Datos personales: Su protección y auditoría desde una visión práctica

Titulación: Ingeniería Técnica Informática de Gestión

Autor: Pedro Delgado Bueno

Tutor: Miguel Ángel Ramos


UNIVERSIDAD CARLOS III DE MADRID
homo
hominis
sacra
res

Título: Datos personales: Su protección y auditoría desde una visión práctica.

Autor: Pedro Delgado Bueno

Director: Miguel Ángel Ramos González

EL TRIBUNAL

Presidenta: Ana Isabel González-Tablas Ferreres

Vocal: Óscar Pérez Alonso

Secretario: Jorge Blasco Alis

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día 26 de Septiembre de 2013 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

AGRADECIMIENTOS

A mi familia que me ha apoyado siempre sin condiciones y siempre me dan los mejores consejos.

A mi tutor que ha estado siempre disponible para mejorar este proyecto.


UNIVERSIDAD CARLOS III DE MADRID
homo
hominis
sacra
res

RESUMEN

Este proyecto de fin de carrera explica qué es una auditoría informática y su importancia para la protección de los datos personales. En el proyecto se desarrollan detalladamente todos los controles necesarios para que los sistemas de información de una entidad cumplan con la normativa española de protección de datos, así como los riesgos a los que se expone una organización al no cumplirla. Para una mejor comprensión del trabajo de auditor y de la auditoría se muestran ejemplos prácticos de papeles de trabajo como cuestionarios, actas y el informe final. Además se habla de los cambios más importantes que traerá la nueva normativa europea de protección de datos, así como las normas generales que se deben seguir para mantener la privacidad de los datos de las personas en la implantación de servicios muy extendidos actualmente como el cloud computing y la utilización de cookies.

ABSTRACT

This study explains what a computer audit is and its importance for the protection of personal data. In the course of the project, all necessary controls for an organization's information systems to comply with Spanish data protection regulations were developed in detail, as well as the risks organizations run through noncompliance. To better understanding the work of auditors and the audit, practical examples are shown of working papers such as questionnaires, reports, and the final report. Also discussed are the major changes that the new European data protection regulations will bring as well as general rules that should be followed to maintain the data privacy of people during the implementation of currently widespread services such as cloud computing and the use of cookies.

ÍNDICE

1. Introducción

¿Es la privacidad un derecho? ¿Conservaremos este derecho en el futuro? Todos los días recibimos llamadas de empresas privadas que obtienen nuestros datos de forma que desconocemos o recibimos publicidad a nuestro nombre que no deseamos, además todos sabemos que actualmente muchísima gente tiene sus datos personales en Internet, en los cuales se incluyen desde sus datos y sus gustos más personales a sus actividades diarias. Todo esto hace preguntarse: ¿Se cumple la ley de protección de datos en España? ¿Es suficientemente restrictiva? ¿Qué nos deparará el futuro?

Muchas empresas cuyo negocio está en la red se quejan de que la normativa en Europa y especialmente en España y Alemania es restrictiva por lo que no pueden desarrollar su negocio completamente en Europa y tienen que realizarlo desde otros países en los que no se da tanto valor a la privacidad como EEUU. ¿Tienen razón? ¿Vale todo en estos momentos de crisis económica? ¿Debería Europa ser más flexible para atraer nuevas inversiones?

Los europeos y especialmente los españoles siempre hemos tenido un carácter en el que protegíamos fuertemente nuestra privacidad. Pero esto está cambiando rápidamente en los últimos años. En mi experiencia profesional he podido comprobar que sigue sin darse importancia a este derecho aun habiendo grandes sanciones por su incumplimiento. ¿Por qué algunas grandes empresas de este país prefieren pagar multas que invertir en seguridad para proteger datos personales de sus clientes? Y lo más importante de todo, ¿se perderá en los próximos años lo que se ha conseguido con esta ley?

A continuación hago un breve resumen de los distintos puntos que contiene este proyecto:

- ¿Qué es la auditoría informática?

  En este apartado se define y se detallan los tipos de auditorías y se nombran cuales son las principales auditorías informáticas. También se describe como debe planificarse una auditoría informática y se explica que es lo que podemos conocer y la gran importancia que tiene realizarla. Finalmente se explica cómo debe ser un auditor informático para que lleve a cabo eficazmente su labor y las certificaciones que puede obtener.

- ¿Qué es la protección de datos?

  En este apartado se define que es un dato personal, se habla de la cultura de protección de datos y de las normas que se han implantado en nuestro país para desarrollarlo.

  Además se resumen los principios y derechos en los que se basa la normativa de protección de datos.

  Finalmente se habla de los riesgos que puede tener una organización si no aplica la normativa y sus consecuencias legales.

- Definición de los controles realizados para su auditoría y el cumplimiento de la ley vigente.

  En este apartado se hace una explicación exhaustiva y práctica del desarrollo del reglamento en una auditoría de protección de datos, incluyendo los cuestionarios que se deben realizar en cada uno de los aspectos de la ley.

- ¿Qué documentación se debe solicitar de forma general para iniciar una auditoría LOPD?

  En este apartado se detalla la documentación general que se debe solicitar al auditado al iniciar una auditoría de protección de datos.

- ¿Qué aspectos técnicos podemos controlar en una auditoría LOPD?

  En este apartado se ponen diversos ejemplos de aspectos técnicos de la LOPD que pueden ser controlados por los auditores de forma técnica.

- Guión de entrevista – Auditoría Ley Orgánica de Protección de Datos

  En este apartado se pretende mostrar cuales serían los puntos generales que se deben abarcar en las reuniones con los responsables de la organización auditada. Además se incluye un ejemplo práctico.

- ¿Qué es el informe de auditoría?

  En este apartado se define que es un informe de auditoría. Además se incluye un ejemplo práctico completo de lo que es un informe de auditoría de cumplimiento LOPD realizado a una entidad.

- Cloud Computing y LOPD.

  En este apartado se define que es el cloud computing y se habla de los principales riesgos que deben ser tenidos en cuenta respecto al cumplimiento de la ley de protección de datos. Además se habla de las principales medidas que debe adoptar una empresa cuando contrate un servicio de cloud computing

- Cookies y LOPD.

En este apartado se define que es una cookie y los tipos de cookies que existen. Se habla de la información que guarda que afecta a la ley de protección de datos. Además se comentan las obligaciones que tienen las partes para el cumplimiento de la ley en este ámbito.

- El nuevo reglamento europeo.

  En este apartado se hablan de las principales novedades y cambios que traerá próximamente el nuevo reglamento de protección de datos

2. Objetivos

Los objetivos de este proyecto de este fin de carrera son:

- **Divulgación de la Auditoría Informática**: Cuando yo comencé la carrera desconocía al igual que la mayor parte de mis compañeros esta rama de la Ingeniería Informática. Mi interés fue creciendo cuando cursé las asignaturas de Auditoría informática y Gestión de la calidad que al no ser asignaturas obligatorias hacen que mucha gente termine la carrera desconociendo esta rama y posteriormente cuando conseguí un trabajo en este sector me hizo darme cuenta de la importancia que tiene en las entidades. Para ello en este proyecto se define y se hace una presentación completa del trabajo de auditor, además se incluyen ejemplos prácticos para hacer más sencilla su comprensión.

- **Devolver la importancia a la privacidad**: Los nuevos tiempos dan cada menos relevancia a la privacidad. Con este proyecto se pretende que el lector comprenda su importancia, para ello conocerá el esfuerzo que supone la correcta aplicación de las medidas de la ley de protección de datos en los sistemas de información de una entidad auditada, para así evitar las repercusiones que tendría un problema en la privacidad tanto a nivel de imagen como económico, evitando así las cuantiosas sanciones de la AEPD. Además el particular conocerá los derechos que tiene gracias a la normativa y cómo ejercerlos.

- **Conocimiento de las medidas que impone la ley:** En este proyecto se hace un análisis que cualquier persona no experta en leyes puede comprender para poder hacer que su organización cumpla con la ley de

protección de datos en sus sistemas de información automatizados y en su tratamiento de datos en documentación en papel.

- **Nuevos retos en el cumplimiento de la ley:** En este proyecto se pretenden resolver algunas dudas que pueden surgir al relacionar la protección de datos con tecnologías como los cookies o el cloud computing. Además se analizan los cambios más importantes que traerá la nueva regulación de protección de datos que va a aprobar la Unión Europea.

3. La auditoría informática

* Partes extraídas de [CURSO] y ampliadas por el autor del PFC

3.1 ¿Qué es la auditoría informática?

La palabra auditoría proviene del latín “Auditorius” y de esta proviene la palabra auditor que se refiere a aquel que tiene la virtud de oír.

ISACA lo define como cualquier revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y los interfaces correspondientes.

Se concluye que se llama auditoría informática al conjunto de procedimientos y técnicas para evaluar los recursos informáticos con que cuenta una entidad con el fin de realizar un informe sobre la situación en que se desarrollan y se utilizan estos recursos.

3.2 ¿Cuál es el objetivo de la auditoría informática?

Al realizar una auditoría informática se recolectan, agrupan y evalúan evidencias para determinar si un sistema de información:

- Salvaguarda los activos
- Mantiene la integridad de los datos
- Lleva a cabo eficazmente los fines de la organización.
- Hace un buen uso de los recursos.
- Cumple con las leyes y regulaciones establecidas.

Los controles realizados en una auditoría deberán evaluar además los sistemas de información desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de datos

El objetivo de la auditoría informática del sistema de información que tiene una entidad auditada es el de mejorar la rentabilidad, seguridad y eficacia del sistema mecanizado de información que sustenta.

Además a través de la auditoría de sistemas de información es necesario controlar el equilibrio entre riesgos y costes de seguridad contra la eficacia del sistema.

La eficacia del sistema viene dada por la aportación a la empresa de una información válida, exacta, completa, actualizada y oportuna que ayude a la toma de decisiones teniendo en cuenta los valores de calidad, plazo y coste.

La rentabilidad del sistema debe ser medida con la relación de los costes actuales, la comparación de esos costes con otros gastos de la organización y la comparación de la cuantía con la de otros sistemas de empresas similares.

3.3 ¿Qué tipos de auditoría existen?

Según la naturaleza de los trabajadores que realicen la auditoría, los tipos de auditoría se dividen en dos:

- **Interna**: Se caracteriza porque los recursos y personas pertenecen a la empresa auditada, la propia organización es la que lleva el control.

- **Externa**: Se caracteriza porque los recursos y personas no pertenecen a la empresa auditada. Los auditores y los auditados no son los mismos por lo que hay una mayor objetividad.

3.4 ¿Cuales son las principales auditorías informáticas?

- **Auditoría del desarrollo**. Revisión de la metodología de desarrollo, control interno de las aplicaciones, satisfacción de usuarios, control de procesos y ejecuciones de programas críticos.
- **Auditoría de bases de datos.** Revisión de los controles de acceso, de actualización, de integridad y calidad de los datos.
- **Auditoría de Sistemas**. Revisión de las medidas de seguridad de los sistemas operativos, optimización de los sistemas, etc.
- **Auditoría de la seguridad**. Referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.
- **Auditoría de redes**. Revisión de la topología de red y determinación de posibles mejoras, análisis de caudales y grados de utilización.
- **Auditoría de aplicaciones.**

- Evaluar la eficiencia y efectividad de los sistemas de información que respalden los procesos de negocio.
- Evaluar el diseño y la implementación de los controles programados y manuales para asegurar que los riesgos identificados para los procesos del negocio estén en un nivel aceptable.

- Mitigar los riesgos de índole económico, de incumplimiento del marco legal y la normativa establecida y de falta de integridad de la información remitida a clientes

➢ **Auditorías de migración de aplicaciones.** Consiste en verificar los procedimientos y pruebas que se han realizado en los sistemas para verificar que la información del sistema antiguo y actual es la misma.

➢ **Auditoría de la gestión.** la contratación de bienes y servicios, documentación de los programas, etc.

➢ **Auditorías legales o de cumplimiento (LOPD, RD 1720/2007, SOX, ISO27001, ISO20000).**

➢ **Auditoría de planes de contingencia y continuidad.**

- Los planes deben estar formalizados por escrito y aprobados por la Dirección.

- Los empleados deben tener asignadas responsabilidades para su ejecución, las conocen y están preparados para realizarlas.

- Deben abarcar todos los ámbitos críticos de la empresa y que en función de dicho aspecto se ha establecido el orden de prioridad en la recuperación.

- Garantizar su actualización mediante revisiones y pruebas periódicas.

➢ **Auditoría de datos masivos.** Consiste en realizar mediante pruebas informáticas con herramientas de tratamiento masivo de datos (IDEA, ACL) para verificar que los cálculos automáticos de las aplicaciones se están realizando correctamente.

- **Auditorías físicas.** Revisión de la protección del hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan, contemplando las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc. Para garantizar las integridad de los activos humanos, lógicos y material de un CPD.
- **Auditoría servicios externalizados en TI.** Se trata de realizar auditorías a los proveedores externos donde se tiene externalizados los servicios para comprobar que los servicios se están realizando con la misma calidad que si fuesen realizados internamente.
- **Test de penetración o hacking ético.** Se trata de una penetración controlada en los sistemas informáticos de una empresa, de la misma forma que lo haría un hacker o pirata informático pero de forma ética.

3.5 ¿Cómo se planifica una auditoría informática?

Para poder planificar correctamente la duración, esfuerzo y recursos que una auditoría informática necesita cuando va a comenzar, se debe recopilar cierta información del entorno de la entidad auditada como la siguiente.

Recopilación de información del entorno:

- Experiencias anteriores en el mismo tipo de auditorías.
- Reuniones con los responsables del entorno informático.
- Recopilación de la información relativa al entorno y a la revisión específica.
- Estructura general de los departamentos involucrados.
- Organigrama del CPD.

- Personal de informática:
  - Responsables de los departamentos.
  - Número de personas en cada departamento.
  - Número de personal externo y empresas.
- Relación de aplicaciones informáticas.
- Tipos de desarrollo.
  - Desarrollo interno.
  - Comprada externamente (suministrador).
  - Desarrollada por terceros (proveedor).
- Metodologías de desarrollo utilizadas.
- Hardware y software de las máquinas.
  - Sistema operativo.
  - Gestor base de datos.
  - Software de control de acceso.
- Redes existentes.
- Interfaces existentes.
- Legislación de obligado cumplimiento.
- Revisión de la documentación.

Ejemplo de cuestionario de recopilación de información del entorno:

Proceso	Aplicaciones y versiones	Nombre Servidor Aplicación	Nombre Servidor Datos	Sistema operativo	Base de Datos	Localización Servidores

3.6 Alcance

El alcance de la auditoría informática es la parte del sistema de información definida por una entidad auditada para el desarrollo de la misma junto con los objetivos establecidos para la revisión.

El alcance deberá definirse claramente en el informe final, detallando los temas examinados y los omitidos.

3.7 ¿Qué podemos conocer al realizar una auditoría informática?

La auditoría informática sirve para mejorar ciertas características en la organización auditada como:

- Desempeño
- Fiabilidad
- Eficacia
- Rentabilidad
- Seguridad

- Privacidad

Al realizar una auditoría informática podemos conocer:

- El flujo de información y el uso de los recursos dentro de una organización
- La información crítica para el cumplimiento del objetivo de la organización, identificando necesidades, duplicidades, costos, valor y barreras, que obstaculicen flujos de información.
- Análisis de la eficiencia de los Sistemas Informáticos.
- Verificar el cumplimiento de la normativa en el ámbito a analizar.
- Revisión eficaz de los recursos informáticos.

3.8 ¿Por qué es importante realizar una auditoría informática?

* Partes extraídas de [SHELLSEC].

La Auditoría Informática, es importante en las organizaciones auditadas por lo siguiente:

- Se puede dar o utilizar información errónea si la calidad de datos de entrada es inexacta o estos son manipulados.
- Los ordenadores, servidores y los Centros de Procesamiento de Datos se han convertido en blancos para fraudes, espionaje, delincuencia y terrorismo informático.

- La continuidad de las operaciones, la administración y organización de la empresa no deben residir en sistemas mal diseñados, ya que los mismos pueden convertirse en un serio peligro para la empresa.
- Las bases de datos pueden ser propensas a ataques y accesos de usuarios no autorizados o intrusos.
- La piratería de software y el uso no autorizado de programas, con las implicaciones legales y respectivas sanciones que esto puede tener para la empresa.
- El robo de secretos comerciales, información financiera, administrativa, la transferencia ilícita de tecnología y demás delitos informáticos.
- Mala imagen e insatisfacción de los usuarios porque no reciben el soporte técnico adecuado o no se reparan los daños de hardware ni se resuelven los problemas en plazos razonables, es decir, el usuario percibe que está abandonado y desatendido permanentemente.
- En el Departamento de Sistemas se observa un incremento desmesurado de costos, inversiones injustificadas o desviaciones presupuestarias significativas.
- Evaluación de nivel de riesgos en lo que respecta a seguridad lógica, seguridad física y confidencialidad.
- Mantener la continuidad del servicio y la elaboración y actualización de los planes de contingencia para lograr este objetivo.
- Los recursos tecnológicos de la empresa incluyendo instalaciones físicas, personal subalterno, horas de trabajo pagadas, programas, aplicaciones, servicios de correo, Internet, o comunicaciones; son utilizados por el personal sin importar su nivel jerárquico, para asuntos

personales, alejados totalmente de las operaciones de la empresa o de las labores para las cuales fue contratado.

- El uso inadecuado del ordenador para usos ajenos de la organización, por ejemplo la copia de programas para fines de comercialización sin reportar los derechos de autor, o utilización de Internet de forma abusiva.

3.9 ¿Cómo debe ser el personal que compone una unidad de auditoría SI?

*Partes extraídas de [RA-MA] y ampliadas por el autor del PFC.

Formación: aunque muchos de los profesionales con más antigüedad en este ámbito son titulados en especialidades relacionadas con la economía o el derecho, dada la naturaleza del trabajo del auditor de SI es adecuado que su formación esté relacionada con las TI, por ejemplo ingenieros informáticos o de telecomunicaciones. Además son valorables las certificaciones como CISA, CIA, CISSP, CISM, estándares ISO, etc.

Trato con personas: ya que a menudo la actividad del auditor es analizar y evaluar actividades realizadas por otras personas de la organización y que además tienen gran experiencia en su trabajo es muy importante que las personas que realiza los trabajos de auditoría sean capaces de:

- Ser empáticos, capaces de colocarse en la posición de la persona auditada.
- Capacidad para escuchar.
- Capacidad de negociación.

- Paciente, prudente y flexible.
- Con capacidad para defender sus puntos de vista.

Desarrollo del trabajo: Un auditor de SI debe ser ordenado, metódico y con gran capacidad de síntesis. Debe saber trabajar en equipo y tener adecuadas habilidades para la redacción de informes y papeles de trabajo.

Honesto y reservado: debe mantener una conducta ética adecuada, cumpliendo el código de ética de ISACA, si se posee la certificación CISA, el cual detallo a continuación y mantener una estricta cautela a la hora de divulgar información.

Los miembros y los poseedores de certificaciones de ISACA deberán:

1. Respaldar la implementación y promover el cumplimiento con estándares y procedimientos apropiados del gobierno y gestión efectiva de los sistemas de información y la tecnología de la empresa, incluyendo la gestión de auditoría, control, seguridad y riesgos.

2. Llevar a cabo sus labores con objetividad, debida diligencia y rigor/cuidado profesional, de acuerdo con estándares de la profesión.

3. Servir en beneficio de las partes interesadas de un modo legal y honesto y, al mismo tiempo, mantener altos niveles de conducta y carácter, y no involucrarse en actos que desacrediten su profesión o a la asociación.
4. Mantener la privacidad y confidencialidad de la información obtenida en el curso de sus deberes a menos que la divulgación sea requerida por una autoridad legal. Dicha información no debe ser utilizada para beneficio personal ni revelada a partes inapropiadas.
5. Mantener la aptitud en sus respectivos campos y asumir sólo aquellas

actividades que razonablemente esperen completar con las habilidades, conocimiento y competencias necesarias

6. Informar los resultados del trabajo realizado a las partes apropiadas, incluyendo la revelación de todos los hechos significativos sobre los cuales tengan conocimiento que, de no ser divulgados, pueden distorsionar el reporte de los resultados.

7. Respaldar la educación profesional de las partes interesadas para que tengan una mejor comprensión del gobierno y la gestión de los sistemas de información y la tecnología de la empresa, incluyendo la gestión de la auditoría, control, seguridad y riesgos.

La certificación más importante que existe para acreditar la capacidad de un profesional para desempeñar o ejecutar labores de auditoría de sistemas es la certificación CISA realizada por ISACA desde 1978 tiene un gran prestigio. Por lo que todos los miembros del departamento deberían tener esta certificación.

Otras certificaciones relacionadas serian:

- CIA: promovida por el IIA (The Institute of Internal Auditors), que tiene gran reconocimiento para los profesionales de auditoría interna.
- CISSP: promovida por ISC y relacionada con la seguridad de los sistemas de información.
- CISM: promovida por ISACA y también relacionada con la seguridad de los sistemas de información.
- La relacionada con los estándares ISO o británicos de seguridad de la información.

4. La protección de datos.

* Partes extraídas de [APDCM] y [CURSO] desarrolladas por el autor del PFC.

4.1 ¿Qué es un dato personal?

Un dato de carácter personal se define como toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable.

Por lo tanto, datos como el correo electrónico, nombre o apellidos, matrícula de un coche, datos biométricos, estudios, trabajo, enfermedades, etc. son datos personales puesto que permiten identificar a la persona.

Sólo los datos de personas físicas, y no los datos de personas jurídicas, como empresas, sociedades, instituciones, etc. se consideran datos de carácter personal.

Así mismo, los datos de carácter personal pueden hacer referencia a datos inherentes a la persona o datos de carácter personal asociados a la evolución de la misma o a la percepción de la sociedad sobre la misma.(Ej: Nacimiento y raza, sufrimiento y salud, desarrollo y académicos e ideología, etc).

4.2 ¿Qué es la protección de datos?

Es el derecho que tienen todos los ciudadanos a que sus datos personales no sean utilizados por parte de terceros sin la autorización debida.

Es un derecho fundamental consistente en el ejercicio de control por parte del titular de los datos sobre quién, cómo, para qué, dónde y cuándo son tratados los datos relativos a su persona. Este control se hace efectivo a su vez a través del ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Junto con el derecho fundamental al honor, la intimidad personal y familiar y la propia imagen, a la inviolabilidad del domicilio y al secreto de la correspondencia y las telecomunicaciones, su carácter de derecho fundamental, viene determinado por su ubicación en la Constitución Española (artículo 18.4) que dice:

"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"

Ante un masivo uso de la informática, el legislador constitucional advirtió el riesgo que el desarrollo de estos medios podría suponer para los derechos de la intimidad de las personas.

El desarrollo legislativo del mandato constitucional ha dado lugar a la creación de un derecho específico a la protección de datos que también ha sido desarrollado en el ámbito europeo.

4.3 La Ley de protección de datos en España

La Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, (LOPD), es una Ley Orgánica española que tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar.

Su objetivo principal es regular el tratamiento de los datos y ficheros, de carácter personal, independientemente del soporte en el cual sean tratados, los derechos de los ciudadanos sobre ellos y las obligaciones de aquellos que los crean o tratan.

El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal comparte con la Ley Orgánica la finalidad de hacer frente a los riesgos que pueden suponer el acopio y tratamiento de datos personales.

Esta norma reglamentaria desarrolla los mandatos contenidos en la Ley Orgánica de acuerdo con los principios que emanan de la Directiva y también los puntos que en los años de vigencia de la Ley se ha demostrado que precisan de un mayor desarrollo normativo dotando una mayor precisión que a su vez le aporta una seguridad jurídica.

4.4 Principios de la protección de datos

Los datos de carácter personal que se recaben deben seguir un principio de calidad de los mismos basado en:

- **Finalidad:** No podrán usarse para finalidades distintas a las que consintió el afectado.
- **Proporcionalidad:** Deben ser los necesarios, o sea, adecuados, pertinentes y no excesivos conforme a la finalidad para la que se hayan recabado.
- **Transparencia:** Nunca serán recogidos o conseguidos por medios fraudulentos o ilícitos.

- **Veracidad:** Los datos deberán ser exactos, en caso contrario deberán ser destruidos.
- **Actualización:** Los datos deberán ser actuales y ser actualizados periódicamente.
- **Limitación temporal:** Los datos deberán ser eliminados cuando dejen de ser necesarios.

A continuación se describen de forma sintetizada el resto de principios relacionados con la protección de datos:

- **Derecho de información**: Se debe informar al interesado de la existencia del fichero, la finalidad, los posibles destinatarios, los derechos ARCO y los datos del responsable del fichero.
- **Consentimiento del afectado:** El consentimiento se debe recabar siempre de forma legal, según el tipo de datos será inequívoco, expreso o escrito y el afectado puede revocarlo en cualquier momento.
- **Seguridad de los datos:** Se deberán adoptar las medidas de índole técnica y organizativa para garantizar la seguridad de los datos, evitando los casos en los que no podamos garantizarlas.
- **Deber de secreto:** Los implicados en el tratamiento de datos deberán mantener el secreto sobre los mismos, obligación que subsistirá aun finalizada la relación contractual.
- **Comunicación de datos:** Los datos sólo podrán comunicarse con fines relacionados con las funciones legítimas del cedente y cesionario previo consentimiento del afectado.

- **Acceso por cuenta de terceros:** El tratamiento por cuenta de terceros deberá estar regulado por un contrato en el cual se indique el fin y las restricciones de utilización de los datos.

4.5 Derechos del titular de los datos (Derechos ARCO)

Derecho de consulta al Registro General de Protección de Datos

Cualquier persona podrá conocer, recabando a tal fin información oportuna del Registro General de Protección de Datos, en consulta pública y gratuita:

- Existencia del fichero o tratamiento.
- Identidad del responsable del fichero.
- Finalidad de los datos recogidos.

La Agencia Española de Protección de Datos en ningún caso dispone de los datos personales que son objeto de tratamiento. Únicamente dispone de los datos que describen el tratamiento que se está efectuando y la identidad de los mismos.

Los derechos ARCO son el conjunto de derechos a través de los cuales la LOPD garantiza a las personas el poder de control sobre sus datos personales, emanando dichos aspectos del derecho fundamental.

Derecho de acceso

El afectado tiene derecho a solicitar y obtener información de sus datos de carácter personal incluidos en ficheros automatizados y, en este sentido, el interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento. Plazo de contestación: 30 días.

Derecho de rectificación

El afectado tiene derecho a la rectificación y cancelación de los datos de carácter personal que obren en los ficheros de la Organización, en particular, si los mismos son inexactos o incompletos, inadecuados o excesivos, pudiendo solicitar éste la rectificación o, en su caso, la cancelación de los mismos. Plazo de contestación: 30 días.

Derecho de cancelación

El afectado tiene el derecho a la cancelación de los datos de carácter personal que obren en los ficheros de la Organización, en particular, si los mismos son inexactos o incompletos, inadecuados o excesivos, pudiendo solicitar éste la rectificación o, en su caso, la cancelación de los mismos.

- Plazo de contestación: 10 días.
- La solicitud sólo podrá ser denegada cuando la haga una persona distinta del titular de los datos, por lo que es necesario aportar fotocopia del D.N.I.
- Si la cancelación es denegada, también se notificará al interesado la negativa y el motivo.
- Se remitirá por un medio que nos permita acreditar el envío y la recepción, la información a la dirección indicada por el interesado en el plazo de 10 días.

Derecho de oposición

Cuando el consentimiento no sea necesario para el tratamiento, el titular de los datos puede oponerse al mismo (Ej. datos recabados fuentes accesibles al público).

- Plazo de contestación: 30 días.
- La solicitud sólo podrá ser denegada cuando la haga una persona distinta del titular de los datos, por lo que es necesario aportar fotocopia del D.N.I.
- Si la cancelación es denegada, también se notificará al interesado la negativa y el motivo.
- Se remitirá por un medio que nos permita acreditar el envío y la recepción, la información a la dirección indicada por el interesado en **el plazo de 30 días.**

4.6 ¿Cuáles son los riesgos de no cumplir la ley de protección de datos?

Imagen / Reputación: Las incidencias relacionadas con protección de datos están a la orden del día en los medios de comunicación, por lo que cualquier descuido puede acabar en conocimiento de nuestros clientes provocando un impacto en la reputación de la organización provocándole graves consecuencias.

Sobrecostes / Ineficiencias: Ante cualquier duda o incidencia, el no estar preparados puede suponer unos sobrecostes elevados en materia de adecuación, atención a los clientes, atención a los fuerzas y cuerpos del Estado, etc.

Legales/Sanciones: Vulneración de derechos de clientes, empleados y proveedores. El incumplimiento de la normativa vigente en materia de protección de datos puede acarrear sanciones económicas de hasta 600.000€ y según la gravedad y ley infringida, incluso penas privativas de la libertad.

Es importante entender el concepto debido a que la legislación no limita qué tipo de información tengamos, sino que impone las medidas a adoptar para protegerla adecuadamente. Así mismo, la materia a tratar es la protección de datos de carácter personal, y es por ello que cualquier información no personal, por muy sensible que sea para la Organización, no entra en el alcance de la mencionada normativa.

4.7 Marco jurídico actual de la protección de datos.

A nivel europeo:

En el Convenio 108 del Consejo de Europa y en la Directiva 95/46/CE se recoge que:

- Los sistemas de tratamiento de datos deben respetar las libertades y derechos fundamentales de las personas físicas.
- Las legislaciones nacionales relativas al tratamiento de datos personales tienen por objeto garantizar el respeto de estos derechos asegurando un alto nivel de protección.
- Un elemento esencial para la protección es la creación de una autoridad de control que ejerza sus funciones con plena independencia en cada uno de los estados miembros.

En España:

- La Ley Orgánica 15/1999 de 13 de diciembre regula la protección de datos de carácter personal y los aspectos básicos del régimen jurídico de la Agencia Española de Protección de Datos.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Normativas, resoluciones e instrucciones complementarias publicadas por la Agencia Española de Protección de Datos.
- Normativa Autonómica de Protección de Datos (Cataluña y País Vasco).
- Normativas sectoriales (sanidad, finanzas, electoral, materias clasificadas, etc.).

De forma complementaria a la ley y a los reglamentos, la AEPD publica puntualmente instrucciones y resoluciones, las cuales tienen por objetivo aclarar temas que han suscitado muchas consultas.

Por otro lado, la AEPD emite también informes jurídicos y guías de recomendaciones, así como todas las resoluciones que se van produciendo, de modo que toda persona interesada tenga acceso a este material y pueda ser utilizado por parte, tanto de organizaciones que quieran alinearse con la normativa, como para ciudadanos que tengan inquietudes sobre el tema.

En algunas autonomías:

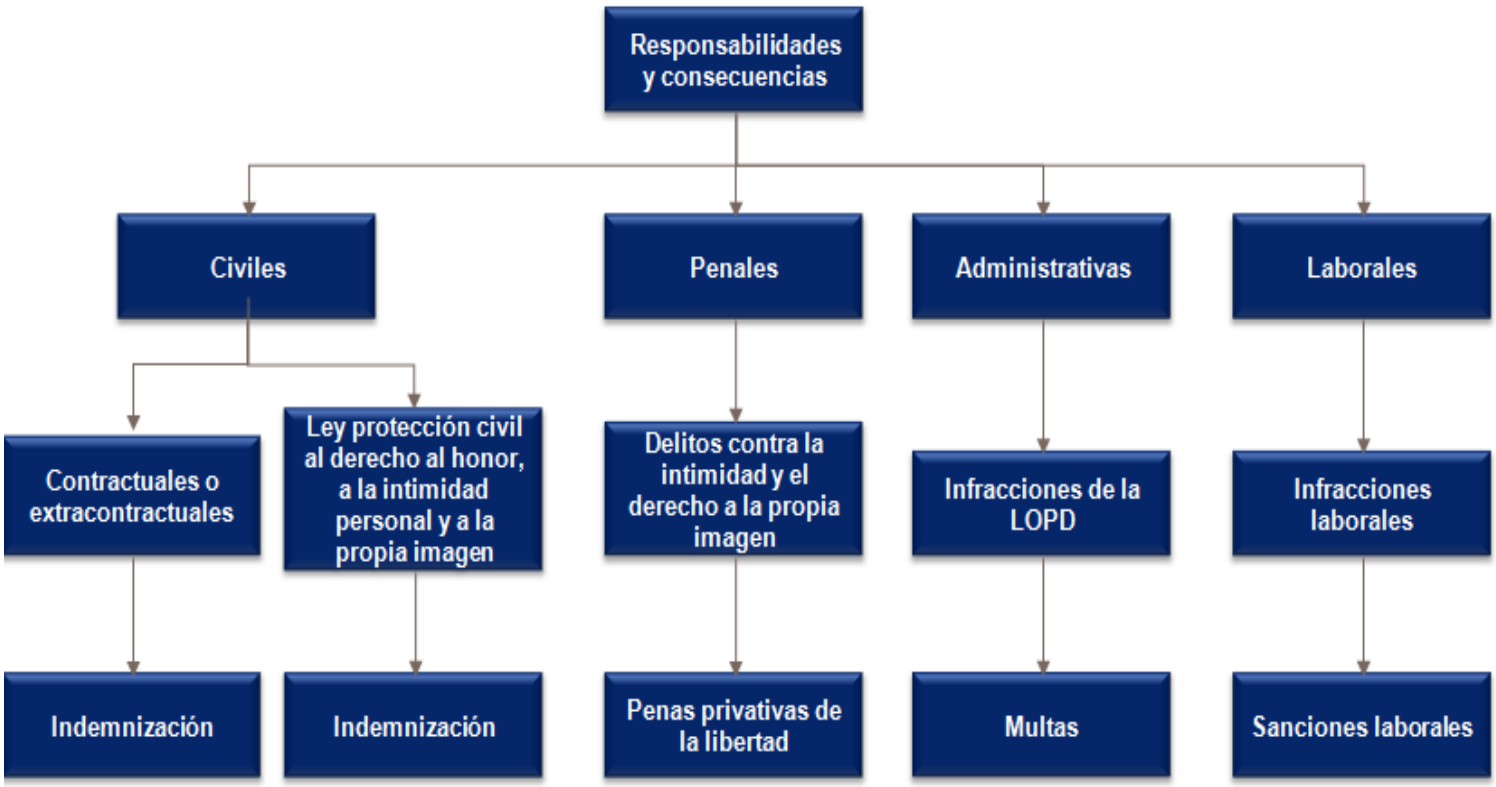
En algunas de las comunidades autonómicas que componen el Estado Español se han transferido las competencias en materia de protección de datos, básicamente orientados a los ficheros de titularidad pública, y es por ello que se han creado distintas agencias locales, las cuales han creado normativa propia, concretamente:

- Ley 5/2002 (Comunidad Autónoma de Cataluña), de 19 de abril, de la Agencia Catalana de Protección de Datos.
- Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.

4.8 Infracciones y sanciones

El incumplimiento de las directrices en materia de protección de datos puede acarrear tres tipologías de infracciones y en consecuencia responsabilidades:

Del incumplimiento de la normativa vigente en materia de Protección de Datos Personales se derivan una serie de conductas tipificadas como infracciones, las cuales sólo son recurribles ante la Audiencia Nacional.



Las infracciones llevan aparejadas un régimen de sanciones que, en el caso de ficheros de titularidad privada, se traducen en multas que pueden oscilar entre las siguientes cantidades:

- Infracciones leves: Multa de 900€ a 40.000€
- Infracciones graves: Multa de 40.001€ a 300.000€
- Infracciones muy graves: Multa de 300.001€ a 600.000€ e incluso inmovilización de ficheros

Dentro de los rangos de las sanciones, la propia Agencia Española de Protección de Datos valora con qué cantidad sancionar, dependiendo de la reincidencia de la empresa, de la valoración de las acciones actuales para el cumplimiento de la LOPD, del grado de concienciación de su personal, etc.

A continuación se detallan algunas de las infracciones así como la clasificación que les ha ido dando la AEPD a las mismas en las diferentes sentencias:

Leves:

- No atender por motivos formales solicitudes de rectificación o cancelación
- No proporcionar la información requerida por la AEPD
- No inscribir ficheros en el Registro General de Protección de Datos
- No cumplir el deber de información
- Vulnerar el deber de secreto

Graves:

- No recabar el consentimiento de los titulares

- Mantener datos inexactos
- No aplicar las medidas de seguridad correspondientes
- Obstrucción a la labor inspectora

Muy graves:

- Recogida de datos de forma engañosa
- Comunicación de datos sin requisitos legales
- Tratar datos de nivel alto sin consentimiento expreso / escrito

Así mismo, de forma relacionada con el incumplimiento de la LOPD, se puede incurrir en infracciones recogidas en el código penal, por ejemplo, el incumplimiento del siguiente articulado:

- Artículo 197: Penas de prisión de 1 a 4 años al que, con el fin de descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico, o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones, etc.
- Artículo 199: El que revele secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de 1 a 3 años y multa de 6 a 12 meses.
- Artículo 278: El que sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Quien acceda, sin estar autorizado por cualquier

medio a los mismos y los altere o utilice en perjuicio del titular de los datos o de un tercero.

En consecuencia, no sólo hay una exposición a sanciones administrativas, sino que además el incumplimiento puede acarrear penas de prisión.

4.9 Entidades de control

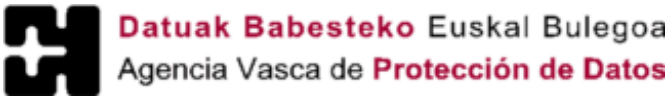
La Agencia Española de Protección de Datos es la autoridad de control independiente que vela por el cumplimiento de la normativa sobre protección de datos y garantiza y tutela el derecho fundamental a la protección de datos de carácter personal.

Las principales funciones de la agencia son:

- Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.
- Atender a peticiones y reclamaciones de afectados, así como informar de sus derechos y promover campañas de difusión en medios.
- Ordenar, en caso de ilegalidad, el cese en el tratamiento y la cancelación de los datos y requerir medidas de corrección.
- Ejercer la potestad sancionadora ante quienes tratan datos.
- Dictar instrucciones y recomendaciones de adecuación de los tratamientos a la LOPD.


AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS


apdcat
Agència Catalana de Protecció de Dades


Datuak Babesteko Euskal Bulegoa
Agencia Vasca de Protección de Datos

5. Definición de los controles realizados para su auditoría y el cumplimiento de la ley vigente.

Tratamiento automatizado

Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico: Título VIII, Capítulo III, Sección 1ª.

Nivel Medio: Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, Título VIII, Capítulo III, Sección 2ª.

Nivel Alto: Además de las medidas de nivel básico y medio, se aplicarán las medidas de seguridad de nivel alto, Título VIII, Capítulo III, Sección 3ª.

5.1. Niveles de seguridad y ficheros

La legislación establece tres niveles de seguridad:

Básico: aplicable a todos los ficheros que contengan datos de carácter personal.
Medio: aplicable a los ficheros que contengan datos económicos de una persona física.
Alto: aplicable a los ficheros que traten datos de carácter personal y contengan información sobre ideología, religión, creencias, afiliación sindical, origen racial, salud, vida sexual o con fines policiales.

La declaración de los ficheros debe ser actualizada y con el nivel de seguridad correcto.

AREA	NIVEL	PREGUNTA	CUMPL.	OBSERVACION	RECOMENDACIÓN
Niveles de Seguridad y Ficheros	B	¿Está el fichero declarado?			
	B	¿La declaración del nivel de seguridad es el correcto?			
	B	¿La declaración del sistema de tratamiento es el correcto?			
	B	¿Se ha detectado algún nuevo fichero?			

5.2 Encargado de tratamiento

El RD 1720/2007 establece que en el caso que el Responsable de Fichero facilite el acceso a datos a un Encargado de Tratamiento, éste deberá constar en el Documento de Seguridad e indicar el fichero o tratamiento que éste realiza.

AREA	NIVEL	PREGUNTA	CUMPL.	OBSERVACION	RECOMENDACIÓN
Encargado de Tratamiento	B	¿Se realiza el tratamiento por una persona distinta al responsable del fichero y consta en el documento de seguridad?			
	B	¿Todos los encargados de tratamiento tienen contrato en vigor?			
	B	Si la empresa es Encargada de Tratamiento de algún tercero, ¿Hace referencia a los ficheros que trata en concepto de Encargado de Tratamiento?			

5.3 Prestación de servicios sin acceso a datos

El RD 1720/2007 establece que, en caso que exista personal que tenga acceso a soportes o recursos sin que tenga que efectuar un tratamiento, se tomen las medidas para limitar el acceso (caso de personal externo el contrato deberá incluir la prohibición y la obligación de secreto).

AREA	NIVEL	PREGUNTA	CUMPL.	OBSERVACION	RECOMENDACIÓN
Prestación sin acceso a datos	B	¿Están identificados todos prestadores sin acceso a datos?			
	B	En caso que los prestadores tengan acceso a soportes o recursos sin necesidad de tratamiento, ¿Se aplican medidas para limitar el acceso?			
	B	¿Recoge el contrato la prohibición expresa de acceder a los datos personales, así como la obligación de secreto respecto a los datos que hubieran podido conocer con motivo de la prestación de servicio?			

5.4 Delegación de autorizaciones

El RD 1720/2007 establece que en el caso que el Responsable del Fichero delegue a otras personas la facultad de autorizar acceso al fichero, estas autorizaciones deberán constar en el Documento de Seguridad.

AREA	NIVEL	PREGUNTA	CUMPL.	OBSERVACION	RECOMENDACIÓN
Delegación de autorizaciones	B	¿Se han delegado las autorizaciones que el Reglamento atribuye al responsable en otras personas?¿Se ha hecho constar en el Documento de Seguridad las personas habilitadas para otorgar estas autorizaciones y las personas en quienes recae dicha delegación?			

5.5 Acceso a través de redes de comunicaciones

El RD 1720/2007 establece que las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

AREA	NIVEL	PREGUNTA	CUMPL.	OBSERVACION	RECOMENDACIÓN
Acceso a datos a través de redes	B	En el caso de que existan accesos a datos mediante redes externas, ¿Se garantiza el mismo nivel de protección como si el acceso se realizara de forma local?			

5.6 Régimen de trabajo fuera de los locales

El RD 1720/2007 establece que 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. Dicha autorización tendrá que constar en el documento de seguridad.

AREA	NIVEL	PREGUNTA	CUMPL.	OBSERVACION	RECOMENDACIÓN
Régimen de trabajo fuera de los locales	B	En caso que los datos se guarden en dispositivos portátiles (portátiles, USB, smartphones...) ¿Se garantiza el nivel de seguridad adecuado en función del nivel del fichero original?			
	B	¿Existe una autorización previa del responsable del fichero o tratamiento, que habilita el uso de dispositivos portátiles?¿Consta en el documento de seguridad?			

5.7 Ficheros temporales

El RD 1720/2007 establece que aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda.

Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

AREA	NIVEL	PREGUNTA	CUMPL.	OBSERVACION	RECOMENDACIÓN
Ficheros temporales	B	Preguntar si de alguno de los ficheros auditados se extraen copias o subficheros que temporalmente estén en otra ubicación distinta a la auditada y saber el nivel de esa subcopia. Si se extraen verificar que cumplen con el nivel de seguridad correspondiente y que se destruyen o borran cuando dejan de ser necesarios.			

5.8 Documento de Seguridad

El RD 1720/2007 establece que el responsable del fichero o tratamiento deberá elaborar un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente, de obligado cumplimiento para el personal con acceso a los sistemas de la información.

El citado documento deberá mantenerse actualizado en todo momento y revisado cuando se produzcan cambios relevantes en los sistemas de información.

AREA	NIVEL	PREGUNTA	CUMPL.	OBSERVACION	RECOMENDACIÓN
	B	¿Existe un Documento de Seguridad actualizado y adecuado a la normativa vigente? El DS puede ser único o individualizado para cada fichero o tratamiento. También podrán agruparse ficheros o tratamientos según el sistema de tratamiento utilizado.			
	B	¿El Documento de Seguridad está accesible a todo el personal con acceso a datos de carácter personal y a los sistemas de Información?			
	B	En caso de que algún tratamiento se realice fuera de los locales de la Organización, ¿se hace constar en el DS?			
	B	¿El DS está actualizado?			
	B	¿El DS describe el ámbito de aplicación?			
	B	El DS contiene las normas, procedimientos, reglas, etc. Encaminados a garantizar el nivel de seguridad exigido por el reglamento?			
	B	¿El DS contiene las funciones y obligaciones del personal con acceso a datos de carácter personal?			
	B	¿Existe un detalle de las funciones o controles delegados por el Responsable de fichero o tratamiento?			

Documento de Seguridad	B	¿Existe un detalle de la estructura de ficheros con datos de carácter personal?			
	B	¿El DS describe los sistemas que tratan cada uno de los ficheros con datos de carácter personal?			
	B	¿El DS contiene un procedimiento de notificación, gestión y respuesta a incidencias?			
	B	¿El DS contiene un procedimiento de Backup y recuperación de datos?			
	B	¿El DS describe las medidas necesarias para el transporte de soportes y documentos así como la destrucción o reutilización de éstos?			
	B	El listado de Encargados de Tratamiento tiene que incluir los ficheros sujetos a tratamiento pero que son responsabilidad de terceros. El listado tiene que contener: - Identificación del fichero o tratamiento - Referencia al Contrato - Identificación del responsable - Periodo de vigencia del contrato			
	B	¿El DS describe la relación de administradores (personal autorizado a conceder/alterar/anular permisos de acceso a datos)?			
	B	¿El DS describe la relación de personal autorizado a acceder a los soportes que contienen datos personales (almacenamiento en lugar seguro)?			
	B	Se hace constatar la autorización del uso de dispositivos portátiles en el Documento de Seguridad?			
	B	¿Existe en el DS un listado de personal autorizado a conceder, alterar o anular el acceso autorizado a los datos? (Administradores de autorizaciones de acceso)			
	B	¿El responsable de fichero autoriza las salidas de soportes de datos fuera de las instalaciones? (Considerando también los anexos en los correos)			
	B	¿Se aplican medidas para el transporte de soportes y documentos?			
	M	¿El DS describe la relación de controles periódicos de verificación del cumplimiento del propio DS?. Pedir evidencia de que se realizan estos controles y que se ajustan al reglamento.			

	M	¿El DS contiene la relación de personal autorizado a acceder a los locales donde se ubican los equipos que soportan los Sistemas de Información?			
	A	¿Se describen las técnicas de cifrado utilizadas en los dispositivos portátiles en el Documento de Seguridad?			
	A	¿Se describen las técnicas utilizadas para evitar el tratamiento de datos personales en dispositivos que no admiten cifrado? ¿Se hacen referencia a éstas medidas en el DS?			

5.9 Funciones y obligaciones del personal

El RD 1720/2007 establece que las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información deberán estar claramente definidas y documentadas en el documento de seguridad. También se deberán definir las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

AREA	NIVEL	PREGUNTA	CUMPL.	OBSERVACION	RECOMENDACIÓN
Funciones y obligaciones del personal	B	¿Se realiza divulgación, se dan a conocer las normas de seguridad al personal con acceso a datos? Preguntar a varias personas al azar			
	B	Comprobar que aparecen las funciones y obligaciones de forma documentada y bien definidas (responsable de seguridad, responsable del fichero, usuarios finales, usuarios de informática, etc.) en el Documento de Seguridad ¿El personal conoce las conscuencias del incumplimiento de las normas de seguridad?			

5.10 Gestión y registro de incidencias

El RD 1720/2007 establece la obligación de disponer de un procedimiento formal de notificación y gestión de incidencias que afecten a los datos de carácter personal, y establece un registro en el que se haga constar el tipo de incidencia, el momento en el que se produzca, o en su caso, detectada, la persona que realiza la notificación, a quien se le comunica, los efectos que se hayan derivado de la misma y las medidas correctoras aplicables.

Datos de nivel medio: En el registro deberán consignarse los procedimientos realizados en la recuperación de los datos, indicando quien lo ejecutó, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

AREA	NIVEL	PREGUNTA	CUMPL.	OBSERVACION	RECOMENDACIÓN
Gestión y Registro de Incidencias	B	¿Existe un procedimiento de notificación y gestión de incidencias en el que esten registradas todas las incidencias producidas (copias de seguridad, intentos fallidos a las aplicaciones, gestión de soportes, etc.)? ¿Conoce todo el personal afectado dicho procedimiento?			
	B	¿Aparecen en el registro los siguientes datos: Tipo de incidencia, momento en el que se produjo la incidencia, persona que realiza la notificación, a quién se le comunica y efectos derivados de la misma (así como las medidas correctoras aplicadas)?			
	M	¿El registro incluye los datos relativos a la recuperación? (indicando persona que realiza la restauración, Datos restaurados y si ha sido necesaria la grabación manual en el proceso de restauración)			
	M	¿El responsable del fichero autoriza la ejecución de los procedimientos de recuperación de datos?			

5.11 Control de Acceso e Identificación y autenticación

El RD 1720/2007 establece la obligación de que los usuarios solamente tengan acceso a aquellos recursos que necesitan para el desarrollo de sus funciones, manteniendo una relación actualizada de usuarios y perfiles así como los accesos autorizados para cada uno de ellos.

Se establece que se deberán aplicar las medidas adecuadas para garantizar la correcta identificación y autenticación de los usuarios. Es necesario adoptar mecanismos que permitan la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

En el caso de uso de contraseñas como mecanismo de autenticación, tiene que existir un procedimiento de asignación, distribución y almacenamiento que garantice la confidencialidad e integridad. Las contraseñas deberán ser cambiadas con cierta periodicidad, no superior a 1 año, y mientras estén en uso se almacenarán de forma ininteligible o no accesible.

Sólo con datos de nivel medio: El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

AREA	NIVEL	PREGUNTA	CUMPL.	OBSERVACION	RECOMENDACIÓN
Control de Acceso	B	¿Existe una relación actualizada de usuarios con acceso a a datos, que incluya los accesos autorizados a cada uno de ellos?			
	B	¿Esiste un control de accesos a datos y recursos? ¿Son razonables dichos accesos?			
Identificación y Autenticación	B	¿Existe un procedimiento de identificación y autenticación?			
	B	¿Existe un procedimiento para identificar a los usuarios de forma inequívoca y personalizada? Controlar adjudicación de usuarios genéricos.			
	B	¿Existe un procedimiento de asignación, distribución segura y almacenamiento de las contraseñas que garantice su confidencialidad e integridad?			
	B	¿Cuál es la política de contraseñas? (caducidad, longitud mínima, intentos de acceso fallidos, número de contraseñas anteriores válidas, lugar y forma de almacenamiento de las contraseñas, te pide cambiar la contraseña la primera vez que te logues, etc.			
	B	¿Las contraseñas se almacenan cifradas?			
	M	¿Están limitados el numero de accesos no autorizados? (Bloqueo por reintentos)			

5.12 Gestión de soportes y documentos

El RD 1720/2007 establece que deberá existir un sistema de gestión de soportes y documentos que permita identificar el tipo de información que contiene, ser inventariados y accesibles solamente por el personal autorizado en el Documento de Seguridad.

Sólo con datos de nivel medio: El RD dispone, además de lo establecido anteriormente, que para la gestión de soportes hay que tener presente la necesidad de establecer un registro de entrada y salida de soportes, que permita controlar los tipos de soporte o documento del que se trata, la fecha y hora, el emisor y destinatario, el numero de soportes o documentos del envío o el tipo de información que contienen, la forma de envío y la persona responsable de la recepción.

Sólo con datos de nivel alto: Para ficheros de nivel alto, es necesario aplicar sistemas de etiquetado comprensibles, así como aplicar técnicas de cifrado en la distribución de soportes o cuando éstos se utilicen en dispositivos portátiles.

AREA	NIVEL	PREGUNTA	CUMPL.	OBSERVACION	RECOMENDACIÓN
Gestión de Soportes y Documentos	B	¿Los soportes de datos están identificados, inventariados y almacenados en lugar seguro?			
	B	¿El acceso a los soportes y documentos está restringido únicamente a personal autorizado? ¿Se especifican en el Documento de Seguridad las personas autorizadas para acceder al lugar donde se encuentran almacenadas las copias de seguridad?			
	B	¿Se aplican medidas para impedir cualquier recuperación posterior de la información en soportes que vayas a ser destruidos o reutilizados? (Borrado destrucción de Soportes)			
	B	¿Existe medidas para evitar la sustracción, pérdida o acceso indebido durante el traslado de la documentación?			
	B	¿Se hace referencia en las funciones y obligaciones a la medidas a aplicar en el borrado/destrucción de soportes?			
	M	¿Existe un registro de Entrada de Soportes?			
	M	¿El registro de Entrada de soportes debe contener: Tipo de Soportes o Documento, fecha y hora de entrada, emisor, número de soportes o documentos, tipo de información que contiene, forma de envío, persona receptora (autorizada por el responsable de fichero).			
	M	¿Existe un registro de Salida de Soportes?			
	M	¿El registro de Salida de soportes debe contener: Tipo de Soportes o Documento, fecha y hora de salida, destinatario, número de soportes o documentos, tipo de información que contiene, forma de envío, persona responsable de la entrega.			
	M	El personal responsable de la entrega (Salidas) de soportes están debidamente autorizados?			
	A	¿Se aplican técnicas de identificación de los soportes utilizando sistemas de etiquetado que permitan a los usuarios autorizados identificar su contenido, pero que sea ininteligible para el resto de personas			
	A	¿Se aplican técnicas de cifrado en la distribución de soportes, o algún mecanismo que garantice la confidencialidad?			
	A	¿Se aplican técnicas de cifrado a los dispositivos portátiles si se encuentran fuera de las instalaciones que controla esl responsable de fichero?			

5.13 Copias de respaldo y recuperación

El RD 1720/2007 determina las pautas del procedimiento a seguir respecto a las Copias de seguridad y de la recuperación de la información a partir de éstas. Por otro lado, establece que la realización de copias se deberá realizar con una periodicidad mínima semanal y efectuar pruebas de restauración semestrales. En caso que lleven a cabo pruebas para tareas de desarrollo no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado

Sólo con datos de nivel alto: En caso de copias de Seguridad con datos de nivel alto, será necesario conservar una copia de respaldo y los procedimientos de recuperación en un lugar diferente al que se encuentran los equipos informáticos.

AREA	NIVEL	PREGUNTA	CUMPL.	OBSERVACION	RECOMENDACIÓN
Copias de respaldo y recuperación	B	¿Existe un procedimiento de backup y recuperación de datos?			
	B	¿Se realizan copias mínimo semanalmente?			
	B	¿Los procedimientos de recuperación garantizan que los datos se restauran correctamente? (Se revisan los logs de las copias de seguridad)			
	B	¿Se realizan pruebas de la correcta restauracion y copia con una periodicidad mínima semestral?			
	B	¿Se deja registro de las pruebas de restauracion y copia?			
	B	¿Se garantiza que las pruebas en los entornos de test se realizan sin datos reales? ¿Se disocian los datos?			
	A	¿Las copias de seguridad y el procedimiento de recuperación se externalizan?			

5.14 Responsable de Seguridad

Sólo nivel medio: El RD 1720/2007 determina que en el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad. En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

AREA	NIVEL	PREGUNTA	CUMPL.	OBSERVACION	RECOMENDACIÓN
Responsable de Seguridad	M	¿El Responsable de Seguridad está claramante identificado y designado en el DS?			

5.15 Auditoría

El RD 1720/2007 establece que los sistemas de información e instalaciones donde se almacenen y traten datos de carácter personal, tienen que someterse al menos cada dos años a una auditoría que verifique el cumplimiento de las medidas de seguridad. Además se deberá realizar una auditoría cuando se produzcan modificaciones en los sistemas de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas.

AREA	NIVEL	PREGUNTA	CUMPL.	OBSERVACION	RECOMENDACIÓN
Auditoría	M	¿Se realizan Auditorias de Cumplimiento Bianual de los sistemas de información y de las instalaciones de Tratamiento de los datos? NOTA: En caso de modificación que afecte a los Sistemas de Información del fichero, será necesario realizar una auditoria extraordinaria sin esperar a los 2 años.			

5.16 Control de acceso físico

Nivel medio: El RD 1720/2007 establece que 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.

AREA	NIVEL	PREGUNTA	CUMPL.	OBSERVACION	RECOMENDACIÓN
Control de Acceso físico	M	¿Existe un Control de acceso físico al CPD?			
	M	¿Existe un listado de usuarios con acceso autorizado al CPD?			

5.17 Registro de accesos

Nivel Alto: El RD 1720/2007 regula los datos a almacenar de cada intento de acceso a los sistemas de información con datos sensibles. Como mínimo hay que almacenar la identificación del usuario, la fecha y hora de accesos, el fichero accedido, el tipo de acceso y se ha autorizado o denegado. En el caso de los accesos autorizados, se deberá almacenar la información que permita identificar el registro accedido.

AREA	NIVEL	PREGUNTA	CUMPL.	OBSERVACION	RECOMENDACIÓN
Registro de Accesos	A	¿Existe un Registro de Accesos lógico? Debe incluir al menos los siguientes datos: identificación del usuario, la fecha y hora de accesos, el fichero accedido, el tipo de acceso y se ha autorizado o denegado			
	A	¿El Registro de accesos tiene una retención mínima de 2 años?			

5.18 Telecomunicaciones

Nivel alto: El RD 1720/2007 establece que las transmisiones de ficheros de nivel alto a través de redes públicas o inalámbricas de comunicaciones se deberán realizar cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

AREA	NIVELL	PREGUNTA	CUMPL.	OBSERVACION	RECOMENDACIÓN
Telecomunicaciones	A	¿Se cifran los datos que circulan por redes de telecomunicaciones?			

Tratamiento no automatizado

Áreas a auditar tanto en automatizado y no automatizado (descritas anteriormente en la parte de automatizado):

- Encargado de tratamiento
- Prestación de servicios sin acceso a datos
- Delegación de autorizaciones
- Funciones y obligaciones del personal
- Gestión y registro de incidencias
- Control de acceso
- Gestión de soportes y documentos
- Responsable de Seguridad
- Auditoría
- Documento de Seguridad
- Régimen de trabajo fuera de los locales

Áreas a auditar exclusivamente en no automatizado:

- Criterios de archivo
- Dispositivos de almacenamiento
- Custodia de soportes
- Almacenamiento

- Copia o reproducción
- Acceso a la documentación
- Traslado de la documentación

5.19 Criterios de archivo

El RD 1720/2007 establece que el archivo de los soportes o documentos se realizará de acuerdo a la legislación específica. Estos criterios deberán garantizar la correcta conservación, localización y consulta de la información y posibilitar el ejercicio de los derechos de Acceso, Rectificación, Cancelación u Oposición. En el caso de no existir norma aplicable, ésta será establecida por el Responsable de Fichero.

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

AREA	NIVEL	PREGUNTA	CUMPL.	OBSERVACIÓN	RECOMENDACIÓN
Criterios de Archivo	B	¿El Responsable de fichero ha establecido los procedimientos y criterios de archivo? (en caso de que no exista legislación especifica)			
	B	¿Existe un procedimiento escrito que describa estos procedimientos?			

5.20 Dispositivos de almacenamiento

El RD 1720/2007 establece que los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura que impidan el acceso de personas no autorizadas.

AREA	NIVEL	PREGUNTA	CUMPL.	OBSERVACIÓN	RECOMENDACIÓN
Dispositivos de almacenamiento	B	¿Los dispositivos que contienen documentos con datos personales tienen mecanismos que obstaculizan la apertura?			
	B	¿Se hace referencia en el DS (o en el criterio de archivo) de las medidas aplicadas para impedir el acceso a personas no autorizadas a los dispositivos de almacenamiento de datos?			

5.21 Custodia de soportes

El RD 1720/2007 establece que la documentación, mientras no se encuentre en sus dispositivos de almacenamiento, será custodiada en todo momento por el personal que se encuentre al cargo de ella, impidiendo el acceso a la misma por personal no autorizado.

AREA	NIVEL	PREGUNTA	CUMPL.	OBSERVACIÓN	RECOMENDACIÓN
Custodia de soportes	B	¿La documentación no archivada, está siempre custodiada?			
	B	¿Existe un procedimiento o una referencia a las funciones y obligaciones del personal donde se haga referencia a la custodia de soportes?			

5.22 Almacenamiento

Nivel alto: El RD 1720/2007 regula para la documentación con datos de carácter personal, que los armarios, archivadores y elementos de almacenaje de los mismos deberán encontrarse en áreas con acceso restringido mediante llave o equivalente.

En caso de no ser posible la aplicación de estas medidas, el responsable adoptará medidas alternativas que, debidamente motivadas, serán incluidas en el Documento de Seguridad.

AREA	NIVEL	PREGUNTA	CUMPL.	OBSERVACIÓN	RECOMENDACIÓN
Almacenamiento	A	¿Los armarios y archivos están ubicados en áreas con acceso protegido mediante llave o dispositivo equivalente?			
	A	¿Estas áreas están cerradas si no es necesario el acceso a la documentación?			
	A	Si los locales del responsable no permiten disponer de un área de acceso restringido ¿ha adoptado el responsable medidas alternativas?, ¿se ha hecho constar esta circunstancia en el Documento de Seguridad?			
	A	¿Se hace referencia en el DS (o criterio de archivo) de las medidas aplicadas respecto al almacenamiento de la información?			

5.23 Copia o reproducción

Nivel alto: El RD 1720/2007 establece que toda copia de los documentos que contengan datos de carácter personal, deberá ser realizada por el personal autorizado en el Documento de Seguridad. Para la destrucción de las copias,

deberán aplicarse mecanismos que eviten el acceso a la información contenida en las mismas.

AREA	NIVEL	PREGUNTA	CUMPL.	OBSERVACIÓN	RECOMENDACIÓN
Copia o reproducción	A	¿Las copias se realizan por el personal autorizado en el DS?			
	A	¿Se destruyen las copias para desechar para evitar el acceso a al información?			
	A	¿Existe un procedimiento o una referencia en las funciones y obligaciones de personal respecto a la copia o reproducción?			

5.24 Acceso a la documentación

Nivel alto: El RD 1720/2007 establece que solamente el personal autorizado disponga de acceso a la documentación. Será necesario establecer mecanismos que permitan identificar los accesos realizados a dichos documentos.

AREA	NIVEL	PREGUNTA	CUMPL.	OBSERVACIÓN	RECOMENDACIÓN
Acceso a la documentación	A	¿Existe un listado en el DS del personal autorizado a acceder a la información?			
	A	¿En el caso de documentos utilizados por múltiples usuarios, existen mecanismos que permitan identificar los accesos realizados y los accesos denegados?			
	A	Existe un procedimiento o una referencia en las funciones y obligaciones del personal donde se haga referencia al acceso a la documentación?			

5.25 Traslado de la documentación

Nivel alto: El RD 1720/2007 establece que para todo traslado de documentación deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la misma.

AREA	NIVEL	PREGUNTA	CUMPL.	OBSERVACIÓN	RECOMENDACIÓN
Traslado de la documentación	A	¿Se adoptan medidas para impedir el acceso o la manipulación de la información cuando sea trasladada físicamente?			
	A	¿Existe un procedimiento o una referencia en las funciones y obligaciones del personal donde se haga referencia al acceso al traslado de documentación?			

6. ¿Qué documentación se solicita de forma general para iniciar una auditoría LOPD?

6.1 Documentación General:

- Organigrama de la empresa
- Documento de Seguridad
- Informe de última Auditoría LOPD
- Declaración de los ficheros ante la Agencia Española de Protección de Datos
- Mapa topológico de red
- Mapa de aplicaciones que gestionan datos personales junto con el listado de usuarios con privilegios de acceso.
- Inventario de HW
- Inventario de SW
- Normativa de uso de Internet y correo electrónico
- Relación de terceros que puedan tener acceso a datos (conjunto de Encargados de Tratamiento)
- Relación de prestadores de servicio sin acceso a datos (limpieza…)
- Protocolo de acceso físico a las instalaciones y al CPD, juntamente con el listado del personal autorizado y el registro de accesos.

6.2 Procedimientos y documentación en el ámbito informático:

- Alta, baja y modificación de usuarios.
- Procedimiento de asignación de privilegios a los sistemas.
- Procedimiento de realización de copias de seguridad y recuperación de datos.
- Procedimiento de Gestión de soportes informáticos (cintas de backup, equipos portátiles, dispositivos USB, etc).
- Políticas de seguridad aplicadas a las contraseñas (caducidad de las contraseñas, longitud mínima, requisitos de complejidad, etc.).
- Procedimiento de Gestión de incidencias informáticas (descripción del procedimiento de resolución, herramienta de gestión utilizada, etc.).
- Listado del personal autorizado para acceso al CPD (sala de servidores).

6.3 Relación de Contratos:

- Contrato tipo con los empleados junto a los anexos de confidencialidad
- Contratos con los diferentes prestadores de Servicios (empresas que hagan desarrollos, hosting y acciones similares relacionadas con sistemas de información)

7. ¿Qué aspectos técnicos podemos controlar en una auditoría LOPD?

En este apartado se muestran diversos ejemplos de controles de aspectos técnicos que podrían darse en una auditoría LOPD. Estos controles pueden ser más o menos complicados según la información conocida y facilitada por la entidad a auditar así como de sus diferentes sistemas operativos, bases de datos, aplicaciones, etc. A continuación se muestran los ejemplos más comunes que se pueden dar al realizar los controles técnicos de la auditoría.

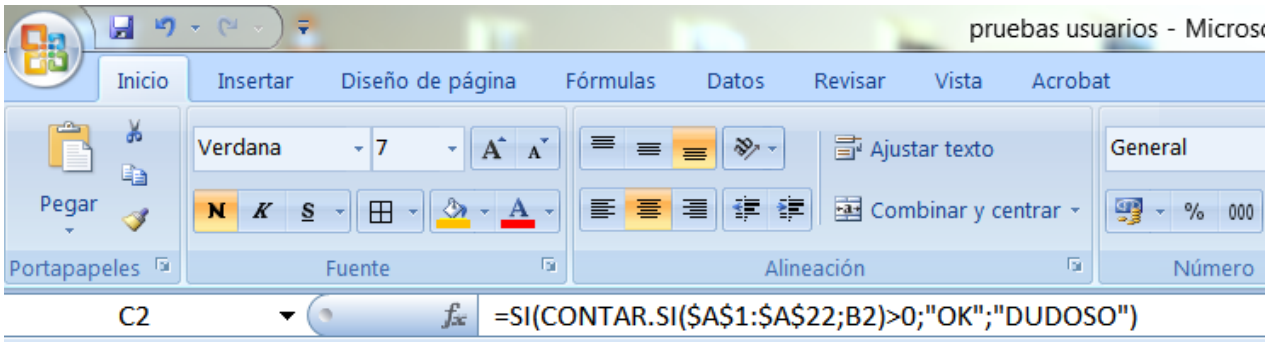
Bases de datos: Uno de los aspectos más importantes que se deben controlar en una auditoría LOPD es la configuración de las bases de datos donde están guardados esos datos. A continuación se detalla la descripción de los distintos campos en una base de datos ORACLE.

Query	Tabla	Comentarios
SELECT * FROM DBA_SYS_PRIVS	Privileges	Comprobar que no existen privilegios de sistema concedidos de carácter público (GRANTEE = 'PUBLIC')
	Privileges	Comprobar los usuarios con capacidad para conceder privilegios (WITH ADMIN o WITH GRANT).
	Privileges	Comprobar que ningún usuario tiene el privilegio SELECT ANY TABLE
	Privileges	Restringir los privilegios de sistema (a excepción de CREATE SESSION), excepto para los DBAs, las cuentas/esquemas de propietarios de aplicación (cuentas bloqueadas) y las cuentas por defecto de Oracle.
	Privileges	Controlar los perfiles con privilegios que contengan la palabra ANY y comprobar la necesidad de aquellos que los contengan, intentando que sean los menos posibles.

Query	Tabla	Comentarios
select * from dba_PROFILES	DBA_PROFILES	Número de intentos consecutivos de acceso fallidos antes de que bloquee la cuenta.
	DBA_PROFILES	Número de días antes de que la contraseña expire y deba cambiarse.
	DBA_PROFILES	Histórico de contraseñas que no pueden reutilizarse.

Query	Tabla	Comentarios
SELECT * FROM DBA_USERS	Users	Comprobar que no existen entradas nulas en la tabla DBA_USERS
	Users	Comprobar que se utilizan diferentes nombres de usuario de sistema operativo y de base de datos - los nombres de usuario no deben tener el prefijo OPS$
	Users	Comprobar los usuarios asignados al perfil default. Oracle asigna este perfil a los que no se les asigne uno implicitamente - tengase en cuenta que "default" tiene todos los parámetros "UNLIMITED".
	Users	Comprobar que los usuarios no están utilizando por defecto el tablespace SYSTEM
	Users	Comprobar que los usuarios no están utilizando como temporary tablespace el SYSTEM
	Users	Se evita en la medida de lo posible la utilización de usuarios genéricos, lo que permite establecer mecanismos de seguimiento y trazabilidad.
	Users	Comprobar que todos los usuarios tienen password
	Users	Comprobar que la password por defecto de las cuentas por defecto ha sido cambiada.
	Users	Comprobar que las cuentas por defecto están bloqueadas

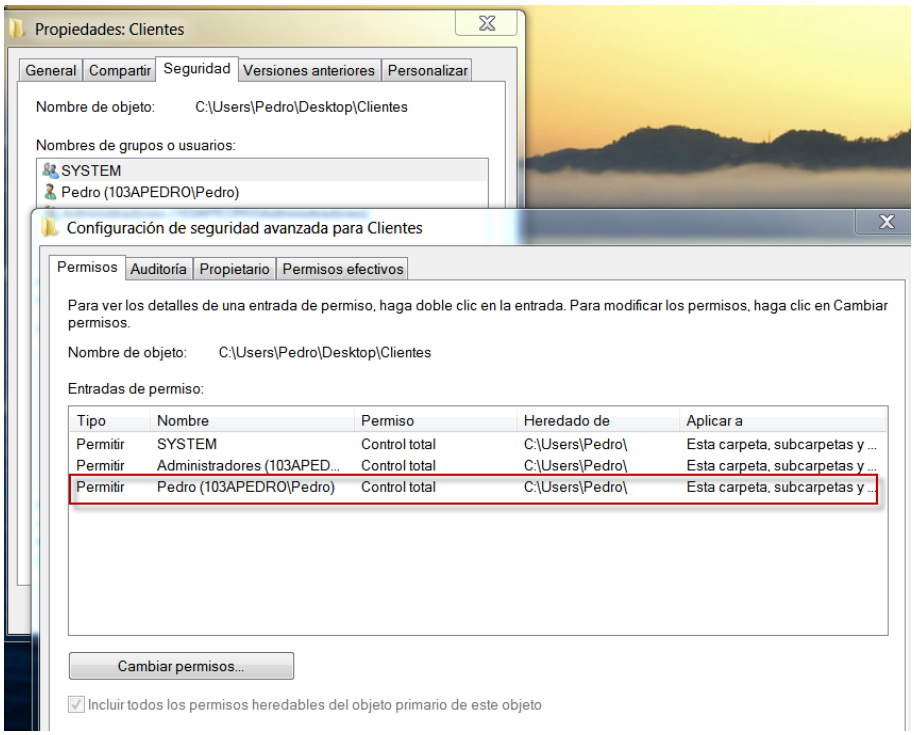
Control de acceso: Por ejemplo si extraemos un listado de usuarios registrados a una aplicación que está utilizando datos de carácter personal. Además de analizar que permisos tiene cada usuario y a que datos puede acceder con cada perfil en la aplicación. Debemos comparar esa lista con una lista de usuarios cuyo último acceso haya sido realizado no hace mucho tiempo para poder encontrar usuarios inactivos que deberían ser dados de baja.



	A	B	C
1	Lista de usuarios registrados en la aplicación	Usuarios con última fecha de acceso reciente	Evaluación
2	ADRIÁN LAVALLE	ADRIANA MENDIZABAL	OK
3	ADRIANA MENDIZABAL	CAMILO ELIZONDO	OK
4	AFRA CUENTAS	BONIFACIO DEL CARRIL	OK
5	AGRIPINA SOLARI	HONORIO VAZQUEZ	OK
6	AGUSTÍN VALVERDE	JORGE GOMEZ	DUDOSO
7	ALBA TARRAGÓS	SHEILA ADRADOS	DUDOSO
8	ALBANO CASARES	DAVID CASADO	DUDOSO
9	HONORIO VAZQUEZ	PEDRO DELGADO	DUDOSO
10	ATILIO MONTREAL	GIL LAVELA	OK
11	BEATRIZ CASTRO	RAUL PEÑA	DUDOSO
12	BENITO GUTIERREZ	ADRIÁN LAVALLE	OK
13	BONIFACIO DEL CARRIL		
14	BRUNO ASCARI		
15	CAMILA TRAVERSO		
16	CAMILO ELIZONDO		
17	CÁNDIDA/DO GONZALEZ		
18	CARIDAD SARMIENTO		
19	CECILIA MNTEAGUDO		
20	GEMA LISANDRO		
21	GIL LAVELA		
22	GLORIA ANDREANI		

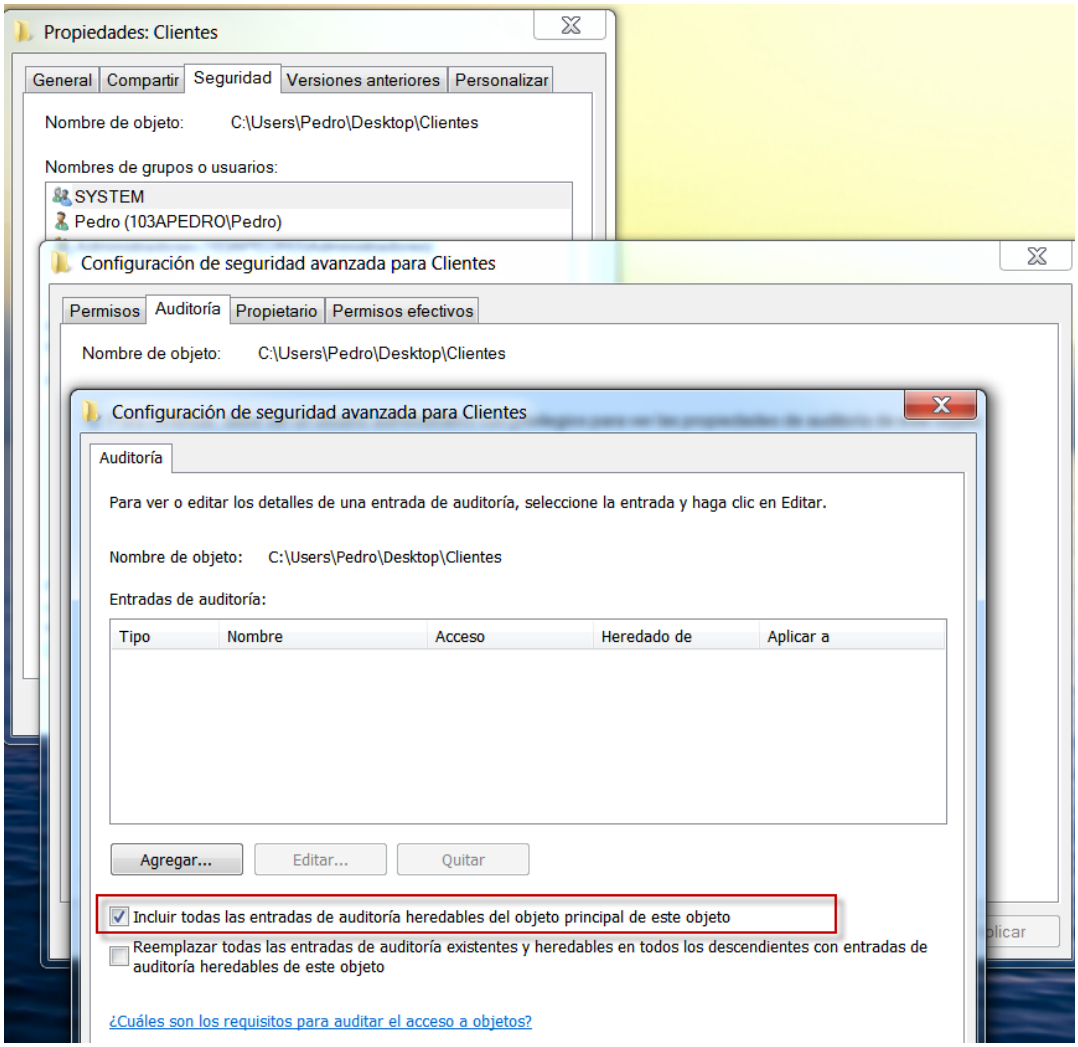
Control de acceso lógico:

Se puede controlar haciendo un muestreo entre los usuarios si los perfiles de acceso a ciertos datos están correctamente configurados.



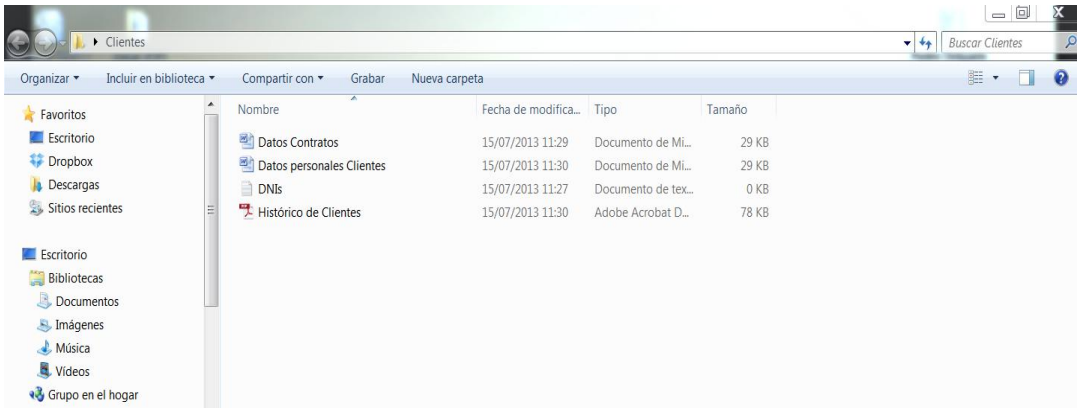
Registros de accesos:

Controlar que existe un registro de accesos a un directorio de Windows que contenga datos de nivel alto se puede realizar de la siguiente manera.



Ficheros temporales:

Preguntar si de alguno de los ficheros auditados se extraen copias que temporalmente estén en otra ubicación distinta a la auditada. Se realiza un muestreo de usuarios a los que se les ha preguntado acerca de si realizan copias en local de ficheros de datos personales y se busca si siguen guardando esas copias una vez que han dejado de utilizarse o por el contrario si se realizan borrados automáticos o manuales.

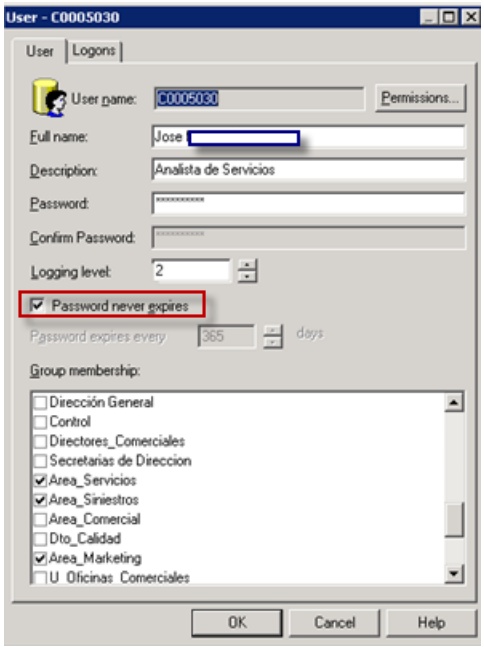


Política de contraseñas:

Ya sea en una aplicación que trate con los datos debe evidenciarse que existe una política de contraseñas que consideremos lo suficientemente segura.

Directivas		hide
Configuración de Windows		hide
Configuración de seguridad		hide
Directivas de cuenta/Directiva de contraseñas		hide
Directiva	**Configuración**	
Exigir historial de contraseñas	13 contraseñas recordadas	
Longitud mínima de la contraseña	8 caracteres	
Vigencia máxima de la contraseña	38 días	
Vigencia mínima de la contraseña	0 días	
Directivas de cuenta/Directiva de bloqueo de cuenta		hide
Directiva	**Configuración**	
Duración del bloqueo de cuenta	0 minutos	
Restablecer recuentos de bloqueo de cuenta tras	99999 minutos	
Umbral de bloqueo de cuenta	10 intentos de inicio de sesión no válidos	

En el siguiente caso no se consideraría segura ya que no expira nunca.

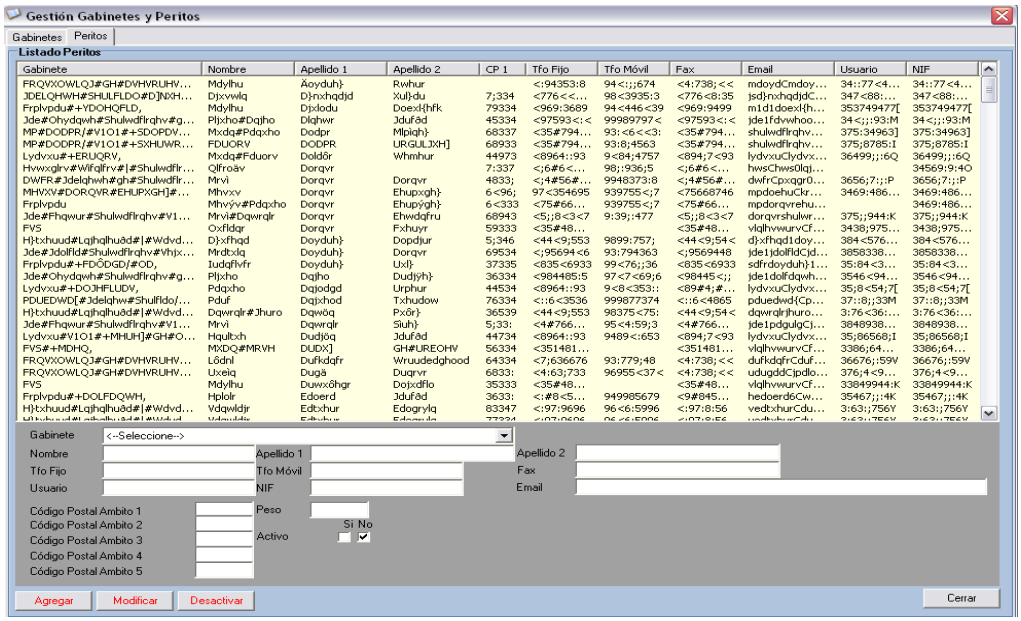


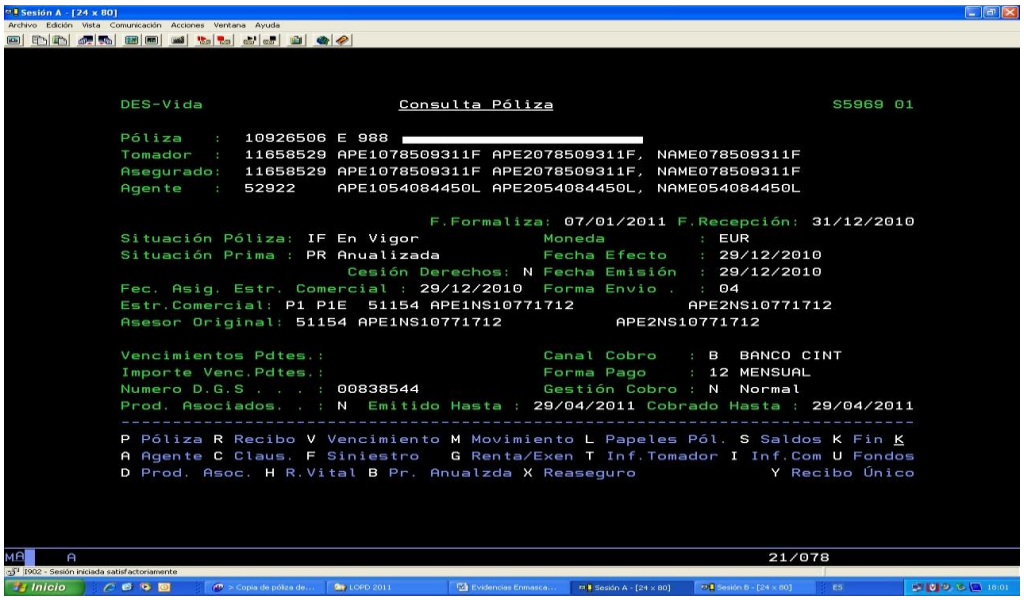
Gestión de contraseñas:

La comunicación de la contraseña se hace de forma segura y confidencial mediante un e-mail automático.

Cifrado y disociación de datos:

Las técnicas de cifrado o disociación son una buena medida de seguridad para evitar accesos a los datos por personas sin permiso para hacerlo. Se utilizan en telecomunicaciones de nivel alto, en documentos que se utilicen en dispositivos portátiles y en el departamento de desarrollo para hacer pruebas con datos reales.





Copias de respaldo y recuperación:

Se debe comprobar la existencia, periodicidad y el buen funcionamiento de las copias de backup y recuperación. Se podría comprobar mediante los log.

```
NetWorker savegroup: (notice) RRHHBW-PRO-S completed, Total 2 client(s), 1 Succeeded with warning(s), 1 Succeeded. P

Succeeded with warning(s): oracle-m-gro-03.entidad
Succeeded: rrhhbw-m-gro-entidad

Start time:   Sun Jan 24 17:00:00 2012
End time:     Sun Jan 24 23:43:49 2012


--- Successful Save Sets ---

* oracle-m-gro-03.entidad:Probe savegrp: suppressed 24 lines of output.
* oracle-m-gro-03.entidad:Probe 7200:(pid 426196): Default client index for scheduled save will be that of gm935041.b
* oracle-m-gro-03.entidad:Probe 7198:(pid 426196): path /env/live/orasapr3/RBP/data/oradata by default belongs to cli
* oracle-m-gro-03.entidad:Probe 7200:(pid 426196): Default client index for scheduled save will be that of gm935041.b
* oracle-m-gro-03.entidad:Probe 7198:(pid 426196): path /env/live/orasapr3/ by default belongs to client gm935041.bar
* oracle-m-gro-03.entidad:Probe 7200:(pid 426196): Default client index for scheduled save will be that of gm935041.b
* oracle-m-gro-03.entidad:Probe savefs oracle-m-gro-03.entidad: succeeded.
```

```
=====================  PuTTY log 2012.01.21 17:31:48  =====================
Using username "uXXX".

###############################################################################
#                                                                             #
#                                    AVISO                                    #
#                                                                             #
#        EL ACCESO A ESTE ORDENADOR ESTA PROHIBIDO A NO SER QUE ESTE VD.      #
#            EXPRESAMENTE AUTORIZADO. EL ACCESO A PROGRAMAS Y DATOS           #
#                 NO RELACIONADOS CON SU TRABAJO ESTA PROHIBIDO               #
#                                                                             #
###############################################################################

Authenticating with public key "imported-openssh-key" from agent
Last unsuccessful login: Thu Oct  8 13:54:20 METDST 2009 on ssh from sz935064.entidad
Last login: Thu Jan 21 17:05:22 MET 2010 on /dev/pts/13 from bpcw-za0935-617.entidad
u8948@sm935027:/home/u8948$ sudo recover -I oracle-m-gro-03.txt -c oracle-m-gro-03 -t "l Mon Jan 18 10:00:00 MET 2010" -p
Recovering 86580 files into their original locations
Total estimated disk space needed for recover is 223 GB.
Requesting 86580 file(s), this may take a while...
./env/live/orasapr3/RBP/data/oradata/lost+found/
./env/live/orasapr3/RBP/data/oradata/control1/control1.dbf
./env/live/orasapr3/RBP/data/oradata/control1/control1.dbf file exists, overwrite (n, y, N, Y) or rename (r, R) [n]? Y
Overwriting ./env/live/orasapr3/RBP/data/oradata/control/control.dbf
./env/live/orasapr3/RBP/data/arc2/salvaarch/arch_1_14477.dbf.gz
39571:recover: ./env/live/orasapr3/RBP/data/arc2/salvaarch/arch_1_14477.dbf.gz: file exists, overwriting
```

8. Guión de entrevista de Auditoría Ley Orgánica de Protección de Datos.

8.1 Puntos principales a tratar

Con el objetivo de analizar y validar el grado de conocimiento y cumplimiento de las diferentes áreas y departamentos de la Organización del Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de 13 de diciembre y analizar los diferentes procesos de negocio que tratan datos personales, se presenta a continuación una relación de los principales temas a tratar durante el desarrollo de las reuniones:

- **Nombre, cargo, departamento, etc**.: descripción del nombre, cargo, departamento y demás temas relevantes de su puesto de trabajo.

- **Principales funciones del área o departamento**: el interlocutor deberá describir brevemente las principales funciones de su área o departamento.

- **Recepción y almacenamiento de datos de carácter personal**: el interlocutor deberá identificar y describir cualquier acción de recogida de información de carácter personal que realice su área o

departamento así como el tipo de almacenamiento que se da a esa información (formato electrónico o papel).

- **Uso y tratamiento de datos de carácter personal para el ejercicio de las funciones**: el interlocutor deberá describir, en caso que aplique, qué datos de carácter personal utiliza para el desempeño de sus funciones y el flujo que siguen dentro del departamento/empresa.

- **Aplicaciones utilizadas en las que intervengan datos de carácter personal**: el interlocutor deberá identificar con que aplicaciones informáticas ejecuta su trabajo, las cuales sean susceptibles de almacenar datos de carácter personal (nombres, DNI's, etc.).

- **Revisión de medidas de seguridad – medios automatizados:** revisión, desde el punto de vista del departamento, de las diferentes medidas de seguridad que se aplican a los datos personales en los medios automatizados.

- **Revisión de medidas de seguridad – medios no automatizados:** revisión, desde el punto de vista del departamento, de las diferentes medidas de seguridad que se aplican a los datos personales en los medios no automatizados.

- **Envío o recepción de datos de carácter personal con terceros:** el interlocutor deberá identificar cualquier envío o recepción de información desde su área o departamento hacia empresas externas a la entidad (nacionales o internacionales).

- **Externalización de tareas:** el interlocutor deberá identificar cualquier tratamiento o servicio que se contrate a terceros y en el que intervengan datos de carácter personal.

- **Otras observaciones que el interlocutor considere relevante para la auditoría de LOPD:** el interlocutor podrá aportar cualquier información adicional que considere relevante para tener en cuenta durante el proceso de auditoría de cumplimiento de la LOPD.

8.2 Desarrollo y ejemplo de acta de una reunión.

La mayoría de las veces el responsable que te atenderá en la reunión no dispondrá demasiado tiempo por lo que se debe hacer una primera reunión no demasiado larga en la que se hablen de todos los puntos. Además lo más probable es que no pueda resolverte todas las dudas por lo que un buen método es realizar un acta de reunión en la que se intenten tocar la mayoría de los puntos de la ley. Por ejemplo una buena manera sería estructurar la reunión por ficheros y aplicaciones que utilizan cada uno de ellos.

Además como seguramente no tendrá toda la información que necesitas se acordarán una serie de peticiones por e-mail o entregas en una segunda reunión si fuese necesario.

Un ejemplo de acta para recordar todo lo hablado en una reunión y poder realizar posteriormente una serie de peticiones o preguntas necesarias sería el siguiente:

<table>
<tr><td colspan="2">Acta de reunión –Auditoría de LOPD 2013 (Entidad_Auditada)</td></tr>
<tr><td colspan="2">Reunión mantenida en las instalaciones de Entidad_Auditada en la calle Real número 17, el 25 de julio de 2013 a las 10 horas.</td></tr>
<tr><td>Asistentes :</td><td><u>EMPRESA AUDITORA</u>
- Pedro Delgado (PD)

<u>ENTIDAD AUDITADA</u>
- Jorge Rodríguez Sánchez (JRS)</td></tr>
</table>

Temas principales tratados durante la reunión

- (JRS) (Responsable de Seguridad de la entidad auditada) asiste a la reunión y responde a preguntas relacionadas con los ficheros declarados por la entidad auditada ante la AEPD, sobre el tratamiento de los ficheros con datos de carácter personal, el documento de seguridad de la entidad auditada y otros temas relacionados con el cumplimiento del Reglamento de Seguridad de la LOPD.

FICHEROS Y DOCUMENTO DE SEGURIDAD:

CLIENTES

Este fichero contiene los datos de los clientes de la entidad auditada que requieren la contratación de alguno de los servicios disponibles.

La mayoría de las aplicaciones declaradas en el ANEXO del Documento de Seguridad contienen información antigua, que se siguen almacenando porque aún puede eliminarse. Actualmente:

- La aplicación Salud que es donde se recogen los datos de salud, al ser la plataforma de seguros de vida.
- La aplicación de DHP no se utiliza ya desde hace años y tienen el equipo apagado.

La documentación en papel que pudiera haber en las oficinas, se traslada al archivo central. En el caso de requerir algún tipo de documentación en papel, ésta no se recibe físicamente, sino mediante peticiones tras las cuales se recibe la documentación en formato electrónico.

PROVEEDOR:

Fichero de nivel básico. No se incluye en la presente auditoría.

DATOS DE INMUEBLES:

No contienen datos personales. Se solicita evidencia para comprobarlo

SERVICIOS CLIENTE Y SERVICIOS A CLIENTES:

Ambos ficheros contienen la misma información, por lo que se les recomendará declararlos en la agencia de forma lógica (se declaran ficheros lógicos y no físicos).

Se pide una captura de pantalla del registro de estos datos, por si acaso hubiera una diferencia entre los datos registrados en estos dos ficheros.

PROFESIONALES:

En este fichero se recoge la información del personal que presta servicios la entidad auditada. Sin embargo, desconocen el motivo por el cual es Mixto, queda pendiente una aclaración a este respecto.

CLIENTELA:

El fichero está declarado con fines históricos. Algo que seguramente no esté autorizado por la AEPD y se deberá verificar para ver si debe ser eliminado.

PARTICIPANTES:

Este fichero recoge los datos de todos los que participan en productor de la entidad. Este fichero no se encuentra especificado en el documento de seguridad que ha sido facilitado y no hay ninguna aplicación relacionada con este fichero.

LISTADOS:

Este fichero recoge cualquier tipo de listado generado desde los sistemas, que pueda considerarse como temporales, y que suelen almacenarse en ficheros ofimáticos. Está declarado como mixto, ya que estos listados se envían por valijas a los destinatarios de las oficinas u otras sedes.

OTROS TEMAS:

GESTIÓN DE USUARIOS DE LAS APLICACIONES:

Se comenta el siguiente protocolo en la gestión de usuarios que es común en todas las aplicaciones.

Cuando un usuario se da de **alta**: se asigna una contraseña igual que el usuario mas alguna letra más. La contraseña es de un solo uso. Entras al sistema y en el primer acceso obliga al usuario a cambiarla.

Cuando un usuario se da de **baja:** (ya sea por maternidad o por otra causa): Se da de baja en el sistema automáticamente.

FICHEROS TEMPORALES

Los listados con datos personales que permiten hacer las aplicaciones con los datos de los clientes, está limitado a ciertos usuarios.

Los ficheros temporales que se crean solo puede contener cierta información personal limitada por la propia aplicación. Se eliminan cada cierto tiempo y se comprueba que se han eliminado en sus controles periódicos de verificación.

ACCESO A CPD

En las instalaciones de la entidad auditada se encuentra uno de los CPD (donde se ubican las máquinas de la intranet y servidores de ficheros). El acceso se realiza mediante tarjeta electrónica, en caso de que este sistema no funciones, seguridad del edificio dispone de una llave. Se cuenta con un registro de acceso y un listado de personas autorizadas para acceder a la sala.

El procedimiento de acceso en el caso de que una persona externa a la empresa o alguien que no tiene autorización, deberá ser acompañado por una persona autorizada.

Hay que destacar, que durante la visita física el CPD, la puerta de acceso al mismo era de madera y de cristal, no siendo estos materiales los más indicados, resaltar que el CPD se encontraba en la planta -1, y que es necesario pasar el control de acceso al edificio para poder acceder al mismo.

COPIA DE RESPALDO Y RECUPERACIÓN

Se encuentra centralizada en toda la empresa. Se solicita evidencia.

PRUEBAS CON DATOS REALES

Se realiza con datos enmascarados, se ha solicitado evidencia de cada uno de los entornos.

COMUNICACIÓN DE RED

Los accesos remotos son los que se realizan por teletrabajo, a través de CITRIX o conexión a VPN. La solicitud se realiza mediante petición, pero casi todos los empleados lo tienen activado por defecto.

Se comenta que la conexión se realiza mediante la URL de la entidad y que se realiza mediante una conexión cifrada, cuyo certificado podemos conocer al conectarnos a esa dirección.

Se pide el manual de VPN para comprobar las medidas de seguridad configuradas.

RECOGIDA DE PAPEL

La recogida de contenedores de papel es un servicio centralizado por el Grupo a través de su proveedor. Se piden certificados de destrucción de papel.

RESPONSABLE DE SEGURIDAD

El responsable de seguridad sigue siendo en este momento Fernando Santa María.

CESIONES DE DATOS

Datos de la empresa auditada a los que tienen acceso empresas externas, como las empresas de asistencia o compañías. Se pide identificarlos y contratos.

MEDIDAS GENERALES DEL EDIFICIO

Medidas de seguridad del edificio: Entrada y salida de dispositivos externos, portátiles, etc. Las dos veces que los auditores de la empresa auditora han entrado al edificio con portátiles, no se ha requerido ningún registro por parte de seguridad del edificio. Nos comentan que intentarán arreglar este problema.

CONCIENCIACIÓN DEL EMPLEADO

La concienciación de los empleados con la LOPD se realiza de forma corporativa. Los empleados reciben la información a través de portal, y formación a través de la plataforma corporativa. Además periódicamente se cuelgan carteles en las instalaciones haciendo recomendaciones de cómo se debe actuar respecto al cumplimiento de la LOPD.

TEMAS PENDIENTES:

- Recibir la documentación solicitada.
- Hacer una próxima visita esta misma semana a ser posible al edificio, para observar las medidas de seguridad de un fichero no automatizado

9. ¿Qué es el informe de auditoría?

* Partes extraídas de [RA-MA] y ampliadas por el autor del PFC

Es el producto final del trabajo de auditoría y la única documentación que va a llegar a quien la ha encargado. Sus objetivos principales consisten en permitir a la entidad entender el trabajo realizado, las circunstancias que afectan a su fiabilidad y las conclusiones del auditor.

Todo informe se trata de un escrito firmado, en el que deben aparecer los antecedentes, el objetivo del proceso de auditoría, las posibles limitaciones y un resumen para la Dirección en términos no técnicos.

En cada punto debe explicarse por qué es un incumplimiento o una debilidad y se debe exponer alguna recomendación. El informe siempre ha de discutirse con los auditados antes de emitirse definitivamente e incluso se pueden recoger propuestas dadas por los auditados.

Un informe debe constar entre otros con los siguientes apartados: título, destinatario, identificación de la entidad auditada, alcance, comparabilidad respecto a auditorías anteriores, firmas y fecha.

El informe de auditoría debe ser un documento que debe ser leído y comprendido sin que los lectores encuentren dificultades o dudas en su interpretación.

En las páginas siguientes expongo un ejemplo de lo que sería un correcto informe de auditoría.

9.1 Ejemplo de informe de auditoría de cumplimiento

NOMBRE_EMPRESA_LARGO

GRUPO NOMBRE_EMPRESA_CORTO

INFORME DE AUDITORÍA DE CUMPLIMIENTO SOBRE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS (Basado en el Real Decreto 1720/2007 de 21 de Diciembre)

Informe de Auditoría de Cumplimiento

Introducción

De acuerdo con los términos de nuestra propuesta de servicios profesionales, les presentamos nuestro informe de Auditoría de cumplimiento de la Ley Orgánica de Protección de Datos, en cumplimiento de los artículos 96 y 110 del Real Decreto 1720/2007, de 21 de diciembre.

Este informe de Auditoría ha sido preparado para uso exclusivo de NOMBRE_EMPRESA_LARGO (en adelante NOMBRE_EMPRESA_CORTO o la Sociedad) y del Responsable de Seguridad de la misma, en el contexto de la Auditoría reglamentaria obligatoria de Medidas de Seguridad, por lo que no deberá ser utilizado para fines distintos al descrito ni ser distribuido, salvo a la Agencia Española de Protección de Datos (en adelante AEPD).

Objetivo

Para dar cumplimiento a la normativa vigente, y de conformidad con los artículos 96 y 110 del citado Real Decreto, hemos procedido, a solicitud de NOMBRE_EMPRESA_CORTO, a revisar la política de protección de datos de

carácter personal y a realizar la preceptiva auditoría de los Sistemas de Información e instalaciones de tratamiento de datos, al objeto de verificar, en relación con los ficheros de carácter personal declarados ante la AEPD, el cumplimento del mencionado Reglamento, así como de los procedimientos e instrucciones vigentes en materia de seguridad de los datos.

Nuestra responsabilidad es la emisión de un informe que exprese un dictamen sobre la adecuación de NOMBRE_EMPRESA_CORTO a las medidas y controles definidos en el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos, identificar sus deficiencias y proponer medidas correctoras o complementarias necesarias. Adicionalmente, nuestro informe incluye, los datos, hechos y observaciones en que se basan los dictámenes alcanzados y recomendaciones propuestas. El Responsable de Seguridad deberá elevar las conclusiones al responsable de los ficheros para que se adopten las medidas correctoras adecuadas.

Objetivos específicos

El objetivo específico del trabajo es la revisión de los diferentes aspectos relativos a las medidas de seguridad requeridas por el Reglamento anteriormente mencionado.

En el ámbito del **tratamiento automatizado** de datos de carácter personal, las áreas sujetas a revisión han sido:

- Niveles de seguridad y ficheros
- Encargado de tratamiento
- Prestación de servicios sin acceso a datos
- Delegación de autorizaciones
- Acceso a datos a través de redes
- Régimen de trabajo fuera de los locales
- Ficheros temporales
- Documento de Seguridad
- Funciones y obligaciones del personal
- Gestión y registro de incidencias
- Control de acceso
- Gestión de soportes y documentos
- Identificación y autenticación
- Copias de respaldo y recuperación
- Responsable de Seguridad
- Auditoría
- Control de acceso físico

- Registro de accesos
- Telecomunicaciones

Por otro lado, en el ámbito del **tratamiento no automatizado** de datos de carácter personal, las áreas sujetas a revisión han sido:

- Niveles de seguridad y ficheros
- Encargado de tratamiento
- Prestación de servicios sin acceso a datos
- Delegación de autorizaciones
- Régimen de trabajo fuera de los locales
- Documento de Seguridad
- Funciones y obligaciones del personal
- Gestión y registro de incidencias
- Control de acceso
- Gestión de soportes y documentos
- Criterios de archivo
- Dispositivos de almacenamiento
- Custodia de soportes
- Responsable de Seguridad

- Auditoría
- Almacenamiento
- Copia o reproducción
- Acceso a la documentación
- Traslado de la documentación

Alcance

El alcance de la revisión ha contemplado únicamente los ficheros de nivel medio/alto declarados ante la Agencia Española de Protección de Datos (en adelante AEPD) por el grupo NOMBRE_EMPRESA_CORTO, y que son enumerados a continuación, con números de inscripción, nivel de seguridad y tratamiento de acuerdo con el artículo 80 del Real Decreto 1720/2007, de 21 de diciembre. Asimismo, se ha asignado un identificador corto a cada fichero (columna IDENT) que identificará los ficheros en algunos de los apartados del presente documento.

Ficheros declarados por NOMBRE_EMPRESA_CORTO

IDENT	NOMBRE DEL FICHERO	ENTORNO	TRATAMIENTO	NIVEL
01CLI	Clientes	CISC/DB2 Teradata Geomarketing Lotus Notes Windows Unix/Oracle Papel	Mixto	Medio
02EXP	Expedientes Judiciales	Infolex Windows	Mixto	Medio
03HIC	Historial Médico	Windows Papel	Mixto	Alto
04PRH	Personal y Recursos Humanos	Papel Windows Unix/Oracle (SAPHR) Intranet	Mixto	Medio

05WHI	Whistleblowing	Windows	Automatizado	Alto
06PBC	Blanqueo de Capitales	Windows Papel	Mixto	Alto
07CTA	Datos de clientes de Tarjetas	CISC/DB2 Papel	Mixto	Medio

Metodología

La metodología empleada para la realización del presente trabajo, ha consistido en:

- Preparación previa: el trabajo de auditoría se ha iniciado con un análisis de la documentación facilitada por NOMBRE_EMPRESA_CORTO a partir de la que se ha planificado la revisión conjuntamente con los responsables del proyecto de la Sociedad.

- Desarrollo de la revisión: se han validado los procedimientos descritos en el Documento de Seguridad, se han realizado las pruebas y comprobaciones necesarias y se ha procedido a realizar las entrevistas necesarias a fin de analizar las funciones de cada área y departamento y asegurar que se adecuan a la normativa y a la definición de ficheros con datos personales que tiene NOMBRE_EMPRESA_CORTO.

- Entrevistas: las personas de EMPRESA_AUDITORA que ha participado en la auditoría se han entrevistado con diferentes responsables de área y departamento de NOMBRE_EMPRESA_CORTO, con la finalidad de revisar la actual declaración de ficheros así como detectar posibles nuevos ficheros o aspectos de mejora a ser considerados en el presente informe.

  Las unidades organizativas entrevistadas en NOMBRE_EMPRESA_CORTO han sido:

Departamento
Blanqueo de Capitales
Fondos
Seguros (Correduría de Seguros)
Inmuebles
Servicios médicos
Asesoría Jurídica
Recursos Humanos
Factoring
Sucursal de la empresa

- Visita a las instalaciones: las entrevistas realizadas se han realizado in-situ desde diversos centros de trabajo, revisando tanto las dependencias donde se encuentran ubicados los sistemas para el tratamiento automatizado de los ficheros como las dependencias en las que se efectúa el tratamiento no automatizado de los datos de carácter personal. Los centros visitados son los siguientes:

  - Direccion1: Se han realizado las revisiones con personal de negocio de los departamentos de RRHH, Servicios Médicos y Asesoría jurídica, además de las sociedades y Seguros S.A para comprobar las medidas de seguridad adoptadas respecto a los ficheros no automatizados. También ha sido visitado el CPD para comprobar las medidas de seguridad física.

  - Direccion2: Se han realizado las revisiones con personal de negocio de la sociedad Factoring S.A. Además, se mantuvo reunión con el departamento de Prevención de Blanqueo de Capitales, para comprobar las medidas de seguridad adoptadas respecto a los ficheros no automatizados.

  - Direccion3: Visita a una de las oficinas comerciales de la empresa para comprobar las medidas de seguridad adoptadas respecto a los ficheros no automatizados

- Validación de observaciones y recomendaciones propuestas: se han presentado las observaciones y recomendaciones a NOMBRE_EMPRESA_CORTO.

Conclusiones del trabajo

Las principales conclusiones obtenidas de nuestro trabajo de auditoría son las que se indican a continuación:

a) El Responsable de los Ficheros dispone del preceptivo Documento de Seguridad conforme con el artículo 88 del Real Decreto 1720/2007 de 21 de diciembre.

b) El Responsable de los Ficheros ha introducido en sus procesos de recogida de datos de carácter personal la información obligatoria, según establece el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

c) No obstante a lo anterior, en la comprobación de la adecuación de las medidas y controles al Reglamento, se han identificado algunos puntos que pueden ser optimizados, y en consecuencia, la necesidad de introducir algunas medidas de mejora en el Documento de Seguridad. Estas medidas de mejora son conocidas por la Sociedad, que ya está trabajando para su implementación. Se concretan en los siguientes temas:

Tratamiento automatizado:

Respecto a Encargados del tratamiento, se ha observado que:

- Se ha comprobado que no existe en el Documento de Seguridad un registro actualizado de encargados de tratamiento con acceso a dichos datos de carácter personal. El mantenimiento del registro actualizado de Encargados del Tratamiento es responsabilidad de NOMBRE_EMPRESA_CORTO.

Respecto al Documento de Seguridad, se ha observado que no se encuentra actualizado, en concreto:

i. No existe un registro actualizado en el Documento de Seguridad de los Encargados de Tratamiento con acceso a datos de carácter personal.

ii. Los entornos Teradata y Lotus Notes se encuentran en Estados Unidos, sin embargo esta circunstancia no consta en el Documento de Seguridad.

iii. En el Documento de Seguridad se especifica que no se realiza ninguna transmisión de datos de nivel alto por telecomunicaciones. Sin embargo existen transmisiones de datos entre las diferentes sedes del grupo.

iv. El fichero "Expedientes judiciales" de NOMBRE_EMPRESA_CORTO, se encuentra declarado como mixto, pero en el Documento de Seguridad sólo aparecen plataformas informáticas.

v. El fichero "Historial Médico" de NOMBRE_EMPRESA_CORTO, aparece en el documento de

seguridad como tratamiento mixto (Windows y papel), sin embargo, en la AEPD está declarado como Tratamiento Manual.

vi. En el documento de seguridad aparece que no hay ninguna aplicación que se utilice para el fichero de correduría de seguros que tenga datos de carácter personal cosa que hemos comprobado que no es cierto.

vii. En el Documento de Seguridad se indica que el fichero Clientes es tratado por el sistema Lotus Notes, pero se nos informa de que dicho sistema ya no gestiona datos de clientes.

Respecto al Control de Acceso, se ha observado que:

- Existen usuarios con fecha de último acceso en 2009, 2010 y 2011 en CISC/DB2, lo que sugiere una inadecuada cancelación de usuarios.
- A pesar de existir un procedimiento de gestión de usuarios, se han identificado usuarios con acceso a los diversos sistemas de información y que ya no trabajan en la Empresa, como por ejemplo el sistema SAP HR.

Tratamiento no automatizado:

Respecto a los Dispositivos de Almacenamiento y el Almacenamiento de la documentación, se ha observado que:

- En la sociedad de Seguros los armarios donde se custodian los expedientes de clientes con datos de nivel alto no se encuentran en una sala independiente. Sólo cuentan con acceso restringido al armario mediante llave.

- La documentación en papel correspondiente al fichero de Blanqueo de Capitales (Nivel Alto) está distribuida en dos armarios cerrados bajo llave, pero dichos armarios no están ubicados en una sala independiente.

- En cuanto al fichero de Expedientes Judiciales, parte de la documentación se encuentra en armarios y en una sala independiente. Sin embargo, tanto los armarios como la sala se encontraban abiertos y con las llaves puestas.

Respecto al Registro de Accesos, se ha observado que:

- No existe registro de accesos para la documentación en papel relativa al fichero de Blanqueo de Capitales.

d) Excepto por todo lo indicado en el punto c) anterior, la política de protección de datos de carácter personal de la Sociedad, sus Sistemas de Información, e instalaciones de tratamiento de datos cumplen con lo dispuesto en el Reglamento de Desarrollo de la LOPD, así como con los procedimientos e instrucciones vigentes en materia de seguridad de los datos

EMPRESA_AUDITORA

Nombre del Socio

Nombre del gerente de auditoría

Madrid, xx de MM de AAAA.

DETALLE DE OBSERVACIONES

NOMBRE_EMPRESA_LARGO

Nombre y logotipo de la empresa

Detalle de observaciones

Cuadro resumen de las medidas de seguridad

Ficheros declarados por NOMBRE_EMPRESA_CORTO.

Ficheros	01CLI	02EXP	03HIC	04PRH	05WHI	06PBC	07CTA
Nivel de seguridad	*Medio*	*Medio*	*Alto*	*Medio*	*Alto*	*Alto*	*Medio*
Tratamiento automatizado							
Niveles de seguridad y ficheros	✓	✓	✓	✓	✓	✓	✓
Encargado de tratamiento	×	×	×	×	✓	×	×
Prestación de servicios sin acceso a datos	✓	✓	✓	✓	✓	✓	✓
Delegación de autorizaciones	✓	✓	✓	✓	✓	✓	✓
Acceso a datos a través de redes	✓	✓	✓	✓	✓	✓	✓
Régimen de trabajo	✓	✓	✓	✓	✓	✓	✓

fuera de los locales							
Ficheros temporales	✓	✓	✓	✓	✓	✓	✓
Documento de Seguridad	×	×	×	×	×	×	×
Funciones y obligaciones del personal	✓	✓	✓	✓	✓	✓	✓
Gestión y registro de incidencias	✓	✓	✓	✓	✓	✓	✓
Control de acceso	✱	✱	✱	✱	✱	✱	✱
Gestión de soportes y documentos	✱	✱	✱	✱	✱	✱	✱
Identificación y autenticación	✱	✱	✱	✱	✱	✱	✱
Copias de respaldo y recuperación	✱	✱	✱	✱	✱	✱	✱
Responsable de Seguridad	✓	✓	✓	✓	✓	✓	✓
Auditoría	✓	✓	✓	✓	✓	✓	✓
Control de acceso físico	✓	✓	✓	✓	✓	✓	✓
Registro de accesos	--	--	✓	--	--	✓	✓

Telecomunicaciones	--	--	❋	--	--	❋	❋
Tratamiento no automatizado							
Criterios de archivo	✓	✓	✓	✓	--	✓	✓
Dispositivos de almacenamiento	✓	×	✓	✓	--	✓	✓
Custodia de soportes	✓	✓	✓	✓	--	✓	✓
Almacenamiento	--	--	✓	--	--	×	--
Copia o reproducción	--	--	✓	--	--	✓	✓
Acceso a la documentación	--	--	✓	--	--	×	✓
Traslado de la documentación	--	--	✓	--	--	✓	✓

Leyenda	
	✓Conforme
	×No Conforme
	❋Limitaciones
	--No Aplica

Detalle de trabajo por áreas

A continuación se presenta el detalle del trabajo de campo realizado en cada una de las áreas identificadas asociadas a los diferentes artículos del Reglamento 1720/2007, de 21 de diciembre.

Definición de plantilla

En las siguientes páginas se detalla cada una de las áreas con la siguiente estructura de plantillas:

Área	**Descripción del área**	**Conclusión**	(1)

Artículo RLOPD: Número

- Descripción o extracto de los artículos del Reglamento 1720/2007, de 21 de diciembre, de Desarrollo de la LOPD relacionados (en adelante RLOPD). Su descripción se realiza en un código de colores que muestra el nivel de ficheros a los que afecta:
- En color negro los artículos aplican a ficheros de nivel básico.
- En color azul los artículos que aplican a ficheros de nivel medio.
- En color rojo los artículos que aplican a ficheros de nivel alto.

Trabajo Realizado

Se detalla el trabajo realizado en esta área concreta.

Observación

Se detallan los posibles aspectos detectados así como observaciones relacionadas con el área.

Evidencias
Se detallan las evidencias recogidas, las cuales dan soporte al trabajo realizado y a las observaciones efectuadas usando la siguiente nomenclatura **EV_NNN**, donde: ▪ **EV** es la abreviatura de evidencia. ▪ **NNN** es el número de evidencia dentro del informe.
Recomendación
Se adjuntan las recomendaciones sobre las observaciones del punto anterior.

Estado	(2)	**Responsable**	(3)	**Plazo**	(4)

(1): Conforme (fondo verde) / No Conforme (fondo rojo) / Limitación (fondo naranja) / No aplica

(2): Pendiente / En curso / -- (en caso de no haber recomendaciones)

(3): Área o persona responsable / -- (en caso de no haber recomendaciones)

(4): 1 mes / 3 meses / 6 meses / + de 6 meses / -- (en caso de no haber recomendaciones)

9.1.1 Tratamiento automatizado

Área A1	Niveles de seguridad y ficheros	Conclusión	Conforme

Artículo RLOPD: 81

Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico: Título VIII, Capítulo III, Sección 1ª.

Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, Título VIII, Capítulo III, Sección 2ª.

Además de las medidas de nivel básico y medio, se aplicarán las medidas de seguridad de nivel alto, Título VIII, Capítulo III, Sección 3ª.

Trabajo Realizado

Se ha realizado una revisión de la estructura, composición y nivel de los ficheros declarados por NOMBRE_EMPRESA a la Agencia Española de Protección de Datos (AEPD). Por otro lado, se ha procedido a revisar la relación de ficheros que se encuentra recogida en el Documento de Seguridad de la Sociedad.

Asimismo, se han realizado entrevistas con los diferentes departamentos de NOMBRE_EMPRESA , encargados de la gestión y tratamiento de dichos ficheros, con el fin de validar la correcta declaración del contenido de los ficheros así como identificar posibles ficheros nuevos a declarar.

Observación
En primer lugar, se ha observado y validado que todos los ficheros o tratamientos de datos de carácter personal bajo el alcance de la auditoría han sido declarados correctamente ante la AEPD y registrados del mismo modo en el Documento de Seguridad elaborado por la Sociedad. En segundo lugar, a raíz de las entrevistas realizadas con el personal entrevistado a lo largo de la auditoría, se ha comprobado que la declaración realizada ante la AEPD es correcta, al mismo tiempo que se ha validado la no existencia de otros ficheros o tratamientos no identificados hasta el momento. Por último, se ha evidenciado la adopción de medidas de seguridad de acuerdo con los niveles de declaración de los ficheros.
Evidencias
Se han obtenido las siguientes evidencias que sustentan las observaciones realizadas: ▪ **EV_001:** Documento_de_Seguridad-(Última versión) ▪ **EV_002:** Ficheros declarados por NOMBRE_EMPRESA ante la AEPD
Recomendación
--

Estado	--	Responsable	--	Plazo	--

Área A2	Encargado de tratamiento	Conclusión	No Conforme

Artículo RLOPD: 82

El RD 1720/2007 establece que en el caso que el Responsable de Fichero facilite el acceso a datos a un Encargado de Tratamiento, éste deberá constar en el Documento de Seguridad e indicar el fichero o tratamiento que éste realiza.

Trabajo Realizado

Se ha procedido a la revisión del Documento de Seguridad de la Sociedad y un fichero de proveedores de servicios con acceso a datos.

Observación

Se ha comprobado que no existe en el Documento de Seguridad un registro actualizado de encargados de tratamiento con acceso a dichos datos de carácter personal, del que es responsable NOMBRE_EMPRESA. En concreto, la empresa encargada de la destrucción de papel no consta en el Documento de Seguridad, ni en el Listado de Proveedores Final (EV_004).

Evidencias

Se han obtenido las siguientes evidencias que sustentan las observaciones realizadas:

- **EV_001:** Documento_de_Seguridad-(Última versión)
- **EV_004:** Listado de proveedores Final

Recomendación					
En base a las observaciones realizadas, se recomienda elaborar y actualizar adecuadamente un registro en el que consten todos los encargados de tratamiento de la Sociedad en su Documento de Seguridad. Asimismo, sería conveniente que en dicho registro se hiciera constar una mención al contrato de prestación de servicios celebrado entre las dos partes, contrato en el que el encargado del tratamiento deberá comprometerse al cumplimiento de las medidas de seguridad previstas por el RD 1720/2007 de desarrollo de la LOPD					
Estado	Pendiente	**Responsable**	Responsable de Seguridad	**Plazo**	1 mes

Área A3	Prestación de servicios sin acceso a datos	Conclusión	Conforme

Artículo RLOPD: 83

El RD 1720/2007 establece que, en caso que exista personal que tenga acceso a soportes o recursos sin que tenga que efectuar un tratamiento, se tomen las medidas para limitar el acceso (caso de personal externo el contrato deberá incluir la prohibición y la obligación de secreto).

Trabajo Realizado

Se ha procedido con la revisión de los contratos suscritos con los diferentes proveedores de servicios sin acceso a datos de carácter personal. Concretamente se han revisado los siguientes contratos:

- Contrato con la empresa General de Limpieza.

Observación

En el contrato identificado de la empresa de limpieza (proveedor de servicios sin acceso a datos personales), se hace referencia a los Arts. 10 y 12 de la LOPD y al Art. 21 del RD 1720/2007, indicándose que no se permiten las subcontrataciones a no ser que sean aprobadas por NOMBRE_EMPRESA

Evidencias

Se han obtenido las siguientes evidencias que sustentan las observaciones realizadas:

- **EV_005:** Memo C.2 Prestación de Servicio sin acceso a datos

▪ **EV_006:** Contrato con la empresa General de Limpieza.					
Recomendación					
--					
Estado	--	**Responsable**	--	**Plazo**	--

Área A4	Delegación de autorizaciones	Conclusión	Conforme

Artículo RLOPD: 84

El RD 1720/2007 establece que en el caso que el Responsable del Fichero delegue a otras personas la facultad de autorizar acceso al fichero, estas autorizaciones deberán constar en el Documento de Seguridad.

Trabajo Realizado

Se ha efectuado una revisión del Documento de Seguridad de la Sociedad con el objetivo de identificar la persona o personas sobre las que recaen las funciones y responsabilidades del Responsable del Fichero.

Observación

En el Documento de Seguridad consta que los Responsables de los Ficheros han asignado a Nombre_ persona la función de Responsable de Seguridad.

Evidencias

Se han obtenido las siguientes evidencias que sustentan las observaciones realizadas:

- **EV_001:** Documento_de_Seguridad-(Última versión)

Recomendación

--

Estado	--	Responsable	--	Plazo	--

Área A5	Acceso a través de redes de comunicaciones	Conclusión	Conforme

Artículo RLOPD: 85

El RD 1720/2007 establece que las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 80.

Trabajo Realizado

Se ha analizado el Documento de Seguridad, concretamente el apartado: Acceso a datos a través de redes de comunicaciones, el cual sólo hace referencia a ficheros de nivel alto, en cuyo caso dicha transmisión, se realizará cifrando los datos de forma que no sean inteligibles ni manipulables por terceras personas.

Complementariamente, se han llevado a cabo reuniones con el fin de validar la posibilidad de acceso a través de redes externas, así como las medidas de seguridad asociadas a estas conexiones.

Observación

No se han establecido en el Documento de Seguridad las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, que deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, para cualquier

fichero, ya sea de nivel básico, medio o alto.

Evidencias

Se han obtenido las siguientes evidencias que sustentan las observaciones realizadas:

- **EV_001:** Documento_de_Seguridad-(Última versión)
- **EV_031:** Memo 8.Redes y Comunicaciones

Recomendación

Se recomienda que en el Documento de Seguridad se detallen las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones.

Estado	Pendiente	**Responsable**	Responsable de Seguridad	**Plazo**	1 mes

Área A6	Régimen de trabajo fuera de los locales	Conclusión	Conforme

Artículo RLOPD: 86

El RD 1720/2007 establece que 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. Dicha autorización tendrá que constar en el documento de seguridad.

Trabajo Realizado

Se ha analizado el Documento de Seguridad, donde se establecen las directrices para el tratamiento de datos de carácter personal fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento.

Observación

En base al trabajo realizado, se ha detectado el uso de dispositivos portátiles en la Sociedad, tanto dentro como fuera de las instalaciones. Los responsables de los ficheros autorizan la salida de soportes –tanto físicos como electrónicos- de las instalaciones del banco, así como ficheros adjuntos en los mensajes de correo electrónico.

Evidencias

Se han obtenido las siguientes evidencias que sustentan las observaciones realizadas:

▪ **EV_001:** Documento_de_Seguridad-(Última versión) ▪ **EV_008:** Memo C.4 Régimen de Trabajo fuera de los locales
Recomendación
--

Estado	--	**Responsable**	--	**Plazo**	--

Área A7	Ficheros temporales	Conclusión	Conforme

Artículo RLOPD: 87

El RD 1720/2007 establece que aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda.

Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

Trabajo Realizado

Se ha analizado el Documento de Seguridad y no se hace referencia al tratamiento de ficheros temporales con datos de carácter personal.

Observación

Se ha revisado el entorno Windows, para verificar la política de borrado de ficheros temporales pudiéndose comprobar que no existían ficheros temporales de más de un día de antigüedad.

Evidencias

Se han obtenido las siguientes evidencias que sustentan las observaciones realizadas:

- **EV_001:** Documento_de_Seguridad-(Última versión)
- **EV_014:** Captura de pantalla de borrado en Windows.

Recomendación					
Se recomienda que en el Documento de Seguridad se detallen las medidas de seguridad exigibles al borrado de ficheros temporales.					
Estado	--	**Responsable**	--	**Plazo**	--

Área A8	Documento de Seguridad	Conclusión	No Conforme

Artículo RLOPD: 88

El RD 1720/2007 establece que el responsable del fichero o tratamiento deberá elaborar un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente, de obligado cumplimiento para el personal con acceso a los sistemas de la información.

El citado documento deberá mantenerse actualizado en todo momento y revisado cuando se produzcan cambios relevantes en los sistemas de información.

Asimismo, el contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

Trabajo Realizado

Se ha revisado el Documento de Seguridad con el objetivo de validar su completa adecuación a los requerimientos establecidos por el artículo 88 del RD 1720/2007 de desarrollo de la LOPD, así como validar su grado de actualización y adecuación del documento respecto a la situación actual de la Sociedad.

En concreto se han identificado todos los campos requeridos por el artículo 88 del RD 1720/2007 y que se detallan a continuación:

i. Ámbito de aplicación del documento con especificación detallada de los

recursos protegidos.

ii. Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

iii. Funciones y obligaciones del personal.

iv. Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

v. Procedimiento de notificación, gestión y respuesta ante las incidencias.

vi. Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

vii. Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

viii. La identificación del responsable o responsables de seguridad.

ix. Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

En base al trabajo realizado, se ha comprobado que el Documento de Seguridad no se encuentra actualizado:

i. No existe un registro actualizado en el Documento de Seguridad de los Encargados de Tratamiento con acceso a datos de carácter personal.

ii. Los entornos Teradata y Lotus Notes se encuentran en Estados Unidos, sin embargo esta circunstancia no consta en el Documento

de Seguridad.

iii. En el Documento de Seguridad se especifica que no se realiza ninguna transmisión de datos de nivel alto por telecomunicaciones. Sin embargo existen transmisiones de datos entre las diferentes sedes del grupo.

iv. El fichero “Expedientes judiciales” de NOMBRE_EMPRESA, se encuentra declarado como mixto, pero en el Documento de Seguridad sólo aparecen plataformas informáticas.

v. El fichero “Historial médico” NOMBRE_EMPRESA, aparece en el documento de seguridad como tratamiento mixto (Windows y papel), sin embargo, en la AEPD está declarado como Tratamiento Manual.

vi. En el documento de seguridad aparece que no hay ninguna aplicación que se utilice para el fichero de correduría de seguros que tenga datos de carácter personal cosa que hemos comprobado que no es cierto.

vii. En el Documento de Seguridad se indica que el fichero Clientes es tratado por el sistema Lotus Notes, pero se nos informa de que dicho sistema ya no gestiona datos de clientes.

Evidencias

Se han obtenido las siguientes evidencias que sustentan las observaciones realizadas:

- **EV_001:** Documento_de_Seguridad-(Última versión)
- **EV_010:** Memo C.6 Documento de Seguridad

Recomendación					
Se recomienda actualizar el documento de seguridad con lo indicado en la redacción.					
Estado	Pendiente	**Responsable**	Responsable de Seguridad	**Plazo**	1 mes

Área A9	Funciones y obligaciones del personal	Conclusión	Conforme

Artículo RLOPD: 89

El RD 1720/2007 establece que las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información deberán estar claramente definidas y documentadas en el documento de seguridad. También se deberán definir las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

Trabajo Realizado

Se ha revisado el Documento de Seguridad, y en concreto el apartado de las funciones y obligaciones del personal de NOMBRE_EMPRESA con acceso a datos de carácter personal responsabilidad de la Sociedad.

Observación

Se ha observado que el Documento de Seguridad contiene una adecuada definición y documentación de las funciones y obligaciones del personal con acceso a datos.

Evidencias

Se han obtenido las siguientes evidencias que sustentan las observaciones realizadas:

- **EV_001:** Documento_de_Seguridad-(Última versión)
- **EV_011:** Memo C.7 Funciones y Obligaciones

Recomendación					
Se recomienda ampliar el alcance de las funciones y obligaciones del personal, de tal modo que se abarquen aquellos tratamientos no automatizados de datos de carácter personal. Asimismo, se recomienda la difusión de tales funciones y obligaciones entre todo el personal de las Sociedades con acceso a datos de carácter personal, así como la realización periódica de tareas de formación/concienciación en materia de la LOPD.					
Estado	--	**Responsable**	--	**Plazo**	--

Área A10	Gestión y registro de incidencias	Conclusión	Conforme

Artículo RLOPD: 90, 100

El RD 1720/2007 establece la obligación de disponer de un procedimiento formal de notificación y gestión de incidencias que afecten a los datos de carácter personal, y establece un registro en el que se haga constar el tipo de incidencia, el momento en el que se produzca, o en su caso, detectada, la persona que realiza la notificación, a quien se le comunica, los efectos que se hayan derivado de la misma y las medidas correctoras aplicables.

En el registro deberán consignarse los procedimientos realizados en la recuperación de los datos, indicando quien lo ejecutó, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

Trabajo Realizado

En primer lugar, se ha procedido a comprobar la correcta definición y descripción del apartado “Procedimiento de notificación, gestión y respuesta ante incidencias” del Documento de Seguridad de la Sociedad.

En base al trabajo realizado, se ha observado que la Sociedad cuenta con el adecuado procedimiento de gestión y registro de incidencias, soportado por una

herramienta. Dicha herramienta registra todas las incidencias que tienen lugar en la Sociedad, existiendo una tipología de incidencias específica para el caso de las relacionadas con la LOPD.
Observación
Teniendo en cuenta lo comentado anteriormente, consideramos el correcto cumplimiento del apartado de Gestión y Registro de Incidencias.
Evidencias
Se han obtenido las siguientes evidencias que sustentan las observaciones realizadas: ▪ **EV_001:** Documento_de_Seguridad-(Última versión)
Recomendación
--

Estado	--	**Responsable**	--	**Plazo**	--

Área A11	Control de Acceso	Conclusión	Limitación

Artículo RLOPD: 91

El RD 1720/2007 establece la obligación de que los usuarios solamente tengan acceso a aquellos recursos que necesitan para el desarrollo de sus funciones, manteniendo una relación actualizada de usuarios y perfiles de usuarios así como los accesos autorizados para cada uno de ellos.

Trabajo Realizado

Se han revisado los siguientes documentos:

- Apartado "Identificación y autenticación de usuarios" del Documento de Seguridad, "Estándar de administración de cuentas con privilegios "
- "Estándar de administración de cuentas sin privilegios "
- "Procedimientos de bajas de empleados"
- "Procedimientos de bajas de empleados (Anexo)"
- "Proc RRHH Cambios de estado de usuarios"
- Los documentos de los diferentes sistemas que nos han podido facilitar.

Asimismo, se ha procedido a la revisión de los siguientes objetivos del RD 1720/2007:

- Exclusivamente el personal autorizado para ello en el documento de seguridad puede conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.
- El personal ajeno a la Sociedad que tenga acceso a los recursos debe estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Se ha validado que en el apartado “Identificación y autenticación de usuarios” del documento de seguridad, se define un adecuado procedimiento de control de acceso lógico a los diferentes sistemas de información.

Adicionalmente, en base al trabajo realizado, comentar que se ha comprobado la existencia de correctos mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados. Concretamente dichos mecanismos se basan en:

- La “identificación y autenticación” de usuarios por medio de un usuario y contraseña unívocos, personales e intransferibles.
- La asignación y control de privilegios de acceso, mediante la creación de grupos de usuarios y su asignación a recursos, o mediante la creación y asignación a usuarios de perfiles de acceso.

Observación

En cuanto a lo comentado anteriormente, destacar que:

- Existen usuarios con fecha de último acceso en 2009, 2010 y 2011 en CISC/DB2.
- Se han encontrado usuarios que ya no trabajan en el grupo y sin embargo

siguen dados de alta en el sistema SAP HR.

- A pesar de existir un procedimiento de gestión de usuarios, se han identificado usuarios con acceso a los diversos sistemas de información y que ya no trabajan en la empresa.
- Faltan varios datos de algunos sistemas de información tales como fecha de último acceso, listados de usuarios, etc.

Adicionalmente no se ha podido comprobar los siguientes procedimientos para todos los sistemas:

- Los usuarios acceden únicamente a aquellos recursos que precisen para sus funciones.
- Existe una relación actualizada de usuarios y perfiles de usuarios.
- Existen mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

Evidencias

Se han obtenido las siguientes evidencias que sustentan las observaciones realizadas:

- **EV_001:** Documento_de_Seguridad-(Última versión)
- **EV_ 016:** Estándar de administración de cuentas con privilegios
- **EV_ 017:** Estándar de administración de cuentas sin privilegios
- **EV_ 018:** Procedimientos de bajas de empleados

- **EV_ 019:** Procedimientos de bajas de empleados (Anexo)
- **EV_ 020:** Proc RRHH Cambios de estado de usuarios
- **EV_ 021:** Identificación-Autenticación-Control de Acceso Lógico CISC/DB2.
- **EV_ 022:** Identificación-Autenticación-Control de Acceso Lógico Host (Intranet)
- **EV_ 023:** Identificación-Autenticación-Control de Acceso Lógico Host (Teradata y Geomarketing)
- **EV_ 024:** Identificación-Autenticación-Control de Acceso Lógico Host (Unix-Oracle (SAP HR))

Recomendación					
--					
Estado	Pendiente	**Responsable**	Responsable de Seguridad	**Plazo**	1 mes

Área A12	Gestión de soportes y documentos	Conclusión	Limitación

Artículo RLOPD: 92, 97, 101

El RD 1720/2007 establece que deberá existir un sistema de gestión de soportes y documentos que permita identificar el tipo de información que contiene, ser inventariados y accesibles solamente por el personal autorizado en el Documento de Seguridad.

El RD dispone, además de lo establecido anteriormente, que para la gestión de soportes hay que tener presente la necesidad de establecer un registro de entrada y salida de soportes, que permita controlar los tipos de soporte o documento del que se trata, la fecha y hora, el emisor y destinatario, el numero de soportes o documentos del envío o el tipo de información que contienen, la forma de envío y la persona responsable de la recepción.

Para ficheros de nivel alto, es necesario aplicar sistemas de etiquetado comprensibles, así como aplicar técnicas de cifrado en la distribución de soportes o cuando éstos se utilicen en dispositivos portátiles.

Trabajo Realizado

Se ha revisado el apartado “Gestión de soportes y documentos” del Documento de Seguridad, el documento “Traslado de copias de seguridad ” y la “Guía de

seguridad en dispositivos electrónicos".

Asimismo, se ha procedido con la revisión de los siguientes objetivos del RD 1720/2007:

- Los soportes y documentos con datos de carácter personal permiten identificar el tipo de información que contienen, están inventariados y solo son accesibles por el personal autorizado en el documento de seguridad.
- La salida de soportes y documentos con datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento está autorizada en el documento de seguridad.
- En el traslado de soportes y documentos se adoptan medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.
- Siempre que vaya a desecharse cualquier documento o soporte con datos de carácter personal se procederse a su destrucción o borrado, evitando el acceso a la información contenida en el mismo o su recuperación posterior.
- La identificación de soportes y documentos con datos de carácter personal especialmente sensibles se realiza utilizando sistemas de etiquetado que dificulten su identificación a aquellas personas con acceso no autorizado.
- Existe un sistema de registro de entrada y salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor o receptor, el número de documentos o soportes incluidos en la entrada o salida, el tipo de información contenida, la forma de envío y la persona responsable de la entrega o recepción que deberá estar debidamente autorizada.

- La distribución de los soportes con datos de nivel alto se realiza cifrando dichos datos.

Observación

En base al trabajo realizado, se ha observado que en la Sociedad existe un procedimiento de gestión de soportes y documentos, que en general cumple con lo establecido por la LOPD y su RD 1720/2007.

Dicho procedimiento establece que en el traslado de soportes y documentos se toman medidas de control para evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

No obstante no se han obtenido evidencias que justifiquen la correcta ejecución de dicho procedimiento.

Evidencias

Se han obtenido las siguientes evidencias que sustentan las observaciones realizadas:

- **EV_001:** Documento_de_Seguridad-(Última versión)
- **EV_029: "**Traslado de copias de seguridad "
- **EV_030:** "Guía de seguridad en dispositivos electrónicos"

Recomendación

--

Estado	Pendiente	**Responsable**	Responsable de Seguridad	**Plazo**	1 mes

Área A13	Identificación y autenticación	Conclusión	Limitación

Artículo RLOPD: 93, 98

El RD 1720/2007 establece que se deberán aplicar las medidas adecuadas para garantizar la correcta identificación y autenticación de los usuarios. Es necesario adoptar mecanismos que permitan la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

En el caso de uso de contraseñas como mecanismo de autenticación, tiene que existir un procedimiento de asignación, distribución y almacenamiento que garantice la confidencialidad e integridad. Las contraseñas deberán ser cambiadas con cierta periodicidad, no superior a 1 año, y mientras estén en uso se almacenarán de forma ininteligible o no accesible.

El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Trabajo Realizado

Se ha revisado el apartado “3.2 Identificación y autenticación de usuarios” del Documento de Seguridad, Los documentos “Estándar de administración de cuentas con privilegios”, “Estándar de administración de cuentas sin privilegios”, “Procedimientos de bajas de empleados” “Procedimientos de bajas de empleados (Anexo)” y “Proc RRHH Cambios de estado de usuarios”.

Asimismo, se ha procedido con la comprobación de los siguientes objetivos del RD 1720/2007:

- Existen mecanismos que garantizan la correcta identificación y autenticación de los usuarios en los diferentes sistemas de información bajo el alcance de la auditoría.
- Existen mecanismos que permiten la identificación de forma inequívoca y personalizada de todo usuario que accede al sistema y la verificación de que está autorizado.
- Existe un adecuado procedimiento de asignación, distribución y almacenamiento de contraseñas que garantiza en todo momento su confidencialidad e integridad.
- El documento de seguridad establece la periodicidad de la caducidad de las contraseñas.
- Existe un mecanismo que limita la posibilidad de intentar reiteradamente el acceso no autorizado a los sistemas de información.

Para ello, se han realizado las siguientes acciones:

i. Se han evidenciado y revisado los mecanismos de identificación y autenticación de los sistemas bajo el alcance de la auditoría que aparecen en el documento de seguridad (no se ha recibido el detalle de todos los sistemas, únicamente los que a continuación se detallan): Teradata, Geomarketing, Intranet, CISC/DB2,Unix/Oracle (SAP HR).

ii. Se ha revisado la política de contraseñas establecida en los siguientes sistemas auditados: Teradata, Geomarketing, CISC/DB2., Unix/Oracle (SAP HR)) así como su procedimiento de asignación, distribución y almacenamiento.

Se ha validado que el apartado “3.2 Identificación y autenticación de usuarios” del documento de seguridad, definen un adecuado procedimiento de control de acceso lógico a los diferentes sistemas de información.

Observación
En base al trabajo realizado, por norma general, se ha evidenciado la existencia de un adecuado mecanismo de identificación y autenticación basado en un usuario y una contraseña, los cuales son personales e intransferibles, para el acceso a los diferentes sistemas que soportan la información de los ficheros auditados. No obstante no se han obtenido evidencias que justifiquen la correcta identificación y autenticación de los usuarios para todos los sistemas.
Evidencias
Se han obtenido las siguientes evidencias que sustentan las observaciones realizadas: ▪ **EV_001:** Documento_de_Seguridad-(Última versión) ▪ **EV_016:** Estándar de administración de cuentas con privilegios ▪ **EV_017:** Estándar de administración de cuentas sin privilegios ▪ **EV_018:** Procedimientos de bajas de empleados ▪ **EV_019:** Procedimientos de bajas de empleados (Anexo) ▪ **EV_020:** Proc RRHH Cambios de estado de usuarios ▪ **EV_021:** Identificación-Autenticación-Control de Acceso Lógico CISC/DB2. ▪ **EV_022:** Identificación-Autenticación-Control de Acceso Lógico Host (Intranet) ▪ **EV_023:** Identificación-Autenticación-Control de Acceso Lógico Host

<table>
<tr><td colspan="6">(Teradata y Geomarketing)

▪ EV_024: Identificación-Autenticación-Control de Acceso Lógico Host (Unix-Oracle (SAP HR))</td></tr>
<tr><td colspan="6">Recomendación</td></tr>
<tr><td colspan="6">--</td></tr>
<tr><td>Estado</td><td>Pendiente</td><td>Responsable</td><td>Responsable de Seguridad</td><td>Plazo</td><td>1 mes</td></tr>
</table>

Área A14	Copias de respaldo y recuperación	Conclusión	Limitación

Artículo RLOPD: 94, 102

El RD 1720/2007 determina las pautas del procedimiento a seguir respecto a las Copias de Seguridad y de la Recuperación de la información a partir de éstas. Por otro lado, establece que la realización de copias se deberá realizar con una periodicidad mínima semanal y efectuar pruebas de restauración semestrales. En caso que lleven a cabo pruebas para tareas de desarrollo no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado

En caso de copias de Seguridad con datos de nivel alto, será necesario conservar una copia de respaldo y los procedimientos de recuperación en un lugar diferente al que se encuentran los equipos informáticos.

Trabajo Realizado

En primer lugar, se ha procedido a revisar el apartado "7.Procedimiento de realización de copias de respaldo y de recuperación de los datos" del Documento de Seguridad.

Cabe destacar que el trabajo se ha realizado con una muestra de un sistema en concreto CISC/DB2 y con los Controles SOX mencionados más adelante en el

apartado de Evidencias.

Asimismo, se ha procedido con la comprobación de los siguientes objetivos del RD 1720/2007:

- La Sociedad mantiene los correspondientes procedimientos de realización de copias de respaldo con frecuencia al menos semanal.
- Existen unos procedimientos de recuperación que garantizan la reconstrucción de los datos
- El Responsable del Fichero mantiene una revisión, como mínimo semestral, de los procedimientos antes descritos.
- Las pruebas no se realizan con datos reales, salvo que se asegure el nivel de seguridad correspondiente. (Limitación)
- Se conserva una copia de los datos reales en un lugar diferente al de las instalaciones donde se tratan los datos (nivel alto). (Limitación)

Para la estimación del nivel de adecuación a estas normas, se han llevado a cabo las siguientes:

i. Se ha verificado la existencia de un plan de ejecución de copias de respaldo para los sistemas de CISC/DB2 Diarios, mensuales y anuales)

ii. Se ha comprobado la existencia de un procedimiento de recuperación para los sistemas que soportan los datos de carácter personal bajo el alcance de la presente auditoría.

iii. Se ha verificado la externalización de las copias de seguridad y de los procedimientos de copia y recuperación en una ubicación diferente al de las

instalaciones de tratamiento de los datos. (Limitación)

Se ha observado que NOMBRE_EMPRESA mantiene unos procedimientos de realización de copias de respaldo y su recuperación adecuados a la normativa vigente, ejecutándose el primero con frecuencias diarias, como mínimo.

Observación

Se ha verificado que todo el procedimiento de Copias de Respaldo y Recuperación, es gestionado desde fuera de España. Por tanto, no se ha podido verificar la adecuación de los procesos implantados relacionados con copias de respaldo y recuperación.

Evidencias

Se han obtenido las siguientes evidencias que sustentan las observaciones realizadas:

- **EV_001:** Documento_de_Seguridad-(Última versión)
- **EV_013:** Estándares de Backup CISC/DB2 y Controles SOX
- **EV_025:** Control SOX1
- **EV_026:** Control SOX2
- **EV_027:** Operaciones_apl.doc

Recomendación

Estado		Responsable		Plazo	

Área A15	Responsable de Seguridad	Conclusión	Conforme

Artículo RLOPD: 95

En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

Trabajo Realizado

Se ha analizado el apartado 'Responsable de Seguridad' en el Documento de Seguridad de la Sociedad, documento en el que se debe formalizar la identificación del Responsable o Responsables de seguridad. Se indica en este documento que la función de Responsable de Seguridad ha sido asignada a una persona del departamento de seguridad.

Observación

--

Evidencias

Se han obtenido las siguientes evidencias que sustentan las observaciones

<table>
<tr><td colspan="6">realizadas:

▪ EV_001: Documento_de_Seguridad-(Última versión)</td></tr>
<tr><td colspan="6">Recomendación</td></tr>
<tr><td colspan="6">--</td></tr>
<tr><td>Estado</td><td>--</td><td>Responsable</td><td>--</td><td>Plazo</td><td>--</td></tr>
</table>

Área A16	Auditoría	Conclusión	Conforme

Artículo RLOPD: 96

El RD 1720/2007 establece que los sistemas de información e instalaciones donde se almacenen y traten datos de carácter personal, tienen que someterse al menos cada dos años a una auditoría que verifique el cumplimiento de las medidas de seguridad. Además se deberá realizar una auditoría cuando se produzcan modificaciones en los sistemas de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas.

Adicionalmente, los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas.

Trabajo Realizado

Se ha solicitado y revisado el último informe de auditoría de cumplimiento de la LOPD realizado en la Sociedad.

Se ha evidenciado que la última auditoría de adecuación a la LOPD efectuada en la Sociedad data de 2010, cumpliendo de esta manera con el período bienal establecido por la Ley.

Asimismo, se han llevado a cabo diversas entrevistas con los departamentos de la Sociedad con la finalidad de evaluar y determinar el grado de seguimiento y

actuación en relación con las recomendaciones efectuadas en el último informe.
Observación
Teniendo en cuenta lo comentado anteriormente, consideramos el correcto cumplimiento del presente apartado de Auditoría.
Evidencias
Se han obtenido las siguientes evidencias que sustentan las observaciones realizadas: ▪ **EV_012:** Informe de Auditoría LOPD
Recomendación
--

Estado	--	**Responsable**	--	**Plazo**	--

Área A17	Control de acceso físico	Conclusión	Conforme

Artículo RLOPD: 99

El RD 1720/2007 establece que 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.

Trabajo Realizado

Se ha realizado el análisis el apartado "Control de acceso físico"

Observación

Teniendo en cuenta lo comentado anteriormente, consideramos el correcto cumplimiento del presente apartado de Control de Acceso Físico.

Evidencias

Se han obtenido las siguientes evidencias que sustentan las observaciones realizadas:

- **EV_001:** Documento_de_Seguridad-(Última versión)

Recomendación

--

Estado	--	Responsable	--	Plazo	--

Área A18	Registro de accesos	Conclusión	Conforme

Artículo RLOPD: 103

El RD 1720/2007 regula los datos a almacenar de cada intento de acceso a los sistemas de información con datos sensibles. Como mínimo hay que almacenar la identificación del usuario, la fecha y hora de accesos, el fichero accedido, el tipo de acceso y se ha se ha autorizado o denegado. En el caso de los accesos autorizados, se deberá almacenar la información que permita identificar el registro accedido.

Trabajo Realizado

Se han identificado los tratamientos automatizados de datos de carácter personal de nivel alto.

Se ha verificado que el tratamiento de datos de nivel alto sólo se realiza mediante el aplicativo de Windows según indica el documento de seguridad.

Observación

Teniendo en cuenta lo comentado anteriormente, consideramos el correcto cumplimiento del presente apartado de Registro de accesos.

Evidencias

Se han obtenido las siguientes evidencias que sustentan las observaciones realizadas:

▪ **EV_001:** Documento_de_Seguridad-(Última versión) ▪ **EV_028:** Ficheros de Nivel Alto LOPD de Recursos Humanos - Accesos Septiembre 2012					
Recomendación					
--					
Estado	--	**Responsable**	--	**Plazo**	--

Área A19	Telecomunicaciones	Conclusión	Limitación

Artículo RLOPD: 104

El RD 1720/2007 establece que las transmisiones de ficheros de nivel alto a través de redes públicas o inalámbricas de comunicaciones se deberán realizar cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Trabajo Realizado

No existe en el Documento de Seguridad ninguna mención al cifrado de datos que se está realizando en las telecomunicaciones de datos con nivel alto. Se nos informa que actualmente si se está realizando el cifrado.

Observación

Se nos informa que actualmente existen medidas de cifrado, aunque a fecha de la presente auditoría no se ha obtenido evidencia que justifique dicho cifrado.

Evidencias

Se han obtenido las siguientes evidencias que sustentan las observaciones realizadas:

- **EV_001:** Documento_de_Seguridad-(Última versión)

Recomendación

Actualizar el Documento de Seguridad indicando las medidas con respecto a telecomunicaciones.

Estado	Pendiente	**Responsable**	Responsable de Seguridad	**Plazo**	--

9.1.2 Tratamiento no automatizado

Las áreas comunes de tratamiento automatizado y tratamiento no automatizado, se han revisado de forma conjunta en los análisis presentados anteriormente y se ha optado por no incluir a continuación dichas fichas repetidas con el fin de evitar la redundancia en el contenido del informe.

Las áreas concretas, de las cuales se han revisado simultáneamente ambos tratamientos y, en consecuencia, no se ha generado otra ficha específica por ser redundante dentro del tratamiento no automatizado, han sido:

- Encargado de tratamiento
- Prestación de servicios sin acceso a datos
- Delegación de autorizaciones
- Funciones y obligaciones del personal
- Gestión y registro de incidencias
- Control de acceso
- Gestión de soportes y documentos
- Responsable de Seguridad
- Auditoría
- Documento de Seguridad
- Régimen de trabajo fuera de los locales

A continuación se presentan las fichas de las áreas que corresponden y/o presentan aspectos específicos en el ámbito del tratamiento no automatizado.

Área N1	Criterios de archivo	Conclusión	Conforme

Artículo RLOPD: 106

El RD 1720/2007 establece que el archivo de los soportes o documentos se realizará acuerdo a la legislación específica. Estos criterios deberán garantizar la correcta conservación, localización y consulta de la información y posibilitar el ejercicio de los derechos de Acceso, Rectificación, Cancelación u Oposición. En el caso de no existir norma aplicable, ésta será establecida por el Responsable de Fichero.

Trabajo Realizado

Se ha procedido a efectuar una revisión del Documento de Seguridad con el objetivo de identificar los criterios de archivo referentes a la documentación en papel asociada a los ficheros declarados.

Asimismo, se han llevado a cabo las siguientes acciones en el marco de las diversas reuniones mantenidas con el personal de los departamentos anteriormente indicados:

i. Se ha verificado que el archivo de los soportes o documentos se realiza de acuerdo con criterios previstos en su respectiva legislación.

ii. Se ha verificado que los criterios garantizan la correcta conservación de los documentos, la localización y consulta de la información y posibilitan el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y

cancelación.

iii. Se ha indagado sobre la existencia y correcta definición de los criterios y procedimientos establecidos en aquellos casos en que no existe legislación aplicable a los mismos, en concreto se ha observado que NOMBRE_EMPRESA dispone de normativas y procedimientos en relación a la gestión de los activos de información.

Observación

En el Documento de Seguridad no se identifican los criterios de archivo referentes a la documentación en papel asociada a los ficheros declarados.

Tampoco se especifica, en caso de no existir un procedimiento aplicable, que sea responsabilidad del Responsable del Fichero.

Evidencias

Se han obtenido las siguientes evidencias que sustentan las observaciones realizadas:

- **EV_001:** Documento_de_Seguridad-(Última versión)
- Visitas realizadas a sucursales y distintos departamentos.

Recomendación

--

Estado	--	**Responsable**	--	**Plazo**	--

Área N2	Dispositivos de almacenamiento	Conclusión	No Conforme

Artículo RLOPD: 107

El RD 1720/2007 establece que los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura que impidan el acceso de personas no autorizadas.

Trabajo Realizado

Se han revisado, en las distintas visitas realizadas a sucursales bancarias y departamentos, las medidas de seguridad aplicadas a documentos que contienen datos de carácter personal.

Observación

Se ha observado en el departamento encargado del fichero de Expedientes Judiciales que disponen de mecanismos para obstaculizar el acceso a los documentos por personal no autorizado, concretamente se encuentran instaladas cerraduras de apertura mediante llave en todos los armarios que contienen documentación con datos de carácter personal, pero tanto los armarios como la sala independiente se encuentran con las llaves puestas.

Evidencias

Se han obtenido las siguientes evidencias que sustentan las observaciones realizadas:

- **EV_001:** Documento_de_Seguridad-(Última versión)

<table>
<tr><td colspan="6">▪ Visitas realizadas a sucursales bancarias y distintos departamentos.</td></tr>
<tr><td colspan="6">Recomendación</td></tr>
<tr><td colspan="6">Se recomienda utilizar correctamente los mecanismos de cierre implantados.</td></tr>
<tr><td>Estado</td><td>Pendiente</td><td>Responsable</td><td>Responsable de Seguridad</td><td>Plazo</td><td>1 mes</td></tr>
</table>

Área N3	Custodia de soportes	Conclusión	Conforme

Artículo RLOPD: 108

El RD 1720/2007 establece que la documentación, mientras no se encuentre en sus dispositivos de almacenamiento, será custodiada en todo momento por el personal que se encuentre al cargo de ella, impidiendo el acceso a la misma por personal no autorizado.

Trabajo Realizado

Se ha revisado el Documento de Seguridad, el apartado 3.3. Control de Acceso a los datos.

Por otro lado, se han mantenido diversas reuniones con el personal involucrado de las diversas áreas encargadas del tratamiento de datos de carácter personal.

Observación

En base al trabajo realizado se ha observado que en el caso de que la documentación se encuentre fuera de su lugar de almacenamiento por estar en proceso de revisión o tramitación, ésta se halla en todo momento custodiada por la persona responsable de la misma, impidiendo cualquier acceso no autorizado.

Evidencias

Se han obtenido las siguientes evidencias que sustentan las observaciones realizadas:

- **EV_001:** Documento_de_Seguridad-(Última versión)

▪ Visitas realizadas a sucursales bancarias y distintos departamentos.					
Recomendación					
--					
Estado	--	**Responsable**	--	**Plazo**	--

Área N4	Almacenamiento	Conclusión	No Conforme

Artículo RLOPD: 111

El RD 1720/2007 regula para la documentación con datos de carácter personal, que los armarios, archivadores y elementos de almacenaje de los mismos deberán encontrarse en áreas con acceso restringido mediante llave o equivalente.

En caso de no ser posible la aplicación de estas medidas, el responsable adoptará medidas alternativas que, debidamente motivadas, serán incluidas en el Documento de Seguridad.

Trabajo Realizado

Se han revisado, en las distintas visitas realizadas a sucursales bancarias y departamentos, las medidas de seguridad aplicadas a documentos que contienen datos de carácter personal.

Observación

Se ha observado en el departamento encargado del fichero de Expedientes Judiciales que disponen de mecanismos para obstaculizar el acceso a los documentos por personal no autorizado, concretamente se encuentran instaladas cerraduras de apertura mediante llave en todos los armarios que contienen documentación con datos de carácter personal, pero tanto los armarios como la sala independiente se encuentran con las llaves puestas.

Adicionalmente se ha observado que en los ficheros de nivel alto de Correduría de Seguros y Prevención de blanqueo de capitales no se dispone de una sala independiente para la custodia de los armarios.
Evidencias
Se han obtenido las siguientes evidencias que sustentan las observaciones realizadas: ▪ **EV_001:** Documento_de_Seguridad-(Última versión) ▪ **EV_015:** Revisiones medidas de seguridad en papel ▪ Visitas realizadas a sucursales bancarias y distintos departamentos.
Recomendación
Se recomienda incluir los armarios con datos de nivel alto en una sala independiente y utilizar correctamente los mecanismos de cierre implantados.

Estado	Pendiente	**Responsable**	Responsable de Seguridad	**Plazo**	1 mes

Área N5	Copia o reproducción	Conclusión	Conforme

Artículo RLOPD: 112

El RD 1720/2007 establece que toda copia de los documentos que contengan datos de carácter personal, deberá ser realizada por el personal autorizado en el Documento de Seguridad. Para la destrucción de las copias, deberán aplicarse mecanismos que eviten el acceso a la información contenida en las mismas.

Trabajo Realizado

Se ha procedido a efectuar una revisión del Documento de Seguridad con el objetivo de identificar las referencias a la generación de copias o la reproducción de los documentos en formato papel.

Se ha observado que en el Documento de Seguridad se ha especificado el personal que se encargará de controlar la generación de copias o la reproducción de documentos que contienen datos de carácter personal en formato no automatizado, así como el procedimiento de destrucción de papel.

Observación

Teniendo en cuenta lo comentado anteriormente, consideramos el correcto cumplimiento del presente apartado de Copia y reproducción.

Evidencias

Se han obtenido las siguientes evidencias que sustentan las observaciones realizadas:

- **EV_001:** Documento_de_Seguridad-(Última versión)

Recomendación					
--					
Estado	--	**Responsable**	--	**Plazo**	--

Área N6	Acceso a la documentación	Conclusión	No Conforme

Artículo RLOPD: 113

El RD 1720/2007 establece que solamente el personal autorizado disponga de acceso a la documentación. Será necesario establecer mecanismos que permitan identificar los accesos realizados a dichos documentos.

Trabajo Realizado

Visitas realizadas a los diferentes archivos de ficheros no automatizados declarados en el Documento de Seguridad para verificar si se cumplen las medidas de seguridad requeridas por la Ley.

Observación

En base al trabajo realizado, se ha observado que:

- Para la documentación en papel correspondiente al fichero de Blanqueo de Capitales (Nivel Alto) no se está registrando los accesos que se realizan a la misma.

Evidencias

Se han obtenido las siguientes evidencias que sustentan las observaciones realizadas:

- **EV_001:** Documento_de_Seguridad-(Última versión)
- **EV_015:** Revisiones medidas de seguridad en papel
- Visitas realizadas a sucursales bancarias y distintos departamentos.

Recomendación					
Se recomienda realizar un registro de acceso para el fichero de Blanqueo de Capitales.					
Estado	Pendiente	**Responsable**	Responsable de Seguridad	**Plazo**	1 mes

Área N7	Traslado de la documentación	Conclusión	Conforme

Artículo RLOPD: 114

El RD 1720/2007 establece que para todo traslado de documentación deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la misma.

Trabajo Realizado

Se han mantenido reuniones con los Encargados del Tratamiento de los datos de las distintas áreas del alcance.

En base al trabajo realizado, se ha observado que el traslado de documentación con datos de carácter personal de nivel de seguridad alto, se realiza mediante valija interna basada en un sobre de características estándar cuyo cierre ha sido grapado en los extremos y con la palabra 'CONFIDENCIAL' escrita en su cara delantera.

El servicio de mensajería, tanto interna como externa, es gestionada a través de proveedores externos.

Observación

Evidencias

Se han obtenido las siguientes evidencias que sustentan las observaciones

realizadas:

- **EV_001:** Documento_de_Seguridad-(Última versión)
- Visitas realizadas a sucursales bancarias y distintos departamentos.

Recomendación					
Teniendo en cuenta lo comentado anteriormente, consideramos el correcto cumplimiento del presente apartado de Traslado de la documentación.					
Estado	--	**Responsable**	--	**Plazo**	--

9.1.3 DETALLE DE EVIDENCIAS

Nombre y logotipo de la empresa

Relación de evidencias

En este apartado se muestra el resumen de las evidencias obtenidas durante todo el proceso de auditoría, referenciadas a lo largo del presente informe. Adjunto a este informe se entrega un soporte con las evidencias obtenidas.

- **EV_001:** Documento_de_Seguridad-(Última versión)
- **EV_002:** Ficheros declarados por NOBMRE_EMPRESA ante AEPD
- **EV_003:** Memo C.1 Encargado de Tratamiento
- **EV_004:** Listado Proveedores Final
- **EV_005:** Memo C.2 Prestación de Servicio sin acceso a datos
- **EV_006:** Contrato con la empresa General de Limpieza
- **EV_007:** Memo C.3 Delegación de Autorizaciones
- **EV_008:** Memo C.4 Régimen de Trabajo fuera de los locales
- **EV_009:** Memo C.5 Ficheros Temporales
- **EV_010:** Memo C.6 Documento de Seguridad
- **EV_011:** Memo C.7 Funciones y Obligaciones
- **EV_012:** Informe de Auditoría LOPD 2010
- **EV_013:** Estándares de Backup CISC/DB2 y Controles SOX
- **EV_014:** Captura de pantalla de borrado en Windows

- **EV_015:** Revisiones medidas de seguridad en papel
- **EV_016:** Estándar de administración de cuentas con privilegios
- **EV_017:** Estándar de administración de cuentas sin privilegios
- **EV_018:** Procedimientos de bajas de empleados
- **EV_019:** Procedimientos de bajas de empleados (Anexo)
- **EV_020:** Proc RRHH Cambios de estado de usuarios
- **EV_021:** Identificación-Autenticación-Control de Acceso Lógico CISC/DB2.
- **EV_022:** Identificación-Autenticación-Control de Acceso Lógico Host (Intranet)
- **EV_023:** Identificación-Autenticación-Control de Acceso Lógico Host (Teradata y Geomarketing)
- **EV_024:** Identificación-Autenticación-Control de Acceso Lógico Host (Unix-Oracle (SAP HR))
- **EV_025:** Control SOX1
- **EV_026:** Control SOX2
- **EV_027:** Operaciones_apl.doc
- **EV_028:** Ficheros de Nivel Alto LOPD de Recursos Humanos - Accesos Septiembre 2012
- **EV_029: "**Traslado de copias de seguridad "
- **EV_030:** "Guía de seguridad en dispositivos electrónicos"

- **EV_031:** Memo C.8 Redes y Comunicaciones

10. Cloud Computing y LOPD

*Extraído de [AEPDGU] y desarrollado por el autor del PFC

10.1 ¿Qué es el Cloud Computing

Es la nueva forma de prestación de los servicios de tratamiento de la información. En concreto es la tendencia a alojar los servicios de forma externa, en la web.

El usuario no requiere la necesidad de invertir grandes cantidades de dinero en infraestructura, utiliza la que le ofrece el prestador del servicio.

En estos entornos, la gestión de la información está de forma virtual en el cliente que contrata estos servicios, el cual la trata a través de Internet (ej: Bases de datos, correo electrónico, nóminas, RRHH, etc). El proveedor puede encontrar en cualquier lugar del mundo y para realizar su objetivo puede realizar prácticas de deslocalización, compartición de recursos y realizando subcontrataciones adicionales.

Por todo esto el proveedor puede desconocer la localización de sus datos y eso puede llevar a que no disponga del control de acceso a los datos, del borrado y de su portabilidad .Esta información con datos de carácter personal aunque no está en su poder si está bajo su responsabilidad.

10.2 Tipos de Cloud Computing

Público: El proveedor proporciona sus servicios a clientes de cualquier tipo mediante un contrato.

Privado: Es cuando un cliente puede realizar una gestión y administración de sus servicios sin que puedan participar entidades externas. No es necesariamente implementado en la misma entidad en la que es utilizado sino que puede contratarse a un tercero que actuará bajo su supervisión.

Otros modelos: Hay modelos híbridos en los cuales determinados servicios se ofrecen de forma pública y otros de forma privada (Ej: Nubes privadas virtuales cuando sobre las nubes públicas se implementan medidas adicionales de seguridad).

10.3 Portabilidad de la información

Cuando se contrate un servicio de Cloud Computing debe tenerse en cuenta la facilidad que dé el proveedor para realizar la transferencia de los datos desde un proveedor a otro al finalizar la relación con el proveedor, ya sea por recisión de contrato por parte del cliente o por otras circunstancias ajenas como el fin de la prestación de algún servicio por parte del proveedor o cambios en su política comercial o marco regulatorio.

10.4 Localización de los datos en un proveedor de Cloud Computing

El proveedor de Cloud Computing puede ser el único prestador de servicios del usuario final o puede subcontratar alguna parte de éste. Pero ¿Cuál se debe elegir?

Es recomendable contratar proveedores de Cloud Computing que estén localizados dentro del Espacio Económico europeo o en países que garanticen un nivel adecuado de protección de los datos de carácter personal. La localización afecta tanto a la sede del proveedor como a la localización de los recursos físicos que se emplean para realizar el servicio al cliente directamente o subcontratados.

Este servicio debe ser auditable y transparente. El contratista debe ser capaz de reclamar la información detallada de dónde, cuándo y quién ha almacenado o procesado sus datos y las condiciones en las que se ha producido

Además en el contrato que firma el cliente y el proveedor de servicios de Cloud Computing debe incorporar en sus cláusulas los puntos a los que obliga la LOPD.

10.5 ¿Qué riesgos ofrece el Cloud Computing?

Esta tecnología tiene grandes ventajas pero ofrece unos riesgos. Deben analizarse todas las condiciones que ofrece el prestador de servicios en el tratamiento de los datos.

- La falta de transparencia: el prestador de servicios tiene que dar una información clara, precisa y completa sobre todo los elementos de la prestación que está realizando (ubicación de los datos, existencia de subencargados, controles de acceso, medidas de seguridad, etc.)
- La falta de control, ya que este modelo puede causar dificultades por ejemplo, conocer la ubicación de los datos, disponer de la información en un formato deseado, ausencia de controles efectivos, etc.

10.6 ¿Qué debe tener en cuenta la persona que contrate un servicio de cloud computing?

El cliente debe evaluar los riesgos que asumirá transfiriendo ciertos datos a los servicios de computación en la nube. Una vez haya decidido su contratación se deberán conocer los tratamientos que se realizan sobre los datos especialmente protegidos por la legislación. Además de forma previa a la contratación de estos servicios se deben verificar entre otras cosas los elementos relativos a la seguridad proporcionada, ubicación del tratamiento, existencia de subencargados, políticas de seguridad, portabilidad de los datos, derechos del usuario y obligaciones legales del prestador de servicio.

Es recomendable comparar las características que ofrecen varios proveedores y no se debe contratar nunca servicios en la nube que no cumplan con las leyes establecidas.

10.7 Dudas en la contratación de servicios de Cloud Computing.

- ¿Quién es el responsable de tratamiento? El cliente que contrata los servicios de Cloud Computing sigue siendo el responsable de tratamiento de los datos personales. La empresa que ofrece los servicios de Cloud Computing en la ley de protección de datos tiene la calificación de encargado de tratamiento.

- ¿Cuál es la legislación aplicable? Siempre será la española y no puede modificarse contractualmente.

- ¿Qué obligaciones tiene el cliente? Debe dar aprobación a la participación de terceras empresas delimitando en que parte del tratamiento de los datos participarán. Además, el proveedor debe dar la garantía jurídica para el tratamiento de los datos en las partes subcontratadas equivalente a la que da él. Así mismo el contrato deberá llevar clausulas de protección de datos.

- ¿Dónde pueden estar ubicados los datos personales? Es de gran importancia porque no todos los países ofrecen las mismas garantías. Si los datos están en países del espacio económico europeo, se consideraría una transferencia internacional de datos en la cual debería proporcionarse una garantía jurídica adecuada.

- ¿Cómo se puede garantizar que se cumplen las medidas de seguridad?

  El cliente debe tener la opción de comprobar las medidas de seguridad y registros de acceso a los datos de los que es responsable. Además puede acordarse de que un tercero audite la seguridad conforme a unos estándares que la empresa conocerá.

El cliente será informado de cualquier incidencia de seguridad que afecte a los datos y de las medidas adoptadas para resolverlas.

- ¿Qué confidencialidad se debe exigir al proveedor? El proveedor debe comprometerse a la confidencialidad de los datos que posee y a dar instrucciones a su personal para que la mantenga.
- ¿Cómo garantizar la portabilidad de los datos? Cuando se termina el servicio, el proveedor debe entregar toda la información al cliente con la garantía completa de haber mantenido la integridad en la información.
- ¿Cómo asegurarse que el proveedor no conserva los datos personales cuando se termina el contrato? Deben establecerse mecanismos de borrados seguro de datos como por ejemplo exigir una certificación de destrucción.
- ¿Cómo se garantiza el poder ejercer los derechos de acceso, rectificación, cancelación y oposición (ARCO)? El responsable del tratamiento de datos, es decir el cliente de cloud computing debe permitir ejercer los derechos ARCO a los ciudadanos para ello debe disponer de las herramientas adecuadas

11. Cookies y LOPD

* Extraído de [AEPDGU] y desarrollado por el autor del PFC

11.1 ¿Qué es una cookie?

Es cualquier archivo que se descarga en un terminal de un usuario para almacenar datos de un usuario que pueden ser recuperados por la entidad responsable de su instalación.

11.2 ¿Qué tipos de cookies existen?

Según la entidad que las gestione:

- Cookies propias: Son las que se envían al terminal del usuario desde un equipo o dominio gestionado por el propio editor y desde el cual se presta el servicio solicitado por el usuario.

-Cookies de tercero: Son las que se envían al terminal del usuario desde un equipo o dominio no gestionado por el editor sino por otra entidad que es la que trata los datos obtenidos a través de las cookies

Según el tiempo que están activadas:

- Cookies de sesión: se utilizan para almacenar datos mientras el usuario accede a una web.

- Cookies persistentes: son las que permanecen almacenadas en el terminal y pueden ser accedidas por un periodo indefinido de tiempo.

Según su finalidad:

- Cookies técnicas: Son las que permiten al usuario la navegación en una página web y hacer uso de las opciones o servicios con las que cuente.

(Ej: Identificar sesión, acceder a partes de acceso restringido, almacenar videos o sonidos, etc.)

- Cookies de personalización: Son las que permiten personalizar los servicios a los que se acceden. (Ej: Idioma, tipo de navegador que se utiliza, etc.)

- Cookies de análisis: Son las que permiten al responsable conocer el comportamiento de los usuarios en el sitio web para introducir mejorar en función de los servicios que el usuario acceda.) estas cookies no se consideran que invadan la privacidad de los usuarios siempre que los datos recabados se utilicen con una finalidad estadística y cabe la posibilidad de que los usuarios decidan que no se utilicen.

- Cookies publicitarias: Son las que permiten la gestión de los espacios publicitarios en los cuales el editor haya incluido en una página.(Ej: frecuencia en la que se muestran los anuncios)

- Cookies de publicidad comportamental: Son las que permiten la gestión de los espacios publicitarios en base al comportamiento que haya observado en los hábitos de navegación del usuario.

11.3 ¿Qué obligaciones tienen las partes?

Se resumen en dos. Deber de información y obtención de consentimiento. Se recomienda hacer un análisis periódico de las cookies para poder saber si las cookies deben estar bajo el alcance de la ley o no. Se deberá además revisar si estas cookies si es necesaria la utilización de cookies persistentes o se podrían usar cookies de sesión y en el caso que sean persistentes si su tiempo de uso atiende a su finalidad.

Deber de información: La información sobre la finalidad de los cookies que se facilita cuando se solicita el consentimiento debe ser suficientemente completa. Además el usuario podrá revocar su consentimiento en cualquier momento.

Esta información le debe llegar al usuario mediante un lenguaje sencillo para que sea entendida por cualquier tipo de usuario. Además para que la visibilidad y accesibilidad de la información sobre cookies sea correcta se deberá poner un enlace que capte la atención y con una denominación descriptica como "Política de cookies".

11.4 Responsabilidades de las partes en la utilización de cookies

Si el editor utiliza las cookies únicamente para servicios de los cuales no necesita dar consentimiento no es necesario que informe de su utilización ni que pida el consentimiento. Pero si son terceros los que tratan estas cookies deberá asegurarse que no se utilizan para ninguna otra finalidad.

Para el usuario es muy difícil ponerse en contacto con las cookies que se instalan de terceros por lo que si esto ocurre porque por ejemplo haya algún servicio en la web que lo ofrezca otro editor, se deberá incluir una cláusula en los contratos entre editores y terceros que asegure que se ofrecerá a los usuarios la información requerida y que se obtendrá su consentimiento.

12. El nuevo reglamento europeo.

* Partes extraídas de [EUR] y ampliadas por el autor del PFC.

El futuro en esta materia se decide actualmente en Bruselas. El 4 de noviembre de 2010 la Comisión europea decía que era necesario reformar esta ley debido a los cambios tecnológicos, empresariales y sociales de los últimos años. De este estudio se ha realizado una propuesta publicada en 2012 cuya aprobación se prevé en el transcurso de este año 2013, ya que la fecha máxima fijada para realizarlo es mayo de 2014. El desarrollo de este reglamento será de gran impacto no sólo a nivel europeo sino también a nuestras empresas. A continuación detallo las diferencias más significativas.

12.1 ¿Cuáles son las novedades que tiene el reglamento?

- **Aplicación de nuevos principios.**

- Rendición de cuentas: La norma europea añade nuevos principios como el de rendición de cuentas o “Accountability” que se refiere a la responsabilidad de las compañías en la implantación de mecanismos que garanticen el cumplimiento de los principios y obligaciones de la norma así como los métodos de validación que garantizan su fiabilidad. Esta responsabilidad afectará tanto a empresas grandes como pequeñas.

- Transparencia: Facilita las relaciones entre el responsable de los datos y el interesado así como el responsable de los datos y las autoridades de control. Se especifica este principio de la siguiente forma:

- Se elimina la obligación de registrar los ficheros antes la autoridad de control (AEPD).
- Se debe conservar la documentación de todas las operaciones de tratamiento de datos. Esta responsabilidad es compartida tanto como por el responsable como por el encargado de tratamiento.
- Necesidad de establecer un mecanismo sencillo para el ejercicio de los derechos, por ejemplo por vía electrónica, y la obligación de informar a los solicitantes la posibilidad de reclamar ante la autoridad de control y recurrir a los tribunales. Además la comisión podrá establecer formularios y procedimientos para las comunicaciones a los interesados.
- No sólo se deberá rendir cuentas con la autoridad de control nacional (AEPD) sino que también se hará con la Comisión y el Consejo Europeo de Protección de Datos.

➢ **Tratamiento de datos de menores.**

Se fija la edad de los menores en menos de 13 años (la española es de 14 años), en relación a la oferta directa de servicios de la sociedad de la información. Además el tratamiento de los datos de los menores sólo será lícito si el padre o tutor ha dado su consentimiento previamente.

➢ **Nuevos derechos para los ciudadanos.**

Es uno de los aspectos más importantes en la nueva normativa.

- Derecho al olvido: Consiste en la eliminación de datos porque ya no son necesarios conforme a la finalidad con la que fueron recabados, porque el interesado ha revocado su consentimiento para el tratamiento de sus datos o porque el tratamiento de los datos no se está realizando conforme al reglamento.
  En este derecho se incluye además eliminar cualquier rastro de los datos publicados, es decir eliminar de la red y de los buscadores cualquier dato de la persona que quiere ejercitar este derecho.

- Oposición a creación de perfiles: La persona puede oponerse a que sus datos se utilicen para creación de perfiles que evalúan de manera automatizada aspectos personales de una persona que pueden analizar o predecir su rendimiento profesional, situación económica, estado de salud, localización, preferencias personales, su fiabilidad o comportamiento.

- Portabilidad de los datos: La posibilidad de portar todos tus datos a otra compañía, por ejemplo cuando cambias de compañía que te ofrece tu correo electrónico o cuando cambias de operadora de telecomunicaciones.

-

➢ **Notificar al usuario problemas de seguridad.**

En el borrador europeo no se dividen los datos por niveles de seguridad sino que se impone al responsable y al encargado que implementen un nivel de seguridad adecuado atendiendo a los criterios de: riegos que se presenten, naturaleza de los datos y costes de implementación.

Se establece la obligación de comunicar cualquier fallo de seguridad. A la autoridad de control en un plazo de 24 horas y al interesado cuando éste se haya visto afectado.

- **Evaluaciones de impacto:**

  Consiste en realizar una evaluación de los riesgos por parte del responsable o del encargado de tratamiento antes de que dicho tratamiento se realice. Permitirá establecer medidas que eviten la pérdida de datos, los accesos y cesiones no autorizados.

- **¿Cuándo habrá que realizar estos estudios?**

  En los casos en los que el tratamiento tenga algún riesgo para los derechos de los interesados. En particular, cuando el tratamiento sirva para la creación de perfiles, en el tratamiento de datos sensibles, datos genéticos o biométricos, en los casos de video-vigilancia y en el tratamiento de datos de menores.

- **Creación de la nueva figura de "Data protection officer" (DPO)**

  Figura de gran relevancia en el nuevo reglamento. Será obligatorio contar con un DPO por un plazo de 2 años, tanto en autoridades y organismos públicos como en empresas con al menos 250 empleados o si sus actividades, con independencia del tamaño de la empresa, implican principalmente operaciones de tratamiento que exijan un seguimiento periódico y sistemático. Su trabajo consistirá entre otras cosas en : supervisar la implementación y aplicación de

las políticas internas, formación del personal, auditorías, información de los interesados y responder a las solicitudes presentadas en el ejercicio de sus derechos, conservar la documentación, ser el contacto con la autoridad de control y realizar evaluaciones de impacto.

12.2 Análisis de la nueva figura del DPO (Delegado de protección de datos).

***** Basado en el análisis de [ASPPROF] y ampliadas por el autor del PFC.

El Parlamento Europeo y el Consejo de la Unión Europea, considera en el borrador del Reglamento, además de las figuras de Responsable y Encargado del Tratamiento una nueva que analizamos en el siguiente apartado.

- **¿Qué empresas deberán contar con un DPO?**

Todas las empresas deberán contar con esta figura si cuentan con 250 empleados o más o si es un organismo público. Además las empresas cuyas actividades, con independencia del tamaño de la empresa, implican principalmente operaciones de tratamiento que exijan un seguimiento periódico y sistemático también deberán tener esta figura.

- **¿Cuáles son las tareas profesionales de un DPO?**

  Las principales tareas que destacan el nuevo reglamento europeo para la nueva figura de DPO son las siguientes.

  - Respecto al Responsable de tratamiento o al Encargado de tratamiento:

    - Informar y asesorar de sus obligaciones en virtud del Reglamento Europeo.

    - Documentar su actividad y propuestas junto a las respuestas recibidas a sus sugerencias y peticiones.

  - Supervisar la implementación y aplicación de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluyendo:

    - La asignación de responsabilidades.

    - La formación del personal que participa en las operaciones de tratamiento.

    - Las auditorías periódicas correspondientes.

  - Supervisar la implementación y aplicación del Reglamento europeo, concretamente los requisitos relativos a:

    - La protección de datos desde el diseño.

    - La protección de datos por defecto.

    - La seguridad de los datos.

- La información de los interesados.
- Las solicitudes presentadas en el ejercicio de sus derechos ARCO.

- Velar por la organización y conservación de la documentación necesaria.

- Supervisar la documentación, notificación y comunicación de las violaciones de datos personales.

- Supervisar la realización de la evaluación de impacto relativa a la protección de datos por parte del responsable o del encargado del tratamiento y la presentación de solicitudes de autorización o consulta previas, si fueran necesarias.

- Supervisar la respuesta a las solicitudes de la autoridad de control y, en el marco de las competencias del DPO, cooperar con la autoridad de control a solicitud de esta o a iniciativa propia.

- Actuar como contacto para la autoridad de supervisión y control sobre:
  - Cuestiones relacionadas con el tratamiento
  - Consultas que se puedan plantear
  - Colaborar con ésta, dentro de sus competencias, ya sea por iniciativa propia o a su solicitud.

- **Desempeño profesional.**

  - Externalización y compartición del DPO: El delegado de protección de datos puede ser compartido por un grupo de empresas, por lo que puede trabajar a tiempo parcial en cada una de ellas. Además esta tarea la puede realizar externamente.

  - Independencia: El mandato de esta figura debe durar un periodo mínimo de dos años para que no haya una excesiva movilidad en el puesto, salvo que incumpla su trabajo.

  - Apoyo a la dirección: El responsable o el encargado del tratamiento velarán por que el delegado de protección de datos desempeñe sus funciones y tareas con independencia y no reciba ninguna instrucción en lo que respecta al ejercicio de sus funciones. El delegado de protección de datos informará directamente a la dirección del responsable o del encargado del tratamiento.

  El responsable o el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de sus tareas y facilitarán el personal, los locales, los equipamientos y cualesquiera otros recursos necesarios para el desempeño de sus funciones.

- **¿Qué perfil formativo debe tener el DPO?**

  No se deja claro en el borrador si el perfil formativo de esta nueva figura debe ser un Licenciado en Derecho con conocimientos de informática o un Ingeniero Informático con conocimiento de la ley. Aunque seguramente ambos perfiles serán válidos.

13. Glosario

- **Activo:** Todo lo que aporta valor a una organización.
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar la extensión en que se cumplen los criterios de auditoría.[BSI]
- **Certificación:** El acto de documentar, por parte de una entidad de certificación, el cumplimiento de los requisitos acordados en una normativa.
- **Cliente:** Persona o organización que recibe un producto.
- **Conformidad:** Cumplimiento de un requisito
- **Control:** Forma de gestionar el riesgo, incluyendo: políticas, procedimientos, guías, prácticas o estructuras organizacionales, que pueden ser naturaleza administrativa, técnica, de gestión o legal.[BSI]
- **Datos de carácter personal:** Cualquier información concerniente a personas físicas identificadas o identificables. *[AEPD]*
- **Datos de carácter personal relacionados con la salud**: Las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética. [AEPD]

- **Dato disociado:** Dato manipulado de tal forma que no permite la identificación de un afectado o interesado.
- **Evidencias de auditoría:** Pruebas que dictaminan que lo que se dice en el informe de auditoría es correcto. .[BSI]
- **Encargado del tratamiento:** La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento. [AEPD]
- **Fichero:** Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. [AEPD]
- **Proceso**: Conjunto de actividades interrelacionadas que transforman entradas en salida.[BSI]
- **Responsable del fichero o tratamiento:** Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento. [AEPD]
- **Riesgo**: Situación que puede ocurrir en los proyectos e impactar de forma negativa
- **Seguridad de la información**: Preservación de la confidencialidad, integridad y disponibilidad de la información, pudiendo abarcar otras propiedades como la autenticidad, la responsabilidad y el no repudio [BSI].
- **Transferencia de datos: El** transporte de los datos entre sistemas informáticos por cualquier medio de transmisión, así como el transporte de soportes de datos por correo o por cualquier otro medio convencional. [AEPD]

- **Transferencia internacional de datos:** Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español. [AEPD]

- **Validación:** Confirmación a través de la provisión de evidencia objetiva de que los requisitos para un uso o aplicación previstos han sido cumplidos. [BSI]

- **Verificación:** Confirmación a través de la provisión de evidencia objetiva de que los requisitos especificados han sido cumplidos [BSI].

- **Vulnerabilidad**: Debilidad de un activo que puede ser explotada por una amenaza. [BSI]

14. Conclusiones y nuevos horizontes de investigación.

En este proyecto se ha conseguido plasmar el trabajo de auditor informático tan desconocido para los estudiantes de Informática como necesario para las organizaciones de hoy en día. Con su lectura el lector puede darse cuenta de la importancia que tiene la auditoría de los sistemas de información de una organización, además gracias a los ejemplos prácticos aportados, el lector ha conocido perfectamente cuál es el día a día de un auditor en su jornada laboral y cómo debe trabajar.

Además el lector ha aprendido como se aplica la ley de protección de datos personales en España, una de las leyes más restrictivas sobre privacidad del mundo, la cual ha demostrado durante estos años ser una ley que ha ayudado a proteger la privacidad de las personas. Con la lectura del proyecto, el lector comprende por qué se está enfrentando a unos de sus momentos más importantes en su historia, las nuevas amenazas que algunas nuevas tecnologías pueden desarrollar y cómo se debe reaccionar ante ellas.

Esta normativa ha aportado a la sociedad española uno de los objetivos que se pretende volver a poner en valor con la lectura de este proyecto: La importancia de la privacidad. Este es uno de nuestros derechos como ciudadanos y debemos ejercerlo ya que si lo perdiéramos podrían surgirnos nuevos problemas derivados del uso fraudulento de nuestros datos.
Es por ello que la ciudadanía debe conocer sus derechos, las medidas que se adoptan para proteger sus datos y los cambios en la regulación que se discuten actualmente en Europa.

Además de los próximos cambios en la normativa, el lector ha conocido las particularidades técnicas a las que se enfrenta la normativa actual ante tecnologías como el cloud computing y el uso de cookies.

Como continuación a este trabajo se podría proponer a nuevos estudiantes un desarrollo más pormenorizado de la nueva regulación europea cuando ésta haya sido aprobada. Además también se podrían poner casos específicos de auditorías con cloud computing, Big data u otras tecnologías que se consideren importantes en el futuro.

15. Presupuesto

El objetivo del proyecto es analizar la protección y la auditoría de cumplimiento que pasan los datos personales para su protección actualmente desde un punto de vista práctico, así como de analizar los próximos cambios en su futuro inmediato.

El desarrollo de este trabajo ha consistido en la búsqueda de información sobre todo de forma práctica y plasmarlo finalmente en este proyecto.

El proyecto comenzó con la creación de un índice con los puntos más importantes que propuse a mi tutor según mi experiencia en el mundo de la auditoría. Posteriormente estos puntos fueron creciendo gracias a la aportación de mi tutor.

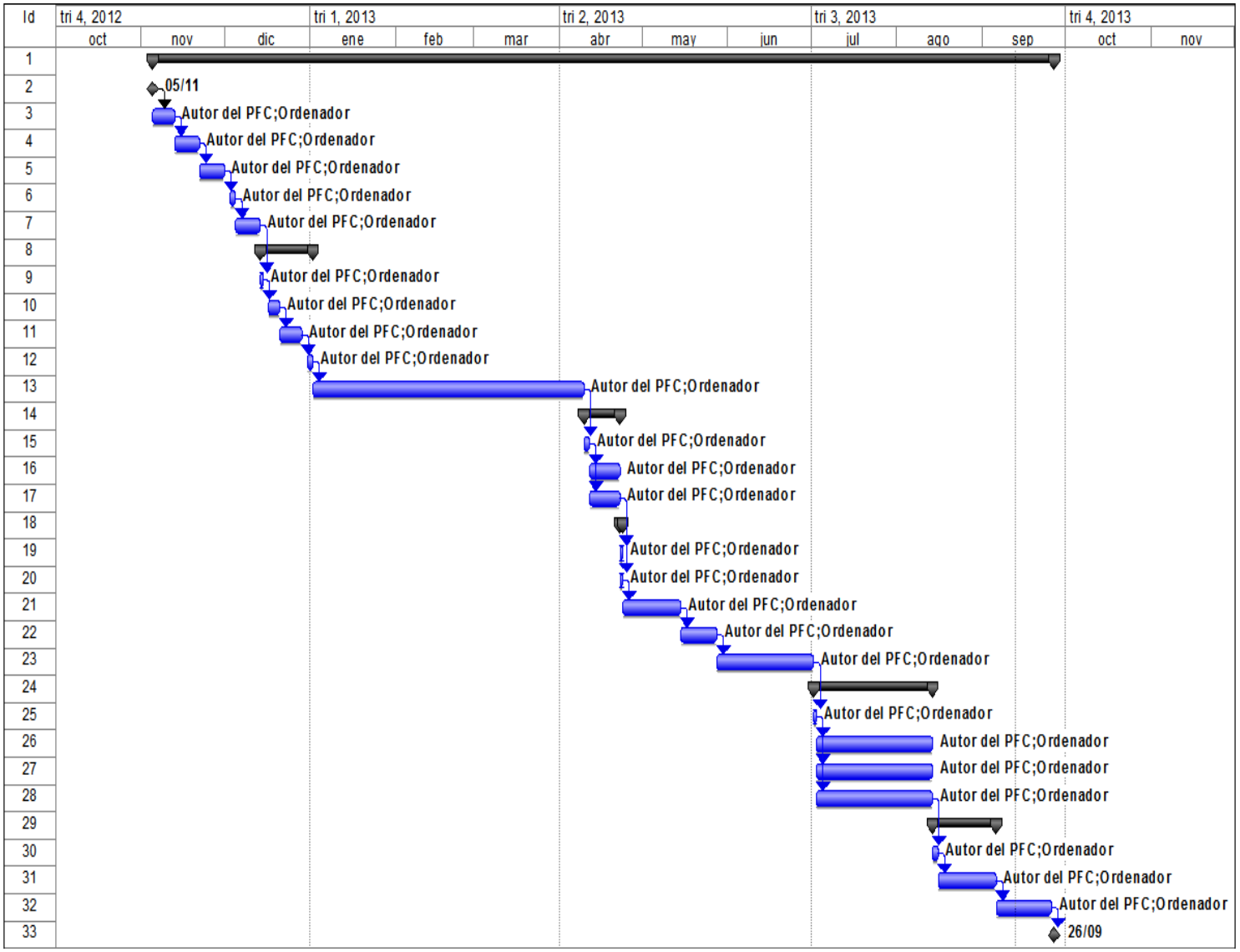
Cada cierto tiempo enviaba copias a mi tutor para que éste revisara mis aportaciones al proyecto. Él me decía lo que debía considerar importante y lo que no, así como mis equivocaciones y cosas que podía mejorar. Cuando me contestaba yo corregía todo lo que me había indicado e incluía las nuevas indicaciones y las que yo consideraba oportuno para que el me las volviese a evaluar.

Éste ciclo se ha repetido hasta que se ha considerado que el trabajo estaba completo y correcto.

Finalmente se ha procedido al repaso general del proyecto y su envío al tribunal poder ser presentado

A continuación se refleja lo escrito en un diagrama de GANTT:

Id	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos
1	PFC	**234 días**	**lun 05/11/12**	**jue 26/09/13**		**Autor del PFC;Ordenador**
2	Inicio	0 días	lun 05/11/12	lun 05/11/12		Autor del PFC;Ordenador
3	Elección de temas a tratar	6 días	lun 05/11/12	lun 12/11/12	2	Autor del PFC;Ordenador
4	Búsqueda de documentación	7 días	mar 13/11/12	mié 21/11/12	3	Autor del PFC;Ordenador
5	Lectura de documentación	7 días	jue 22/11/12	vie 30/11/12	4	Autor del PFC;Ordenador
6	Elección índice	2 días	lun 03/12/12	mar 04/12/12	5	Autor del PFC;Ordenador
7	Redacción de borrador	7 días	mié 05/12/12	jue 13/12/12	6	Autor del PFC;Ordenador
8	**Revisión índice de temas**	**13 días**	**vie 14/12/12**	**mar 01/01/13**		**Autor del PFC;Ordenador**
9	Revisión del tutor	1 día	vie 14/12/12	vie 14/12/12	7	Autor del PFC;Ordenador
10	Búsqueda de documentació	4 días	lun 17/12/12	jue 20/12/12	9	Autor del PFC;Ordenador
11	Modificar índice y borrador	6 días	vie 21/12/12	vie 28/12/12	10	Autor del PFC;Ordenador
12	Revisión del tutor	2 días	lun 31/12/12	mar 01/01/13	11	Autor del PFC;Ordenador
13	Redactar PFC	70 días	mié 02/01/13	mar 09/04/13	12	Autor del PFC;Ordenador
14	**Revisión de contenido**	**9 días**	**mié 10/04/13**	**lun 22/04/13**		**Autor del PFC;Ordenador**
15	Revisión del tutor	2 días	mié 10/04/13	jue 11/04/13	13	Autor del PFC;Ordenador
16	Aplicar modificaciones	7 días	vie 12/04/13	lun 22/04/13	15	Autor del PFC;Ordenador
17	Redactar PFC	7 días	vie 12/04/13	lun 22/04/13	15	Autor del PFC;Ordenador
18	**Revisión de contenido**	**1 día**	**mar 23/04/13**	**mar 23/04/13**		**Autor del PFC;Ordenador**
19	Sugerencias al tutor	1 día	mar 23/04/13	mar 23/04/13	17	Autor del PFC;Ordenador
20	Contestación del tutor	1 día	mar 23/04/13	mar 23/04/13	17	Autor del PFC;Ordenador
21	Búsqueda de documentación	15 días	mié 24/04/13	mar 14/05/13	20	Autor del PFC;Ordenador
22	Realizar modificaciones	9 días	mié 15/05/13	lun 27/05/13	21	Autor del PFC;Ordenador
23	Redactar PFC	25 días	mar 28/05/13	lun 01/07/13	22	Autor del PFC;Ordenador
24	**Revisión de contenido**	**31 días**	**mar 02/07/13**	**mar 13/08/13**		**Autor del PFC;Ordenador**
25	Revisión del tutor	1 día	mar 02/07/13	mar 02/07/13	23	Autor del PFC;Ordenador
26	Aplicar modificaciones	30 días	mié 03/07/13	mar 13/08/13	25	Autor del PFC;Ordenador
27	Búsqueda de documentación	30 días	mié 03/07/13	mar 13/08/13	25	Autor del PFC;Ordenador
28	Redactar PFC	30 días	mié 03/07/13	mar 13/08/13	25	Autor del PFC;Ordenador
29	**Revisión de contenido**	**17 días**	**mié 14/08/13**	**jue 05/09/13**		**Autor del PFC;Ordenador**
30	Revisión del tutor	2 días	mié 14/08/13	jue 15/08/13	28	Autor del PFC;Ordenador
31	Aplicar modificaciones	15 días	vie 16/08/13	jue 05/09/13	30	Autor del PFC;Ordenador
32	Repaso y preparación exposición	14 días	vie 06/09/13	mié 25/09/13	31	Autor del PFC;Ordenador
33	Fin	1 día	jue 26/09/13	jue 26/09/13	32	Autor del PFC;Ordenador


Id
tri 4, 2012
oct
nov
dic
tri 1, 2013
ene
feb
mar
tri 2, 2013
abr
may
jun
tri 3, 2013
jul
ago
sep
tri 4, 2013
oct
nov
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
05/11
Autor del PFC;Ordenador
26/09

El coste del proyecto en material no ha sido alto, gracias a que se ha podido encontrar mucha información gratuitamente en bibliotecas, Internet, empresas públicas y la documentación se ha podido conseguir de primera mano en una empresa privada del sector. Por lo que consideraríamos como gastos la conexión a Internet y la electricidad (70€/mes), fotocopias (15€/mes) y transporte público (40€/mes).

El coste humano tampoco ha sido excesivo ya que sólo una persona ha podido realizar toda esta labor por lo que el coste en su sueldo ha sido de 1000 euros/mes. “El presupuesto total de este proyecto asciende a la cantidad de 12.635 euros.

UNIVERSIDAD CARLOS III DE MADRID
Escuela Politécnica Superior

PRESUPUESTO DE PROYECTO

1.- Autor: Pedro Delgado Bueno

2.- Departamento: Informática

3.- Descripción del Proyecto: Proyecto de fin de carrera de Pedro Delgado Bueno
- Título: Datos personales: Su protección y auditoría desde una visión práctica
- Duración (meses): 11

4.- Presupuesto total del Proyecto (valores en Euros): 12.635 Euros

5.- Desglose presupuestario (costes directos)

PERSONAL

Apellidos y nombre	N.I.F. (no rellenar - solo a título informativo)	Categoría	Dedicación (hombres mes)	Coste hombre mes	Coste (Euro)
Delgado Bueno, Pedro		Ingeniero Informático	11	1.000,00	11.000,00
		Hombres mes	11,00	Total	11.000,00

COSTES DEL PROYECTO

Descripción	Coste (Euro)	% Uso dedicado proyecto	Dedicación (meses)	Coste (Euro)
Conexión a Internet y electricidad	70,00	100	11	770,00
Fotocopias	15,00	100	11	165,00
Microsoft Project	0,00	100	11	0,00
			Total	935,00

OTROS COSTES

Descripción	Coste (Euro)
Dietas	300,00
Transporte público	400,00
Total	700,00

COSTES TOTALES

Presupuesto Costes Totales	Presupuesto Costes Totales
Personal	11.000
Costes del proyecto	935
Otros costes	700
Total	12.635,00

Leganés a X de MMMM de 2013

El ingeniero proyectista

Fdo. Pedro Delgado Bueno

16.Bibliografía y Referencias

- [ASPPROF] Aspectos profesionales: Protección de Datos, Cloud Computing y Sistemas de Gestión. (Internet):< http://www.aspectosprofesionales.info/>

- [AEPD] Web de la AEPD (Internet): <http://www.agpd.es/>

- [AEPDCL] Guía para clientes que contraten servicios de Cloud Computing y Guía para el uso de Cookies <https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php>

- [APDCM] Cuaderno informativo sobre Protección de Datos de la agencia de protección de datos de la comunidad de Madrid (Internet): <http://www.protecciondedatos.urjc.es/proteccion_de_datos/PD/interespdf/guiainformativa.pdf>

- [BSI] Curso de formación en The British Standars Institution (BSI Spain)

- [CURSO] Curso de formación para empleados de auditoría Informática en empresa de Auditoría.

- [EUR] 6 Novedades que traerá el Reglamento Europeo de Protección de Datos a la empresa- Belén Viyella Molina, Asociada Senior de Information Technology de ECIJA. (Internet): <http://www.microsoft.com/business/es-es/Content/Paginas/article.aspx?cbcid=609>

- [LOPD] LEY ORGÁNICA 15/1999, de 13 de Diciembre, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL. (BOE)

- [MAR] Apuntes UC3M, Auditoría Informática. Profesor Miguel Ángel Ramos

- [PERU] Ingeniería de Sistema e Informática - Universidad Alas Peruanas (Internet): <http://es.slideshare.net/ema_89/tema1-la-informacin >

- [RA-MA] Auditoría de tecnologías y sistemas de información. Ed. RA-MA

- [RD] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

- [SHELLSEC] Noticias Diarias de seguridad informática (Internet): <http://www.shellsec.net/articulo/auditoria-empresas/>