CAPÍTULO 6
INFORME DE LA AUDITORÍA: FASE 3ª

1. INTRODUCCIÓN

El Reglamento de Medidas de Seguridad de los ficheros de carácter personal en sus artículos 96.2 y 3 establece que:

> 2. *"El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.*
> 3. *Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia de Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas."*

Una vez se han realizado las entrevistas necesarias, se ha revisado la documentación requerida, y se han inspeccionado las instalaciones auditadas, se trata de exponer las primeras conclusiones a la entidad auditada. Para ello se realiza una reunión final que consta de dos etapas:

1. **Preparación de la reunión**: donde el auditor prepara las conclusiones a exponer al auditado y el modo de exponerlas, comprobando para cada uno de los hallazgos.

2. **Llegar a un consenso sobre estos hallazgos.**

Una vez realizada esta reunión final, el auditor le hará entrega al auditado del informe final, que se explicará más adelante.

2. Síntesis del análisis de la documentación requerida para realizar la auditoría

Para cada fichero o tratamiento se analizan las áreas aplicables para identificar todas las deficiencias encontradas y dar propuestas de las mediadas correctoras o complementarias correspondientes, así como de las recomendaciones del auditor.

Revisión del Documento de Seguridad

El objetivo de la revisión del Documento de Seguridad es que el auditor analice que su contenido cumple con los requisitos establecidos en el Reglamento para el mismo. Además, permite al auditor identificar los procedimientos y controles de seguridad definidos en la instalación, para posteriormente verificar su cumplimiento.

Recuerde

En el Documento de Seguridad, se analizan aquellos procedimientos que afectan tanto a su desarrollo, mantenimiento y actualización.

Análisis de los sistemas de información de la empresa

Conlleva establecer los sistemas de información que contienen datos personales, e identificar los ficheros de los distintos niveles en ellos existentes. La importancia de esta tarea reside en que el cumplimiento de determinadas y específicas medidas de seguridad solo es exigido por el Reglamento para los ficheros de nivel medio y alto. Este análisis de los sistemas de información permite al auditor centrar revisión de algunos de los controles exclusivamente en los sistemas y ficheros para los que, en función de su nivel, el Reglamento exige su aplicación.

Identificación, autenticación y controles de acceso

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.

Funciones del Responsable de Seguridad

El Reglamento obliga a nombrar uno o más responsables de seguridad para el cumplimiento de las medidas de seguridad de los ficheros de nivel medio y alto. En la auditoría se ha comprobado si las funciones definidas para estos responsables son coherentes con las definidas en el Reglamento y evaluar el grado de cumplimiento de las mismas.

Soportes de datos

En relación con los soportes de datos, se ha revisado:

- La identificación de los soportes.
- El inventario de soportes.
- El registro de entrada/salida de soportes.

Copias de seguridad

Los procedimientos respecto a las copias de seguridad y restauración del sistema han sido exhaustivamente analizados por el auditor, para establecer que las copias de seguridad se realizan y custodian correctamente.

Registro de incidencias

El registro de incidencias es la parte del Documento de Seguridad que permite la realización de estudios e informes que permitan evolucionar la seguridad dentro del sistema informático de la organización, por lo que el auditor ha comprobado la realización y almacenamiento de las incidencias, en caso de que las hubiera.

Control de acceso físico a la sala de servidores

Al igual que se implantan medidas de seguridad de acceso a los sistemas informáticos y a los ficheros, el acceso físico a la sala de servidores debe estar restringido exclusivamente a personal autorizado, medida que el auditor ha comprobado que se lleva acabo.

Transmisiones

Un sistema de información es el de los sistemas de transmisión o de telecomunicaciones. Apartado que el auditor ha analizado todas las redes locales, como las conexiones externas que pueden afectar a la seguridad de los ficheros.

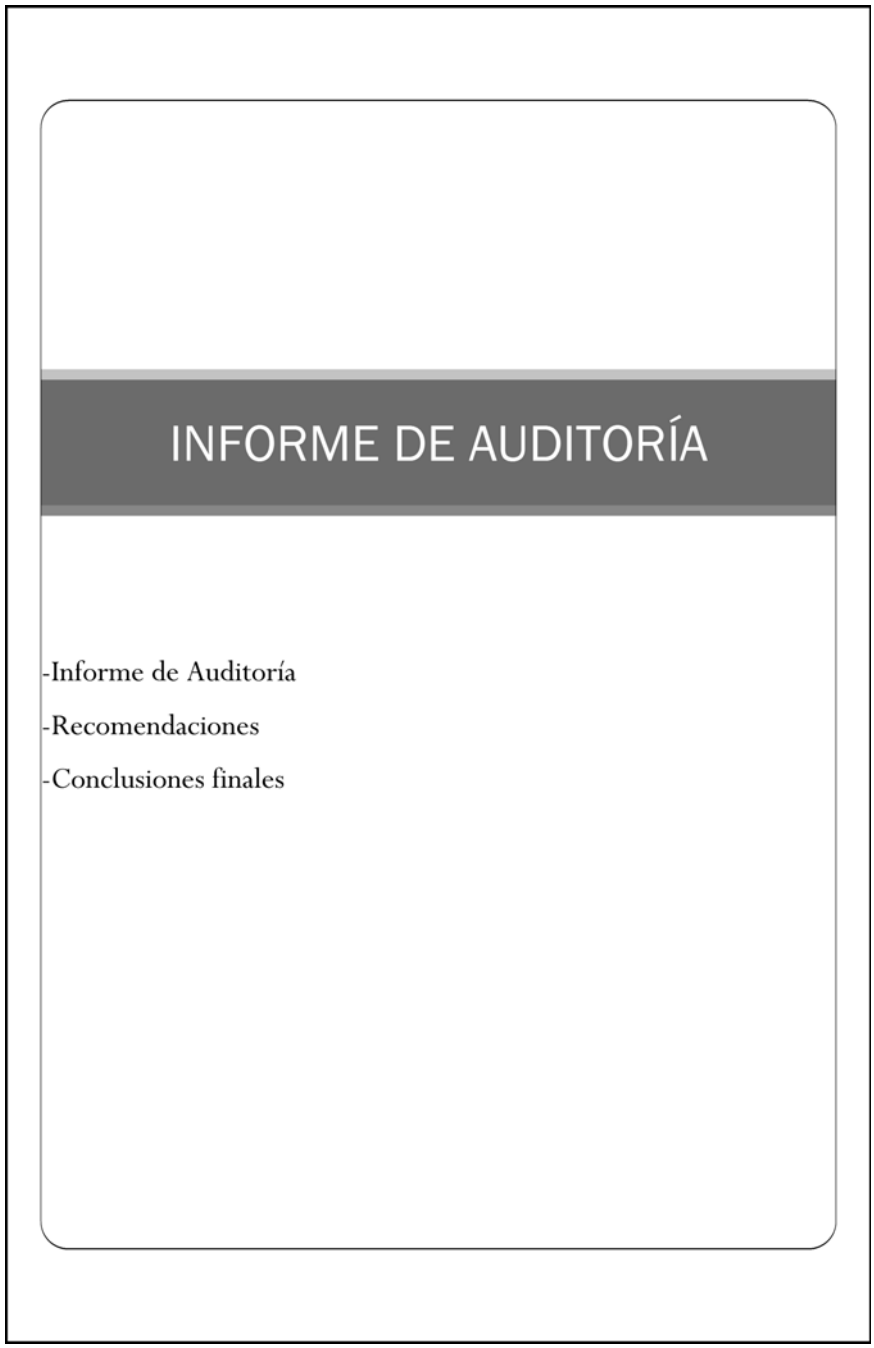
ANALISIS DEL AUDITORÍA	
PUNTO AUDITADO	CONCLUSIÓN
Niveles de seguridad	Análisis de los arts. 80, 81, 87 y 105.1.g). Satisfactorio/ con deficiencias leves, graves o muy graves.
Revisión del documento de seguridad	Análisis de los arts. 79, 84, 88, 95, 109 y 105.1.a), e) y h). Satisfactorio/ con deficiencias leves, graves o muy graves.
.Funciones y obligaciones del personal	Análisis de los arts. 89 y 105.2.a). Satisfactorio/ con deficiencias leves, graves o muy graves.
Registro de incidencias	Análisis de los arts. 90, 100 y 105.2.b). Satisfactorio/ con deficiencias leves, graves o muy graves.
Identificación y autenticación	Análisis de los arts. 93 y 98. Satisfactorio/ con deficiencias leves, graves o muy graves.
Control de acceso a los datos de carácter personal	Análisis de los arts. 91, 99, 103, 105.2.c), 107 y 113. Satisfactorio/ con deficiencias leves, graves o muy graves.
Gestión de los soportes que contienen datos	Análisis de los arts. 92, 97, 101, 105.2.d), 106, 108, 111 y 114. Satisfactorio/ con deficiencias leves, graves o muy graves.
Copias de respaldo y recuperación	Análisis de los arts. 94, 102 y 112. Satisfactorio/ con deficiencias leves, graves o muy graves.
Telecomunicaciones	Análisis de los arts. 85 y 104. Satisfactorio/ con deficiencias leves, graves o muy graves.

3. RECOMENDACIONES

Tal como se describe en el punto 2 del Art. 96 del R.D. 1720/2007:

> *"El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente Reglamento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas"*

Respecto a los datos hechos y observaciones enumeradas a lo largo del Documento de Seguridad y analizados, se debe establecer las medidas correctoras.


INFORME DE AUDITORÍA
-Informe de Auditoría
-Recomendaciones
-Conclusiones finales

A continuación establecemos cada uno de los apartados analizados, en los cuales el auditor establece sus recomendaciones:

Revisión del documento de seguridad

Recomendación:

- Comprobación del contenido y alcance.
  - Debe tener una mayor difusión entre los usuarios.
  - El documento de seguridad debe incluir los nombramientos de las diferentes personas como responsable del fichero, responsable de seguridad, etc.
  - Documentar todos los procesos que afectan al documento de seguridad como son los controles que se hacen con un carácter mensual, medidas sobre la reutilización de soportes, períodos de contraseñas, etc.
- Revisión de las políticas relacionadas con el Documento de seguridad.
  - El documento debe ser actualizado.
  - El documento debe tener difusión entre los diferentes proveedores y colaboradores externos como Informática externa.
- Conocimiento práctico entre los empleados.
  - Los empleados deben no solo conocer la existencia del documento de seguridad del fichero que le afecta como usuario, sino además poner en práctica el contenido del mismo, especialmente la comunicación de las incidencias, etc.
- Revisión del documento.
  - El documento ha de ser revisado y se recomienda su evolución continua.

Análisis de los sistemas de información de la empresa

Recomendación:

- Establecer un protocolo de mantenimiento de los sistemas de información de la empresa.

Identificación, autenticación y controles de acceso

Recomendación:

- Establecimiento de los controles de acceso y nombramiento de personal que se responsabilice de ese control.

Funciones del responsable de seguridad

Recomendación:

- Elaboración de un informe que establezca sus funciones respecto de la auditoría llevada acabo.

Soportes de datos

Recomendación:

- Debe ser actualizado el procedimiento de salida de datos.

Copias de seguridad

Recomendación:

- Cifrar las copias de seguridad.

Registro de incidencias

Recomendación:

- Informar de todas las incidencias y establecer un protocolo de registro y actuación.

Control de acceso físico a la sala

Recomendación:

- El acceso a la sala debe estar restringido al personal de autorizado.

Registro de accesos

Recomendación:

- Debe incluirse en el procedimiento de las copias de seguridad su período de conservación.

Transmisiones

Recomendaciones:

- Debe incluirse una política sobre el acceso a Internet.

4. CONCLUSIÓN FINAL

En la conclusión final, el auditor establece una valoración de la auditoría realizada al responsable del fichero. Esta valoración puede ser positiva, positiva con algunas deficiencias y negativa, de acuerdo con el análisis de toda la documentación referente a la protección de datos requerida.

Modelo de informe de conclusiones con opinión positiva con algunas deficiencias

En_____, a_____de_____

Se ha realizado una auditoría interna de los sistemas de información e instalaciones de tratamiento y almacenamiento de datos de carácter personal de la entidad_____ para comprobar que se cumple con el Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como de los procedimientos e instrucciones vigentes en materia de protección de datos.

De acuerdo con nuestra valoración, podemos establecer que los sistemas de información e instalaciones de tratamiento y almacenamiento de la entidad_____ _____se adecuan a la legislación aplicable en seguridad de tratamiento de datos de carácter personal, a excepción de las deficiencias observadas que se detallan en el presente informe, que además incluye las correspondientes medidas correctoras o complementarias.

En el presente informe se ha propuesto una serie de recomendaciones para que el Responsable de seguridad las valore y aplique.

Por último, se recuerda a la entidad_____ que el Responsable de Seguridad debe analizar el presente informe de auditoría, y elevar a la Dirección las conclusiones que resulten para que esta adopte las medidas correctoras adecuadas.

Firma

Modelo de informe de conclusiones con opinión positiva

En _____, a _____ de _____

Se ha realizado una auditoria interna de los sistemas de información e instalaciones de tratamiento y almacenamiento de datos de carácter personal de la entidad. Para comprobar que se cumple el Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como de los procedimientos e instrucciones vigentes en materia de protección de datos.

De acuerdo con nuestra valoración, podemos establecer, que los sistemas de información e instalaciones de tratamiento y almacenamiento de la entidad _____ se adecuan a la legislación aplicable en seguridad de tratamiento de datos de carácter personal.

En el presente informe se ha propuesto una serie de recomendaciones para que el responsable de seguridad las valore y aplique.

Por último, se recuerda a la entidad _____ que su/s Responsable/s de Seguridad deben analizar el presente informe de auditoría, y elevar a la Dirección las conclusiones del mismo para adoptar las recomendaciones pertinentes.

Firma

Modelo de informe de conclusiones con opinión negativa

En_____, a_____ de_____

Se ha realizado una auditoría interna de los sistemas de información e instalaciones de tratamiento y almacenamiento de datos de carácter personal de la entidad_____ para comprobar que se cumple con el Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como de los procedimientos e instrucciones vigentes en materia de protección de datos.

De acuerdo con nuestra valoración, podemos establecer que los sistemas de información e instalaciones de tratamiento y almacenamiento de la entidad_____ no se adecuan a la legislación aplicable en seguridad de tratamiento de datos de carácter personal, debido a la importancia de las deficiencias observadas, que se detallan en el presente informe, que además incluye las correspondientes medidas correctoras o complementarias.

En el presente informe se ha propuesto una serie de recomendaciones para que el Responsable de seguridad las valore y aplique.

Por último, se recuerda a la entidad_____ que el Responsable de Seguridad debe analizar el presente informe de auditoría, y elevar a la Dirección las conclusiones que resulten para que esta adopte las medidas correctoras adecuadas.

Firma

5. INFORME DE AUDITORÍA

La auditoría concluye cuando el auditado recibe del auditor el informe de auditoría, y este es aceptado.

El informe de auditoría debe ser elaborado por el auditor jefe (en caso de más de un auditor), y se debe entregar a la persona que se determine en la reunión final. Este informe debe contener:

- Objetivos de la auditoría.
- Identificación de los auditores.
- Personas contactadas.
- Fecha de la auditoría.
- Normas de referencia.
- Descripción de las no conformidades encontradas, y la toma de las acciones correctivas.
- Eficacia del Sistema para el cumplimiento de los requisitos de la norma y documentos.
- Lista de distribución del informe.

- Adjuntar observaciones y recomendaciones para adecuar la empresa a la protección de datos.

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

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

Estructura del informe:

- Entidad auditada.
- Auditor interno.
- Objetivos de la auditoría.
- Ficheros y tratamiento auditados.
- Ejecución del trabajo.
- Entrega del informe.
- Análisis de los niveles de seguridad asignados.
- Tabla resumen de medidas correctoras o complementarias.
- Tabla resumen de recomendaciones del auditor.
- Conclusiones.

MODELO DE INFORME DE AUDITORÍA

1. ENTIDAD AUDITADA

Nombre	
CIF	
Domicilio Social	
Actividad	
Responsable de contacto	
Centros de trabajo:	
Empresas vinculadas:	

2. AUDITOR INTERNO

Nombre	
NIF	
Auditores que han participado:	

3. OBJETIVOS DE LA AUDITORÍA

Verificar el cumplimiento de:

– Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.
– Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
– Procedimientos vigentes en materia de seguridad de datos.
– Instrucciones vigentes en materia de seguridad de datos.

4. FICHEROS Y TRATAMIENTOS AUDITADOS

Nombre	Fichero…
Ubicación	
Finalidad	
Medidas de seguridad	
Código de inscripción	
Fecha de inscripción	

Nombre	Fichero…
Ubicación	
Finalidad	
Medidas de seguridad	
Código de inscripción	
Fecha de inscripción	

- *Centro de trabajo auditado*

Nombre	
Dirección	
Actividad centro	

5. EJECUCIÓN DEL TRABAJO

Todos los trabajos han sido efectuados en el plazo de... días.

Para la revisión, se han realizado las entrevistas indicadas y se ha recibido la documentación indicada.

6. ENTREGA DEL INFORME

Se entregará ejemplar de este informe a:

Nombre y apellidos	Cargo y Departamento

7. ANÁLISIS DE LOS NIVELES DE SEGURIDAD ASIGNADOS

Tras analizar la calidad de los datos incluidos en los ficheros y tratamientos a auditar y compararla con la información proporcionada por el Responsable del Fichero o Tratamiento, realizamos la siguiente valoración:

Fichero o Tratamiento	Nivel asignado por el Responsable del Fichero o Tratamiento	Nivel que corresponde según el auditor
Comentarios:		

8. MEDIDAS CORRECTORAS

Fichero	Art.	Nivel	Deficiencia	Medida correctora

9. RECOMENDACIONES DEL AUDITOR

Fichero	Nivel	Deficiencia	Recomendación

10. CONCLUSIONES

MODELO DE INFORME DE CONCLUSIONES CON OPINIÓN POSITIVA

En_____ a ___ de _____ de _____

Se ha realizado una auditoría interna de los sistemas de información e instalaciones de tratamiento y almacenamiento de datos de carácter personal de la entidad… para comprobar que se cumple con el Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como de los procedimientos e instrucciones vigentes en materia de protección de datos.

De acuerdo con nuestra valoración, podemos establecer que los sistemas de información e instalaciones de tratamiento y almacenamiento de la entidad… se adecuan a la legislación aplicable en seguridad de tratamiento de datos de carácter personal.

En el presente informe se han propuesto una serie de recomendaciones para que el Responsable de seguridad las valore y aplique.

Por último, se recuerda a la entidad… que el Responsable de Seguridad debe analizar el presente informe de auditoría, y elevar a la Dirección las conclusiones que resulten para que ésta adopte las medidas correctoras adecuadas.

Firma

MODELO DE INFORME DE CONCLUSIONES CON OPINIÓN POSITIVA CON ALGUNAS DEFICIENCIAS

En_____, a ___ de _____ de _____

Se ha realizado una auditoría interna de los sistemas de información e instalaciones de tratamiento y almacenamiento de datos de carácter personal de la entidad… para comprobar que se cumple con el Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como de los procedimientos e instrucciones vigentes en materia de protección de datos.

De acuerdo con nuestra valoración, podemos establecer que los sistemas de información e instalaciones de tratamiento y almacenamiento de la entidad… se adecuan a la legislación aplicable en seguridad de tratamiento de datos de carácter personal, a excepción de las deficiencias observadas que se detallan en el presente informe, que además incluye las correspondientes medidas correctoras o complementarias.

En el presente informe se han propuesto una serie de recomendaciones para que el Responsable de seguridad las valore y aplique.

Por último, se recuerda a la entidad… que el Responsable de Seguridad debe analizar el presente informe de auditoría, y elevar a la Dirección las conclusiones que resulten para que esta adopte las medidas correctoras adecuadas.

Firma

MODELO DE INFORME DE CONCLUSIONES CON OPINIÓN NEGATIVA

En_____, a ___ de _____ de _____

Se ha realizado una auditoría interna de los sistemas de información e instalaciones de tratamiento y almacenamiento de datos de carácter personal de la entidad… para comprobar que se cumple con el Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como de los procedimientos e instrucciones vigentes en materia de protección de datos.

De acuerdo con nuestra valoración, podemos establecer que los sistemas de información e instalaciones de tratamiento y almacenamiento de la entidad… no se adecuan a la legislación aplicable en seguridad de tratamiento de datos de carácter personal, debido a la importancia de las deficiencias observadas, que se detallan en el presente informe, que además incluye las correspondientes medidas correctoras o complementarias.

En el presente informe se han propuesto una serie de recomendaciones para que el Responsable de seguridad las valore y aplique.

Por último, se recuerda a la entidad… que el Responsable de Seguridad debe analizar el presente informe de auditoría, y elevar a la Dirección las conclusiones que resulten para que esta adopte las medidas correctoras adecuadas.

Firma

MODELO DE INFORME DE AUDITORÍA

1. ENTIDAD AUDITADA

Nombre	ANTONIO RUIZ ESCALANTE, S.L.
CIF	B98761234
Domicilio Social	C/SAN DAVID nº 24 JAÉN
Actividad	
Responsable de contacto	ANTONIO RUIZ ESCALANTE
Centros de trabajo: CARPINTERÍA ESCALANTE. C/ BUENA VISTA, S/N	
Empresas vinculadas:	

2. AUDITOR INTERNO

Nombre	ENCARNACIÓN CASTILLO GÓMEZ
NIF	25123456-R
Auditores que han participado: CARMEN PARADAS DELGADO Y ENRIQUE LÓPEZ ALGARRA	

3. OBJETIVOS DE LA AUDITORÍA

Verificar el cumplimiento de:

– Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.
– Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
– Procedimientos vigentes en materia de seguridad de datos.
– Instrucciones vigentes en materia de seguridad de datos.

4. FICHEROS Y TRATAMIENTOS AUDITADOS

Nombre	Fichero PERSONAL
Ubicación	DESPACHO DEL GERENTE
Finalidad	GESTIÓN DEL PERSONAL: NÓMINAS, SEGUROS SOCIALES Y PREVENCIÓN DE RIESGOS LABORALES
Medidas de seguridad	Medidas de seguridad de nivel básico
Código de inscripción	21081172758
Fecha de inscripción	26 de Enero de 2008

Nombre	Fichero CLIENTE
Ubicación	DESPACHO DEL GERENTE
Finalidad	GESTIÓN DE LOS CLIENTES
Medidas de seguridad	Medidas de seguridad de nivel medio
Código de inscripción	21081182858
Fecha de inscripción	6 de Enero de 2008

- *Centro de trabajo auditado*

Nombre	CARPINTERIA ESCALANTE, S.L.
Dirección	C/SAN DAVID, Nº 24 JAÉN
Actividad centro	CONSTRUCCIÓN

5. EJECUCIÓN DEL TRABAJO

Todos los trabajos han sido efectuados en el plazo de 12 días.

Para la revisión, se han realizado las entrevistas indicadas y se ha recibido la documentación indicada.

6. ENTREGA DEL INFORME

Se entregará ejemplar de este informe a:

Nombre y apellidos	Cargo y Departamento
ANTONIO RUIZ ESCALANTE	GERENTE. DEPARTAMENTO DE GERENCIA
CORAL DUEÑAS GAONA	DIRECTORA DE ADMINISTRACIÓN. DEPARTAMENTO DE ADMINISTRACIÓN
EVA DELGADO GALINDO	DIRECTORA DE VENTAS. DEPARTAMENTO DE VENTAS.

7. ANÁLISIS DE LOS NIVELES DE SEGURIDAD ASIGNADOS

Tras analizar la calidad de los datos incluidos en los ficheros y tratamientos a auditar y compararla con la información proporcionada por el Responsable del Fichero o Tratamiento, realizamos la siguiente valoración:

Fichero o Tratamiento	Nivel asignado por el Responsable del Fichero o Tratamiento	Nivel que corresponde según el auditor
FICHERO PERSONAL	BÁSICO	BÁSICO
FICHERO CLIENTES	MEDIO	MEDIO

Comentarios: LOS NIVELES ESTÁN ESTABLECIDOS CORRECTAMENTE.

DEL FICHERO PERSONAL NO SE DEBE DE REALIZAR UNA AUDITORÍA PORQUE ES DE NIVEL BÁSICO, POR LO QUE LA AUDITORÍA SE CENTRA EN EL FICHERO DE CLIENTES.

8. MEDIDAS CORRECTORAS

Fichero	Art.	Nivel	Deficiencia	Medida correctora
FICHERO CLIENTE	Arts.93 y 98	MEDIO	Identificación y autenticación. No se han cambiado las contraseñas a los usuarios en los dos años desde que se realizó la implantación de la LOPD hasta que se ha realizado la auditoría.	Medida correctora: el Responsable de Seguridad debe cambiar las contraseñas de los usuarios como mínimo cada año, el tiempo que transcurra desde que se atribuye una contraseña a los usuarios hasta que la cambia no puede superar el año.

9. RECOMENDACIONES DEL AUDITOR

Fichero	Nivel	Deficiencia	Recomendación
FICHERO CLIENTE	MEDIO	Control de accesos	Se recomienda que exista una persona responsable de este control de accesos y un exhaustivo registro del mismo

10. CONCLUSIONES

En Jaén, a 12 de Octubre de 2009

Se ha realizado una auditoría interna de los sistemas de información e instalaciones de tratamiento y almacenamiento de datos de carácter personal de la entidad ANTONIO RUIZ ESCALANTE, SL. para comprobar que se cumple con el Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como de los procedimientos e instrucciones vigentes en materia de protección de datos.

De acuerdo con nuestra valoración, podemos establecer que los sistemas de información e instalaciones de tratamiento y almacenamiento de la entidad ANTONIO RUIZ ESCALANTE, SL. se adecuan a la legislación aplicable en seguridad de tratamiento de datos de carácter personal.

En el presente informe se han propuesto una serie de recomendaciones para que el Responsable de seguridad las valore y aplique.

Por último, se recuerda a la entidad ANTONIO RUIZ ESCALANTE, SL. que el Responsable de Seguridad debe analizar el presente informe de auditoría, y elevar a la Dirección las conclusiones que resulten para que ésta adopte las medidas correctoras adecuadas.

Firma

6. IMPLANTACIÓN DE LAS MEDIDAS CORRECTORAS RECOGIDAS EN EL INFORME DE AUDITORÍA

Es competencia del responsable del fichero implantar las medidas correctoras establecidas en el informe de auditoría, realizado por el equipo auditor encargado de realizar la auditoría. Estas medidas se establecerán de acuerdo con el análisis realizado de todos los puntos de la auditoría. No se pueden establecer unas medidas correctoras generales, ya que dependerán de cada empresa en particular y del análisis realizado en el fase 2º de la auditoría.

A continuación exponemos un ejemplo de medidas correctoras:

FICHERO	ART.	NIVEL	DEFICIENCIA	MEDIDA CORRECTORA
Fichero cliente	Arts. 85 y 104.	Medio	**Telecomunicaciones**: la red de comunicación inalámbrica de comunicación electrónica se encuentra sin cifrar.	**La medida correctora**: se debe establecer cifrado en la red de comunicación inalámbrica de comunicación electrónica, para asegurar que los datos personales con los que se trabaja en este fichero no sean manipulados por terceros.

Recuerde

Toda la documentación obtenida de la auditoría debe ser archivada para posibles consultas en el futuro.

1. Etapas de la reunión final.

2. ¿Qué se analiza en el Documento de Seguridad?

3. ¿Qué se revisa en relación a los soportes de datos?

4. ¿Cómo puede ser la valoración de auditor en la conclusión final?

5. ¿Qué debe contener el informe de auditoría?

EJERCICIOS DE REPASO Y AUTOEVALUACIÓN