Capítulo 5
Realización y ejecución de la auditoría: fase 2ª

1. Introducción

Para llevar a cabo la realización de la auditoría, se seguirá el orden lógico establecido en el programa acordado, el cual ha de permitir las evidencias de las cuestiones planteadas en la lista de comprobación conocido con el nombre de **check list.**

Esta lista ha de considerarse un documento guía, que puede sufrir las modificaciones que el auditor considere necesarias en el transcurso de la auditoría, como la inclusión de nuevas cuestiones o la eliminación de algunas existentes, que veremos más adelante.

El objetivo de la auditoría es determinar la adecuación de la empresa a la protección de datos.

Para la obtención de las evidencias, el auditor utilizará los siguientes métodos:

- Examen de la documentación aportada por la entidad auditada.
- Entrevistas con el personal.
- Inspección visual de las actividades auditadas.

El auditor examinará el conjunto de los documentos relativos a la protección de datos, incluyendo la política, los objetivos, el programa, el manual, y los procedimientos e instrucciones técnicas, así como los registros relativos a la protección de datos. Se actuará del siguiente modo:

- Ver si la documentación relativa a la protección de datos cumple con los requisitos establecidos en el Reglamento de desarrollo de la LOPD.
- Ver si se dispone de la documentación necesaria en los lugares donde ésta se utilice (aunque el auditor ya disponga de ella).

2. ENTREVISTAS CON EL PERSONAL

Para realizar las entrevistas tenemos que tener en cuenta lo siguiente:

- Presentarse, y explicar por qué y para qué se está allí.
- Utilizar un lenguaje adecuado al interlocutor, no actuar con prepotencia, explicar cuanto sea necesario, ser paciente, etc.
- Ser puntual, educado, etc.

Para realizar las preguntas lo haremos de la siguiente forma:

- Realizar preguntas abiertas para tantear, y acotar aquello que se desee obtener o evidenciar y realizar preguntas cerradas con bases sólidas y evidenciales que permitan emitir un veredicto.
- Emplear argumentos positivos y formular preguntas siempre de modo afirmativo.
- No resultar capcioso a la hora de formular las cuestiones.
- Las preguntas se formulan a la persona que realiza el trabajo o responsable de la actividad auditada.
- Repetir la pregunta si es preciso o formularla de otro modo, si no es entendida.
- Tomar notas sin inferir en el desarrollo de la entrevista.

Finalizar la entrevista siempre de una manera positiva, haciendo un breve resumen al entrevistado y agradeciéndole su ayuda y tiempo prestado.

3. INSPECCIÓN VISUAL DE LAS ACTIVIDADES AUDITADAS

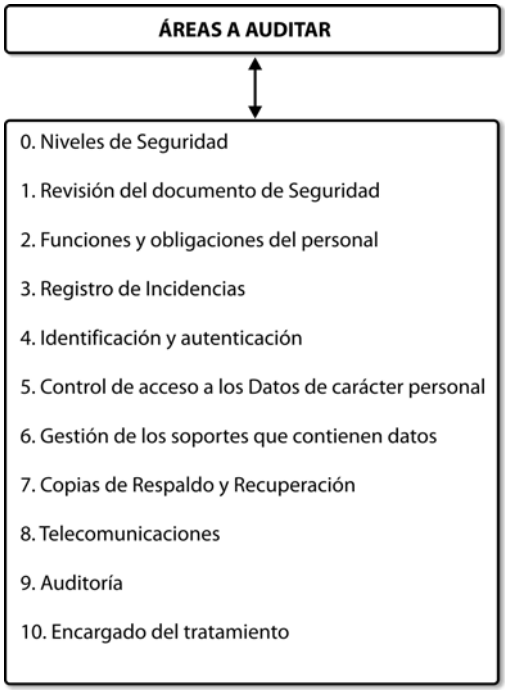
Existen, en el transcurso de una auditoría, determinadas instalaciones, equipos o similar, que lógicamente no pueden ser entrevistados, y no generan ningún tipo de registro, por lo que requiere de una visita para comprobar lo que se recoge en la documentación.

La auditoría ya se realice mediante la revisión de la documentación, entrevista con el personal o inspección visual el auditor ha de procurar:

- Describir el momento en que se detectan los hechos que no son conformes con los criterios de auditoría.
- Detectar los puntos que han de ser investigados con mayor profundidad y asegurarse de que todos han estado comprobados.
- Basar las no conformidades en hechos objetivos y demostrables.
- Contrastar la información en diversas fuentes y con el resto de integrantes de la auditoría.

Para la realización organizada de esta auditoría se ha preparado una tabla de control o de *checklist*. Esta tabla está divida en once áreas de manera que se puedan identificar aquellos ítems a auditar de una manera lógica.

De esta manera las áreas serán las que se presentan a continuación con la siguiente tabla:



REVISIÓN Y VERIFICACIÓN DE LA INFORMACIÓN Y DOCUMENTACIÓN RECIBIDA PARA LLEVAR A CABO LA AUDITORÍA. NIVEL MEDIO

Debemos revisar la documentación para asegurar que se encuentra allí donde se necesita y que el personal la conoce y actúa en consecuencia. El estudio y análisis de la documentación y los registros ha de ser los más exhaustiva posible. Durante la auditoría, han de establecer criterios objetivos, y que aseguren, en la medida de lo posible, una revisión lo más completa posible.

En cuanto a los registros, debemos elegir carpetas al azar de los archivos, (los elige el auditor, no el auditado, pues podrían estar preparados).

La importancia de esta tarea reside en que el cumplimiento de determinadas normas de seguridad, solo es exigido por el Reglamento para los ficheros de nivel medio y alto. La identificación de los sistemas que contienen estos ficheros puede,

por un lado, permitir a la empresa restringir la aplicación de las medidas de seguridad de esos niveles exclusivamente a aquellos sistemas para los que es obligado, lo que a su vez, puede redundar en un abaratamiento de costes si la empresa es grande, sus sistemas de información tiene un alto grado de descentralización y la aplicación de las medidas supone la realización de una inversión.

AUDITORÍA DE PROTECCIÓN DE DATOS		
REVISIÓN DEL DOCUMENTO DE SEGURIDAD N.º: 0. NIVELES DE SEGURIDAD		
Entidad: Gestoría Solano		
Nombre Fichero/Tratamiento: Personal	N.º Inscripción del Fichero: 32548	
Nivel de Seguridad: **MEDIO**	Fecha Auditoría: 14/03/09	
Aprobado por: D. Antonio Ruiz Escalante		Fecha: 18/03/09
Realizado por: : D. Antonio Ruiz Escalante		Fecha: 20/03/09

4. ¿QUÉ CUESTIONES DEBE PLANTEARSE EL AUDITOR PARA LA COMPROBACIÓN Y VERIFICACIÓN DE LOS NIVELES DE SEGURIDAD APLICADOS EN LA IMPLANTACIÓN DE LA LOPD?

Hay que tener en cuenta lo siguiente:

- Ver si la clasificación del nivel de seguridad es adecuada respecto a la naturaleza de la información contenida en cada uno de lo ficheros.
- Comprobar si se han creado, modificado o suprimido ficheros con datos de carácter personal desde la última auditoría.

¿Qué documentación se necesita para comprobarlo?

Es necesario solicitar la siguiente documentación:

- Notificación de la inscripción del fichero emitida por la Agencia Española de Protección de Datos.
- Copia del formulario a cumplimentar para la inscripción o modificación del fichero, emitido por la Agencia Española de protección de datos, a petición de la entidad titular del fichero (no puede darse por válido un formulario proporcionado por la propia entidad auditada, pues podría no coincidir con el enviado en su día a la AEPD).
- Documento de Seguridad-la parte estática: las políticas y normas generales de actuación.

¿Cómo realizar el análisis de la documentación?

1.	**Análisis de la documentación:**
1.1.	Comprobar la correlación entre la notificación de la inscripción del fichero enviada por la Agencia Española de Protección de Datos (AEPD) y la copia, emitida por la misma Agencia, del formulario para notificación del tratamiento de datos de carácter personal.
1.2.	Rellenar el encabezado de los papeles de la auditoría con los datos detallados en la notificación de la inscripción del fichero ante la AEPD.
1.3.	Confirmar que el nivel de seguridad incluido en el Documento de Seguridad coincide con el declarado ante la AEPD.
1.4.	Identificar aquellos campos que justifican el nivel de seguridad asignado con base en la información incluida en la copia del formulario para notificación del tratamiento de datos de carácter personal emitida por la AEPD.
1.5.	En el caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud, o vida sexual objeto de auditoría, comprobar si existe motivo para aplicar las medidas de seguridad de nivel básico en lugar de las de nivel alto. Se aplicarán las medidas de nivel básico si: – Los datos se utilizan con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros. – Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad. – Se trata de un fichero o tratamiento con datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.
1.6.	Comprobar si el Documento de Seguridad incluye:

	Visto	Apartado Documento Seguridad
La aplicación de normativa específica debido al tipo de actividad desarrollada por la entidad, por el tipo de datos tratados o por su finalidad.		
La segregación de sistemas de tratamiento por ficheros, para una aplicación diferencias de las medidas de seguridad.		
Procedimientos para el uso, clasificación y eliminación de ficheros temporales o copias de documentos.		

En este punto del plan de trabajo, el auditor obtuvo un inventario de los ficheros y sistemas de información con datos personales existentes, que la empresa había realizado en un momento anterior, con ocasión de la elaboración del Documento de Seguridad.

Comprobación de registros

Para comprobar los registros debemos solicitar las fuentes utilizadas para la recogida de datos, (formularios, Web, papel etc.).

2.	Comprobación de Registros:
2.1.	Acceder a las diferentes plantillas y formularios de recogida de datos del fichero para detectar campos no incluidos en la declaración o en el contrato de tratamiento por cuenta del Responsable del Fichero, especialmente si éstos suponen un cambio en la calificación del nivel de seguridad del fichero.

Inspección visual

Se debe indicar si existen discordancias entre los datos tratados por la entidad y los declarados en la inscripción del fichero en la AEPD.

3.	Inspección visual:
3.1.	Verificar que la realidad global observada en la entidad en relación con los datos personales tratados es coherente con la tipología de datos declarados.
3.2.	Observar si, en caso de segregación de sistemas de tratamiento, hay una efectiva delimitación de acceso a datos y usuarios.

Para cada uno de los sistemas que contienen datos de carácter personal, el auditor ha revisado los controles y normas relacionados con la identificación y autenticación de usuarios, así como los derechos de acceso concedidos.

4.1. REVISIÓN DEL DOCUMENTO DE SEGURIDAD. NIVEL MEDIO

El auditor para llevar a cabo la revisión y verificación del Documento de Seguridad debe plantearse una serie de cuestiones que son las siguientes:

- ¿Ha elaborado el Responsable del Fichero el Documento de Seguridad?
- ¿Contiene los aspectos mínimos exigidos por el Reglamento?
- ¿Está el documento actualizado?, ¿se ha revisado cuando se han producido cambios relevantes desde la auditoría anterior?
- ¿Está su contenido adecuado a la normativa vigente en este momento en materia de seguridad de los datos de carácter personal?
- ¿Se ha indicado con qué periodicidad se deben cambiar las contraseñas?, ¿es inferior o igual a un año?
- ¿Se especifica cuál es el personal autorizado para la concesión, alteración o anulación de accesos autorizados sobre datos o recursos?
- ¿Se especifica cuál es el personal autorizado para acceder a los lugares donde se almacenan los soportes informáticos?
- Si el tratamiento se realiza por cuenta de terceros, ¿se han reflejado los ficheros afectados por el encargo, con referencia expresa al contrato, así como la identificación del Responsable y el período de vigencia?
- ¿Se ha reflejado en el Documento de Seguridad si los datos personales se incorporan y tratan exclusivamente en los sistemas del encargado?
- ¿Se ha delegado en el Encargado del Tratamiento la llevanza del Documento de Seguridad para los ficheros objeto del contrato?, ¿se ha reflejado esta circunstancia en el contrato?
- ¿Establece la identidad del Responsable o Responsables de Seguridad?, ¿se especifica si la designación es única para todos los ficheros o está diferenciada según el sistema de tratamiento utilizado?
- ¿Contiene los procedimientos y controles periódicos a realizar para verificar el cumplimento de lo dispuesto en el propio documento?
- ¿Especifica qué medidas hay que adoptar en caso de desechado o reutilización de soportes?
- ¿Relaciona las personas que están autorizadas a acceder físicamente a los locales donde se ubican los sistemas de información?

AUDITORÍA DE PROTECCIÓN DE DATOS		
REVISIÓN DEL DOCUMENTO DE SEGURIDAD N.º: 1. DOCUMENTO DE SEGURIDAD		
Entidad: Cristalería Garcia		
Nombre Fichero/Tratamiento: clientes y proveedores	N.º Inscripción del Fichero: 032568	
Nivel de Seguridad: **MEDIO**	Fecha Auditoría: 12/04/09	
Aprobado por: D. Antonio Ruiz Escalante		Fecha: 16/04/09
Realizado por: : D. Antonio Ruiz Escalante		Fecha: 12/04/09

¿Qué documentación es necesaria para realizar la comprobación?

Hay que solicitar la siguiente documentación:

- Documento de Seguridad: normas generales de actuación.
- Organigrama funcional de la entidad.

En la siguiente tabla vamos a ver el análisis de la documentación:

1.1.	**Análisis de la documentación:**
1.1.1.	Obtener el o los Documentos de Seguridad y comprobar si su alcance se corresponde con el alcance de la auditoría.
1.1.2.	Identificar si en el Documento de Seguridad obtenido se hace referencia a la existencia de otros Documentos de Seguridad según sea el tratamiento de los datos o ficheros utilizados.

1.1.3. Comprobar que el Documento de Seguridad contiene los puntos mínimos exigibles según el RDLOPD y referenciar en qué apartados del Documento están incluidos estos puntos:

		Visto	Apartado Documento Seguridad
1.	Ámbito de aplicación.		
2.	Detalle de los recursos protegidos.		
3.	Medidas, normas, procedimientos, reglas y estándares de seguridad.		
4.	Funciones y obligaciones del personal.		
5.	Estructura de los ficheros.		
6.	Descripción de los sistemas de información.		
7.	Procedimiento de notificación de incidencias. Cruzar la información de esta prueba con la realizada en el PT-3.1.1.		
8.	Procedimiento de gestión de incidencias. Cruzar la información de esta prueba con la realizada en el PT-3.1.1.		
9.	Procedimiento de respuesta ante incidencias.		
10.	Procedimiento de realización de copias de respaldo. Cruzar la información de esta prueba con la realizada en el PT-7.1.1.		
11.	Procedimiento de recuperación de datos. Cruzar la información de esta prueba con la realizada en el PT-3.1.2 y 7.1.1.		
12.a)	Medidas para el transporte de soportes. Cruzar la información de esta prueba con la realizada en el PT-6.1.3.c).		
12.b)	Medidas para el transporte de documentos. Cruzar la información de esta prueba con la realizada en el PT-6.1.3.c).		
13.a)	Medidas para la destrucción de soportes. Cruzar la información de esta prueba con la realizada en el PT-6.1.3.b).		
13.b)	Medidas para la destrucción de documentos. Cruzar la información de esta prueba con la realizada en el PT-6.1.3.b).		
14.	Medidas para la reutilización de soportes.		
15.	Relación de autorizados para delegar responsabilidades. Cruzar la información de esta prueba con la realizada en el PT-2.1.2.		
16.	Relación de responsables por delegación. Cruzar la información de esta prueba con la realizada en el PT-2.1.2.		

1.1.4. Comprobar que el Documento de Seguridad incluye información acerca del tratamiento de datos por cuenta de terceros y referenciar en qué apartados del Documento están incluidos estos puntos:

		Visto	Apartado Documento Seguridad
1.	Identificación de los ficheros tratados como Encargado del Tratamiento.		
2.	Referencia al contrato suscrito para cada tratamiento de los datos por cuenta ajena.		
3.	Identificación de cada Responsable del Fichero tratado como Encargado del Tratamiento.		
4.	Periodo de vigencia del encargo.		

1.1.5. Comprobar si en el Documento de Seguridad se declara que en el fichero auditado los datos personales se incorporan y tratan de forma exclusiva en las instalaciones del Encargado del Tratamiento.

1.1.6. Con base al punto anterior, comprobar si el Documento de Seguridad ha sido elaborado por el Encargado del Tratamiento por delegación. Cruzar la información de esta prueba con la realizada en el PT-1.2.3.

1.1.7. Comprobar que el Documento de Seguridad incorpora las novedades en la normativa de protección de datos personales. Cruzar la información de esta prueba con la realizada en el PT-1.2.6.

1.1.8. Comprobar que el Documento de Seguridad contiene los puntos mínimos exigibles según el RDLOPD y referenciar en qué apartados del Documento están incluidos estos puntos:

		Visto	Apartado Documento Seguridad
1.	Identificación del Responsable de Seguridad.		
2.	Procedimiento de realización de los controles periódicos.		

1.1.9. Analizar si la posición ocupada por el Responsable de Seguridad en el organigrama le permite el correcto desempeño de sus funciones.

1.1.10 Comprobar si en el Documento de Seguridad se recoge la designación del Responsable de Seguridad y si es única o diferenciada por ficheros o tratamientos.

¿Qué documentos son necesarios para la comprobación de registros?

Es necesario solicitar los siguientes registros:

- Documento de Seguridad- la parte dinámica, registros.
- Listado de las actualizaciones del documento.
- Carta/s de nombramiento del Responsable de Seguridad encargado de coordinar y controlar las medidas definidas en el Documento de Seguridad.
- Comunicación a las personas autorizadas para delega responsabilidad.
- Comunicación a las personas a las que se ha delegado alguna responsabilidad en materia de seguridad en el tratamiento de datos personales.
- Registro de controles periódicos, auditorías o informes.
- Registro de contratos realizados por la entidad como Encargado del Tratamiento de datos personales por cuenta de la entidad.
- Contrato realizado con el Encargado del Tratamiento que gestiona el Documento de Seguridad por cuenta de la entidad.
- Registro de actualizaciones o de control de versiones del Documento de Seguridad.
- Copia del formulario a cumplimentar para la modificación del fichero, emitida por la Agencia Española de Protección de Datos, a petición de la entidad titular del fichero.

1.2.	**Comprobación de Registros:**
1.2.1.	Comprobar la existencia de las comunicaciones a los autorizados para delegar responsabilidades por cuenta del Responsable del Fichero o Tratamiento e igualmente sobre los que recaen dichas responsabilidades.
1.2.2.	Verificar mediante los contratos suscritos como Encargado del Tratamiento que estos se encuentran relacionados en el Documento de Seguridad, se identifica el Responsable del Fichero o Tratamiento y el periodo de vigencia.
1.2.3.	Comprobar que los contratos de confidencialidad suscritos entre la entidad y los Encargados del Tratamiento incluyen la delegación de realizar el Documento de Seguridad para los ficheros o tratamientos tratados en exclusivo. *Cruzar la información de esta prueba con la realizada en el PT-1.1.6.*
1.2.4.	Verificar la actualización periódica del Documento de Seguridad, si existe, con el anexo sobre gestión de versiones o con los registros de los controles periódicos realizados.
1.2.5.	Comprobar si se han producido modificaciones en la inscripción del fichero posteriores a la última actualización del Documento de Seguridad.
1.2.6.	Comprobar la adecuación legal del Documento de Seguridad mediante el registro de actualizaciones y las fechas de entrada en vigor de la normativa aplicable a fecha de la auditoria. *Cruzar la información de esta prueba con la realizada en el PT-1.1.7.*
1.2.7.	Verificar mediante registros que acrediten la realización de los controles periódicos, que las fechas de éstos coinciden con la periodicidad establecida en el Documento de Seguridad.
1.2.8.	Averiguar si el Responsable de Seguridad ha sido designado mediante carta de nombramiento.
1.2.9.	Comprobar que el Responsable de Seguridad se encuentra en la lista actualizada del personal o existe contrato como Encargado del Tratamiento.

¿Cómo se lleva a cabo la inspección visual?

En este apartado hay que indicar si se observan indicios que denoten la implantación, divulgación e integración de la normativa interna de seguridad en la entidad y si esta se encuentra actualizada.

1.3.	**Inspección visual:**
1.3.1.	Comprobar si existen carteles informativos u otras advertencias que sean fácilmente visibles sobre el cumplimiento de medidas de seguridad.
1.3.2.	Según la actividad realizada por la entidad auditada, deducir la existencia de tratamientos de datos por cuenta de terceros no identificados en el Documento de Seguridad.
1.3.3.	Observar, en visita general, si la descripción de las instalaciones de la entidad en el Documento de Seguridad es adecuada y actual.

4.1.1. Revisión del Documento de Seguridad. Funciones y Obligaciones del Personal

AUDITORÍA DE PROTECCIÓN DE DATOS		
REVISIÓN DEL DOCUMENTO DE SEGURIDAD N.º: 2. FUNCIONES Y OBLIGACIONES DEL PERSONAL		
Entidad: Cristalería Gómez		
Nombre Fichero/Tratamiento: Personal	N.º Inscripción del Fichero: 0254871	
Nivel de Seguridad: **MEDIO**	Fecha Auditoría: 10/05/09	
Aprobado por: D. Antonio Ruiz Escalante		Fecha: 15/05/09
Realizado por: : María Palma Rodríguez		Fecha: 10/05/09

¿Qué cuestiones debe plantearse el auditor para la comprobación y verificación del apartado "Funciones y obligaciones del personal"?

El auditor debe plantearse las siguientes cuestiones:

- ¿Están las funciones y obligaciones del personal con acceso a datos de carácter personal y los sistemas de información claramente definidos?
- ¿Están documentadas y reflejadas en el Documento de Seguridad?

- ¿Se han definido las funciones de control o autorizaciones delegadas por el Responsable del Fichero?
- ¿Conoce el personal las medidas de seguridad que afectan al desarrollo de sus funciones?
- ¿Conoce las consecuencias de su incumplimiento?

Para comprobar la documentación es necesario solicitar:

- La descripción de las funciones de los usuarios y perfiles de usuarios dentro del Documento de Seguridad.
- Manual del empleado.
- Organigrama funcional del la entidad.
- Planes de formación de la empresa a sus trabajadores en materia de seguridad de la información.

Documentación necesaria para la comprobación

Son necesarios solicitar los siguientes documentos:

- Descripción de las funciones de los usuarios y perfiles de usuarios dentro del Documento de Seguridad.
- Manual del empleado.
- Organigrama funcional de la entidad.
- Planes de formación de la empresa a sus trabajadores en materia de seguridad de la información.

2.1.	**Análisis de la documentación:**
2.1.1.	Comprobar que las funciones de los usuarios o perfiles de usuario descritos en el Documento de Seguridad concuerdan con las descritas en el Manual de Empleado (si existe) y son coherentes con el organigrama funcional. Con el listado de funciones completar la prueba del *PT-5.2.3 Control de Acceso.*
2.1.2.	Comprobar que en el Documento de Seguridad se definen las funciones de control o las autorizaciones delegadas. *Cruzar la información de esta prueba con la realizada en el PT-1.1.3.*
2.1.3.	Comprobar si en el Documento de Seguridad se establece la difusión de su contenido entre el personal de la entidad.

Comprobación de registros

Para comprobar la documentación es necesario solicitar los siguientes registros:

- Justificantes de recepción por parte de los trabajadores de la comunicación del Responsable del Fichero o Tratamiento, sobre la existencia y obligado cumplimiento de las normas establecidas en el Documento de Seguridad, así como de las consecuencias de su incumplimiento.
- Listado actualizado (altas/bajas) o muestra de los usuarios activos en el sistema, obtenido del Departamento Informático.
- Listado o muestra de personal actualizado, por departamentos y categorías, y la fecha de alta en la entidad, obtenido del Departamento de Recursos Humanos.
- Justificantes de asistencia por parte de los usuarios a jornadas formativas en seguridad de la información, y más concretamente de protección de datos personales.

2.2.	**Comprobación de registros:**
2.2.1.	Analizar el listado actualizado de personal y el listado actualizado de usuarios del sistema, para comprobar que éstos son coherentes con las funciones detalladas en el Documento de Seguridad.
2.2.2.	Comprobar si hay justificantes de recepción por parte de los trabajadores de la comunicación del Responsable del Fichero sobre la existencia y obligado cumplimiento de las normas establecidas en el Documento de Seguridad, así como de las consecuencias de su incumplimiento.
2.2.3.	Obtener evidencia de asistencia a cursos de formación por parte de los usuarios en materia de seguridad de la información y protección de datos personales.

Inspección visual

En este apartado se indicará si se observan indicios de discordancias entre las funciones teóricas y las reales desarrolladas por el personal.

2.3.	**Inspección visual:**
2.3.1.	Observar durante la ejecución *in situ* de la auditoría si hay discordancias entre las funciones desarrolladas por los empleados y sus funciones según el Documento de Seguridad.

4.1.2. Revisión del Documento de Seguridad. Registro de incidencias

AUDITORÍA DE PROTECCIÓN DE DATOS		
REVISIÓN DEL DOCUMENTO DE SEGURIDAD N.º: 3. REGISTRO DE INCIDENCIAS		
Nombre Fichero/Tratamiento: Nóminas	N.º Inscripción del Fichero: 0231654	
Nivel de Seguridad: **MEDIO**	Fecha Auditoría: 23/02/09	
Aprobado por: D. Antonio Ruiz Escalante		Fecha:26/02/029
Realizado por: : D. Antonio Ruiz Escalante		Fecha: 23/02/09

¿Qué cuestiones debe plantearse el auditor para la comprobación y verificación del apartado "Registro de incidencias"?

- ¿Existe un procedimiento de notificación y gestión de incidencias de seguridad?, ¿el procedimiento está bien diseñado y es eficaz?
- ¿Conoce todo el personal afectado dicho procedimiento?
- ¿Existe un registro de incidencias donde se reflejen todos los datos exigidos en el Reglamento?, ¿se han registrado todas las incidencias ocurridas?
- ¿Se revisa periódicamente el registro de incidencias para su análisis y adopción de medidas correctoras de las incidencias anotadas?

- ¿Se han anotado las ejecuciones de los procedimientos de recuperación de datos realizados?
- ¿Figuran en estas anotaciones los datos exigidos por el Reglamento?
- ¿Existe la autorización por escrito del Responsable del Fichero?

¿Qué documentación es necesaria para la comprobación?

En este apartado es necesario solicitar la descripción de la gestión de incidencias, contenida en el Documento de Seguridad.

3.1.	**Análisis de la documentación:**
3.1.1.	Comprobar que el Documento de Seguridad incluye el procedimiento de notificación y gestión de incidencias. *Cruzar la información de esta prueba con la realizada en el PT-1.1.3.*
3.1.2.	Comprobar que el Documento de Seguridad incluye el procedimiento de recuperación de datos. *Cruzar la información de esta prueba con la realizada en el PT-1.1.3.*
3.1.3.	Comprobar que el procedimiento de recuperación de datos indica la obligación de disponer de autorización.

Comprobación de los registros

Se deben solicitar los siguientes registros:

- Registros de incidencias.
- Registros de las aplicaciones, antivirus, cortafuegos y copias de seguridad, que permitan detectar incidencias acontecidas en la entidad.
- Autorizaciones por escrito del Responsable del Fichero para la ejecución de los procedimientos de recuperación de datos.

- La comprobación de los registros, se realiza de la siguiente manera:

3.2.	**Comprobación de Registros:**		
3.2.1	Comprobar que el formulario del registro de incidencias contiene los campos mínimos fijados en el Documento de Seguridad. Debe contener:	*Visto*	*Notas*
	a) Tipo de incidencia.		
	b) Fecha en la que se produjo.		
	c) Persona que la notificó.		
	d) Persona que atendió la notificación.		
	e) Efectos derivados de la incidencia.		
	f) Medidas correctoras aplicadas.		
3.2.2.	Analizar si se rellenan todos los campos del registro de incidencias.		
3.2.3.	Averiguar, mediante los registros de actividad de algunas aplicaciones como antivirus, cortafuegos y copias de respaldo, si se han producido incidencias no incluidas en el registro de incidencias.		
3.2.4.	Comprobar que el formulario del registro de incidencias contiene los campos mínimos fijados en el Documento de Seguridad. Debe contener:	*Visto*	*Notas*
	a) Procedimientos realizados de recuperación de datos.		
	b) Persona que ejecutó el proceso.		
	c) Relación de datos restaurados.		
	d) Relación de datos grabados manualmente.		
3.2.5.	Comprobar que el Responsable del Fichero autoriza cada una de las recuperaciones de datos.		

Inspección visual

Se debe indicar si existen indicios de incidencias no registradas, también se deben realizar entrevistas con los Responsables y usuarios del sistema.

3.3.	Inspección visual:
3.3.1.	Observar si en los centros de trabajo existen elementos característicos relacionados con la gestión de alguna incidencia que pudiera no estar registrada, como por ejemplo la presencia de profesionales externos.

4.1.3. Revisión del Documento de Seguridad. Identificación y autentificación

AUDITORÍA DE PROTECCIÓN DE DATOS		
REVISIÓN DEL DOCUMENTO DE SEGURIDAD N.º: 4. IDENTIFICACIÓN Y AUTENTICACIÓN		
Entidad: Imprenta Gráficas		
Nombre Fichero/Tratamiento: Proveedores	N.º Inscripción del Fichero: 256498	
Nivel de Seguridad: **MEDIO**	Fecha Auditoría: 04/03/09	
Aprobado por: D. Antonio Ruiz Escalante		Fecha: 08/04/099
Realizado por: : D. Antonio Ruiz Escalante		Fecha: 04/08/09

El auditor para la comprobación y verificación del apartado "Identificación y autenticación" deben plantearse las siguientes cuestiones:

- ¿Existe una relación de usuarios con acceso autorizado?, ¿se mantiene actualizada?
- ¿Existen procedimientos de identificación y autenticación para dicho acceso?, ¿garantiza la correcta identificación del usuario?
- El mecanismo de acceso y verificación de autorización de los usuarios ¿les identifica de forma inequívoca y personalizada?
- ¿Existe un procedimiento de asignación, distribución y almacenamiento de contraseñas?, ¿garantiza su confidencialidad e integridad?
- ¿Se cambian las contraseñas con la periodicidad establecida en el Documento de Seguridad?
- ¿Se almacenan las contraseñas de forma ininteligible mientras están en vigor?
- ¿Se limita el intento reiterado de acceso no autorizado al sistema?, ¿se anotan estos intentos en el registro de incidencias?

¿Qué documentos necesitamos solicitar para la comprobación?

Debemos solicitar la descripción de los procedimientos de identificación y autentificación de la asignación, distribución, y almacenamiento de contraseñas dentro del Documento de Seguridad.

<table>
<tr><th colspan="2">4.1. Análisis de la documentación:</th></tr>
<tr><td>4.1.1.</td><td>Comprobar que el mecanismo de identificación y autenticación establecido garantiza el acceso de forma inequívoca y personalizada.</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>4.1.2.</td><td>Describir cómo se verifica la autorización de acceso al sistema de información.</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>4.1.3.</td><td>Comprobar que el procedimiento de identificación y autenticación descrito en el Documento de Seguridad se adecua a las exigencias de la normativa. Debe contener:
<table>
<tr><th></th><th>Visto</th><th>Notas</th></tr>
<tr><td>a) Procedimiento de asignación de contraseñas.</td><td></td><td></td></tr>
<tr><td>b) Procedimiento de distribución de contraseñas.</td><td></td><td></td></tr>
<tr><td>c) Procedimiento de almacenamiento de contraseñas.</td><td></td><td></td></tr>
<tr><td>d) Periodicidad del cambio de contraseñas.</td><td></td><td></td></tr>
<tr><td>e) Almacenamiento ininteligible de contraseñas.</td><td></td><td></td></tr>
</table></td></tr>
<tr><td>4.1.4.</td><td>Verificar que estos procedimientos garantizan la confidencialidad e integridad.</td></tr>
<tr><td colspan="2"></td></tr>
</table>

Comprobación de los registros

Se deben solicitar los siguientes registros:

- Listado de parámetros de las políticas de seguridad del sistema de nombres de usuario y sus contraseñas.
- Registro de accesos no autorizados y del histórico de usuarios bloqueados.
- Listado actualizado (altas /bajas) de usuarios activos en el sistema, obtenido del Departamento Informático.
- Listado del personal actualizado, por departamentos y categorías, y la fecha de alta en la entidad, obtenido del Departamento de Recursos Humanos.

Cuando se haya obtenido toda la información comprobamos los registros de la siguiente manera:

4.2.	**Comprobación de Registros:**
4.2.1.	Comprobar en el listado de usuarios, que no hay usuarios genéricos para grupos de personas: debe establecerse un usuario para cada persona.
4.2.2.	Comprobar que existe una relación de usuarios y perfiles de usuarios.
4.2.3.	Comprobar que todos los integrantes del listado de usuarios (Departamento de Informática) están incluidos en el listado de personal (Departamento de Recursos Humanos) o en el de Encargados del Tratamiento. – Para el personal no incluido en el listado de usuarios, averiguar el motivo: se trata de personal sin acceso al sistema de información, o bien el listado de usuarios no está actualizado. – Para los usuarios no incluidos en la lista de personal o de Encargados del Tratamiento, verificar que sus perfiles de usuario se encuentran deshabilitados.
4.2.4.	Analizar los parámetros del registro de políticas de seguridad para ver si el sistema está configurado para obligar a los usuarios a cambiar las contraseñas con la periodicidad establecida en el Documento de Seguridad.
4.2.5.	Comprobar mediante el listado de accesos no autorizados y del histórico de usuarios bloqueados que se limita el intento reiterado de acceso al sistema de información.

Inspección visual

Deberán observarse los siguientes aspectos:

- Almacenamiento ininteligible de las contraseñas vigentes: confidencialidad e integridad.
- Limitación del número de intentos de acceso no autorizado al sistema de información.
- Entrevistas con Responsables y Usuarios del Sistema.

4.3.	**Inspección visual:**
4.3.1.	Observar la confidencialidad de las contraseñas, en caso de que se almacenen por escrito (agendas en papel y electrónicas, documentos informáticos, etc.).
4.3.2.	Observar que no hay apuntadas contraseñas en los puestos de trabajo.
4.3.3.	Comprobar mediante la introducción de contraseñas aleatorias cuántos intentos fallidos son necesarios para bloquear a los usuarios de la entidad.

4.1.4. Revisión del Documento de Seguridad. Control de accesos

AUDITORÍA DE PROTECCIÓN DE DATOS		
REVISIÓN DEL DOCUMENTO DE SEGURIDAD N.º: 5. CONTROL DE ACCESO		
Entidad: Cristalería García		
Nombre Fichero/Tratamiento: Clientes y proveedores	N.º Inscripción del Fichero: 326584	
Nivel de Seguridad: **MEDIO**	Fecha Auditoría: 02/02/09	
Aprobado por: D. Antonio Ruiz Escalante		Fecha: 07/02/09
Realizado por: : D. Antonio Ruiz Escalante		Fecha: 02/02/09

¿Qué cuestiones debemos plantearnos para la verificación del control de accesos?

- ¿Los accesos autorizados de los usuarios se corresponden exclusivamente con los datos y recursos que requieren para el desarrollo de sus funciones?
- ¿Existen mecanismos que impidan que los usuarios accedan a datos o recursos distintos de los autorizados?
- ¿Existe una relación de usuarios?, ¿especifica qué datos y recursos tiene autorizados para cada uno de ellos? ¿Está actualizada?
- ¿La concesión, alteración o anulación de accesos autorizados sobre datos y recursos la realiza exclusivamente el personal autorizado para ello en el Documento de Seguridad?
- ¿Ha establecido el Responsable del Fichero los criterios conforme a los cuales se otorga la autorización de los accesos a los datos y a los recursos?

- El personal ajeno al Responsable que tiene acceso a los datos y recursos de éste ¿se encuentra sometido a las mismas condiciones y obligaciones que el personal propio?
- ¿El acceso a los locales donde se encuentran ubicados los sistemas de información se realiza exclusivamente por el personal autorizado en el Documento de Seguridad?

Documentación necesaria para la comprobación

Debemos comprobar los siguientes documentos:

- Descripción de los procedimientos de control de acceso dentro del Documento de Seguridad.
- Descripción de las funciones de los usuarios y perfiles de usuarios, concretamente acerca de los pertenecientes a entidades externas a la entidad, dentro del Documento de Seguridad.
- Informes mensuales del Responsable de Seguridad con las revisiones realizadas del registro de accesos y de los problemas detectados.

5.1.	**Análisis de la documentación:**
5.1.1.	Analizar la idoneidad de los procedimientos de control de acceso a los recursos autorizados, utilizados por la entidad.
5.1.2.	Comprobar qué procedimientos se establecen para comunicar la aplicación de las medidas de seguridad al personal externo con acceso a datos.
5.1.3.	Analizar la idoneidad de los procedimientos de control de acceso a los lugares con equipos que dan soporte a los sistemas de información.
5.1.6.	Comprobar si el Documento de Seguridad incluye las medidas que impidan el acceso de personas no autorizadas a ficheros y tratamientos no automatizados.

Comprobación de los registros

Es necesario solicitar los siguientes registros:

- Listado detallado de los recursos, niveles y privilegios de acceso al sistema para cada usuario o perfil de usuarios.

- Relación del personal autorizado para conceder, alterar o anular el acceso autorizado, dentro del Documento de Seguridad.
- Listado de funciones de los usuarios y perfiles de usuarios (ya verificadas en apartados anteriores).
- Justificantes de comunicación a los usuarios pertenecientes a entidades externas y con acceso a los recursos, de las medidas de seguridad que deben aplicar.
- Listado autorizado del personal autorizado a acceder a los locales donde se encuentran ubicados los sistemas de información.
- Registro de accesos.
- Listado de usuarios autorizados y de la documentación a que tienen acceso.

5.2. Comprobación de registros:

5.2.1. Comprobar que existe una relación de usuarios, perfiles y sus accesos al sistema.

5.2.2. Verificar la vigencia del listado de usuarios.

5.2.3. Comparar las funciones de los usuarios verificadas en el PT - 2.1.1. *Funciones y obligaciones del personal,* con el listado de recursos, niveles y privilegios de acceso.

Usuario	Listado de funciones según PT- 2	Listado de recursos, niveles y privilegios de acceso

5.2.4. Comprobar que en el Documento de Seguridad se identifica el personal autorizado para conceder, alterar o anular los accesos a los recursos.

5.2.5. Verificar la existencia de notificaciones sobre la aplicación de las medidas de seguridad por parte del personal externo. C*ruzar la información de esta prueba con la realizada en el PT-10.2.1.*

5.2.6. Comprobar que existe un listado actualizado en el cual se identifica el personal con acceso autorizado a los lugares donde se ubiquen los equipos que den soporte a los sistemas de información.

Inspección visual

Consiste en observar la eficacia de los distintos mecanismos utilizados por la entidad para el control de acceso a los recursos.

5.3.	**Inspección visual:**
5.3.1.	Observar si hay usuarios con acceso a recursos no necesarios para sus funciones.
5.3.2.	Observar la presencia de personal externo a la entidad con acceso a recursos, y que debe haber sido informado acerca de las medidas de seguridad que debe aplicar.
5.3.3.	Observar el funcionamiento de las medidas de control de acceso físico a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.
5.3.4.	Observar si los mecanismos para evitar el acceso no autorizado a los ficheros y tratamientos no automatizados son adecuados.

4.1.5. Revisión del Documento de Seguridad. Gestión de soportes

AUDITORÍA DE PROTECCIÓN DE DATOS		
REVISIÓN DEL DOCUMENTO DE SEGURIDAD N.º: 6. GESTIÓN DE SOPORTES		
Entidad: Carnicería Ramos		
Nombre Fichero/Tratamiento: Personal	N.º Inscripción del Fichero: 236541	
Nivel de Seguridad: **MEDIO**	Fecha Auditoría: 15/05/09	
Aprobado por: D. Antonio Ruiz Escalante		Fecha: 20/05/09
Realizado por: : D. Antonio Ruiz Escalante		Fecha: 15/05/099

¿Qué cuestiones debemos plantearnos para realizar la comprobación y verificación de "Gestión de soportes y documentos"?

- ¿Está identificado el tipo de información contenida en el soporte o documento?
- ¿Existe y se mantiene un inventario de soportes?
- ¿Se almacenan los soportes o documentos en lugares de acceso restringido?

- ¿Existen mecanismos por los que solamente puedan acceder las personas autorizadas en el Documento de Seguridad?, ¿funcionan adecuadamente estos mecanismos?
- ¿Se ha dejado constancia en el Documento de Seguridad, si fuera el caso, de la imposibilidad de cumplir con las obligaciones establecidas en el Reglamento sobre identificación, inventariado y acceso a los soportes dadas sus características físicas?
- ¿La salida de soportes y documentos fuera de los locales donde se ubica el fichero está siendo autorizada por el Responsable del Fichero o está debidamente autorizada en el Documento de Seguridad?
- ¿Se están tomando las medidas adecuadas en el traslado de documentación para evitar la sustracción, pérdida o acceso indebido durante su transporte?
- Cuando se desecha un soporte o documento conteniendo datos de carácter personal, ¿se adoptan las medidas adecuadas para evitar el acceso a la información o su recuperación posterior cuando se procede a su destrucción o borrado?, ¿son adecuadas estas medidas?
- ¿Se dan de baja en el inventario estos soportes o documentos desechados?
- Para los soportes con datos de carácter personal considerados especialmente sensibles por la organización, ¿se utilizan sistemas de etiquetado que permitan la identificación de su contenido a las personas autorizadas y dificulten su identificación al resto?, ¿son adecuados y cumplen su finalidad?
- ¿Existe un registro de entrada de soportes o documentos?, ¿y un registro de salida?
- ¿Contienen estos registros de entrada y salida de soportes toda la información exigida en el Reglamento?
- ¿Las personas encargadas de la recepción y la entrega de soportes están debidamente autorizadas?, ¿consta en el Documento de Seguridad dicha autorización?
- ¿Se han anotado todas las entradas y salidas de soportes?

¿Qué documentación debemos solicitar para la comprobación?

Debemos solicitar los siguientes documentos:

- Descripción de los procedimientos de gestión de soportes dentro del Documento de Seguridad.

- Descripción de los procedimientos de cifrado de los datos en la distribución de soportes.
- Descripción de los criterios de archivo de documentos dentro del Documento de Seguridad.

6.1. Análisis de la documentación:

6.1.1. Comprobar que el procedimiento de gestión de soportes descrito en el Documento de Seguridad se adecua a las exigencias de la normativa. Esto significa comprobar la inclusión de:

	Visto	*Notas*
a) Criterios para identificar la información incluida en los soportes y documentos.		
b) Criterios para autorizar el acceso a los soportes y documentos y listado de personal autorizado.		
c) Criterios para inventariar los soportes y documentos.		

6.1.2. Comprobar si se motiva la no aplicación de las medidas anteriores debido a las características físicas del soporte.

6.1.3. Comprobar que el procedimiento de gestión de soportes descrito en el Documento de Seguridad se adecua a las exigencias de la normativa. Esto significa comprobar la inclusión de:

	Visto	*Notas*
a) Especificaciones de que las salidas de soportes con datos personales fuera de la entidad deben estar autorizadas por el Responsable del Fichero.		
b) Instrucciones para la destrucción de soportes y documentos que vayan a ser desechados. C*ruzar la información de esta prueba con la realizada en el PT-1.1.3.*		
c) Medidas de seguridad para el transporte de documentación que eviten la sustracción, pérdida o acceso indebido. *Cruzar la información de esta prueba con la realizada en el PT-1.1.3.*		
d) Procedimientos de clasificación e identificación de soportes según su contenido y los usuarios autorizados a conocer este procedimiento.		

6.1.7. Comprobar si el Documento de Seguridad establece para los ficheros no automatizados:

	Visto	*Notas*
a) Criterios y procedimientos de archivo de los soportes y documentos.		
b) Instrucciones para la custodia de la documentación pendiente o que esté fuera del archivo.		

Comprobación de registros

Se deben solicitar los registros siguientes:

- Inventario de soportes.
- Registro de entradas y salidas de soportes.
- Autorizaciones del Responsable del Fichero para las salidas de soportes.

Los registros se comprobaran de la siguiente forma:

<table>
<tr><td>6.2.</td><td>Comprobación de registros:</td></tr>
<tr><td>6.2.1.</td><td>Comprobar que la entidad dispone de un listado del personal autorizado a acceder a los soportes.</td></tr>
<tr><td></td><td></td></tr>
<tr><td>6.2.2.</td><td>Comprobar que existe un inventario actualizado de soportes y documentos.</td></tr>
<tr><td></td><td></td></tr>
<tr><td>6.2.3.</td><td>Comprobar que las autorizaciones de salida de soportes y documentos de la entidad están debidamente autorizadas por el Responsable del Fichero.</td></tr>
<tr><td></td><td></td></tr>
<tr><td>6.2.4.</td><td>Comprobar mediante el registro de inventario de soportes las bajas realizadas y el procedimiento empleado para su destrucción o borrado.</td></tr>
<tr><td></td><td></td></tr>
<tr><td>6.2.5.</td><td>Comprobar en el registro de inventario de soportes si éstos se identifican de forma ininteligible para usuarios no autorizados.</td></tr>
<tr><td></td><td></td></tr>
<tr><td>6.2.6.</td><td>Comprobar que los registros de entrada y salida de documentos o soportes están actualizados y contienen los campos mínimos fijados en el Reglamento:
<table>
<tr><th></th><th>Visto</th><th>Notas</th></tr>
<tr><td>a) Tipo de soporte o documento.</td><td></td><td></td></tr>
<tr><td>b) Fecha.</td><td></td><td></td></tr>
<tr><td>c) Hora.</td><td></td><td></td></tr>
<tr><td>d) Emisor/Destinatario.</td><td></td><td></td></tr>
<tr><td>e) Número de soportes o documentos en el envío.</td><td></td><td></td></tr>
<tr><td>f) Tipo de información almacenada.</td><td></td><td></td></tr>
<tr><td>g) Forma de envío.</td><td></td><td></td></tr>
<tr><td>h) Responsable de la recepción/entrega.</td><td></td><td></td></tr>
<tr><td>i) Autorización.</td><td></td><td></td></tr>
</table></td></tr>
<tr><td>6.2.7.</td><td>Verificar la existencia y periódica actualización del registro de salidas de soportes y documentos.</td></tr>
<tr><td></td><td></td></tr>
</table>

Inspección visual

En la inspección visual debemos observar los siguientes puntos:

- Identificación de soportes.
- Almacenamiento de soportes en lugar restringido.
- Cumplimiento de las medidas establecidas para el desechado o reutilizado de soportes.
- Distribución cifrada de los soportes que contienen datos personales.
- Medidas de seguridad utilizadas para la protección de la documentación en general: acceso, archivo, custodia, etc.

6.3.	**Inspección visual:**
6.3.1.	Verificar que los soportes y documentos utilizados por la entidad cumplen los siguientes requisitos:

	Visto	*Notas*
a) Tienen identificada la información que contienen.		
b) Están inventariados.		
c) Se almacenan en lugar de acceso restringido.		
d) Son reutilizados de forma segura.		
e) Son desechados de forma segura.		

6.3.2.	Observar la existencia de los medios para la destrucción de soportes que hubiesen sido mencionados en el procedimiento de gestión de soportes del Documento de Seguridad. Cruzar la información de esta prueba con la realizada en el PT-7.2.8.
6.3.3.	Ver que los soportes están identificados de forma ininteligible para los usuarios no autorizados.
6.3.4.	En visita a los archivos comprobar que se garantiza la correcta conservación, localización y consulta de la información almacenada.
6.3.5.	Observar si se sigue una política de mesas limpias cuando los usuarios abandonan su lugar de trabajo.

4.1.6. Revisión del Documento de Seguridad. Copias de Respaldo y Recuperación

AUDITORÍA DE PROTECCIÓN DE DATOS		
REVISIÓN DEL DOCUMENTO DE SEGURIDAD N.º: 7. COPIAS DE RESPALDO Y RECUPERACIÓN		
Entidad: Carpintería Muñoz		
Nombre Fichero/Tratamiento: Personal	N.º Inscripción del Fichero: 326545	
Nivel de Seguridad: **MEDIO**	Fecha Auditoría: 12/03/09	
Aprobado por: D. Antonio Ruiz Escalante		Fecha: 16/03/09
Realizado por: : D. Antonio Ruiz Escalante		Fecha: 12/03/09

Cuestiones que debemos plantearnos para la comprobación y verificación del apartado "Copias de respaldo y recuperación"

- ¿El Responsable del Fichero ha definido los procedimientos de realización de copias de respaldo y recuperación de los datos?, ¿es adecuada esta definición?
- ¿Están reflejados estos procedimientos en el Documento de Seguridad?
- ¿Ha verificado el Responsable del Fichero la correcta aplicación de estos procedimientos?, ¿realiza esta verificación cada seis meses?
- ¿Garantizan los procedimientos establecidos la reconstrucción de los datos al estado en que se encontraban antes de producirse la pérdida o destrucción?
- Si esta pérdida o destrucción afecta a ficheros parcialmente automatizados ¿se ha procedido a grabar manualmente los datos?, ¿queda constancia motivada de este hecho en el Documento de Seguridad?
- ¿Se realizan copias de respaldo al menos semanalmente? Si no es así, ¿se debe a que no ha habido actualizaciones en ese período?
- ¿Las pruebas previas a la implantación o modificación de los sistemas de información se realizan con datos reales? En caso afirmativo, ¿se están aplicando las mismas medidas de seguridad que las que le corresponde por la naturaleza de los datos que contiene?, ¿se anota su realización en el Documento de Seguridad?, ¿se hacen copias de seguridad previas a la realización de pruebas con datos reales?

¿Qué documentación necesitamos para la comprobación?

Debemos solicitar la siguiente documentación:

- Descripción del procedimiento de gestión de copias de respaldo y de recuperación de los datos dentro del Documento de Seguridad.
- Descripción del procedimiento de gestión de copias de documentos y su destrucción dentro del Documento de Seguridad.

4.1. Análisis de la documentación:

7.1.1. Comprobar que el procedimiento de copias de respaldo y recuperación descrito en el Documento de Seguridad se adecua a las exigencias de la normativa (artículos 94 y 102 del RDLOPD). Esto significa comprobar la inclusión de *(Cruzar la información de esta prueba con la realizada en el PT-1.1.3.)*:

	Visto	*Notas*
a) Identificación del responsable de la definición y gestión de las copias de respaldo y de su recuperación.		
b) Instrucciones para la realización de las copias de respaldo.		
c) Instrucciones para recuperación de los datos que garantice la reconstrucción y en qué ocasiones esta puede ser manual.		
d) Definición de una periodicidad de realización de copias (debe ser como mínimo semanal).		
e) Restricciones al uso de datos reales para la realización de pruebas en el sistema de información.		
f) Instrucciones con la obligación de realizar copias de seguridad de los datos previos a la realización de pruebas con datos reales.		

Comprobación de registros

Se deben solicitar los siguientes registros:

- Inventarios de soportes (registro ya solicitado en el apartado de Gestión de soportes).
- Registro de las entradas y salidas de soportes (registro ya solicitado en el apartado de Gestión de soportes).

- Registro de realización de copias de respaldo.
- Listado de funciones de los usuarios y perfiles de usuarios (registro ya solicitado en el apartado de funciones y obligaciones del personal).
- Registro de incidencias (registro ya solicitado en el apartado de Registro de Incidencias).
- Registro de controles periódicos, auditorías o informes (registro ya solicitado en el apartado Documento de Seguridad).
- Contratos con Encargados del Tratamiento para la destrucción de documentos.

7.2.	**Comprobación de registros:**
7.2.1.	Verificar la efectividad del procedimiento establecido para las copias de respaldo mediante el registro de las comprobaciones realizadas por la empresa.
7.2.2.	Verificar la periodicidad con la que se realizan las copias de respaldo, mediante el registro de copias de respaldo o en el propio inventario de soportes.
7.2.3.	Verificar la efectividad del procedimiento establecido de recuperación de copias de respaldo mediante el registro de las comprobaciones realizadas por la empresa y el registro de incidencias para encontrar recuperaciones de datos realizadas.
7.2.4.	Comprobar que la verificación de la definición, funcionamiento y aplicación de procedimientos de las copias de respaldo y de recuperación se realiza cada 6 meses mediante el registro de control establecido a tal efecto.
7.2.5.	Comprobar mediante registros de copias de seguridad que se hicieron con fecha anterior a la realización de las pruebas con datos reales.

Inspección visual

Debemos indicar el resultado de la observación de los siguientes aspectos:

- Existencia física de las copias de respaldo.
- Verificación de que una copia de respaldo (y los procedimientos para su recuperación) se guarda en un lugar diferente de aquel en el cual se encuentran los equipos informáticos de tratamiento.

- Verificación de que las copias de respaldo que salen fuera del lugar de los equipos informáticos de tratamiento se cifran.
- Comprobación del proceso de recuperación de datos.
- Entorno de pruebas.
- Verificación de las condiciones y recursos para la copia y destrucción efectiva de documentos.

7.3.	**Inspección visual:**
7.3.1.	Ver el lugar y condiciones en las cuales se guardan las copias de respaldo, para comprobar que se garantiza su integridad.
7.3.2.	Buscar la existencia de aplicaciones en entorno de pruebas con datos personales reales y verificar en ellas la totalidad de las medidas de seguridad aplicadas.
7.3.3.	Comprobar in situ (si es posible) un proceso de recuperación de datos.

4.1.7. Revisión del documento de Seguridad. Telecomunicaciones

AUDITORÍA DE PROTECCIÓN DE DATOS	
REVISIÓN DEL DOCUMENTO DE SEGURIDAD N.º: 8. TELECOMUNICACIONES	
Entidad: Panadería S.Vicente	
Nombre Fichero/Tratamiento: Proveedores	N.º Inscripción del Fichero: 235648
Nivel de Seguridad: **MEDIO**	Fecha Auditoría: 01/06/09
Aprobado por: D. Antonio Ruiz Escalante	Fecha: 06/06/09
Realizado por: : D. Antonio Ruiz Escalante	Fecha: 01/06/09

Las cuestiones que debemos plantearnos, para la comprobación y verificación del apartado de telecomunicaciones, es si los accesos a datos mediante redes de comunicaciones garantizan un nivel de seguridad equivalente a los accesos en modo local.

¿Cuál es la documentación necesaria para comprobarlo?

Debemos solicitar la siguiente documentación:

- Descripción del procedimiento de gestión de las telecomunicaciones en el Documento de Seguridad.
- Diagrama de la red informática de la Entidad.

8.1.	Análisis de la documentación:
8.1.1.	Comprobar que el procedimiento de gestión de telecomunicaciones descrito en el Documento de Seguridad es coherente con el diagrama de la red informática.

Comprobación de registros

Debemos solicitar los siguientes registros:

- Listado de usuarios que dispongan de conexiones remotas a los ficheros de datos personales ubicados en la entidad.
- Autorizaciones motivadas para las conexiones remotas de los usuarios.
- Listado de personal actualizado, por departamentos y categorías, y la fecha de alta en la entidad, obtenido del Departamento de Recursos Humanos (registro ya solicitado en el apartado "Funciones y obligaciones del personal").

8.2.	Comprobación de registros:
8.2.1.	Verificar que las conexiones remotas están vinculadas, bien a personal dado de alta en la auditada (mediante el listado de personal) o bien, a entidades que prestan servicios relacionados con el mantenimiento del fichero o tratamiento.
8.2.2.	Verificar que todos los usuarios con conexión remota están debidamente autorizados y que, en caso de vencimiento de la autorización, esta quede anulada.

Inspección visual

Debemos indicar el resultado de la observación de los siguientes aspectos:

- Método que se ha utilizado para cifrar las comunicaciones con datos personales.

- Procedimiento a seguir en el cifrado de las transmisiones de datos de carácter personal a través de redes de telecomunicaciones públicas o inalámbricas.

8.3.	Inspección visual:
8.3.1.	Identificar el método utilizado por la entidad para garantizar la seguridad en los accesos remotos a los datos y analizar su fiabilidad.

4.1.8. Revisión del Documento de Seguridad. Auditoría

AUDITORÍA DE PROTECCIÓN DE DATOS		
REVISIÓN DEL DOCUMENTO DE SEGURIDAD N.º: 9. AUDITORÍA		
Entidad: Imprenta Graficas		
Nombre Fichero/Tratamiento: Personal	N.º Inscripción del Fichero: 2236541	
Nivel de Seguridad: **MEDIO**	Fecha Auditoría: 21/05/09	
Aprobado por: D. Antonio Ruiz Escalante		Fecha: 28/05/09
Realizado por: : D. Antonio Ruiz Escalante		Fecha: 21/05/09

¿Qué cuestiones debemos plantearnos para llevar a cabo una auditoría de protección de datos?

- ¿Se realiza la actual auditoría en el plazo establecido desde la anterior?
- Si ha habido modificaciones sustanciales en el sistema de información, ¿se ha realizado a continuación una auditoría para verificar la adaptación, adecuación y eficacia de las medidas de seguridad?
- ¿Los informes de las auditorías anteriores incluían los datos, hechos y observaciones en los que se basaban sus dictámenes?
- ¿Se han implementado las medidas correctoras propuestas por auditorías anteriores?, ¿han sido eficaces y han corregido las deficiencias encontradas?

Documentación que debemos solicitar para la comprobación

Debemos solicitar:

- Los informes de las auditorías realizadas.

- Informes de conclusiones del Responsable de Seguridad asociados a las auditorías realizadas.

9.1. Análisis de la documentación:

9.1.1. Comprobar que los informes de auditoría se adecuan a las exigencias de la normativa. Debe contener:

	Visto	*Notas*
a) Fecha.		
b) Identificación de la persona que lo firma.		
c) Detalle de la metodología utilizada en el proceso auditor.		
d) Concluye con una opinión sobre la adecuación de las medidas de seguridad y controles a la Ley y al RDLOPD.		
e) Identifica las deficiencias.		
f) Propone medidas correctoras o complementarias para cada deficiencia.		
g) Presenta recomendaciones.		
h) Incluye los datos, hechos y observaciones que soportan las conclusiones y recomendaciones realizadas.		

9.1.2. Comprobar que el informe de conclusiones del Responsable de Seguridad cumple los requisitos formales siguientes:

	Visto	*Notas*
a) Fecha.		
b) Se identifica la persona que lo firma.		
c) Analiza cada una de las deficiencias detalladas en el informe de auditoria.		
d) Emite conclusiones.		
e) Hay acuse de recibo del Responsable del Fichero.		

9.1.3. En caso de tratarse de una auditoria interna, analizar si se cumple el principio de independencia del auditor.

9.1.4. Con base al trabajo realizado, analizar si en el momento de la ejecución de la auditoria se han aplicado las medidas correctoras o complementarias (así como las recomendaciones) propuestas en los informes precedentes.

9.1.5. Comprobar si existe un procedimiento que identifique cuáles son los supuestos que hacen necesario realizar una auditoria.

Comprobación de registros

Solicitar los siguientes registros:

- Registro de auditorías realizadas.
- Notificación de la inscripción del fichero emitida por la Agencia Española de Protección de Datos.

9.2.	**Comprobación de registros:**
9.2.1.	En caso de que la entidad no disponga de ningún informe de auditoría, comprobaremos que no hayan transcurrido más de 2 años desde la fecha de creación del fichero (ver notificación de la Inscripción del Fichero emitida por la Agencia Española de Protección de Datos), hasta la fecha de encargo de la auditoria en curso.
9.2.2.	En caso de no ser primera auditoría, comprobar mediante el registro de auditorías realizadas y las fechas de los informes entregados que no hayan transcurrido más de dos años entre la realización de cada una de las auditorías.
9.2.3.	Comprobar mediante las versiones del Documento de Seguridad que no se han producido cambios significativos en el sistema de información que obligaran a la realización de auditoría extraordinaria.

Inspección visual

En este supuesto no se aplica la inspección visual.

4.1.9. Revisión del documento de seguridad. Encargado de Tratamiento

AUDITORÍA DE PROTECCIÓN DE DATOS		
REVISIÓN DEL DOCUMENTO DE SEGURIDAD N.º: 10. ENCARGADO DEL TRATAMIENTO		
Entidad: Empresa de construcción		
Nombre Fichero/Tratamiento: Personal	N.º Inscripción del Fichero: 235461	
Nivel de Seguridad: **MEDIO**	Fecha Auditoría: 12/08/09	
Aprobado por: D. Antonio Ruiz Escalante		Fecha: 16/08/09
Realizado por: : D. Antonio Ruiz Escalante		Fecha: 12/08/09

Cuestiones que debe plantearse el auditor para la comprobación y verificación del apartado "Encargo del tratamiento"

- ¿Se realiza el tratamiento por persona distinta al Responsable del Fichero?, ¿se ha formalizado mediante contrato conforme lo establecido el artículo 12 de la LOPD?
- Si la realización de este encargo se realiza en los locales del Responsable, ¿se ha hecho constar esta circunstancia en el Documento de Seguridad?, ¿consta por escrito en el contrato el compromiso del personal del encargado de tratamiento respecto al cumplimiento de las medidas de seguridad recogidas en el Documento de Seguridad del Responsable?
- Cuando el tratamiento se realiza mediante acceso remoto a los sistemas del Responsable, ¿se le ha prohibido al encargado de tratamiento la incorporación de los datos a sistemas o soportes distintos de los del Responsable?, ¿se ha hecho constar tal circunstancia en el Documento de Seguridad del Responsable?
- Si la prestación se hace en locales propios del encargado de tratamiento (distintos de los del Responsable), ¿ha elaborado el encargado el documento de seguridad?, ¿identifica el fichero o tratamiento y el Responsable del mismo?, ¿detalla las medidas de seguridad a implementar en relación con su tratamiento?

¿Qué documentación es necesaria para la comprobación?

Debemos solicitar los siguientes documentos:

- Descripción del procedimiento que regula el tratamiento de datos personales fuera de los locales, dentro del Documento de Seguridad.
- Descripción del ámbito de aplicación del Documento de Seguridad.
- Procedimiento de contratación de Encargados del Tratamiento dentro de las funciones propias del Responsable del Fichero o Tratamiento.
- Procedimiento que regula las condiciones de seguridad del teletrabajo en la entidad.

10.1.	**Análisis de la documentación:**
10.1.1.	Comprobar si el Documento de Seguridad hace mención del acceso a los datos, soportes o recursos del sistema por parte del Encargado del Tratamiento en los locales del responsable.
10.1.2.	Comprobar si el Documento de Seguridad autoriza los accesos remotos por parte del Encargado del Tratamiento y la prohibición de recoger en sus sistemas los datos accedidos.
10.1.3.	Comprobar si existen unas condiciones generales de contratación de los Encargados del Tratamiento, con el detalle de los requisitos mínimos que deben cumplir en materia de protección de datos personales.
10.1.4.	Comprobar si en las condiciones generales de contratación de los Encargados del Tratamiento se solicita copia del Documento de Seguridad elaborado por estos en caso de prestación de servicios en sus locales.
10.1.5.	Comprobar si se establecen medidas para el control de aplicación de las medidas de seguridad por parte de los Encargados del Tratamiento.
10.1.6.	Comprobar que en los contratos de prestación de servicios se prohíbe el acceso a datos personales o, en caso de conocerse, la obligación de secreto.
10.1.7.	Comprobar en el ámbito de aplicación del Documento de Seguridad si incluye procedimientos de trabajo fuera de las instalaciones y las medidas de seguridad a aplicar.
10.1.8.	Verificar que el procedimiento de tratamiento de datos personales en el exterior de los locales exige autorización.
10.1.9.	Comprobar si estas autorizaciones se realizan por usuario o por perfil de usuarios.
10.1.10.	Comprobar que el Documento de Seguridad incluye un procedimiento de renovación y revocación de las autorizaciones.

¿Cómo se realiza la comprobación de registros?

Debemos solicitar los siguientes registros:

- Contratos con Encargados del Tratamiento (o muestra de los más representativos).
- Autorizaciones del Responsable del fichero para los tratamientos fuera de los locales.
- Registro de controles practicados a los Encargados del Tratamiento dentro de las funciones propias del Responsable del Fichero o Tratamiento.

10.2.	**Comprobación de registros:**
10.2.1.	Obtener evidencia de la comunicación al personal a cargo del Encargado del Tratamiento, de las medidas de seguridad que deben cumplir durante su estancia en los locales del Responsable del Fichero o en los accesos remotos que realicen. *Cruzar la información de esta prueba con la realizada en el PT-5.2.5.*
10.2.2.	Comprobar si en las condiciones de contratación de los Encargados del Tratamiento se solicita información acerca de su Documento de Seguridad. Si se identifican en él, el fichero que trata, el responsable del mismo y las medidas de seguridad aplicadas.
10.2.3.	Comprobar la existencia de registros de control de los Encargados del Tratamiento (auditorías, revisiones de documentación, etc.).
10.2.4.	Comprobar que existen las autorizaciones del Responsable del Fichero o Tratamiento, para el almacenaje y tratamiento externo de datos, y éstas se incluyen en el Documento de Seguridad.
10.2.6.	Comprobar que las autorizaciones para el almacenaje y tratamiento externo de datos tienen fijado un periodo de validez.
10.2.7.	Comprobar que la validez de las autorizaciones es correcta a la fecha de verificación.
10.2.8.	Verificar que no hay salida de dispositivos con la validez de la autorización caducada.

Inspección visual

Se deben observar los siguientes aspectos:

- Acceso a datos personales, soportes o recursos del sistema de información por parte del personal sin necesidad de acceso.
- Tratamiento de datos personales fuera de los locales.

10.3.	**Inspección visual:**
10.3.1.	Observar si personal sin necesidad de acceso a datos personales, soportes que los contengan o recursos del sistema de información puede en la práctica acceder a ellos.
10.3.2.	Observar si hay tratamiento de datos fuera de los locales de la entidad mediante las autorizaciones de salida de soportes y documentos como indicio.

4.2. AUDITORÍA DE PROTECCIÓN DE DATOS: REVISIÓN DEL DOCUMENTO DE SEGURIDAD. NIVEL ALTO

AUDITORÍA DE PROTECCIÓN DE DATOS		
REVISIÓN DEL DOCUMENTO DE SEGUIRIDAD N.º: 0. NIVELES DE SEGURIDAD		
Entidad: Gestoría Avilés		
Nombre Fichero/Tratamiento: Nóminas	N.º Inscripción del Fichero: 369584	
Nivel de Seguridad: **ALTO**	Fecha Auditoría: 23/02/09	
Aprobado por: D. Antonio Ruiz Escalante		Fecha: 01/03/09
Realizado por: : Dª. María Palma Rodríguez		Fecha: 23/02/09

Cuestiones que debe plantearse el auditor para la comprobación y verificación de los niveles de seguridad aplicados en la implantación de la protección de datos

- ¿La clasificación del nivel de seguridad es adecuada respecto a la naturaleza de la información contenida en cada uno de los ficheros y su finalidad?
- ¿Se han creado, modificado o suprimido ficheros con datos de carácter personal desde la última auditoría?

Documentación necesaria para la comprobación

Solicitar los siguientes documentos:

- Notificación de la inscripción del fichero emitida por la Agencia Española de Protección de Datos.
- Copia del formulario a cumplimentar para la inscripción o modificación del fichero, emitida por la Agencia Española de Protección de Datos, a petición de la entidad titular del fichero (no puede darse por válido un formulario proporcionado por la propia entidad auditada, pues podría no coincidir con el enviado en su día a la AEPD).
- Documento de Seguridad- La parte estática: las políticas y normas generales de actuación.

0.1.	**Análisis de la documentación:**
0.1.1.	Comprobar la correlación entre la notificación de la inscripción del fichero enviada por la Agencia Española de Protección de Datos (AEPD) y la copia, emitida por la misma Agencia, del formulario para notificación del tratamiento de datos de carácter personal.
0.1.2.	Rellenar el encabezado de los papeles de la auditoría con los datos detallados en la notificación de la inscripción del fichero ante la AEPD.
0.1.3.	Confirmar que el nivel de seguridad incluido en el Documento de Seguridad coincide con el declarado ante la AEPD o detallado en el contrato que regula el tratamiento por cuenta del Responsable del Fichero.
0.1.4.	Identificar aquellos campos que justifican el nivel de seguridad asignado con base en la información incluida en la copia del formulario para notificación del tratamiento de datos de carácter personal emitida por la AEPD.
0.1.5.	Comprobar si existe motivo para aplicar las medidas de seguridad de nivel básico al fichero objeto de auditoría. Se dará el caso si: – La única finalidad del uso de los datos es la transferencia dineraria por parte de los miembros o socios de la entidad. – Se trata de un fichero o tratamiento no automatizado que contiene datos de forma accesoria y sin guardar relación con su finalidad. – Se trata de un fichero o tratamiento con datos referentes al grado de discapacidad, la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.
0.1.6.	Comprobar si el Documento de Seguridad incluye:

	Visto	*Apartado Documento Seguridad*
La aplicación de normativa específica debido al tipo de actividad desarrollada por la entidad, por el tipo de datos tratados o por su finalidad.		
La segregación de sistemas de tratamiento por ficheros, para una aplicación diferencias de las medidas de seguridad.		
Procedimientos para el uso, clasificación y eliminación de ficheros temporales o copias de documentos.		

Comprobación de registros

Para hacer la comprobación de registros es necesario solicitar:

- Las fuentes que se han utilizado para la recogida de datos que constituyen el fichero (formularios en papel, Web, etc.)

0.2.	Comprobación de Registros:
0.2.1.	Acceder a las diferentes plantillas y formularios de recabación de datos del fichero para detectar campos no incluidos en la declaración o en el contrato de tratamiento por cuenta del Responsable del Fichero, especialmente si estos suponen un cambio en la calificación del nivel de seguridad del fichero.

¿Cómo se realiza la inspección visual?

En la inspección visual se observan las discordancias que puede haber entre los datos tratados por la entidad y los declarados en la inscripción del fichero en la AEPD o detallados en el contrato que regula el tratamiento por cuenta del Responsable del Fichero.

0.3.	Inspección visual:
0.3.1.	Verificar que la realidad global observada en la entidad en relación con los datos personales tratados es coherente con la tipología de datos declarados.
0.3.2.	Observar si, en caso de segregación de sistemas de tratamiento, hay una efectiva delimitación de acceso a datos y usuarios.

4.2.1. Revisión del Documento de Seguridad. Documento de Seguridad

AUDITORÍA DE PROTECCIÓN DE DATOS		
REVISIÓN DEL DOCUMENTO DE SEGURIDAD N.º: 1. DOCUMENTO DE SEGURIDAD		
Entidad: Muebles Gómez		
Nombre Fichero/Tratamiento: Personal	N.º Inscripción del Fichero: 365241	
Nivel de Seguridad: **ALTO**	Fecha Auditoría: 23/04/09	
Aprobado por: D. Antonio Ruiz Escalante		Fecha: 29/04/09
Realizado por: : Dª. María Palma Rodríguez		Fecha: 23/04/09

Cuestiones que debe plantearse el auditor para la comprobación y verificación del apartado "Documento de Seguridad"

- ¿Ha elaborado el Responsable del Fichero el Documento de Seguridad?
- ¿El Documento de Seguridad contiene los aspectos mínimos exigidos por el Reglamento?
- ¿El Documento se ha actualizado?, ¿Se ha revisado cuando se han producido cambios relevantes desde la auditoría anterior?
- ¿Su contenido es adecuado a la normativa vigente en este momento en materia de seguridad de los datos de carácter personal?
- ¿Se ha indicado con qué periodicidad se deben cambiar las contraseñas?, ¿es inferior o igual a un año?
- ¿Se especifica cuál es el personal autorizado para la concesión, alteración o anulación de accesos autorizados sobre datos o recursos?
- ¿Se especifica cuál es el personal autorizado para acceder a los lugares donde se almacenan los soportes informáticos?
- Si el tratamiento se realiza por cuenta de terceros, ¿se han reflejado los ficheros afectados por el encargo, con referencia expresa al contrato, así como la identificación del Responsable y el período de vigencia?
- ¿Se ha reflejado en el Documento de Seguridad si los datos personales se incorporan y tratan exclusivamente en los sistemas del encargado?

- ¿Se ha delegado en el Encargado del Tratamiento la llevanza del Documento de Seguridad para los ficheros objeto del contrato?, ¿se ha reflejado esta circunstancia en el contrato?

¿Qué Documentos son necesarios para comprobarlo?

Debemos solicitar los siguientes documentos:

- Documento de Seguridad-La parte estática: las normas generales de actuación.
- Organigrama funcional de la entidad.

1.1.	**Análisis de la documentación:**
1.1.1.	Obtener el o los Documentos de Seguridad y comprobar si su alcance se corresponde con el alcance de la auditoría.
1.1.2.	Identificar si en el Documento de Seguridad obtenido se hace referencia a la existencia de otros Documentos de Seguridad según sea el tratamiento de los datos o ficheros utilizados.

1.1.3. Comprobar que el Documento de Seguridad contiene los puntos mínimos exigibles según el RDLOPD y referenciar en qué apartados del Documento están incluidos estos puntos:

		Visto	Apartado Documento Seguridad
1.	Ámbito de aplicación.		
2.	Detalle de los recursos protegidos.		
3.	Medidas, normas, procedimientos, reglas y estándares de seguridad.		
4.	Funciones y obligaciones del personal.		
5.	Estructura de los ficheros.		
6.	Descripción de los sistemas de información.		
7.	Procedimiento de notificación de incidencias. Cruzar la información de esta prueba con la realizada en el PT-3.1.1.		
8.	Procedimiento de gestión de incidencias. Cruzar la información de esta prueba con la realizada en el PT-3.1.1.		
9.	Procedimiento de respuesta ante incidencias.		
10.	Procedimiento de realización de copias de respaldo. Cruzar la información de esta prueba con la realizada en el PT-7.1.1.		
11.	Procedimiento de recuperación de datos. Cruzar la información de esta prueba con la realizada en el PT-3.1.2 y 7.1.1.		
12.a)	Medidas para el transporte de soportes. Cruzar la información de esta prueba con la realizada en el PT-6.1.3.c).		
12.b)	Medidas para el transporte de documentos. Cruzar la información de esta prueba con la realizada en el PT-6.1.3.c).		
13.a)	Medidas para la destrucción de soportes. Cruzar la información de esta prueba con la realizada en el PT-6.1.3.b).		
13.b)	Medidas para la destrucción de documentos. Cruzar la información de esta prueba con la realizada en el PT-6.1.3.b).		
14.	Medidas para la reutilización de soportes.		
15.	Relación de autorizados para delegar responsabilidades. Cruzar la información de esta prueba con la realizada en el PT-2.1.2.		
16.	Relación de responsables por delegación. Cruzar la información de esta prueba con la realizada en el PT-2.1.2.		

1.1.4. Comprobar que el Documento de Seguridad incluye información acerca del tratamiento de datos por cuenta de terceros y referenciar en qué apartados del Documento están incluidos estos puntos:

		Visto	Apartado Documento Seguridad
1.	Identificación de los ficheros tratados como Encargado del Tratamiento.		
2.	Referencia al contrato suscrito para cada tratamiento de los datos por cuenta ajena.		
3.	Identificación de cada Responsable del Fichero tratado como Encargado del Tratamiento.		
4.	Periodo de vigencia del encargo.		

1.1.5. Comprobar si en el Documento de Seguridad se declara que en el fichero auditado los datos personales se incorporan y tratan de forma exclusiva en las instalaciones del Encargado del Tratamiento.

1.1.6. Con base al punto anterior, comprobar si el Documento de Seguridad ha sido elaborado por el Encargado del Tratamiento por delegación. Cruzar la información de esta prueba con la realizada en el PT-1.2.3.

1.1.7. Comprobar que el Documento de Seguridad incorpora las novedades en la normativa de protección de datos personales. Cruzar la información de esta prueba con la realizada en el PT-1.2.6.

1.1.8. Comprobar que el Documento de Seguridad contiene los puntos mínimos exigibles según el RDLOPD y referenciar en qué apartados del Documento están incluidos estos puntos:

		Visto	Apartado Documento Seguridad
1.	Identificación del Responsable de Seguridad.		
2.	Procedimiento de realización de los controles periódicos.		

1.1.9. Analizar si la posición ocupada por el Responsable de Seguridad en el organigrama le permite el correcto desempeño de sus funciones.

1.1.10 Comprobar si en el Documento de Seguridad se recoge la designación del Responsable de Seguridad y si es única o diferenciada por ficheros o tratamientos.

1.1.4. Comprobar que el Documento de Seguridad incluye información acerca del tratamiento de datos por cuenta de terceros y referenciar en qué apartados del Documento están incluidos estos puntos:

		Visto	Apartado Documento Seguridad
1.	Identificación de los ficheros tratados como Encargado del Tratamiento.		
2.	Referencia al contrato suscrito para cada tratamiento de los datos por cuenta ajena.		
3.	Identificación de cada Responsable del Fichero tratado como Encargado del Tratamiento.		
4.	Periodo de vigencia del encargo.		

1.1.5. Comprobar si en el Documento de Seguridad se declara que en el fichero auditado los datos personales se incorporan y tratan de forma exclusiva en las instalaciones del Encargado del Tratamiento.

1.1.6. Con base al punto anterior, comprobar si el Documento de Seguridad ha sido elaborado por el Encargado del Tratamiento por delegación. Cruzar la información de esta prueba con la realizada en el PT-1.2.3.

1.1.7. Comprobar que el Documento de Seguridad incorpora las novedades en la normativa de protección de datos personales. Cruzar la información de esta prueba con la realizada en el PT-1.2.6.

1.1.8. Comprobar que el Documento de Seguridad contiene los puntos mínimos exigibles según el RDLOPD y referenciar en qué apartados del Documento están incluidos estos puntos:

		Visto	Apartado Documento Seguridad
1.	Identificación del Responsable de Seguridad.		
2.	Procedimiento de realización de los controles periódicos.		

1.1.9. Analizar si la posición ocupada por el Responsable de Seguridad en el organigrama le permite el correcto desempeño de sus funciones.

1.1.10 Comprobar si en el Documento de Seguridad se recoge la designación del Responsable de Seguridad y si es única o diferenciada por ficheros o tratamientos.

Comprobación de registros

Solicitar los siguientes registros:

- Documento de Seguridad-Registros.
- Listado de las actualizaciones del documento.
- Carta/s de nombramiento del Responsable de Seguridad encargado de coordinar y controlar las medidas definidas en el Documento de Seguridad.
- Comunicación a las personas autorizadas para delegar responsabilidad.
- Comunicación a las personas a las que se ha delegado alguna responsabilidad en materia de seguridad en el tratamiento de datos personales.
- Registro de controles periódicos, auditorías o informes.
- Registro de contratos realizados por la entidad como Encargado del Tratamiento de datos personales por cuenta de la entidad.
- Contrato realizado con el Encargado del Tratamiento que gestiona el Documento de Seguridad por cuenta de la entidad.
- Registro de actualizaciones o de control de versiones del Documento de Seguridad.
- Copia del formulario a cumplimentar para la modificación del fichero, emitida por la Agencia Española de Protección de Datos, a petición de la entidad titular del fichero.

1.2.	**Comprobación de Registros:**
1.2.1.	Comprobar la existencia de las comunicaciones a los autorizados para delegar responsabilidades por cuenta del Responsable del Fichero o Tratamiento e igualmente sobre los que recaen dichas responsabilidades.
1.2.2.	Verificar mediante los contratos suscritos como Encargado del Tratamiento que estos se encuentran relacionados en el Documento de Seguridad, se identifica el Responsable del Fichero o Tratamiento y el período de vigencia.
1.2.3.	Comprobar que los contratos de confidencialidad suscritos entre la entidad y los Encargados del Tratamiento incluyen la delegación de realizar el Documento de Seguridad para los ficheros o tratamientos tratados en exclusivo. *Cruzar la información de esta prueba con la realizada en el PT-1.1.6.*
1.2.4.	Verificar la actualización periódica del Documento de Seguridad, si existe, con el anexo sobre gestión de versiones o con los registros de los controles periódicos realizados.
1.2.5.	Comprobar si se han producido modificaciones en la inscripción del fichero posteriores a la última actualización del Documento de Seguridad.
1.2.6.	Comprobar la adecuación legal del Documento de Seguridad mediante el registro de actualizaciones y las fechas de entrada en vigor de la normativa aplicable a fecha de la auditoria. *Cruzar la información de esta prueba con la realizada en el PT-1.1.7.*
1.2.7.	Verificar mediante registros que acrediten la realización de los controles periódicos, que las fechas de estos coinciden con la periodicidad establecida en el Documento de Seguridad.
1.2.8.	Averiguar si el Responsable de Seguridad ha sido designado mediante carta de nombramiento.
1.2.9.	Comprobar que el Responsable de Seguridad se encuentra en la lista actualizada del personal o existe contrato como Encargado del Tratamiento.

Inspección visual

Debemos tener en cuenta si hay indicios que denoten la implantación, divulgación e integración de la normativa interna de seguridad en la entidad y si esta se encuentra actualizada.

1.3.	**Inspección visual:**
1.3.1.	Comprobar si existen carteles informativos u otras advertencias que sean fácilmente visibles sobre el cumplimiento de medidas de seguridad.
1.3.2.	Según la actividad realizada por la entidad auditada, deducir la existencia de tratamientos de datos por cuenta de terceros no identificados en el Documento de Seguridad.
1.3.3.	Observar, en visita general, si la descripción de las instalaciones de la entidad en el Documento de Seguridad es adecuada y actual.

4.2.2. Revisión del Documento de Seguridad. Funciones y obligaciones del personal

AUDITORÍA DE PROTECCIÓN DE DATOS		
REVISIÓN DEL DOCUMENTO DE SEGURIDAD N.º: 2. FUNCIONES Y OBLIGACIONES DEL PERSONAL		
Entidad: Zapatos Gutiérrez		
Nombre Fichero/Tratamiento: Proveedores	N.º Inscripción del Fichero: 321654	
Nivel de Seguridad: **ALTO**	Fecha Auditoría: 12/03/09	
Aprobado por: D. Antonio Ruiz Escalante		Fecha: 18/03/09
Realizado por: Dª. María Palma Rodríguez		Fecha: 12/03/09

Cuestiones que debe plantearse el auditor para la comprobación y verificación del apartado "Funciones y obligaciones del personal"

- Definición de las funciones y obligaciones del personal, con acceso a datos de carácter personal y los sistemas de información.
- ¿Están documentadas y reflejadas en el documento de seguridad?
- ¿Se han definido las funciones de control o autorizaciones delegadas por el Responsable del Fichero?
- ¿Conoce el personal las medidas de seguridad que afectan al desarrollo de sus funciones?
- ¿Conoce las consecuencias de su incumplimiento?

Documentación necesaria para la comprobación

Solicitar los siguientes documentos:

- Descripción de las funciones de los usuarios y perfiles de usuarios dentro del Documento de Seguridad.
- Manual del empleado.
- Organigrama funcional de la entidad.
- Plan de formación de la empresa a sus trabajadores en materia de seguridad de la información.

2.1.	**Análisis de la documentación:**
2.1.1.	Comprobar que las funciones de los usuarios o perfiles de usuario descritos en el Documento de Seguridad concuerdan con las descritas en el Manual de Empleado (si existe) y son coherentes con el organigrama funcional. Con el listado de funciones completar la prueba del *PT-5.2.3 Control de Acceso*.
2.1.2.	Comprobar que en el Documento de Seguridad se definen las funciones de control o las autorizaciones delegadas. *Cruzar la información de esta prueba con la realizada en el PT-1.1.3.*
2.1.3.	Comprobar si en el Documento de Seguridad se establece la difusión de su contenido entre el personal de la entidad.

Comprobación de registros

Debemos solicitar los siguientes registros:

- Justificantes de recepción por parte de los trabajadores de la comunicación del Responsable del Fichero o Tratamiento, sobre la existencia y obligado cumplimiento de las normas establecidas en el Documento de Seguridad, así como de las consecuencias de su incumplimiento.
- Un listado actualizado (altas/bajas) o muestra de los usuarios activos en el sistema, obtenido del Departamento Informático.
- Listado de personal actualizado, por departamentos y categorías, y la fecha de alta en la entidad.
- Justificantes de asistencia por parte de los usuarios a jornadas formativas en seguridad de la información, y más concretamente de protección de datos personales.

2.2.	**Comprobación de registros:**
2.2.1.	Analizar el listado actualizado de personal y el listado actualizado de usuarios del sistema, para comprobar que estos son coherentes con las funciones detalladas en el Documento de Seguridad.
2.2.2.	Comprobar si hay justificantes de recepción por parte de los trabajadores de la comunicación del Responsable del Fichero sobre la existencia y obligado cumplimiento de las normas establecidas en el Documento de Seguridad, así como de las consecuencias de su incumplimiento.
2.2.3.	Obtener evidencia de asistencia a cursos de formación por parte de los usuarios en materia de seguridad de la información y protección de datos personales.

Inspección visual

Debemos indicar si ser observan indicios de discordancias entre las funciones teóricas y las reales desarrolladas por el personal.

2.3.	**Inspección visual:**
2.3.1.	Observar durante la ejecución *in situ* de la auditoría si hay discordancias entre las funciones desarrolladas por los empleados y sus funciones según el Documento de Seguridad.

4.2.3. Revisión del Documento de Seguridad. Registro de Incidencias

AUDITORÍA DE PROTECCIÓN DE DATOS		
REVISIÓN DEL DOCUMENTO DE SEGURIDAD N.º: 3. REGISTRO DE INCIDENCIAS		
Entidad: Comercial del Bricolaje		
Nombre Fichero/Tratamiento: Clientes	N.º Inscripción del Fichero: 36584	
Nivel de Seguridad: ALTO	Fecha Auditoría: 08/05/09	
Aprobado por: D. Antonio Ruiz Escalante		Fecha: 14/05/09
Realizado por: : Dª. María Palma Rodríguez		Fecha: 08/05/09

Cuestiones que debe plantearse el auditor para la comprobación y verificación del apartado "Registro de incidencias"

- ¿Existe un procedimiento de notificación y gestión de incidencias de seguridad?, ¿existe, está bien diseñado y es eficaz?
- ¿Conoce todo el personal afectado, dicho procedimiento?
- ¿Existe un registro de incidencias donde se reflejen todos los datos exigidos en el Reglamento?, ¿se han registrado todas las incidencias ocurridas?
- ¿Se revisa periódicamente el registro de incidencias para su análisis y adopción de medidas correctoras de las incidencias anotadas?

Documentación necesaria para la comprobación

- Solicitar la descripción de la gestión de incidencias, contenida en el Documento de Seguridad.

3.1.	**Análisis de la documentación:**
3.1.1.	Comprobar que el Documento de Seguridad incluye el procedimiento de notificación y gestión de incidencias. *Cruzar la información de esta prueba con la realizada en el PT-1.1.3.*
3.1.2.	Comprobar que el Documento de Seguridad incluye el procedimiento de recuperación de datos. *Cruzar la información de esta prueba con la realizada en el PT-1.1.3.*
3.1.3.	Comprobar que el procedimiento de recuperación de datos indica la obligación de disponer de autorización.

Comprobación de los registros

Se deben solicitar los siguientes registros:

- Registros de incidencias.
- Registros de las aplicaciones, antivirus, cortafuegos y copias de seguridad, que permitan detectar incidencias acontecidas en la entidad.
- Autorizaciones por escrito del Responsable del Fichero para la ejecución de los procedimientos de recuperación de datos.

Una vez solicitada dicha información se procederá a la comprobación de los registros de la siguiente manera:

3.2.	**Comprobación de Registros:**		
3.2.1	Comprobar que el formulario del registro de incidencias contiene los campos mínimos fijados en el Documento de Seguridad. Debe contener:	*Visto*	*Notas*
	a) Tipo de incidencia.		
	b) Fecha en la que se produjo.		
	c) Persona que la notificó.		
	d) Persona que atendió la notificación.		
	e) Efectos derivados de la incidencia.		
	f) Medidas correctoras aplicadas.		
3.2.2.	Analizar si se rellenan todos los campos del registro de incidencias.		
3.2.3.	Averiguar, mediante los registros de actividad de algunas aplicaciones como antivirus, cortafuegos y copias de respaldo, si se han producido incidencias no incluidas en el registro de incidencias.		
3.2.4.	Comprobar que el formulario del registro de incidencias contiene los campos mínimos fijados en el Documento de Seguridad. Debe contener:	*Visto*	*Notas*
	a) Procedimientos realizados de recuperación de datos.		
	b) Persona que ejecutó el proceso.		
	c) Relación de datos restaurados.		
	d) Relación de datos grabados manualmente.		
3.2.5.	Comprobar que el Responsable del Fichero autoriza cada una de las recuperaciones de datos.		

Inspección visual

- Indicar si existen indicios en la entidad que denoten la existencia de incidencias no registradas.
- Realizar entrevistas con Responsables y usuarios del sistema.

3.3.	Inspección visual:
3.3.1.	Observar si en los centros de trabajo existen elementos característicos relacionados con la gestión de alguna incidencia que pudiera no estar registrada, como por ejemplo la presencia de profesionales externos.

4.2.4. Revisión del Documento de Seguridad. Identificación y Autentificación

AUDITORÍA DE PROTECCIÓN DE DATOS		
REVISIÓN DEL DOCUMENTO DE SEGURIDAD N.º: 4. IDENTIFICACIÓN Y AUTENTICACIÓN		
Entidad: Gestoría Avilés		
Nombre Fichero/Tratamiento: Personal	N.º Inscripción del Fichero: 12654	
Nivel de Seguridad: ALTO	Fecha Auditoría: 25/08/09	
Aprobado por: D. Antonio Ruiz Escalante		Fecha: 31/08/09
Realizado por: : Dª. María Paloma Rodríguez		Fecha: 25/08/09

¿Qué Cuestiones debe plantearse el auditor para la comprobación y verificación del apartado "Identificación y autenticación"?

- ¿Existe una relación de usuarios con acceso autorizado?, ¿se mantiene actualizada?
- ¿Existen procedimientos de identificación y autenticación para dicho acceso?, ¿garantiza la correcta identificación del usuario?
- El mecanismo de acceso y verificación de autorización de los usuarios, ¿les identifica de forma inequívoca y personalizada?
- ¿Existe un procedimiento de asignación, distribución y almacenamiento de contraseñas?, ¿garantiza su confidencialidad e integridad?
- ¿Se cambian las contraseñas con la periodicidad establecida en el Documento de Seguridad?
- ¿Se almacenan las contraseñas de forma ininteligible mientras están en vigor?

Documentación necesaria para la comprobación

Solicitar el siguiente documento:

- Descripción de los procedimientos de identificación y autentificación y, en su caso de la asignación, distribución, y almacenamiento de contraseñas dentro del Documento de Seguridad.

4.1.	**Análisis de la documentación:**
4.1.1.	Comprobar que el mecanismo de identificación y autenticación establecido garantiza el acceso de forma inequívoca y personalizada.
4.1.2.	Describir cómo se verifica la autorización de acceso al sistema de información.
4.1.3.	Comprobar que el procedimiento de identificación y autenticación descrito en el Documento de Seguridad se adecua a las exigencias de la normativa. Debe contener:

	Visto	*Notas*
a) Procedimiento de asignación de contraseñas.		
b) Procedimiento de distribución de contraseñas.		
c) Procedimiento de almacenamiento de contraseñas.		
d) Periodicidad del cambio de contraseñas.		
e) Almacenamiento ininteligible de contraseñas.		

4.1.4.	Verificar que estos procedimientos garantizan la confidencialidad e integridad.

Comprobación de los registros

Debe solicitar los siguientes registros:

- Listado de parámetros de las políticas de seguridad del sistema de nombres de usuario y sus contraseñas.
- Registro de accesos no autorizados y del histórico de usuarios bloqueados.
- Listado actualizado (altas /bajas) de usuarios activos en el sistema, obtenido del Departamento Informático.
- Listado del personal actualizado, por departamentos y categorías, y la fecha de alta en la entidad, obtenido del Departamento de Recursos Humanos.

Una vez obtenida dicha información, procederemos a la comprobación de dichos registros de la siguiente manera:

4.2. Comprobación de Registros:
4.2.1. Comprobar en el listado de usuarios, que no hay usuarios genéricos para grupos de personas: debe establecerse un usuario para cada persona.
4.2.2. Comprobar que existe una relación de usuarios y perfiles de usuarios.
4.2.3. Comprobar que todos los integrantes del listado de usuarios (Departamento de Informática) están incluidos en el listado de personal (Departamento de Recursos Humanos) o en el de Encargados del Tratamiento. – Para el personal no incluido en el listado de usuarios, averiguar el motivo: se trata de personal sin acceso al sistema de información, o bien el listado de usuarios no está actualizado. – Para los usuarios no incluidos en la lista de personal o de Encargados del Tratamiento, verificar que sus perfiles de usuario se encuentran deshabilitados.
4.2.4. Analizar los parámetros del registro de políticas de seguridad para ver si el sistema está configurado para obligar a los usuarios a cambiar las contraseñas con la periodicidad establecida en el Documento de Seguridad.
4.2.5. Comprobar mediante el listado de accesos no autorizados y del histórico de usuarios bloqueados que se limita el intento reiterado de acceso al sistema de información.

Inspección visual

Deberán observarse los siguientes aspectos:

- Almacenamiento ininteligible de las contraseñas vigentes: Confidencialidad e integridad.
- Limitación del número de intentos de acceso no autorizado al sistema de información.
- Entrevistas con Responsables y Usuarios del Sistema.

4.3.	**Inspección visual:**
4.3.1.	Observar la confidencialidad de las contraseñas, en caso de que se almacenen por escrito (agendas en papel y electrónicas, documentos informáticos, etc.).
4.3.2.	Observar que no hay apuntadas contraseñas en los puestos de trabajo.
4.3.3.	Comprobar mediante la introducción de contraseñas aleatorias cuántos intentos fallidos son necesarios para bloquear a los usuarios de la entidad.

4.2.5. Revisión del Documento de Seguridad. Control de accesos

AUDITORÍA DE PROTECCIÓN DE DATOS		
REVISIÓN DEL DOCUMENTO DE SEGURIDAD N.º: 5. CONTROL DE ACCESO		
Entidad: Transportes Gómez		
Nombre Fichero/Tratamiento: Clientes	N.º Inscripción del Fichero: 231564	
Nivel de Seguridad: **MEDIO**	Fecha Auditoría: 12/05/09	
Aprobado por: D. Antonio Ruiz Escalante		Fecha: 19/05/09
Realizado por: : Dª. María Palma Rodríguez		Fecha: 12/05/09

Cuestiones que debe plantearse el auditor para la comprobación y verificación del apartado "Control de accesos"

- ¿Los accesos autorizados de los usuarios se corresponden exclusivamente a los datos y recursos que precisan para el desarrollo de sus funciones?
- ¿Existen mecanismos que impidan que los usuarios accedan a datos o recursos distintos de los autorizados?
- ¿Existe una relación de usuarios?, ¿especifica qué datos y recursos tiene autorizados para cada uno de ellos? ¿Está actualizada?

- ¿La concesión, alteración o anulación de accesos autorizados sobre datos y recursos la realiza exclusivamente el personal autorizado para ello en el Documento de Seguridad?
- ¿Ha establecido el Responsable del Fichero los criterios conforme a los cuales se otorga la autorización de los accesos a los datos y a los recursos?
- El personal ajeno al Responsable que tiene acceso a los datos y recursos de este ¿se encuentra sometido a las mismas condiciones y obligaciones que el personal propio?
- ¿Se encuentran los archivadores u otros elementos de almacenamiento en áreas de acceso restringido dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente?, ¿están cerradas estas áreas mientras no sea preciso el acceso a los documentos incluidos en el fichero?
- 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?, ¿se ha motivado adecuadamente?

Documentación necesaria para la comprobación

Se deben solicitar los siguientes documentos:

- Descripción de los procedimientos de control de acceso dentro del Documento de Seguridad.
- Descripción de las funciones de los usuarios y perfiles de usuarios, concretamente acerca de los pertenecientes a entidades externas a la entidad, dentro del Documento de Seguridad.
- Informes mensuales del Responsable de Seguridad con las revisiones realizadas del registro de accesos y de los problemas detectados.

5.1.	**Análisis de la documentación:**
5.1.1.	Analizar la idoneidad de los procedimientos de control de acceso a los recursos autorizados, utilizados por la entidad.
5.1.2.	Comprobar qué procedimientos se establecen para comunicar la aplicación de las medidas de seguridad al personal externo con acceso a datos.
5.1.3.	Analizar la idoneidad de los procedimientos de control de acceso a los lugares con equipos que dan soporte a los sistemas de información.
5.1.4.	Analizar los informes que debe emitir el Responsable de Seguridad (con periodicidad mensual, como mínimo) para comprobar que este realmente se encarga de detectar problemas, así como de controlar que la información del registro es correcta y completa.
5.1.5.	En el caso de que la entidad no aplique el registro del control de accesos, comprobar si en el Documento de Seguridad se incluye y se justifica la no aplicación.
5.1.6.	Comprobar si el Documento de Seguridad incluye las medidas que impidan el acceso de personas no autorizadas a ficheros y tratamientos no automatizados.
5.1.7.	Comprobar que en el Documento de Seguridad se establece un procedimiento para el registro de accesos a documentos utilizados por múltiples usuarios.
5.1.8.	Comprobar que en el Documento de Seguridad se establece un procedimiento para el registro de accesos no autorizados a la documentación. Documentado en informe mensual por el responsable de seguridad y las medidas correctoras para subsanar los errores en accesos no consentidos.

Comprobación de los registros

Para hacer la comprobación de registros debemos solicitar los siguientes documentos:

- Listado detallado de los recursos, niveles y privilegios de acceso al sistema para cada usuario o perfil de usuarios.
- Relación del personal autorizado para conceder, alterar o anular el acceso autorizado, dentro del Documento de Seguridad.

- Listado de funciones de los usuarios y perfiles de usuarios (ya verificadas en apartados anteriores).
- Justificantes de comunicación a los usuarios pertenecientes a entidades externas y con acceso a los recursos, de las medidas de seguridad que deben aplicar.
- Listado autorizado del personal autorizado a acceder a los locales donde se encuentran ubicados los sistemas de información.
- Registro de accesos.
- Listado de usuarios autorizados y de la documentación a la que tienen acceso.

5.2. Comprobación de registros:

5.2.1. Comprobar que existe una relación de usuarios, perfiles y sus accesos al sistema.

5.2.2. Verificar la vigencia del listado de usuarios.

5.2.3. Comparar las funciones de los usuarios verificadas en el PT - 2.1.1. *Funciones y obligaciones del personal,* con el listado de recursos, niveles y privilegios de acceso.

Usuario	Listado de funciones según PT- 2	Listado de recursos, niveles y privilegios de acceso

5.2.4. Comprobar que en el Documento de Seguridad se identifica el personal autorizado para conceder, alterar o anular los accesos a los recursos.

5.2.5. Verificar la existencia de notificaciones sobre la aplicación de las medidas de seguridad por parte del personal externo. C*ruzar la información de esta prueba con la realizada en el PT-10.2.1.*

5.2.6. Comprobar que existe un listado actualizado en el cual se identifica el personal con acceso autorizado a los lugares donde se ubiquen los equipos que den soporte a los sistemas de información.

5.2.7.	Comprobar que el registro de accesos contiene como mínimo la siguiente información de cada intento de acceso: a) Usuario. b) Fecha. c) Hora. d) Fichero accedido. e) Tipo de acceso. f) Acceso autorizado o denegado. g) Identificación del registro para accesos autorizados.	*Visto*	*Notas*
5.2.8.	Obtener constancia a través del registro de accesos de cuándo se ha detenido y reanudado, y de quién ha provocado o ha podido provocar tal circunstancia.		
5.2.9.	Verificar mediante el análisis de las fechas que se guarda la información del registro de accesos de los 2 últimos años.		
5.2.10.	Si la entidad no aplica el registro de accesos con base al artículo 103.6 del RDLOPD, comprobar mediante las inscripciones en el Registro General de la Agencia Española de Protección de Datos que el Responsable del Fichero o Tratamiento es una persona física.		
5.2.11.	Comprobar que el registro de personal autorizado a acceder a la documentación está actualizado y se corresponde con las funciones atribuidas.		
5.2.12.	Comprobar la estructura, efectividad y consistencia de los registros creados para controlar el acceso a documentos utilizados por múltiples usuarios.		
5.2.13.	Comprobar la existencia del registro de accesos a documentación por parte de personas no autorizadas y su estructura.		

Inspección visual

Observación de la eficacia de los distintos mecanismos utilizados por la entidad para el control de acceso a los recursos y en especial para prevenir y detectar accesos no autorizados.

5.3.	**Inspección visual:**
5.3.1.	Observar si hay usuarios con acceso a recursos no necesarios para sus funciones.
5.3.2.	Observar la presencia de personal externo a la entidad con acceso a recursos, y que debe haber sido informado acerca de las medidas de seguridad que debe aplicar.
5.3.3.	Observar el funcionamiento de las medidas de control de acceso físico a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.
5.3.4.	Observar el acceso por parte de un usuario autorizado al fichero y verificar el correcto registro del acceso a la información.
5.3.5.	Observar las medidas de control adicionales que garanticen que el Responsable del Fichero o Tratamiento es el único con acceso a los datos susceptibles de aplicar el registro de accesos.
5.3.6.	Observar si los mecanismos para evitar el acceso no autorizado a los ficheros y tratamientos no automatizados son adecuados.
5.3.7.	Observar si se aplica el procedimiento de registro de accesos autorizados a documentos utilizados por múltiples usuarios y si se corresponde con el descrito en el Documento de Seguridad.
5.3.8.	Observar si se aplica el procedimiento de registro de accesos no autorizados a la documentación y si se corresponde con el descrito en el Documento de Seguridad.

4.2.6. Revisión del Documento de Seguridad. Gestión de Soportes

AUDITORÍA DE PROTECCIÓN DE DATOS		
REVISIÓN DEL DOCUMENTO DE SEGURIDAD N.º: 6. GESTIÓN DE SOPORTES		
Entidad: Gestoría Hermanos Pastrana		
Nombre Fichero/Tratamiento: Clientes-proveedores	N.º Inscripción del Fichero:	
Nivel de Seguridad: **ALTO**	Fecha Auditoría: 30/05/09	
Aprobado por: D. Antonio Ruiz Escalante		Fecha: 05/06/09
Realizado por: : Dª. María Palma Rodríguez		Fecha: 30/05/09

Cuestiones que debe plantearse el auditor para la comprobación y verificación del apartado "Gestión de soportes y documentos"

- Si está identificado el tipo de información contenido en el soporte o documento.
- Si existe y se mantiene un inventario de soportes.
- ¿Se almacenan los soportes o documentos en lugares de acceso restringido?
- ¿Existen mecanismos por los que solamente puedan acceder las personas autorizadas en el Documento de Seguridad?, ¿funcionan adecuadamente estos mecanismos?
- Si se ha dejado constancia en el Documento de Seguridad, si fuera el caso, de la imposibilidad de cumplir con las obligaciones establecidas en el Reglamento sobre identificación, inventariado y acceso a los soportes dadas sus características físicas.
- ¿La salida de soportes y documentos fuera de los locales donde se ubica el fichero está siendo autorizada por el Responsable del Fichero o está debidamente autorizada en el Documento de Seguridad?
- ¿Se están tomando las medidas adecuadas en el traslado de documentación para evitar la sustracción, pérdida o acceso indebido durante su transporte?
- Cuando se desecha un soporte o documento conteniendo datos de carácter personal, ¿se adoptan las medidas adecuadas para evitar el acceso a la información o su recuperación posterior cuando se procede a su destrucción o borrado?, ¿son adecuadas estas medidas?

- ¿Se dan de baja en el inventario estos soportes o documentos desechados?
- Para los soportes con datos de carácter personal considerados especialmente sensibles por la organización, ¿se utilizan sistemas de etiquetado que permitan la identificación de su contenido a las personas autorizadas y dificulten su identificación al resto?, ¿son adecuados y cumplen su finalidad?
- ¿Se utilizan sistemas de etiquetado que permitan la identificación de su contenido a las personas autorizadas y dificulten su identificación al resto?
- ¿Son adecuados y cumplen su finalidad?
- ¿La distribución de soportes se realiza de forma cifrada, o por otro mecanismo que garantice que no sea inteligible o manipulable durante el transporte?
- ¿Se cifran los datos en los dispositivos portátiles cuando estos salen de las instalaciones del Responsable del Fichero?
- Si fuera imprescindible el tratamiento de datos en dispositivos portátiles que no permitan el cifrado de datos, ¿se ha hecho constar motivadamente en el Documento de Seguridad?, ¿se han adoptado medidas para minimizar los riesgos derivados de este tratamiento en entornos desprotegidos?, ¿son adecuadas?
- ¿Se adoptan medidas que impidan el acceso o manipulación de la información en los casos de traslado físico de la documentación contenida en un fichero?, ¿son apropiadas estas medidas?
- La generación de copias o reproducción de documentos, ¿se realiza exclusivamente por el personal autorizado en el Documento de Seguridad?
- ¿Se destruyen las copias o reproducciones desechadas de forma que no se pueda acceder a la información contenida en las mismas?

Documentación necesaria para la comprobación

Se deben solicitar los siguientes documentos:

- Descripción de los procedimientos de gestión de soportes dentro del Documento de Seguridad.
- Descripción de los procedimientos de cifrado de los datos en la distribución de soportes.
- Descripción de los criterios de archivo de documentos dentro del Documento de Seguridad.

Análisis de la Documentación

Para llevar a cabo el análisis de la documentación analizaremos lo siguiente:

<table>
<tr><th colspan="3">6.1. Análisis de la documentación:</th></tr>
<tr><td>6.1.1.</td><td colspan="2">Comprobar que el procedimiento de gestión de soportes descrito en el Documento de Seguridad se adecua a las exigencias de la normativa. Esto significa comprobar la inclusión de:</td></tr>
<tr><td></td><td>a) Criterios para identificar la información incluida en los soportes y documentos.
b) Criterios para autorizar el acceso a los soportes y documentos y listado de personal autorizado.
c) Criterios para inventariar los soportes y documentos.</td><td><table><tr><th>Visto</th><th>Notas</th></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr></table></td></tr>
<tr><td>6.1.2.</td><td colspan="2">Comprobar si se motiva la no aplicación de las medidas anteriores debido a las características físicas del soporte.</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td>6.1.3.</td><td colspan="2">Comprobar que el procedimiento de gestión de soportes descrito en el Documento de Seguridad se adecua a las exigencias de la normativa. Esto significa comprobar la inclusión de:</td></tr>
<tr><td></td><td>a) Especificaciones de que las salidas de soportes con datos personales fuera de la entidad deben estar autorizadas por el Responsable del Fichero.
b) Instrucciones para la destrucción de soportes y documentos que vayan a ser desechados. Cruzar la información de esta prueba con la realizada en el PT-1.1.3.
c) Medidas de seguridad para el transporte de documentación que eviten la sustracción, pérdida o acceso indebido. Cruzar la información de esta prueba con la realizada en el PT-1.1.3.
d) Procedimientos de clasificación e identificación de soportes según su contenido y los usuarios autorizados a conocer este procedimiento.</td><td><table><tr><th>Visto</th><th>Notas</th></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr></table></td></tr>
<tr><td>6.1.4.</td><td colspan="2">Analizar la idoneidad del procedimiento del sistema de cifrado de datos personales utilizado para la distribución de soportes y dispositivos portátiles.</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td>6.1.5.</td><td colspan="2">Comprobar si las excepciones a la utilización de dispositivos portátiles que no permitan su cifrado está motivada en el Documento de Seguridad.</td></tr>
<tr><td colspan="3"></td></tr>
</table>

6.1.6. En el caso de utilizar dispositivos portátiles que no permitan su cifrado, comprobar si se aplican medidas de seguridad compensatorias y su idoneidad.

6.1.7. Comprobar si el Documento de Seguridad establece para los ficheros no automatizados:

	Visto	*Notas*
a) Criterios y procedimientos de archivo de los soportes y documentos.		
b) Instrucciones para la custodia de la documentación pendiente o que esté fuera del archivo.		
c) Medidas de seguridad para impedir el acceso no autorizado a los ficheros.		
d) Medidas alternativas y motivo de su aplicación, cuando las características de los locales impidan aplicar medidas de control de acceso a los ficheros.		
e) Medidas de seguridad para impedir el acceso o la manipulación a la documentación durante su traslado.		

Comprobación de registros

Se deben solicitar los siguientes registros:

- Inventario de soportes.
- Registro de entradas y salidas de soportes.
- Autorizaciones del Responsable del Fichero para las salidas de soportes.

Una vez solicitada dicha información se procederá a la comprobación de los registros de la siguiente manera:

<table>
<tr><td>6.2.</td><td>Comprobación de registros:</td></tr>
<tr><td>6.2.1.</td><td>Comprobar que la entidad dispone de un listado del personal autorizado a acceder a los soportes.</td></tr>
<tr><td></td><td></td></tr>
<tr><td>6.2.2.</td><td>Comprobar que existe un inventario actualizado de soportes y documentos.</td></tr>
<tr><td></td><td></td></tr>
<tr><td>6.2.3.</td><td>Comprobar que las autorizaciones de salida de soportes y documentos de la entidad están debidamente autorizadas por el Responsable del Fichero.</td></tr>
<tr><td></td><td></td></tr>
<tr><td>6.2.4.</td><td>Comprobar mediante el registro de inventario de soportes las bajas realizadas y el procedimiento empleado para su destrucción o borrado.</td></tr>
<tr><td></td><td></td></tr>
<tr><td>6.2.5.</td><td>Comprobar en el registro de inventario de soportes si estos se identifican de forma ininteligible para usuarios no autorizados.</td></tr>
<tr><td></td><td></td></tr>
<tr><td>6.2.6.</td><td>Comprobar que los registros de entrada y salida de documentos o soportes están actualizados y contienen los campos mínimos fijados en el Reglamento:
<table>
<tr><th></th><th>Visto</th><th>Notas</th></tr>
<tr><td>a) Tipo de soporte o documento.</td><td></td><td></td></tr>
<tr><td>b) Fecha.</td><td></td><td></td></tr>
<tr><td>c) Hora.</td><td></td><td></td></tr>
<tr><td>d) Emisor/Destinatario.</td><td></td><td></td></tr>
<tr><td>e) Número de soportes o documentos en el envío.</td><td></td><td></td></tr>
<tr><td>f) Tipo de información almacenada.</td><td></td><td></td></tr>
<tr><td>g) Forma de envío.</td><td></td><td></td></tr>
<tr><td>h) Responsable de la recepción/entrega.</td><td></td><td></td></tr>
<tr><td>i) Autorización.</td><td></td><td></td></tr>
</table></td></tr>
<tr><td>6.2.7.</td><td>Verificar la existencia y periódica actualización del registro de salidas de soportes y documentos.</td></tr>
<tr><td></td><td></td></tr>
<tr><td>6.2.8.</td><td>Comprobar mediante registro de autorizaciones de salida de soportes e inventario, la existencia de dispositivos portátiles y ver si se cifran los datos incluidos según el procedimiento establecido.</td></tr>
<tr><td></td><td></td></tr>
</table>

Inspección visual

Proceder a la observación de los siguientes aspectos:

- Identificación de soportes.
- Almacenamiento de soportes en lugar restringido.
- Cumplimiento de las medidas establecidas para el desechado o reutilizado de soportes.
- Distribución cifrada de los soportes que contienen datos personales.
- Medidas de seguridad utilizadas para la protección de la documentación en general: acceso, archivo, custodia, etc.

6.3.	**Inspección visual:**
6.3.1.	Verificar que los soportes y documentos utilizados por la entidad cumplen los siguientes requisitos:

	Visto	*Notas*
a) Tienen identificada la información que contienen.		
b) Están inventariados.		
c) Se almacenan en lugar de acceso restringido.		
d) Son reutilizados de forma segura.		
e) Son desechados de forma segura.		

6.3.2.	Observar la existencia de los medios para la destrucción de soportes que hubiesen sido mencionados en el procedimiento de gestión de soportes del Documento de Seguridad. *Cruzar la información de esta prueba con la realizada en el PT-7.2.8.*
6.3.3.	Ver que los soportes están identificados de forma ininteligible para los usuarios no autorizados.
6.3.4.	Detectar soportes distribuidos (tras análisis de la operativa general de gestión de soportes de la entidad) y verificar si están cifrados.
6.3.5.	En visita a los archivos comprobar que se garantiza la correcta conservación, localización y consulta de la información almacenada.
6.3.6.	Observar si se sigue una política de mesas limpias cuando los usuarios abandonan su lugar de trabajo.
6.3.7.	Ver qué dispositivo se utiliza para impedir el acceso a los ficheros no automatizados y si existe diferencia con el descrito en el Documento de Seguridad.
6.3.8.	Ver si hay áreas accesibles sin atender.
6.3.9.	Ver si el uso de medidas alternativas se justifica con la motivación ofrecida y se corresponde en lo descrito en el Documento de Seguridad.

4.2.7. Revisión del Documento de Seguridad. Copias de Respaldo y Recuperación

AUDITORÍA DE PROTECCIÓN DE DATOS		
REVISIÓN DEL DOCUMENTO DE SEGURIDAD N.º: 7. COPIAS DE RESPALDO Y RECUPERACIÓN		
Entidad: Gestoría Avilés		
Nombre Fichero/Tratamiento: Personal	N.º Inscripción del Fichero: 213654	
Nivel de Seguridad: **ALTO**	Fecha Auditoría: 23/08/09	
Aprobado por: D. Antonio Ruiz Escalante		Fecha: 29/08/09
Realizado por: : Dª. María Palma Rodríguez		Fecha: 23/08/09

Cuestiones que debe plantearse el auditor para la comprobación y verificación del apartado "Copias de respaldo y recuperación"

- ¿El Responsable del Fichero ha definido los procedimientos de realización de copias de respaldo y recuperación de los datos?, ¿es adecuada esta definición?
- ¿Están reflejados estos procedimientos en el Documento de Seguridad?
- ¿Ha verificado el Responsable del Fichero la correcta aplicación de estos procedimientos?, ¿realiza esta verificación cada seis meses?
- ¿Garantizan los procedimientos establecidos la reconstrucción de los datos al estado en que se encontraban antes de producirse la pérdida o destrucción?
- Si esta pérdida o destrucción afecta a ficheros parcialmente automatizados, ¿se ha procedido a grabar manualmente los datos?, ¿queda constancia motivada de este hecho en el Documento de Seguridad?
- ¿Se realizan copias de respaldo al menos semanalmente? Si no es así ¿se debe a que no ha habido actualizaciones en ese período?
- ¿Las pruebas previas a la implantación o modificación de los sistemas de información se realizan con datos reales? En caso afirmativo, ¿se están aplicando las mismas medidas de seguridad que las que le corresponde por la naturaleza de los datos que contiene?, ¿se anota su realización en el Documento de Seguridad?, ¿se hacen copias de seguridad previas a la realización de pruebas con datos reales?
- ¿Se conserva una copia de respaldo y de los procedimientos de recuperación de datos en lugar diferente al de los equipos que los tratan?

- ¿Cumple este lugar las medidas de seguridad exigidas en el Reglamento?

Documentación necesaria para la comprobación

Se deben solicitar los siguientes documentos:

- Descripción del procedimiento de gestión de copias de respaldo y de recuperación de los datos dentro del Documento de Seguridad.
- Descripción del procedimiento de gestión de copias de documentos y su destrucción dentro del Documento de Seguridad.

4.1. Análisis de la documentación:

7.1.1. Comprobar que el procedimiento de copias de respaldo y recuperación descrito en el Documento de Seguridad se adecua a las exigencias de la normativa (artículos 94 y 102 del RDLOPD). Esto significa comprobar la inclusión de *(Cruzar la información de esta prueba con la realizada en el PT-1.1.3.)*:

	Visto	*Notas*
a) Identificación del responsable de la definición y gestión de las copias de respaldo y de su recuperación.		
b) Instrucciones para la realización de las copias de respaldo.		
c) Instrucciones para recuperación de los datos que garantice la reconstrucción y en qué ocasiones esta puede ser manual.		
d) Definición de una periodicidad de realización de copias (debe ser como mínimo semanal).		
e) Restricciones al uso de datos reales para la realización de pruebas en el sistema de información.		
f) Instrucciones con la obligación de realizar copias de seguridad de los datos previos a la realización de pruebas con datos reales.		
g) Instrucciones para el archivo de una copia de respaldo y de sus procedimientos de recuperación.		

7.1.2. Comprobar si existe un procedimiento para la realización de copias de documentos y, de ser así, si se identifica en el Documento de Seguridad el personal autorizado para ello.

7.1.3. Comprobar si existe un procedimiento para la destrucción de copias de documentos desechados.

Comprobación de registros

Se deben solicitar los siguientes registros:

- Inventarios de soportes (registro ya solicitado en el apartado de Gestión de soportes.).
- Registro de las entradas y salidas de soportes (registro ya solicitado en el apartado de Gestión de soportes.).
- Registro de realización de copias de respaldo.
- Listado de funciones de los usuarios y perfiles de usuarios (Registro ya solicitado en el apartado de funciones y obligaciones del personal).
- Registro de incidencias (Registro ya solicitado en el apartado de "Registro de Incidencias").
- Registro de controles periódicos, auditorias o informes (Registro ya solicitado en el apartado "Documento de Seguridad").
- Contratos con Encargados del Tratamiento para la destrucción de documentos.

7.2.	**Comprobación de registros:**
7.2.1.	Verificar la efectividad del procedimiento establecido para las copias de respaldo mediante el registro de las comprobaciones realizadas por la empresa.
7.2.2.	Verificar la periodicidad con la que se realizan las copias de respaldo, mediante el registro de copias de respaldo o en el propio inventario de soportes.
7.2.3.	Verificar la efectividad del procedimiento establecido de recuperación de copias de respaldo mediante el registro de las comprobaciones realizadas por la empresa y el registro de incidencias para encontrar recuperaciones de datos realizadas.
7.2.4.	Comprobar que la verificación de la definición, funcionamiento y aplicación de procedimientos de las copias de respaldo y de recuperación se realiza cada 6 meses mediante el registro de control establecido a tal efecto.
7.2.5.	Comprobar mediante registros de copias de seguridad que se hicieron con fecha anterior a la realización de las pruebas con datos reales.
7.2.6.	Comprobar el almacenamiento de copias de respaldo y de los procedimientos de recuperación fuera de las instalaciones de la entidad, mediante el análisis del registro de entradas y salidas de soportes.
7.2.7.	Comprobar la existencia de una relación del personal autorizado que controle la generación de copias o reproducción de documentos.
7.2.8.	Comprobar si la entidad dispone de medios para la destrucción de documentos o si se ha contratado un servicio de destrucción certificada de documentación en caso de grandes cantidades. *Cruzar la información de esta prueba con la realizada en el PT-6.3.2.*

Inspección visual

Deben indicar el resultado de la observación de los siguientes aspectos:

- Existencia física de las copias de respaldo.
- Verificación de que una copia de respaldo (y los procedimientos para su recuperación) se guarda en un lugar diferente de aquel en el cual se encuentran los equipos informáticos de tratamiento.

- Verificación de que las copias de respaldo que salen fuera del lugar de los equipos informáticos de tratamiento se cifran.
- Comprobación del proceso de recuperación de datos.
- Entorno de pruebas.
- Verificación de las condiciones y recursos para la copia y destrucción efectiva de documentos.

7.3.	**Inspección visual:**
7.3.1.	Ver el lugar y condiciones en las cuales se guardan las copias de respaldo, para comprobar que se garantiza su integridad.
7.3.2.	Buscar la existencia de aplicaciones en entorno de pruebas con datos personales reales y verificar en ellas la totalidad de las medidas de seguridad aplicadas.
7.3.3.	Comprobar *in situ* (si es posible) un proceso de recuperación de datos.
7.3.4.	Ver el lugar y condiciones donde se guardan aquellas copias de respaldo que se conservan en un lugar diferente de la ubicación de los equipos informáticos de tratamiento, para comprobar que se garantiza su integridad.
7.3.5.	Verificar que se cifra el contenido de las copias de respaldo que se trasladan fuera de la entidad.
7.3.6.	Ver si existen medidas adicionales que garanticen la integridad y recuperación de la información, en caso de que no se guarden copias de respaldo fuera de los lugares donde se tratan los datos.
7.3.7.	Ver si los dispositivos de copia tienen limitado el uso o no están disponibles en las instalaciones de tratamiento, para evitar copias o reproducciones no autorizadas.
7.3.8.	Ver si hay depósitos para recoger las copias a destruir o máquinas destructoras de documentos.
7.3.9.	Ver si hay avisos sobre la destrucción de copias desechadas de los documentos.

4.2.8. Revisión del Documento de Seguridad. Telecomunicaciones

AUDITORÍA DE PROTECCIÓN DE DATOS		
REVISIÓN DEL DOCUMENTO DE SEGURIDAD N.º: 8. TELECOMUNICACIONES		
Entidad: Empresa de informática Ramos		
Nombre Fichero/Tratamiento: Personal	N.º Inscripción del Fichero: 231644	
Nivel de Seguridad: **ALTO**	Fecha Auditoría: 15/07/09	
Aprobado por: D. Antonio Ruiz Escalante		Fecha: 22/07/09
Realizado por: : Dª. María Palma Rodríguez		Fecha: 15/07/09

Cuestiones que debe plantearse el auditor para la comprobación y verificación del apartado "Telecomunicaciones"

- ¿Los accesos a datos mediante redes de comunicaciones garantizan un nivel de seguridad equivalente a los accesos en modo local?
- ¿La transmisión de datos a través de redes se realiza de forma cifrada (o por cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros)?, ¿este mecanismo de cifrado es eficaz?

Documentación necesaria para la comprobación

Se debe solicitar los siguientes documentos:

- Descripción del procedimiento de gestión de las telecomunicaciones en el Documento de Seguridad.
- Diagrama de la red informática de la entidad.

8.1.	**Análisis de la documentación:**
8.1.1.	Comprobar que el procedimiento de gestión de telecomunicaciones descrito en el Documento de Seguridad es coherente con el diagrama de la red informática.
8.1.2.	Comprobar que el procedimiento de gestión de telecomunicaciones descrito en el Documento de Seguridad incluye instrucciones para el cifrado de datos en las transmisiones por redes públicas o inalámbricas.

Comprobación de los registros

Se deben solicitar los siguientes registros:

- Listado de usuarios que dispongan de conexiones remotas a los ficheros de datos personales ubicados en la entidad.
- Autorizaciones motivadas para las conexiones remotas de los usuarios.
- Listado de personal actualizado, por departamentos y categorías, y la fecha de alta en la entidad, obtenido del Departamento de Recursos Humanos (Registro ya solicitado en el apartado "Funciones y obligaciones del personal").

Inspección visual

Deben indicar el resultado de la observación de los siguientes aspectos:

- Método utilizado para cifrar las comunicaciones con datos personales.
- Procedimiento a seguir en el cifrado de las transmisiones de datos de carácter personal, a través de redes de telecomunicaciones públicas o inalámbricas.

8.3.	**Inspección visual:**
8.3.1.	Identificar el método utilizado por la entidad para garantizar la seguridad en los accesos remotos a los datos y analizar su fiabilidad.
8.3.2.	Verificar el proceso seguido por la entidad para el cifrado de datos enviados por las redes de telecomunicaciones públicas o inalámbricas.

4.2.9. REVISIÓN DEL DOCUMENTO DE SEGURIDAD. AUDITORÍA

AUDITORÍA DE PROTECCIÓN DE DATOS		
REVISIÓN DEL DOCUMENTO DE SEGURIDAD N.º: 9. AUDITORÍA		
Entidad: Calzados Lujan		
Nombre Fichero/Tratamiento: Clientes- Proveedores	N.º Inscripción del Fichero: 235649	
Nivel de Seguridad: **ALTO**	Fecha Auditoría: 11/08/09	
Aprobado por: D. Antonio Ruiz Escalante		Fecha: 17/08/09
Realizado por: : Dª. María Palma Rodríguez		Fecha: 11/08/09

Cuestiones que debe plantearse el auditor para realizar una auditoría de protección de datos

- ¿Se realiza la actual auditoría en el plazo establecido desde la anterior?
- Si ha habido modificaciones sustanciales en el sistema de información ¿se ha realizado a continuación una auditoría para verificar la adaptación, adecuación y eficacia de las medidas de seguridad?
- ¿Los informes de las auditorías anteriores incluían los datos, hechos y observaciones en los que se basaban sus dictámenes?
- ¿Se han implementado las medidas correctoras propuestas por auditorías anteriores?, ¿han sido eficaces y han corregido las deficiencias encontradas?

Documentación necesaria para comprobar

Debe solicitarse la siguiente documentación:

- Informes de las auditorías realizadas.
- Informes de conclusiones del Responsable de Seguridad asociados a las auditorías realizadas.

9.1. Análisis de la documentación:

9.1.1. Comprobar que los informes de auditoría se adecuan a las exigencias de la normativa. Debe contener:

	Visto	*Notas*
a) Fecha.		
b) Identificación de la persona que lo firma.		
c) Detalle de la metodología utilizada en el proceso auditor.		
d) Concluye con una opinión sobre la adecuación de las medidas de seguridad y controles a la Ley y al RDLOPD.		
e) Identifica las deficiencias.		
f) Propone medidas correctoras o complementarias para cada deficiencia.		
g) Presenta recomendaciones.		
h) Incluye los datos, hechos y observaciones que soportan las conclusiones y recomendaciones realizadas.		

9.1.2. Comprobar que el informe de conclusiones del Responsable de Seguridad cumple los requisitos formales siguientes:

	Visto	*Notas*
a) Fecha.		
b) Se identifica la persona que lo firma.		
c) Analiza cada una de las deficiencias detalladas en el informe de auditoría.		
d) Emite conclusiones.		
e) Hay acuse de recibo del Responsable del Fichero.		

9.1.3. En caso de tratarse de una auditoria interna, analizar si se cumple el principio de independencia del auditor.

9.1.4. Con base al trabajo realizado, analizar si en el momento de la ejecución de la auditoria se han aplicado las medidas correctoras o complementarias (así como las recomendaciones) propuestas en los informes precedentes.

9.1.5. Comprobar si existe un procedimiento que identifique cuáles son los supuestos que hacen necesario realizar una auditoría.

Comprobación de registros

Solicitar los siguientes registros:

- Registro de auditorías realizadas.
- Notificación de la inscripción del fichero emitida por la Agencia Española de Protección de Datos.

9.2.	Comprobación de registros:
9.2.1.	En caso de que la entidad no disponga de ningún informe de auditoría comprobaremos que no hayan transcurrido más de 2 años desde la fecha de creación del fichero (ver notificación de la Inscripción del Fichero emitida por la Agencia Española de Protección de Datos), hasta la fecha de encargo de la auditoría en curso.
9.2.2.	En caso de no ser primera auditoría, comprobar mediante el registro de auditorías realizadas y las fechas de los informes entregados que no hayan transcurrido más de dos años entre la realización de cada una de las auditorías.
9.2.3.	Comprobar mediante las versiones del Documento de Seguridad que no se han producido cambios significativos en el sistema de información que obligaran a la realización de auditoría extraordinaria.

Inspección visual

En este caso no se aplica la inspección visual.

4.2.10. Revisión del Documento de Seguridad. Encargado de Tratamiento

AUDITORÍA DE PROTECCIÓN DE DATOS		
REVISIÓN DEL DOCUMENTO DE SEGURIDAD N.º: 10. ENCARGADO DEL TRATAMIENTO		
Entidad: Construcciones Ramírez		
Nombre Fichero/Tratamiento: Nóminas	N.º Inscripción del Fichero: 321654	
Nivel de Seguridad: **ALTO**	Fecha Auditoría: 23/01/09	
Aprobado por: D. Antonio Ruiz Escalante		Fecha: 30/01/09
Realizado por: : Dª. María Palma Rodríguez		Fecha: 23/01/09

Cuestiones que debe plantearse el auditor para la comprobación y verificación del apartado "Encargado del tratamiento"

- ¿Se realiza el tratamiento por persona distinta al Responsable del Fichero?, ¿se ha formalizado mediante contrato conforme lo establecido el artículo 12 de la LOPD?
- Si la realización de este encargo se realiza en los locales del Responsable, ¿se ha hecho constar esta circunstancia en el Documento de Seguridad?, ¿consta por escrito en el contrato el compromiso del personal del encargado de tratamiento respecto al cumplimiento de las medidas de seguridad recogidas en el Documento de Seguridad del Responsable?
- Cuando el tratamiento se realiza mediante acceso remoto a los sistemas del Responsable ¿se le ha prohibido al Encargado de Tratamiento la incorporación de los datos a sistemas o soportes distintos de los del Responsable?, ¿se ha hecho constar tal circunstancia en el Documento de Seguridad del Responsable?
- Si la prestación se hace en locales propios del Encargado de Tratamiento (distintos de los del Responsable), ¿ha elaborado el encargado el Documento de Seguridad?, ¿identifica el fichero o tratamiento y el Responsable del mismo?, ¿detalla las medidas de seguridad a implementar en relación con su tratamiento?

Documentación necesaria para la comprobación

Deben solicitar los siguientes documentos:

- Descripción del procedimiento que regula el tratamiento de datos personales fuera de los locales, dentro del Documento de Seguridad.
- Descripción del ámbito de aplicación del Documento de Seguridad.
- Procedimiento de contratación de Encargados del Tratamiento dentro de las funciones propias del Responsable del Fichero o Tratamiento.
- Procedimiento que regula las condiciones de seguridad del teletrabajo en la entidad.

10.1.	**Análisis de la documentación:**
10.1.1.	Comprobar si el Documento de Seguridad hace mención del acceso a los datos, soportes o recursos del sistema por parte del Encargado del Tratamiento en los locales del responsable.
10.1.2.	Comprobar si el Documento de Seguridad autoriza los accesos remotos por parte del Encargado del Tratamiento y la prohibición de recoger en sus sistemas los datos accedidos.
10.1.3.	Comprobar si existen unas condiciones generales de contratación de los Encargados del Tratamiento, con el detalle de los requisitos mínimos que deben cumplir en materia de protección de datos personales.
10.1.4.	Comprobar si en las condiciones generales de contratación de los Encargados del Tratamiento se solicita copia del Documento de Seguridad elaborado por estos en caso de prestación de servicios en sus locales.
10.1.5.	Comprobar si se establecen medidas para el control de aplicación de las medidas de seguridad por parte de los Encargados del Tratamiento.
10.1.6.	Comprobar que en los contratos de prestación de servicios se prohíbe el acceso a datos personales o, en caso de conocerse, la obligación de secreto.
10.1.7.	Comprobar en el ámbito de aplicación del Documento de Seguridad si incluye procedimientos de trabajo fuera de las instalaciones y las medidas de seguridad a aplicar.
10.1.8.	Verificar que el procedimiento de tratamiento de datos personales en el exterior de los locales exige autorización.
10.1.9.	Comprobar si estas autorizaciones se realizan por usuario o por perfil de usuarios.
10.1.10.	Comprobar que el Documento de Seguridad incluye un procedimiento de renovación y revocación de las autorizaciones.

Comprobación de registros

Solicitar los siguientes registros:

- Contratos con Encargados del Tratamiento (o muestra de los más representativos).
- Autorizaciones del Responsable del Fichero para los tratamientos fuera de los locales.
- Registro de controles practicados a los Encargados del Tratamiento dentro de las funciones propias del Responsable del Fichero o Tratamiento.

10.2.	**Comprobación de registros:**
10.2.1.	Obtener evidencia de la comunicación al personal a cargo del Encargado del Tratamiento, de las medidas de seguridad que deben cumplir durante su estancia en los locales del Responsable del Fichero o en los accesos remotos que realicen. *Cruzar la información de esta prueba con la realizada en el PT-5.2.5.*
10.2.2.	Comprobar si en las condiciones de contratación de los Encargados del Tratamiento se solicita información acerca de su Documento de Seguridad. Si se identifican en él, el fichero que trata, el responsable del mismo y las medidas de seguridad aplicadas.
10.2.3.	Comprobar la existencia de registros de control de los Encargados del Tratamiento (auditorías, revisiones de documentación, etc.)
10.2.4.	Comprobar que existen las autorizaciones del Responsable del Fichero o Tratamiento, para el almacenaje y tratamiento externo de datos, y estas se incluyen en el Documento de Seguridad.
10.2.6.	Comprobar que las autorizaciones para el almacenaje y tratamiento externo de datos tienen fijado un periodo de validez.
10.2.7.	Comprobar que la validez de las autorizaciones es correcta a la fecha de verificación.
10.2.8.	Verificar que no hay salida de dispositivos con la validez de la autorización caducada.

Inspección visual

Se deben observar los siguientes aspectos:

- Acceso a datos personales, soportes o recursos del sistema de información por parte de personal sin necesidad de acceso.
- Tratamiento de datos personales fuera de los locales.

10.3.	**Inspección visual:**
10.3.1.	Observar si personal sin necesidad de acceso a datos personales, soportes que los contengan o recursos del sistema de información puede en la práctica acceder a ellos.
10.3.2.	Observar si hay tratamiento de datos fuera de los locales de la entidad mediante las autorizaciones de salida de soportes y documentos como indicio.

1. ¿Qué objetivo tiene la auditoría de protección de datos?

2. ¿En qué consiste la inspección visual de las actividades auditadas?

3. Para la revisión del Documento de Seguridad, en el apartado Telecomunicaciones, ¿Qué documentación es necesaria para comprobarlo?

4. ¿Qué cuestiones debe plantearse el auditor para la comprobación y verificación del apartado "Registro de incidencias"? Nivel Alto.

5. ¿Qué documentación tendremos que solicitar para la comprobación del control de accesos, en el Documento de Seguridad? Nivel Alto.

6. ¿En qué consiste la inspección visual cuando se quiere revisar la Gestión de Soportes, en el Nivel Alto?

7. ¿En qué consiste la inspección visual cuando se quiere revisar la gestión de soportes Nivel Alto?

Ejercicios de Repaso y Autoevaluación