal.

- La seguridad de los centros de tratamiento de datos personales será responsabilidad del Responsable del Fichero, que será soportado por el Responsable de Seguridad y Directores de Áreas.

- Los equipos, soportes y documentos que contengan datos personales, no serán sacados de las dependencias sin la autorización expresa del Responsable de Fichero.

- Los accesos no autorizados a las dependencias quedarán reflejados en el Registro de Incidencias.

- Todos los empleados de los departamentos y delegaciones que traten datos personales, son responsables de aplicar adecuadamente los procedimientos de seguridad y de informar cualquier sospecha de violación de las medidas de seguridad.

- El personal del centro tiene la responsabilidad compartida de asegurar que se guarden adecuadamente los activos de la Entidad que contienen datos personales (Equipos, accesorios, documentación, listas impresas, documentos bancarios, documentos oficiales, etc).

- Cuando los usuarios vayan a dejar su puesto de trabajo desatendido deberán guardar todos los soportes que contengan datos de carácter personal (disquetes, CD, DVD, papeles, etc) de forma que se eviten accesos no autorizados a los mismos.

- El procedimiento establecido para el control de acceso físico al CPD y a las salas de comunicaciones consiste en rellenar un formulario de solicitud de acceso en el control de vigilancia de la entrada y, si se autoriza, se facilita temporalmente el acceso mediante una tarjeta.

El Responsable de Seguridad revisará con periodicidad la información del control registrada y elaborará un informe detallado.

## 4.3 Gestión de soportes

Los soportes que contengan datos de carácter personal deben ser etiquetados para permitir su identificación, inventariados y almacenados en <indicar el lugar de acceso restringido donde se almacenarán>, lugar de acceso restringido al que solo tendrán acceso las personas con autorización que se relacionan a continuación:

- <Especificar el personal autorizado a acceder al lugar donde se almacenan los soportes informáticos que contengan datos de carácter personal, el procedimiento establecido para habilitar o retirar el permiso de acceso y los controles de acceso existentes. Tener en cuenta el procedimiento a seguir para casos en que personal no autorizado tenga que tener acceso a los locales por razones de urgencia o fuerza mayor>.

Los soportes informáticos se almacenarán de acuerdo a las siguientes normas:

- Cada soporte debe ir correctamente etiquetado con un nombre identificativo claro y conciso.
- El etiquetado debe incluir la fecha de almacenamiento siguiendo el formato DD/MM/AAAA

La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en donde esté ubicado el sistema de información, únicamente puede ser

autorizada por el responsable del fichero o aquel en que se hubiera delegado de acuerdo al siguiente procedimiento.

Esta sección describe los procesos, mecanismos y soluciones técnicas implementadas para la gestión segura de cualquier tipo de soporte u otro medio removible y transportable que contenga datos de carácter personal propiedad de la Entidad.

Dentro del ámbito del presente Documento de Seguridad, se entiende por soporte u otro medio removible y transportable a:

- Discos duros, CD's, disquetes, memoras externas, etc.
- Ordenadores portátiles, agendas electrónicas, etc.
- Copias de Seguridad.
- Etc.

### 4.3.1 Gestión de copias de respaldo y recuperación

Esta sección describe los procesos, mecanismos y soluciones técnicas que permiten realizar copias de los datos en un soporte que posibilite su recuperación.

Asimismo se identifica los sistemas, bases de datos y aplicaciones sometidos a la política corporativa de realización de copias de seguridad, indicando la periodicidad con la que se realizan y si existe algún otro método de replica para los datos tratados.

**Según estipula el Reglamento en el art. 94 (Copias de respaldo y recuperación):**

**1.** "Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho periodo no se hubiera producido ninguna actualización de los datos.

**2.** Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la perdida o destrucción."

Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el Documento de Seguridad.

**3.** "El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos."

**Según estipula el Reglamento en el art. 102 (copias de respaldo y recuperación):**

"Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los

equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación."

En este sentido, la Entidad ha firmado compromisos de confidencialidad con las Entidades que tratan sus datos, en los que se garantiza el cumplimiento de la legislación vigente en cuanto al tratamiento de datos de carácter personal.

Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

La política de copia podría ser:

- Copia incremental: diaria.
- Copia completa: semanal.

### 4.3.2 Traslado de Documentación y autorización para la salida de soportes

**Según estipula el Reglamento en el art. 92 (gestión de soportes y documentos):**

2. "La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o ajenos a un correo electrónico, fuera de los locales bajo el control del responsable de fichero o tratamiento, deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el Documento de Seguridad.

1. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte."

En el traslado de documentos físicos fuera de la Entidad, se aplicarán adicionalmente las siguientes medidas de seguridad:

- Se utilizarán sistemas de transportes internos, o de usarse un servicio externo, éste deberá haber firmado un compromiso de confidencialidad.

**DOCUMENTO DE SEGURIDAD**

- La documentación se entregará en sobre cerrado. No podrá estar desatendida, obligándose el transportista a custodiarla mientras no esté bajo llave, y a impedir acceso a la misma a cualquier persona que no esté cubierta por el compromiso de confidencialidad.
- El remitente debe especificar el destinatario de la documentación al transportista, y éste sólo podrá entregarla al destinatario designado.

- El destinatario confirmará al remitente la recepción de la documentación.

### 4.3.3 Proceso de inventariado de soportes

**Según estipula el Reglamento en el art. 92 (Gestión de soportes y documentos):**

1. "Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y sólo deberán ser accesibles por el personal autorizado para ello en el Documento de Seguridad.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el Documento de Seguridad.

5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas."

**Según estipula el Reglamento en el art. 101 (Gestión y distribución de soportes):**

1. "La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas."

### 4.3.4 Registro de entradas y salidas de soportes

**Según estipula el Reglamento en el art. 97 (Gestión de soportes y documentos):**

1. "Deberá establecerse un sistema de registro de entrada de soportes que permita conocer el tipo de documento o soporte, la fecha y la hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

2. Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y la hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada."

## 4.4 Acceso a través de redes de Telecomunicaciones

**Según estipula el Reglamento en el art. 85 y art. 104 (Acceso a datos a través de redes de comunicaciones):**

"Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no publicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el art.80 (Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto).

Cuando conforme al art. 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes publicas o redes inalámbricas de comunicaciones electrónicas se realizara cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea ininteligible ni manipulada por terceros."

Por ejemplo, los empleados que por necesidades de su trabajo necesitan acceder a los sistemas de información a través de las redes de comunicaciones, utilizaran exclusivamente el servicio autorizado de VPN, sobre el que se aplican las siguientes medidas de seguridad:

- El servicio VPN se concede sólo a los usuarios que lo necesitan, con la autorización de su Director de Área.
- A los usuarios autorizados del servicio se les genera un certificado digital personal e intransferible a efectos de autenticación. Dicho certificado se revoca cuando el usuario pierde el privilegio de acceso por cualquier razón, cuando se detecta un compromiso de seguridad asociado al mismo, y en cualquier caso, como parte del proceso de baja de un empleado.
- La conexión VPN está autenticada y cifrada, y una vez establecida, se aplican las mismas medidas de seguridad y restricciones que si el empleado estuviera trabajando en la red local.

## 4.5 Régimen de trabajo fuera de los locales de ubicación de los ficheros

Esta sección describe las medidas adoptadas para el tratamiento seguro de los datos de carácter personal desde fuera de los locales de la ubicación del fichero, incluyendo las restricciones de trabajo estipuladas para limitar el tratamiento fuera de los locales de ubicación del fichero.

Dentro del ámbito del presente Documento de Seguridad, se entiende por tratamiento fuera de los locales de ubicación del fichero a cualquier tratamiento realizado desde fuera de las instalaciones en las que se ubica el fichero. Este tratamiento podrá ser realizado tanto por empleados de la Entidad como por colaboradores externos, independientemente del soporte y canal en el que se facilita la información.

**Según estipula el Reglamento en el art. 86 (Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento):**

1. "Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

2. La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas."

## 4.6 Relaciones con terceros

En estos tratamientos, la Entidad puede actuar como Responsable del Fichero o como Encargado del Tratamiento, según si existe un tercero que está llevando determinados tratamientos de la Entidad o por el contrario es ésta quien está realizando tratamientos a terceros, respectivamente.

**Según estipula el Reglamento en el art. 82 (Encargado de Tratamiento):**

"1. Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacerse constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

2. Si el servicio fuera prestado por el encargado del tratamiento en sus propio locales ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad en los términos exigidos por el art. 88 de este reglamento o completar el que ya hubiera

elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

3. En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este reglamento."

**Según estipula el Reglamento en su art. 83 (Prestaciones de servicios sin acceso a datos personales):**

"El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio."

**Según estipula el Reglamento en su art. 88 (El Documento de Seguridad):**

"5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargo, así como de la identificación del responsable y del periodo de vigencia del encargo.

6. En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros de tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del art. 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados.

En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento. "

*<Establecer responsable/s de controlar y custodiar todos los documentos contractuales y/o de compromisos que regulan las relaciones con terceros>*

2. Tratamientos realizados por terceros, distinguiendo los siguientes matices:
    - Si existe acceso a datos personales en las instalaciones de la Entidad.
    - Si existe acceso a datos personales mediante acceso remoto a los sistemas de la Entidad.

- Si existe acceso a datos personales en las instalaciones del Encargado del Tratamiento.
- Si no existe acceso a datos personales

3. Encargos del tratamiento realizados por la Entidad

# 5 | Evaluaciones periódicas de cumplimiento

Esta sección describe las medidas establecidas para la realización de evaluaciones periódicas que se realizan para determinar el grado de implantación de las medidas de seguridad existentes en relación a la protección de datos de carácter personal a lo largo del ciclo de vida de los mismos.

El proceso de evaluaciones periódicas de cumplimiento se realiza sobre las siguientes áreas de revisión de la LOPD y RLOPD:

- **Documento de Seguridad**, en la cual se evalúan los aspectos relacionados con el grado de completitud y actualización del Documento de Seguridad.
- **Disposiciones generales**, en la cual se evalúan todos los aspectos relativos con el cumplimiento de la legalidad dentro de la Entidad con los interesados.
- **Cada una de las áreas del Reglamento**, en las cuales se evalúa el nivel de cumplimiento en los aspectos relacionados con la seguridad física, copias de respaldo y recuperación, gestión de incidencias, gestión de soportes, gestión de usuarios, pruebas con datos reales, etc.

Teniendo en cuenta que según la normativa de Protección de Datos vigente en España (art. 110) las empresas están obligadas a realizar auditorias cada dos años, siendo opcional que la auditoria sea de carácter interno o externo.

A este respecto, se adjunta un documento con los acuerdos de la Comisión directiva relativo a la manera en la que se realizan estas auditorias

Otros controles que por lo general son de carácter genérico que permiten verificar el cumplimiento de los procedimientos e instrucciones vigentes en materia de Seguridad se pueden agrupar en:

- **Informes de las Auditorias:** Se refiere a las distintas auditorias que se realizan anualmente en la entidad (- si se hicieran -). Dentro de este apartado, también se debe considerar todo lo que está relacionado, en materia de seguridad de la información.
- **Análisis de Incidencias:** Sobre los distintos tipos de incidencias que relacionadas con la seguridad se producen, y en los tratamientos externos de información.
- **Control de Inventarios:** Relativo a los cierres que de forma periódica se realizan sobre los distintos inventarios existentes.

- **Revisiones Internas del Área de Seguridad:** Referente a las revisiones y controles periódicos y puntuales que el Área de Seguridad ha establecido internamente.
- **Revisiones Externas de Seguridad:** Trata las revisiones y controles establecidos de manera periódica, así como también de las que pueden ser de carácter puntual, sobre aspectos de seguridad de la información.

El Responsable del Fichero junto con el Responsable de Seguridad, analizaran con periodicidad las incidencias registradas en el registro correspondiente, para independientemente de las medidas particulares que se hayan adoptado en el momento que se produjeron, poner las medidas correctoras que limiten esas incidencias en el futuro.

# 6 | Procedimiento General de Información del personal

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal a los sistemas de información están descritas en el capítulo siguiente.

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias del incumplimiento de las mismas, serán informadas de acuerdo al procedimiento establecido.

Adicionalmente, existe un curso online interactivo obligatorio para todos los empleados, de formación básica sobre protección de datos.

Este Documento de Seguridad y las políticas que referencia están accesibles para todo el personal <*lugar donde se puede acceder*> y se emite una notificación cada vez que hay una modificación de su contenido.

# 7 | Funciones y Obligaciones del personal

## 7.1 Funciones y Obligaciones del Personal

Las funciones que los empleados de la entidad puedan desarrollar en relación con los ficheros que contengan datos de carácter personal, serán aquellas para las que hayan sido autorizados expresamente, independientemente de las limitaciones automáticas que se establecen para controlar los accesos.

Estarán obligados a respetar las normas, que tanto con carácter general como de carácter específico se han establecido para ficheros concretos.

A efectos de garantizar el cumplimiento de estas obligaciones, existe una política general contenida en los planes de formación/divulgación, circulares de carácter general, firma de documentos de compromiso de confidencialidad, además de otras normas específicas que se extienden a los usuarios de las aplicaciones y sistemas de la información.

Con independencia de las funciones y responsabilidades específicas asignadas a los usuarios de los respectivos ficheros, a cualquier empleado de la entidad se les exige con carácter general:

- Confidencialidad respecto de la información y documentación que reciben o usan por motivo de sus funciones.
- No incorporar a la empresa información o datos obtenidos sin la autorización de la Entidad.
- En especial, no ceder datos de carácter personal ni usarlos con finalidad distinta a la del fichero al que se hallen incorporados.
- Utilizar las contraseñas según las instrucciones recibidas al efecto. Manteniendo la debida reserva de las mismas para garantizar su uso exclusivo por parte de sus titulares.
- Comunicar al Área de Seguridad (JSIE) cualquier incidencia respecto a la seguridad de los datos de carácter personal o de las medidas de seguridad.

### 7.1.1 Personal con acceso privilegiado y personal técnico

El personal que administra el sistema de acceso a los Ficheros se puede a su vez clasificar en varias categorías, que no necesariamente deberán estar presentes en todos los casos, siendo en algunas ocasiones asumidas por una misma persona o personas. Por ejemplo, estas categorías son:

**Administradores**: (Red, Sistemas Operativos y Bases de Datos) Serán los responsables de los máximos privilegios y por tanto de máximo riesgo de que una actuación errónea

pueda afectar al sistema. Tendrán acceso al software del sistema, a las herramientas necesarias para su trabajo y a los ficheros o bases de datos necesarios para resolver los problemas que surjan.

**Operadores**: (Red, Sistemas Operativos, Bases de Datos y Aplicación) Sus actuaciones están limitadas a la operación de los equipos y redes utilizando las herramientas de gestión disponibles. No deben, en principio, tener acceso directo a los datos del Fichero, ya que su actuación no precisa de dicho acceso.

**Mantenimiento de los sistemas y aplicaciones**: Personal responsable de la resolución de incidencias que puedan surgir en el entorno Hardware/Software de los sistemas informáticos o de la propia aplicación de acceso al Fichero.

Cualquier otro que la organización establezca.

### 7.1.2 Personal con perfil de usuario

Los usuarios de Ficheros, sólo podrán acceder a aquellos datos para los que estén autorizados, es decir, a aquellos que sean necesarios para el desempeño de la función que realicen.

Por tanto, las obligaciones que a continuación se detallan, afectarán a cada uno de los usuarios de acuerdo con las funciones propias de su puesto de trabajo:

- Guardar el secreto de la información a la que tuviere acceso en el desempeño de su función, obligación que subsistirá aún después de haber abandonado la Compañía (art. 10 L.O. 15/99).
- Conocer la normativa interna en materia de seguridad, y especialmente lo referente a protección de datos de carácter personal. Dicha normativa puede consistir en: normas, procedimientos, reglas y estándares, así como posibles guías.
- Cumplir en todo momento, lo dispuesto en la normativa interna vigente.
- Conocer las consecuencias y responsabilidades en que pudiera incurrir en caso de incumplimiento de la normativa interna, con especial mención de las sanciones que se podrán imponer por tal causa.
- Respetar siempre los mecanismos y dispositivos de seguridad, evitando cualquier intento de acceso no autorizado o recursos no permitidos, y en su caso, informar de posibles debilidades en los controles, para no poner en peligro la disponibilidad de los datos, ni la confidencialidad o integridad delos mismos.

- No utilizar el correo electrónico u otros medios de comunicación de la Empresa, ya sea interna o con el exterior, para transmitir mensajes que contengan o lleven adjuntos datos de carácter personal que por sus características, volumen o destinatarios puedan poner en peligro la confidencialidad o la integridad de los mismos.

- Usar de forma adecuada, los mecanismos de identificación y autenticación ante los sistemas de información, ya sean contraseñas como sistema más avanzados (biométricos y otros), y en ambos casos, mediante acceso local o a través de redes de comunicaciones, cuando esté así previsto. En el caso de las contraseñas se habrá de cumplir lo específicamente previsto al efecto en la normativa interna, especialmente en cuanto a la asignación, sintaxis, distribución, custodia y almacenamiento de las mismas, así como en su cambio, con la periodicidad que así se determine.

- Dirigir a impresoras protegidas, los listados que contengan datos de carácter personal que requieran protección, y recogerlos con celeridad para evitar su difusión, copia o sustracción.

- No sacar equipos o soportes delas instalaciones sin la autorización necesaria, y en todo caso, con los controles que para cada supuesto, se hayan establecido.

- Proteger los datos personales de los que la Compañía sea responsable, que con carácter excepcional tuvieran que almacenarse o usarse fuera del lugar de trabajo (en las oficinas de los clientes, en el propio domicilio o en otras instalaciones alternativas, ya sea en sistemas fijos o en portátiles).

- Salir de los ordenadores personales o terminales, cuando se encuentre ausente de su puesto de trabajo por periodo superior al fijado en los procedimientos para cada caso, en cuyo caso, el sistema le pedirá de nuevo que se identifique.

- Entregar cuando sea requerido por la Dirección, y especialmente cuando vaya a causar baja de la empresa, las llaves, claves, tarjetas de identificación, material, documentación, equipos, contraseñas, y cuantos activos sean propiedad de la misma.

## 7.2 Funciones del Responsable del Fichero

El Responsable del Fichero debe estar sensibilizado con la seguridad de la información, y en particular con la de carácter personal, y que se eviten:

- La pérdida de datos (disponibilidad).
- La alteración de los mismos (integridad).
- El tratamiento o acceso no autorizado (confidencialidad).

Entre sus principales funciones, se pueden destacar:

- Es el encargado jurídicamente de la seguridad de los ficheros y de las medidas establecidas en el presente documento, así como de que se implanten las medidas de seguridad establecidas en él.

- Adoptará las medidas necesarias para que el personal afectado por este documento conozca las nomas que afecten al desarrollo de sus funciones.

- Deberá encargarse de que se adopten las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, perdida, 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 dela acción humana o del medio físico o natural.

- Está obligado al secreto profesional respecto de los datos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

- Elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información.

- Deberá mantenerlo actualizado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

- Deberá adecuar en todo momento el contenido del mismo a las disposiciones vigentes en materia de seguridad de datos.

- Adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

- Se encargará de que exista una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso.

- Establecerá mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

- Será el responsable de autorizar la salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado los ficheros.

- Se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

- Notificará a la AEDP las altas, modificaciones y bajas de los ficheros que contengan datos personales.

- Tendrá la obligación de hacer efectivo el derecho de consulta, rectificación o cancelación del interesado en el plazo establecido por la Ley.

- Comunicará a la AEPD los cambios que se produzcan en la finalidad de los ficheros automatizados, en su responsable y en la dirección de su ubicación.

- Se encargará de describir los sistemas de información que realizan el tratamiento de ficheros que contenga datos personales.

- Se encargará de que los sistemas informáticos de acceso a los ficheros tengan su acceso restringido mediante un identificador de usuario y una contraseña.

- Se encargará de describir la estructura de los ficheros que contengan datos personales.

- Establecer los periodos de destrucción de información del fichero, así como controlar el ciclo de vida de la misma.

- Será el responsable de autorizar por escrito la ejecución de los procedimientos de recuperación de los datos de nivel alto. Deberá dejarse constancia en el registro de incidencias de las manipulaciones que hayan debido realizarse para dichas recuperaciones, incluyendo la persona que realizó el proceso, los datos restaurados y los datos que hayan debido ser grabados manualmente en el proceso de recuperación.

- Designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al Responsable del Fichero de acuerdo con este Reglamento.

- Es el responsable de verificar que se cumplen todos los requisitos que deberán ser periódicamente comprobados, de forma que puedan detectarse y subsanarse anomalías.

- Es el responsable de nombrar a la persona o entidad encargada de realizar las auditorias periódicas que establece la ley, siendo la persona asignada para esta función el Responsable de Seguridad.

- Los Responsables de los Ficheros y los Encargados de los Tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley.

## 7.3 Funciones del Responsable de Seguridad

El Responsable de Seguridad es la persona en la que el Responsable del Fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables. Entre otras atribuciones, el Responsable de Seguridad tiene las siguientes:

- Se encargará de revisar periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes.

- Velará por el cumplimiento de las normas de seguridad recogidas en este documento.

- Recopilará y describirá las medidas, normas, procedimientos, reglas y estándares de seguridad adoptados.

- Determinará el ámbito de aplicación del Documento de Seguridad.

- Definirá los recursos informáticos a los que aplica este Documento de Seguridad.

- Definirá y comprobará la aplicación del procedimiento de notificación y gestión de incidencias.

- Definirá y comprobará la aplicación del procedimiento de realización de copias de respaldo y recuperación de datos.

- Comprobará el cumplimiento del procedimiento establecido para la realización de copias de respaldo, con especial atención a la periodicidad.

- Determinará y mantendrá actualizada la lista de usuarios que tengan acceso autorizado al sistema informático, especificando el nivel de acceso de cada usuario.

- Desarrollará y comprobará la aplicación de un procedimiento de identificación y autenticación de usuarios de acuerdo a lo descrito en este documento.

- Desarrollará y asegurará la aplicación del procedimiento de asignación, distribución y almacenamiento de contraseñas definido en este documento.

- Comprobará el mantenimiento de la confidencialidad de las contraseñas de los usuarios.

- Establecerá y comprobará la aplicación del procedimiento de cambio periódico de la contraseña de los usuarios.

- Establecerá y comprobará la aplicación de un procedimiento que garantice el almacenamiento de las contraseñas vigentes de forma ininteligible.

- Establecerá y comprobará la aplicación de un sistema que limite el acceso de los usuarios únicamente a aquellos datos y recursos que precise para el desarrollo de sus funciones.

- Establecerá y comprobará la aplicación y los mecanismos necesarios para evitar que un usuario pueda acceder a datos o recursos con derechos distintos a los autorizados.

- Conceder, alterar o anular los accesos autorizados a los datos y recursos, de acuerdo con los criterios establecidos por el Responsable del Fichero.

- Establecerá y comprobará la aplicación de un sistema que permita identificar, inventar y almacenar en lugar seguro los soportes informáticos que contienen datos de carácter personal.

- Autorizará la salida de soportes informáticos que contengan datos de carácter personal.

- Velará por el cumplimiento de las medidas de seguridad, comunicando al responsable de personal las infracciones cometidas, para el establecimiento de las correspondientes medidas correctoras.

- Coordinará la puesta en marcha de las medidas de seguridad, colaborará con el Responsable del Fichero en la difusión del Documento de Seguridad y cooperará con el Responsable del Fichero controlando el cumplimiento de las mismas.

# 8 | Procedimientos de notificación, gestión y respuesta ante las incidencias

## 8.1 Gestión de incidencias

Esta sección describe el proceso de gestión de incidencias, así como los mecanismos y soluciones técnicas involucradas en el proceso.

**Según estipula el Reglamento en el art. 5.2.i (Definiciones):**

"Se considera incidencia a cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos."

Asimismo se considerará incidencia de LOPD cualquier detección de un hecho que pudiera constituir infracción de la LOPD o del RDLOPD. Finalmente, se considerara incidencia cualquier solicitud de recuperación de datos de una copia de seguridad, si afecta a los datos identificados como de nivel medio. En tales casos se notificara la incidencia y deberá ser autorizada por el responsable del fichero.

El mantener un registro de las incidencias que puedan comprometer la seguridad de un fichero es una herramienta imprescindible para la prevención de posibles ataques a los sistemas de información, así como la investigación y aclaración de cualquier anomalía.

Todas las incidencias se deberán comunicar directamente al Responsable de LOPD.

## 8.2 Revisión de incidencias

El Responsable de Seguridad revisará periódicamente el estado de las incidencias pendientes, remitiendo a quien proceda la resolución de las mismas.

También revisará el conjunto del registro de incidencias para detectar anomalías, recurrencias o tendencias que pudieran suponer una No Conformidad del Sistema de Gestión.

## 8.3 Registro de incidencias

Sera el Responsable de LOPD quien deberá llevar a cabo un registro de las mismas que incluya los siguientes datos:

- Numero identificativo único
- Clasificación según el tipo de incidencia:
    - Genérico
    - Control de acceso
    - Confidencialidad
    - Soportes
    - Privilegios
    - Acceso, Rectificación, Cancelación, Oposición
    - Recuperación
    - Otros
- Fecha de ocurrencia
- Comunicado por
- Acciones a tomar
- Responsable de la subsanación
- Fecha limite de subsanación
- Fecha de verificación
- Resultado de verificación
- Fecha de cierre

# 9 | Procedimientos de revisión

El Documento de Seguridad será modificado siempre que lo requieran cambios en los ficheros de datos, en los sistemas de información, en las medidas de seguridad o en la legislación aplicable, así como siempre que se detecten incorrecciones o insuficiencias en el mismo. El Responsable de Seguridad velará porque se mantenga la vigencia tanto del documento como de sus anexos y procedimientos referenciados.

Pueden solicitar cambios:

- El Responsable de Seguridad, si son orientados a actualizar la validez del documento, o a subsanar incorrecciones del mismo.
- El Responsable del Fichero, si implican cambios en la política de Seguridad de la organización.
- Cualquier otra persona que considere que debe realizarse un cambio lo remitirá como incidencia, con lo que quedarán sometidos a la valoración del Responsable de Seguridad.

Cualquier cambio sustancial en el Documento de Seguridad, será notificado a toda la organización, que podrá consultar la nueva versión a partir de entonces.

# 10 | Consecuencias del incumplimiento del Documento de Seguridad

La Ley Orgánica de Protección de Datos impone a todas las organizaciones una serie de requisitos en lo que respecta al tratamiento de datos personales, cuyo incumplimiento puede dar lugar a la imposición de fuertes multas para las empresas privadas y a actuaciones disciplinarias para las Administraciones públicas, con las sanciones que establece su régimen disciplinario.

Seguir las directrices de la LOPD y de su normativa de desarrollo conlleva la adopción de unos modelos de gestión en las empresas y organismos públicos aplicables de forma general a la gestión de los sistemas de información. Las entidades respetuosas con el cumplimiento de la normativa dan una sensación externa de control, eficacia y orden en lo relativo a los tratamientos de datos. Por el contrario, su incumplimiento puede dar lugar a denuncias, inspecciones y a la imposición de sanciones que supondrán un importante golpe a la imagen de la entidad, con las correspondientes consecuencias económicas.

La adecuación a la LOPD y a su normativa de desarrollo permite establecer procesos de trabajo seguros en cada uno de los departamentos que gestionen datos personales, mitigando tanto los riesgos técnicos (virus, intrusiones en la red, etc.), como el mal uso de las aplicaciones informáticas.

El responsable de Seguridad velará por el cumplimiento de las normas descritas en este documento, y si detecta incumplimiento de las mismas, que puede ser deliberado o accidental, alertará a los causantes del mismo realizando un seguimiento hasta asegurarse de que desaparece el problema.

En caso de incumplimiento deliberado donde concurran alguna de las siguientes circunstancias:

- No colaboración por parte de los causantes para resolver el problema causado.
- Reincidencia.
- Gravedad del hecho (infracción consciente para obtener un beneficio).

El Responsable de Seguridad pondrá el hecho en conocimiento del Responsable del Fichero, que como miembro del Comité, valorará las circunstancias pudiendo decidir la imputación de una falta disciplinaria leve, grave o muy grave en función de la infracción cometida.

En tal caso, se adoptarán las provisiones previstas, y sin perjuicio de que en caso de determinarse que ha tenido lugar un delito, se procediera a informar a las autoridades competentes.

## Sanciones por incumplimiento de la LOPD

- ✓ **Sanciones Leves**
  De 601,01 a 60.101,21 euros
- ✓ **Sanciones Graves**
  De 60.101,21 a 300.506,05 euros
- ✓ **Sanciones Muy Graves**
  De 300.506,05 a 601.012,10 euros

La cuantía se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de incumplimiento jurídico y de culpabilidad presentes en la concreta actuación infractora.

# 11 | Anexo

## 11.1 Aspectos relativos al fichero <fichero>

**Actualizado a:** < fecha de la última actualización del anexo >

<Se incluirá un anexo de este tipo por cada fichero incluido en el ámbito del documento de seguridad, podrían denominarse ANEXO I b, c, etc.>

**Nombre del fichero o tratamiento:** <rellenar con nombre del fichero>

**Unidad/es con acceso al fichero o tratamiento:** <especificar departamento o unidad con acceso al fichero, si aporta alguna información>

**Identificador y nombre del fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos:** <rellenar los siguientes campos con los datos relativos a la inscripción del fichero en el Registro General de Protección de Datos (RPGD)>

- **Identificador:** <código de inscripción>
- **Nombre:** <nombre inscrito>
- **Descripción:** <descripción inscrita>

**Nivel de medidas de seguridad a adoptar:** <básico, medio o alto>

**#nivel medio# Responsable de seguridad:** <Persona designada por el responsable del fichero al objeto de coordinar y controlar las medidas incluidas en este documento>.

**Administrador:** <Persona designada para conceder, alterar, o anular el acceso autorizado a los datos>.

**Leyes o regulaciones aplicables que afectan al fichero o tratamiento:** <si existen>

**Código Tipo Aplicable:** <se indicará aquí si el fichero esta incluido en el ámbito de alguno de los códigos tipo regulados por el articulo 32 de la LOPD>.

**Estructura del fichero principal:** <Incluir los tipos de datos personales incluidos, con especificación de los que, por su naturaleza, afectan a la diferente calificación del nivel de medidas de seguridad a adoptar, según lo indicado en el artículo 4 del Reglamento de Seguridad>.

**Información sobre el fichero o tratamiento:**

- Finalidad y usos previstos

- Personas o colectivos sobre los que se pretenda obtener o que resulten obligados a suministrar los datos personales
- Cesiones previstas
- Transferencias Internacionales: <relacionar las transferencias internacionales, especificando si ha sido necesaria la autorización del Director de la Agencia Española de Protección de Datos>
- Procedencia de los datos: <indicar quien suministra los datos>
- Procedimiento de recogida: <encuestas, formularios en papel, Internet, etc>
- Soporte utilizado para la recogida de datos: <papel, informático, telemático>

**Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición:** <indicar la unidad y/o dirección. Deben preverse además, los procedimientos internos para responder a las solicitudes de ejercicio de derechos de los interesados>

**Descripción del sistema de información:** <Describir los sistemas de información automatizados o no en los que se realiza el tratamiento de los datos. En el caso de ficheros automatizados, incluir los equipos físicos>.

**Descripción detallada de las copias de respaldo y de los procedimientos de recuperación** <En el caso de sistemas automatizados. Especificar la periodicidad de las copias (que debe ser al menos semanal). Si se trata de ficheros manuales y tienen prevista alguna medida en este sentido, detallarla>.

**Información sobre conexión con otros sistemas:** <Describir las posibles relaciones con otros ficheros del mismo responsable>.

**Funciones del personal con acceso a los datos personales:** <Especificar las diferentes funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y sistema de información específicos de este fichero>.

**Descripción de los procedimientos de control de acceso e identificación:** <Cuando sean específicos para el fichero>.

**Relación actualizada de usuarios con acceso autorizado:** <Relacionar todos los usuarios que acceden al fichero, con especificación del tipo o grupo de usuarios al que pertenecen, su clave de identificación, nombre y apellidos, unidad, fecha de alta y fecha de baja>.

<Si la relación se mantiene de forma informatizada, indicar aquí cual es el sistema utilizado y la forma de obtener el listado. No obstante, siempre que sea posible, es

conveniente imprimir la relación de usuarios y adjuntarla periódicamente a este Anexo>.

**Terceros que acceden a los datos para la prestación de un servicio**: <Relacionar las empresas de mantenimiento, de servicios, etc., que tienen acceso a los datos. Cuando sea necesario realizar un contrato escrito según lo dispuesto en el artículo 12 de la LOPD, se incluirá una copia del mismo o de las cláusulas al efecto en el Anexo VI del documento>.

**Relación de actualizaciones de este Anexo:** <incluyendo fecha, resumen de aspectos modificados y motivo>

Para facilitar la revisión de los ficheros declarados ante la AEDP, se recomienda incluir un cuadro resumen con todos los ficheros declarados, número de inscripción, responsable del fichero, responsable de seguridad, nivel de seguridad, descripción y finalidad, etc.

### 11.1.1 Ejemplo de fichero con datos de carácter personal de nivel básico

**Nombre del fichero o tratamiento:** Contactos Comerciales

**Identificador y nombre del fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos:**

- **Identificador:** **********.
- **Nombre:** Contactos comerciales
- **Descripción:** Gestión Interna de los contactos comerciales que tienen relaciones o solicitan información a Satec S.A.

**Nivel de medidas de seguridad a adoptar:** básico

**Administrador:** **********.

**Estructura del fichero principal:** Nombre y Apellidos; Teléfono; Dirección; Datos de Detalles de Empleo; Datos de Información Comercial.

**Información sobre el fichero o tratamiento:**

- **Finalidad y usos previstos:** Publicidad y Prospección comercial.
- **Cesiones previstas:** Convex Supercomputer, S.A.E; Cybermercado, S.S.; Innovative Secure Communications, S.L; Servicios de Hosting en Internet, S.A.
- **Transferencias Internacionales:** Portugal-Convex Informatica Sistemas De Comunicaçoes Portug;
- **Procedimiento de recogida:** Formularios de inscripción a eventos, tarjetas de visita, o datos proporcionados directamente por el interesado vía email. Todos los datos sea cual sea su procedencia pasan por el mismo filtro para su alta en la misma base de datos. En el caso de formularios de inscripción, el cliente dispone de casillas para solicitar el alta de datos y si quiere o no recibir publicidad. En el resto de casos esta información se contrasta directamente con el cliente.
- **Soporte utilizado para la recogida de datos:** informático.
- **Sistema de tratamiento:** Mixto.

**Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición:**

- **Nombre de la Oficina:** Sistemas Avanzados de Tecnología S.A
- **Dirección:** Av Europa 34 A

- **Código Postal – Población:** 28023 – Aravaca
- **Teléfono – Fax :** 917089000 - 917089090

**Datos incluidos:**

| | | | |
|---|---|---|---|
| NOMBRE | APELLIDOS | CARGO | EMPRESA |
| DEPARTAMENTO | DIRECCION | TELEFONO / FAX | E-MAIL |
| RECIBE O NO PUBLICIDAD | SECTOR | CLIENTE DE FORMACION | FACULTAD / SECCION |
| ASISTENTE | FECHADE LOS DATOS | FECHA ULTIMO CONTACTO | |

**Componentes:**

Distintas aplicaciones corporativas.

Tipo de tratamiento automático / manual.

Personas autorizadas: xX.

**Encargos de tratamiento:** No aplican con carácter general. En los casos en que se organiza un evento conjunto con otra empresa, se firman acuerdos de tratamiento ad-hoc, vigentes sólo durante la organización y celebración del evento, para posibilitar el tratamiento conjunto de los datos.

### 11.1.2 Ejemplo de fichero con datos de carácter personal de nivel medio

**Nombre del fichero o tratamiento:** Gestión de Solicitudes de Empleo.

**Identificador y nombre del fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos:**

- **Identificador:** **********.
- **Nombre:** Gestión de Solicitudes de Empleo.
- **Descripción:** Gestión del proceso de selección de personal para ofertas de empleo relacionadas con la empresa.

**Nivel de medidas de seguridad a adoptar:** Medio

**#nivel medio# Responsable de seguridad:** *********.

**Administrador:** **********.

**Estructura del fichero principal:** DNI/NIF; Nombre y Apellidos; Teléfono; Imagen/Voz; Dirección; Num SS/Mutualidad; Datos de características personales; Datos académicos y profesionales; Datos de detalles de empleo; Datos Información comercial; Datos de circunstancias sociales.

**Información sobre el fichero o tratamiento:**

- **Finalidad y usos previstos:** Recursos Humanos.
- **Cesiones previstas:** No aplica.
- **Transferencias Internacionales:** No Aplica.
- **Procedimiento de recogida:** Currículum Vitae entregado por los interesados, formulario de datos
- **Soporte utilizado para la recogida de datos:** informático.
- **Sistema de tratamiento:** Mixto.

**Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición:**

- **Nombre de la Oficina:** Sistemas Avanzados de Tecnología S.A
- **Dirección:** Av Europa 34 A
- **Código Postal – Población:** 28023 – Aravaca
- **Teléfono – Fax :** 917089000 - 917089090

**Datos incluidos:**

| | | | |
|---|---|---|---|
| NOMBRE | APELLIDOS | DIRECCIÓN | E-MAIL |
| REFERENCIAS ENTREVISTAS | HISTORICO PROFESIONAL | TELEFONO / FAX | PUESTO AL QUE OPTA |
| FECHA DE LOS DATOS | | | |

**Componentes:**

Documento ofimático conteniendo el CV del aspirante.

Tipo de tratamiento automático / manual.

Se guardan los CV's de los candidatos que son de interés durante unos 3 meses, al cabo de los cuales se destruyen.

Se hace uso de la BBDD de CV's publicados en portales web de trabajo.

**Encargos de tratamiento:** No aplican.

### 11.1.3 Ejemplo de fichero con datos de carácter personal de nivel alto

**Nombre del fichero o tratamiento:** Historial Asistencial.

**Identificador y nombre del fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos:**

- **Identificador:** **********.
- **Nombre:** Historial Asistencial.
- **Descripción:** Historial Asistencial en soporte físico (informes y documentación en papel, radiografías, etc) de pacientes atendidos.

**Nivel de medidas de seguridad a adoptar:** Alto

**#nivel medio# Responsable de seguridad:** *********.

**Administrador:** **********.

**Estructura del fichero principal:** DNI/NIF; Num SS/Mutualidad; Nombre y Apellidos; Otros datos de carácter identificativo; Imagen/Voz; Teléfono; Dirección; Nombre de los padres; Datos de características personales; Datos académicos y profesionales; Datos de detalles de empleo; Datos de transacciones, datos económicos financieros y de seguros; Datos de circunstancias sociales

**Información sobre el fichero o tratamiento:**

- **Finalidad y usos previstos:** Fines estadísticos, históricos o científicos; gestión y control sanitario, investigaciones epidemiológicas y actividades análogas; historial clínico.
- **Cesiones previstas:** Otros órganos de la administración publica; administración publica con competencia en la materia; administración publica (sanidad, estadística).
- **Transferencias Internacionales:** No Aplica.
- **Procedimiento de recogida:** El propio interesado.
- **Soporte utilizado para la recogida de datos:** papel/informatico.
- **Sistema de tratamiento:** Mixto.

**Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición:**

- **Nombre de la Oficina:** Clínica Psiquiátrica Padre Menni Hermanas Hospitalarias.
- **Dirección:** C\ Joaquín Beunza 45
- **Código Postal – Población:** 31014 – Pamplona
- **Teléfono – Fax :** 948140611 – 948120238

**Componentes:**

Base de datos que contiene el histórico de los pacientes.

Tipo de tratamiento automatizado / no automátizado.

Personas autorizadas: xX.

## 11.2 Nombramientos

<Adjuntar original o copia de los nombramientos que afecten a los diferentes perfiles incluidos en este documento, como el del responsable de seguridad>

### 11.2.1 Ejemplo de Nombramiento de Responsable de Seguridad

El Responsable del Fichero designa a Xx Xx Xx como Responsable de Seguridad para todos los ficheros referenciados en el presente Documento de Seguridad. Con carácter general se encargará de coordinar y controlar las medidas estipuladas en este documento. En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde a los Responsables de Ficheros y a los Encargados de Tratamiento.

Firmado:

Responsable del Fichero

## 11.3 Autorizaciones para salida o recuperación de datos

<Adjuntar original o copia de las autorizaciones que el responsable del fichero ha firmado para la salida de soportes que contengan datos de carácter personal, así como aquellas relativas a la ejecución de los procedimientos de recuperación de datos >

### 11.3.1 Ejemplo de Autorización de Salida de Información

Cualquier información que salga de la Entidad debe ser controlada, máxime cuando puede verse afectada por la LOPD. En este sentido, las áreas antes de proceder a su envío deben consultar al Área de Seguridad de la Información, si la misma puede ser enviada, así como la forma de proceder. Siempre y cuando esta información no esté previamente catalogada, dentro de este manual, como información periódica de salida, la cual de manera implícita ya tiene su correspondiente autorización.

Independientemente de que se registre la salida de esta información, será necesario atender a factores, tales como:

- El tipo de información de que se trate.
- El destinatario de la información.

- El motivo del envío.
- El uso que se hará de la misma.
- La ubicación geográfica de destino de la información.

## 11.4 Inventario de soportes

<Si el inventario de soportes se gestiona de forma no automatizada recoger en este anexo la información al efecto, según lo indicado en el Capítulo 3.3.3 de este documento. Los soportes deberán permitir identificar el tipo de información, que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en este documento >

### 11.4.1 Ejemplo de Archivo de Registro de Entradas/Salidas de datos

Todos los registros de Entradas y Salidas de Información deberán archivarse, atendiendo a los siguientes criterios:

- Inicialmente se clasificarán los registros por periodos. El año y el mes correspondiente a la entrada o salida de la información. (2005-01 para indicar enero).
- Se mantendrán de forma separada las entradas y salidas de información.
- Se ordenarán según se les catalogue; pagos a bancos, declaraciones a Hacienda, etc.

El lugar de almacenamiento destinado para estos registros será la sala catalogada como “Registro” situada en el edificio B.

### 11.4.2 Ejemplo de Eliminación de Registros de Entradas/Salidas del archivo

Los registros generados en el día a día de la actividad de las distintas áreas de la organización, se mantendrán en el archivo durante 12 meses. Por lo tanto, cada mes se eliminarán todos los registros correspondientes al mismo mes del año anterior.

## 11.5 Registro de incidencias

<Si el registro de incidencias se gestiona de forma no automatizada, recoger en este anexo la información al efecto, según lo indicado en el Capítulo 7.3 de este documento>

### 11.5.1 Ejemplo de Registro de incidencias

Se establecen tres niveles para las incidencias:

- **Leve:** Incidencias que por su naturaleza, aún cuando constituyan un peligro potencial para la seguridad de los datos a que se refiere este documento, pueda ser resuelta de una forma rápida y sin mayores consecuencias.
- **Grave:** Incidencias que por su naturaleza constituyan una degradación o supresión de los ficheros que contienen datos de carácter personal.
- **Muy Grave:** Incidencias que por su naturaleza constituyan la pérdida o substracción incontrolada de estos datos, pudiendo ser estos transmitidos o publicados sin consentimiento expreso del interesado.

**1. Si la incidencia se considera leve:**

1.1. Se desconectará la máquina donde se esté produciendo de cualquier medio de comunicación.

1.2. Se requisará y bloqueará cualquier medio que contenga ficheros de carácter personal que no haya sido autorizado.

1.3. Se procederá resolviendo el problema acontecido y restaurando la máquina para su proceso normal.

1.4. Se destruirá el soporte en cuestión y se generará la pertinente autorización para validar y controlar su contenido.

1.5. Se anotará la incidencia en el Libro de Incidencias.

**2. Si la incidencia se considera grave:**

2.1. Se desconectará la máquina donde se esté produciendo de cualquier medio de comunicación.

2.2. Se informará al responsable de seguridad de la incidencia.

2.3. Se determinará la degradación sufrida por los ficheros.

2.4. Se procederá a la restauración de dichos datos con la última copia de seguridad no afectada por la incidencia.

2.5. Se comunicará a los usuarios afectos de esta restauración de lo ocurrido y de la fecha de validez de los datos que contiene en esos momentos el fichero.

2.6. Se procederá restaurando la máquina a su proceso normal.

2.7. Se anotará la incidencia en el Libro de incidencias.

**3. Si la incidencia es considerada muy grave:**

3.1. Se procederá a desconectar el sistema de comunicaciones de la Entidad.

3.2. Se informará al responsable del fichero y al responsable de seguridad de la incidencia y a autoridades de la Entidad.

3.3. Se determinará el grado de pérdida, degradación o substracción de los datos a que se refiere este documento.

3.4. Se determinará la máquina objeto de la pérdida.

3.5. Se determinarán las posibles causas que hayan desembocado en dicha incidencia.

3.6. Se revisarán todas las máquinas con las mismas características por si pudiesen provocar una incidencia similar.

3.7. Se instalarán los procedimientos necesarios para que la incidencia no se vuelva a producir en todas las máquinas de similares características y con agujeros de seguridad que puedan provocar la repetición del accidente.

3.8. Se revisarán todas las máquinas que pudieran haber sido afectadas por dicha incidencia.

3.9. Se instalarán los procedimientos necesarios para impedir que estas puedan provocar otra incidencia derivada de la anterior.

3.10. Se restaurarán la última copia de seguridad de los datos que no hayan sido afectados por dicha incidencia.

3.11. Se comunicará a los usuarios afectos de esta restauración de lo ocurrido y de la fecha de validez de los datos que contienen en esos momentos el fichero.

3.12. Se volverá a conectar el sistema de comunicaciones.

3.13. Se comunicará a los afectados o interesados cuyos datos hayan sido sustraídos la incidencia.

3.14. Se anotará la incidencia en el Libro de Incidencias.

## 11.6 Encargos de Tratamiento

<Cuando el acceso de un tercero a los datos del responsable del fichero sea necesario para la prestación de un servicio a este último, no se considera que exista comunicación de datos. Recoger aquí el contrato que deberá constar por escrito o de alguna otra forma que permita acreditar su celebración y contenido, y que establecerá expresamente que el encargado de tratamiento tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizara con fin distinto al que figure en dicho contrato, ni los comunicarán ni siquiera para su conservación a otras personas.

El contrato estipulará las medidas de seguridad a que se refiere el artículo 9 de la LOPD que el encargado del tratamiento esta obligado a implementar>

### 11.6.1 Ejemplo de Encargo de tratamiento de datos en la prestación del servicio

Todos los datos que se encuentren en las instalaciones del cliente así como los que proporcione a <La Entidad> en virtud del presente contrato, con independencia del soporte en que se encuentren o entreguen, son propiedad del cliente y tienen carácter absolutamente reservado y confidencial.

En consecuencia, <La Entidad> se compromete expresa y formalmente a:

1. Tratar y conservar con carácter estrictamente reservado y confidencial todos los datos, informaciones, procedimientos y documentos que el cliente le facilite o entregue por cualquier medio o soporte, así como aquellos que conozca a los que tenga acceso con motivo de la prestación de los servicios contratados.

2. Utilizar dichos datos, informaciones, procedimientos y documentos exclusivamente para la finalidad que constituye el objeto del presente contrato, a no emplearlos en la actividad que desempeñe para otras empresas o clientes y a observar el secreto más estricto sobre los mismos.

3. No reproducir, comunicar, ceder, divulgar ni transmitir total o parcialmente los citados datos, informaciones, procedimientos y documentos a personas o entidades cuya intervención no sea estrictamente necesaria para la prestación de sus servicios ni con fines distintos a los contemplados en este contrato, salvo autorización escrita del cliente o en los supuestos en que <La Entidad> venga obligada a su transmisión de conformidad con lo dispuesto en la legislación vigente. En este último caso, <La Entidad> se compromete a informar previamente al cliente de la identidad del solicitante y de los datos requeridos.

4. No extraer bajo ningún concepto material ni documentación de los locales del cliente, ni reproducir total o parcialmente cualquier dato o información que se encuentre en sus instalaciones, proceder a su transmisión de ninguna forma por cualquier medio –ya sea electrónico, mecánico, por fotocopia grabación u otro-, sin autorización expresa al efecto.

5. Adoptar y cumplir todas las medidas técnicas y organizativas exigidas por la normativa vigente en cada momento sobre protección de datos de carácter personal para garantizar la integridad y seguridad de dichos datos y evitar su alteración, pérdida, tratamiento o acceso no autorizado, en particular las medidas de seguridad que sean necesarias según el R.D. 1720/2007, de 21 de diciembre, y la legislación complementaria o de desarrollo así como cualquier otra que la modifique o sustituya en el futuro.

6. Impartir las instrucciones precisas a todas las personas que intervengan o vayan a intervenir en el futuro en el desarrollo del objeto del presente contrato o en la prestación de los servicios contratados –empleados, asociados, auxiliares, colaboradores, etc – para que conozcan efectivamente y asuman las mismas obligaciones contenidas en el presente acuerdo, siendo <La Entidad> responsable del incumplimiento de las mismas.

7. Devolver al cliente o destruir puntualmente, a petición y según las indicaciones del mismo, toda la información, datos, procedimientos y documentos transferidos cualquiera que fuera su soporte, y necesariamente al vencimiento a la finalización del presente contrato por cualquier causa. No obstante lo anterior, <La Entidad> podrá conservar, durante el plazo establecido legalmente, la documentación del servicio prestado que constituya prueba y soporte del trabajo profesional realizado debiendo ser destruido o devuelto al cliente una vez transcurrido dicho plazo.

<La Entidad> reconoce que el deber de confidencialidad asumido en virtud del presente documento constituye una condición esencial para la contratación de sus servicios, y que se mantendrá aún finalizado el presente contrato. En consecuencia, <La Entidad> será responsable de los datos y perjuicios que se ocasionen al cliente con motivo del incumplimiento de lo establecido en la presente cláusula, incluido el importe de cualquiera de las sanciones que se impongan al cliente por tal circunstancia, todo ello sin perjuicio de la responsabilidad contractual por incumplimiento del presente contrato.

### 11.6.2 Ejemplo de tratamiento de datos de carácter personal del cliente

El contratante conoce y acepta que el tratamiento de los datos personales que se suministren voluntariamente a través del presente contrato tendrá como objeto el cumplimiento del propio contrato, la realización de estudios, análisis y estadísticas, y autoriza a que se pueda remitir información, incluso por vía electrónica, sobre productos y servicios de las distintas entidades de la compañía, todo ello, incluso una vez extinguida la relación contractual existente.

Asimismo, sus datos podrán ser cedidos, exclusivamente para las finalidades indicadas anteriormente, a otras con entidades del grupo así como a otras personas físicas o jurídicas con las que las distintas entidades de la compañía concluyan acuerdos de colaboración, todo ello incluso si no se formaliza operación alguna, respetando en todo caso la legislación española sobre protección de datos de carácter personal y sin necesidad de que le sea comunicada cada primera cesión que se efectúe a los referidos cesionarios.

Todos los datos son tratados con absoluta confidencialidad, no siendo accesibles a terceros para finalidades distintas para las que han sido autorizados.

El fichero creado se encuentra bajo la supervisión y control de <La Entidad>, quien asume la adopción de las medidas de seguridad de índole técnica y organizativa para proteger la confidencialidad e integridad de la información, de acuerdo con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y demás legislación aplicable y ante quien el titular de los datos puede ejercitar sus derechos de acceso, rectificación, oposición y cancelación de sus datos de carácter personal suministrados mediante comunicación escrita dirigida a <dirección de la Entidad>.

En caso de que los datos facilitados se refieran a personas físicas distintas del contratante, este deberá, con carácter previo a facilitar los mismos, informarles de los extremos contenidos en los párrafos anteriores.

## 11.7 Registro de Entrada y Salida de soportes

<Si el registro de entrada y salida de soportes al que se refiere el Capítulo 3.3.4 que es obligatorio a partir del nivel medio, se gestiona de forma no automatizada, recoger en este anexo la información al efecto, según lo indicado los artículos 20.1 y 20.2 del Reglamento de Seguridad.>

### 11.7.1 Ejemplo de Registro de Entrada/Salida de información no catalogada

De cara al cumplimiento con la LOPD, cualquier entrada de información, con independencia del número de ficheros que se generen, deberá ser registrada de acuerdo con el siguiente procedimiento:

1. Se cumplimentará una “Ficha de Entrada/Salida de Información”, según la plantilla establecida al efecto correspondiente a la Enditad de que se trate y al tipo de archivo que se envía.

   En la ficha, será necesario indicar los campos que se solicitan en la misma, tales como: Fecha de recepción, tipo y número de soportes recibidos, persona que lo envía, etc. Debiendo ser firmada por la persona que recibe la información.

2. Se archivará a modo de registro, tanto la Ficha de Entrada de Información, como la carta o cualquier otro documento de referencia del envío.

### 11.7.2 Ejemplo de Sistema de Gestión de Entrada/Salida de información catalogada

De acuerdo con lo establecido por el art. 92 del RLOPD, referido a la gestión de soportes, se establece que:

1. "Cualquier entrada o salida de información de la compañía, con información de carácter personal, deberá ser registrada.
2. Se debe controlar la eliminación de soportes.
3. Se debe controlar la información que sale fuera de la compañía."

La documentación correspondiente se encuentra en: Xxx

## 11.8 Confidencialidad y Deber de Secreto

### 11.8.1 Ejemplo de Contrato de Confidencialidad y Deber de Secreto

Todos los datos que se encuentren en las instalaciones de la entidad, así como los que proporcione a <Prestador de servicios> en virtud del presente contrato, con independencia del soporte en que se encuentren o entreguen, son propiedad de la compañía y tienen carácter absolutamente reservado y confidencial.

En consecuencia, <Prestador de Servicios> se compromete expresa y formalmente a:

1. Tratar y conservar con carácter estrictamente reservado y confidencial todos los datos, informaciones, procedimientos y documentos que la compañía le facilite o entregue por cualquier medio o soporte, así como aquellos que conozca o al os que tenga acceso con motivo de la prestación de los servicios contratados.
2. Utilizar dichos datos, informaciones, procedimientos y documentos exclusivamente para la finalidad que constituya el objeto presente contrato, a no emplearlos en la actividad que desempeñe para otras empresas o clientes y a observar el secreto más estricto sobre los mismos.
3. No reproducir, comunicar, ceder, divulgar ni transmitir total o parcialmente los citados datos a personas o entidades cuya intervención no sea estrictamente necesaria para la prestación de sus servicios ni con fines distintos a los contemplados en este contrato, salvo autorización escrita de <La Entidad> o en los supuestos en que <Prestador de Servicios> venga obligada a su transmisión de conformidad con lo dispuesto en la legislación vigente. En este ultimo caso, <Prestador de Servicios> se compromete a informar previamente a la compañía de la identidad del solicitante y de los datos requeridos.

4. No extraer bajo ningún concepto material ni documentación de los locales de la Entidad, ni reproducir total o parcialmente cualquier dato o información que se encuentre en sus instalaciones, proceder a su transmisión de ninguna forma o por cualquier medio –ya sea electrónico, mecánico, por fotocopia, grabación y otro-, sin la autorización expresa al efecto.

5. Adoptar y cumplir todas las medidas técnicas y organizativas exigidas por la normativa vigente en cada momento sobre protección de datos de carácter personal para garantizar la integridad y la seguridad de dichos datos y evitar su alteración, perdida, tratamiento o acceso no autorizado, en particular las medidas de seguridad que sean necesarias según el R.D 1720/2007, de 21 de diciembre, y la legislación complementaria o de desarrollo así como cualquier otra que la modifique o sustituya en el futuro.

6. Impartir las instrucciones precisas a todas las personas que intervengan o vayan a intervenir en el futuro en el desarrollo del objeto del presente contrato o en la prestación de los servicios contratados –empleados, asociados, auxiliares, colaboradores, etc- para que conozcan efectivamente y asuman las mismas obligaciones contenidas en el presente acuerdo, siendo <Prestador de servicios> responsable del incumplimiento de las mismas.

7. Devolver a la compañía o destruir puntualmente, a petición y según las indicaciones de <La Entidad>, toda la información, datos, procedimientos y documentos transferidos cualquiera que fuera su soporte, y necesariamente al vencimiento y a la finalización del presente contrato por cualquier causa. No obstante lo anterior, <Prestador de servicios> podrá conservar, durante el plazo establecido legalmente, la documentación del servicio prestado que constituya prueba y soporte del trabajo profesional realizado debiendo ser destruido o devuelto a <La Entidad> una vez transcurrido dicho plazo.

<Prestador de Servicios> reconoce que el deber de confidencialidad asumido en virtud del presente documento constituye una condición esencial para la contratación de sus servicios, y que se mantendrá aun finalizado el presente contrato. En consecuencia, <Prestador de Servicios> será el responsable de los daños y perjuicios que se ocasionen a <La Entidad> con motivo del incumplimiento de lo establecido en la presente cláusula, incluido el importe de cualesquiera de las sanciones que se impongan a <La Entidad> por tal circunstancia; todo ello sin perjuicio de la responsabilidad contractual por incumplimiento del presente contrato.

<Prestador de Servicios> autoriza que sus datos de carácter personal facilitados a <La Entidad> en virtud de los servicios prestados, sean tratados por dicha entidad, con la finalidad de gestionar y liquidar los impuestos derivados de la facturación de los referidos servicios.

Los datos de carácter personal recabados adoptarán las medidas de seguridad técnicas y organizativas adecuadas para proteger la confidencialidad e integridad de la información, de acuerdo con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y demás legislación aplicable.

Todos los datos serán tratados con absoluta confidencialidad, no siendo accesibles a terceros para finalidades distintas para las que han sido autorizados.

<Prestador de Servicios> tiene la facultad de ejercitar los derechos de acceso, rectificación, oposición y cancelación de sus datos de carácter personal, mediante comunicación escrita dirigida a <La Entidad>, con domicilio en <Domicilio social de la Entidad>.

## 11.9 Glosario

- **AEPD:** Agencia Española de Protección de Datos (www.agdp.es)
- **Afectado o interesado:** Persona física o titular de los datos que sean objeto del tratamiento a que se refiere la definición de tratamiento de datos.
- **Aplicación:** Engloba la relación de programas que intervienen en el tratamiento de los datos de carácter personal.
- **Autenticación:** Proceso por el cual se garantiza que el usuario que accede a un sistema informático es quien dice ser. Pro lo general, los sistemas de autenticación están basados en el cifrado mediante una clave o contraseña probada y secreta que sólo conoce el auténtico emisor.
- **Cancelación:** Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.
- **Centro de tratamiento:** Engloba los distintos recursos (locales, equipos, sistemas, comunicaciones, etc) que intervienen en el tratamiento de los datos de carácter personal.
- **Cesión o comunicación de datos:** Toda revelación de datos realizada a una persona distinta al interesado.
- **Cifrado:** Transformación de un mensaje en otro, utilizando una clave para impedir que el mensaje transformado pueda ser interpretado por aquellos que no conocen la clave.
- **Confidencialidad:** Garantía que la información se accesible sólo para aquellos con autorización de acceso.
- **Consentimiento del interesado:** Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
- **Dato disociado:** Aquél que no permite la identificación de un afectado o interesado.
- **Datos de carácter personal:** Cualquier información concerniente a personas físicas identificadas o identificables.

- **Destinatario o cesionario:** La persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos. Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el trafico como sujetos diferenciados.

- **Encargado de tratamiento:** Es la persona física o jurídica, pública o probada, 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.

- **Fichero:** Engloba todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso tanto automatizado como no automatizado.

- **Fichero no automatizado:** Todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

- **Fuentes accesibles al público**: Aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencias que, en su caso, el abono por contraprestación.

- **Integridad:** Garantía de la exactitud de la información frente a la alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.

- **LOPD:** Ley Orgánica de Protección de Datos de Carácter Personal.

- **Persona:** Refiriéndose a todas aquellas personas, pertenecientes o no a la Entidad, que intervienen en el tratamiento y gestión de los datos de carácter personal.

- **Procedimiento de disociación:** Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

- **Responsable de fichero o tratamiento:** Es la Entidad, persona o el órgano administrativo que decide sobre la finalidad, el contenido y el uso del tratamiento de los datos personales.

- **Responsable de seguridad de datos:** Persona física a la que el Responsable del Fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

- **Tratamiento de datos:** Operaciones, procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

# 12 | Conclusiones

Para la realización de este proyecto de fin de carrera, ha sido necesario dedicarle mucho tiempo a la recopilación de información, y al entendimiento y aplicación de leyes en el ámbito de las tecnologías.

Una vez superada esta fase de preparación apoyada en el trabajo diario de auditoría, la realización del Documento de Seguridad depende en gran medida de la complejidad de las medidas de seguridad que se quieran escoger y del sector en el que se encuentre el cliente auditado.

Este proyecto me ha servido para comprender que las tecnologías forman parte de los pilares principales sobre los que se sujetan la mayoría de las empresas, y de lo importante que es saber gestionar los activos, y sobre todo, elaborar las medidas de seguridad necesarias para que ningún sujeto o ningún desastre natural, ponga en peligro la existencia y supervivencia de la empresa.

El tiempo aproximado para la realización de este proyecto han sido los seis meses de la beca que he disfrutado en el Departamento de Seguridad en una consultora, más un mes de trabajo adicional.

En horas, el tiempo estimado aproximado está entre 650-700 horas repartidas en:

- ✓ Beca de 660 horas.
- ✓ 20-40 horas aproximadas de trabajo adicional

# 13 | Bibliografia

1. Web de la Agencia Española de Protección de Datos: www.agpd.es

   - Folleto Introductorio:
     - https://www.agpd.es/portalweb/common/FOLLETO.pdf

   - LOPD:
     - https://www.agpd.es/portalweb/canaldocumentacion/legislacion/estatal/common/pdfs/Ley-15_99.pdf

   - RLOPD:
     - https://www.agpd.es/portalweb/canaldocumentacion/legislacion/estatal/common/pdfs/RD_1720_2007.pdf

   - Guía de Seguridad de datos:
     - https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia_seguridad_datos_2008.pdf

   - Guía de VideoVigilancia:
     - http://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia.pdf

   - Guía del Responsable del Fichero:
     - http://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf

2. Web: http://www.noticias.jurídicas.com

3. Libro Buenas Practicas en Protección de Datos – Pedro Serrera Cobos