Unidad Didáctica 8

Auditoría

Contenido

1. Qué y cuándo revisar

Este apartado define la normativa a aplicar para la realización de auditorías en la organización con objeto de confirmar fehacientemente que las prácticas y medidas de seguridad aplicadas son las adecuadas y que siguen las normas y procedimientos indicados en el documento de seguridad.

La organización realizará, al menos cada dos años, una auditoría que verifique el cumplimiento de las medidas de seguridad del Reglamento 1720/2007, de 21 de diciembre. Dicha auditoría deberá realizarse con carácter extraordinario con anterioridad al transcurso de los dos años, cuando se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años mencionados anteriormente. La realización de la auditoría es obligatoria para ficheros de nivel medio y alto. La auditoría puede ser interna o externa, es decir, realizada por personal propio de la organización o a través de la contratación de empresas consultoras externas. En el segundo caso, deberá firmarse un contrato de acceso a datos por cuenta de terceros con la empresa o persona que realice de forma externa el procedimiento de auditoría. El contrato deberá incluir las cláusulas de tratamiento y confidencialidad de la información a las que hace referencia el artículo 12 de la LOPD. La auditoría es una norma de seguridad aplicable a ficheros de nivel medio y alto. Su aplicación a ficheros de nivel básico es opcional, pero recomendable.

A la hora de realizar una auditoría se debe establecer cuáles son los ficheros con datos de carácter personal objeto de la misma, sistemas de tratamiento, procedimientos, etc. También se ha de determinar los recursos necesarios para llevar a cabo la auditoría, las fuentes de información, la ubicación del fichero, o las instalaciones.

Las auditorías deben contemplar como mínimo los siguientes puntos:

- Adecuación a la normativa, procedimientos y controles contemplados en el documento de seguridad a lo dispuesto en el reglamento de la LOPD y a las disposiciones legales que en materia de datos de carácter personal puedan establecer en el futuro las autoridades competentes.

- Verificación del correcto cumplimiento de las medidas, procedimientos y normativas que en materia de seguridad se establecen en el documento de seguridad respecto de las instalaciones y sistemas de información que manejan datos de carácter personal.
- Identificación de las deficiencias que en materia de seguridad relacionadas con la LOPD se encuentren en instalaciones, sistemas de información, normativas, procedimientos y prácticas de la organización.
- Recomendaciones de medidas correctoras o complementarias para solventar las deficiencias encontradas.
- Inclusión de todos aquellos datos, hechos y observaciones en los que se basen los dictámenes, recomendaciones y propuestas emitidas.

Nota

Para ello, el auditor tendrá que tener al menos un conocimiento genérico de la empresa, de su ámbito de negocio, de los sistemas de información de que disponen, de su estructura administrativa, y sus relaciones con otras empresas o instituciones.

El auditor deberá realizar un programa de trabajo en el que detallará las actividades o tareas a auditar, teniendo en cuenta los requisitos de revisión exigidos o impuestos por el reglamento con relación a la auditoría, y por otro lado, el ámbito de negocio y sistemas de la empresa.

Para ello el auditor deberá solicitar a la empresa auditada toda la documentación necesaria para verificar el cumplimiento de la normativa vigente en materia de protección de datos, así como la realización de entrevistas con el personal e inspección visual del centro auditado para ver *in situ* si se aplican las medidas de seguridad reflejadas en el documento de seguridad.

Deberá realizar un análisis de toda la documentación e información que ha recabado para establecer los puntos débiles existentes en la empresa en materia de protección de datos, así como exponer las conclusiones a las que

ha llegado, y en su caso, establecer las medidas correctoras ante un deficiente cumplimiento de la normativa vigente como de las posibles recomendaciones para mejorar la seguridad de la empresa en protección de datos.

Por último, el auditor deberá realizar un informe donde se refleje todo lo mencionado anteriormente.

Los controles de auditoría se realizarán en las siguientes áreas:

- Control de la aplicación de documentos de seguridad.
- Control del sistema de acceso lógico.
- Control del sistema de acceso físico.
- Identificación, autenticación y controles de acceso.
- Funciones del responsable de seguridad.
- Revisión del conocimiento práctico de las normas de seguridad por parte del personal.
- Control de los procedimientos de gestión de soportes.
- Control de antivirus.
- Control del procedimiento de copias de respaldo y recuperación de datos.
- Control de la notificación y gestión de incidencias.
- Pruebas con datos reales.
- Transmisiones.

El responsable de seguridad transmitirá los informes de auditoría al responsable del fichero de la organización.

El contenido de las auditorías (tanto si son internas como externas) será analizado por el responsable de seguridad, quien tomará las medidas correctoras oportunas.

Recuerde

Las auditorías realizadas se depositarán y archivarán en la organización, manteniéndose las mismas a disposición de la Agencia Española de Protección de Datos.

2. El informe de auditoría

Es recomendable que el personal que lleve a cabo la auditoría sea externo a la entidad con el propósito de garantizar la imparcialidad e independencia. Los resultados de la auditoría se recogen en el informe sobre la adecuación a las medidas de seguridad recogidas en el Reglamento 1720/2007, de 21 de diciembre, que desarrolla a la Ley Orgánica 15/1999 de Protección de Datos Personales.

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

El informe de auditoría deberá dictaminar sobre:

- Adecuación de las medidas y controles establecidos en lo dispuesto en el Título VIII del reglamento.
- Identificación de deficiencias y propuesta de medidas correctoras o complementarias.
- Incluirá los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.
- Será analizado por el responsable de seguridad, y elevará sus conclusiones al responsable del fichero para que adopte las medidas adecuadas.
- Deberá quedar a disposición de la Agencia Española de Protección de Datos, o de las autoridades de control de las comunidades autónomas.

El informe de auditoría debe contener:

- Objetivos de la auditoría.
- Identificación de los auditores.
- Personas contactadas.
- Fecha de la auditoría.
- Normas de referencia.
- Resultados del análisis de la documentación e información de la empresa y de los sistemas de información, e instalaciones de tratamiento y almacenamiento de datos.
- Descripción de las deficiencias encontradas, y la toma de las actuaciones correctivas.

- Lista de distribución del informe.
- Adjuntar observaciones y recomendaciones para adecuar la empresa a la protección de datos.

La estructura básica del informe podría ser la siguiente:

- Fecha de realización de la auditoría.
- Entidad auditada.
- Auditor interno.
- Objetivos de la auditoría.
- Ficheros y tratamientos auditados.
- Ejecución del trabajo.
- Entrega del informe.
- Análisis de los niveles de seguridad asignados.
- Resultados de la auditoría.
- Medidas correctoras o complementarias.
- Recomendaciones del auditor.
- Conclusiones.

3. Evaluación de las pruebas

Se relacionan a continuación algunas comprobaciones que se pueden realizar para verificar el cumplimiento de las disposiciones del reglamento:

ASPECTOS GENERALES	
SISTEMA DE TRATAMIENTO	TODOS
COMPROBACIONES A REALIZAR	- ¿La clasificación del nivel de seguidad 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?
NIVEL	

ENCARGADO DE TRATAMIENTO	
SISTEMA DE TRATAMIENTO	TODOS
COMPROBACIONES A REALIZAR	- ¿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 de la persona 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 del 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?
NIVEL	

PRESTACIÓN DE SERVICIO SIN ACCESO A DATOS PERSONALES	
SISTEMA DE TRATAMIENTO	TODOS
COMPROBACIONES A REALIZAR	- Si el tratamiento no afecta a datos personales ¿Se han adoptado las medidas necesarias para limitar el acceso del personal a los datos personales, soportes y recursos? - Si se trata de personal ajeno ¿recoge el contrato la prohibición expresa de acceder a los datos personales, así como la obligación de secreto respecto a los datos que hubieran podido conocer con motivo de la prestación de servicio?
NIVEL	

DELEGACIÓN DE AUTORIZACIONES	
SISTEMA DE TRATAMIENTO	TODOS
COMPROBACIONES A REALIZAR	- ¿Se han delegado las autorizaciones que el Reglamento atribuye al responsable en otras personas? ¿Se ha hecho constar en el Documento de Seguridad las personas habilitadas, para otorgar estas autorizaciones y las personas en quienes recae dicha delegación?
NIVEL	

ACCESO A DATOS A TRAVÉS DE REDES	
SISTEMA DE TRATAMIENTO	TODOS
COMPROBACIONES A REALIZAR	- ¿Los accesos a datos mediante redes de comunicaciones, garantizan un nivel de seguridad equivalente a los accesos en modo local?
NIVEL	

RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL FICHERO	
SISTEMA DE TRATAMIENTO	TODOS
COMPROBACIONES A REALIZAR	- El almacenamiento de datos personales, en dispositivos portátiles o los tratamientos fuera de los locales del responsable o del encargado ¿han sido autorizados expresamente por el responsable del fichero? ¿Consta dicha autorización en el Documento de Seguridad?
NIVEL	

FICHEROS TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS	
SISTEMA DE TRATAMIENTO	TODOS
COMPROBACIONES A REALIZAR	- ¿Cumplen el nivel de seguridad correspondiente? ¿Se han destruido o borrado, cuando ya no han sido necesarios para los fines que motivaron su creación?
NIVEL	

DOCUMENTO DE SEGURIDAD	
SISTEMA DE TRATAMIENTO	TODOS
COMPROBACIONES A REALIZAR	- ¿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 periodo 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?
NIVEL	BÁSICO

DOCUMENTO DE SEGURIDAD	
SISTEMA DE TRATAMIENTO	TODOS
COMPROBACIONES A REALIZAR	- ¿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 cumplimiento 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?
NIVEL	MEDIO

FUNCIONES Y OBLIGACIONES	
SISTEMA DE TRATAMIENTO	TODOS
COMPROBACIONES A REALIZAR	- ¿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?
NIVEL	BÁSICO

REGISTRO DE INCIDENCIAS	
SISTEMA DE TRATAMIENTO	TODOS
COMPROBACIONES A REALIZAR	- ¿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?
NIVEL	BÁSICO
SISTEMA DE TRATAMIENTO	AUTOMATIZADOS
COMPROBACIONES A REALIZAR	- ¿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?
NIVEL	MEDIO

CONTROL DE ACCESO	
SISTEMA DE TRATAMIENTO	TODOS
COMPROBACIONES A REALIZAR	- ¿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 o recursos distintos de los autorizados? - ¿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?
NIVEL	BÁSICO
SISTEMA DE TRATAMIENTO	AUTOMATIZADO
COMPROBACIONES A REALIZAR	- ¿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?
NIVEL	MEDIO
SISTEMA DE TRATAMIENTO	NO AUTOMATIZADO
COMPROBACIONES A REALIZAR	- ¿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?
NIVEL	ALTO

GESTIÓN DE SOPORTES Y DOCUMENTOS	
SISTEMA DE TRATAMIENTO	TODOS
COMPROBACIONES A REALIZAR	- ¿Está identificado el tipo de información contenido 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?
NIVEL	BÁSICO

GESTIÓN DE SOPORTES Y DOCUMENTOS	
SISTEMA DE TRATAMIENTO	TODOS
COMPROBACIONES A REALIZAR	- ¿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 con su finalidad?

Continúa en página siguiente >>

<< Viene de página anterior

GESTIÓN DE SOPORTES Y DOCUMENTOS	
NIVEL	BÁSICO
SISTEMA DE TRATAMIENTO	TODOS
COMPROBACIONES A REALIZAR	- ¿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?
NIVEL	MEDIO
SISTEMA DE TRATAMIENTO	AUTOMATIZADO
COMPROBACIONES A REALIZAR	- ¿Se utilizan sistemas de etiquetado que permitan la identificación de su contenido a las personas autorizadas y dificulten su identificación al resto? - ¿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?
NIVEL	ALTO

Continúa en página siguiente >>

<< Viene de página anterior

GESTIÓN DE SOPORTES Y DOCUMENTOS	
SISTEMA DE TRATAMIENTO	NO AUTOMATIZADO
COMPROBACIONES A REALIZAR	- ¿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?
NIVEL	ALTO

IDENTIFICACIÓN Y AUTENTICIDAD	
SISTEMA DE TRATAMIENTO	AUTOMATIZADO
COMPROBACIONES A REALIZAR	- ¿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?
NIVEL	BÁSICO

INDETIFICACIÓN Y AUTENTICIDAD	
Sistema de tratamiento	AUTOMATIZADO
Comprobaciones a realizar	- ¿Se limita el intento reiterado de acceso no autorizado al sistema? - ¿Se anotan estos intentos en el registro de incidencias?
Nivel	MEDIO

COPIAS DE RESPALDO Y RECUPERACIÓN	
SISTEMA DE TRATAMIENTO	AUTOMATIZADO
COMPROBACIONES A REALIZAR	- ¿El responsable del fichero ha definido los procedimientos de realización de copias de respaldo y recuperación de los datos? ¿Es adecuada esta definición?
COMPROBACIONES A REALIZAR	¿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?
NIVEL	BÁSICO

COPIAS DE RESPALDO Y RECUPERACIÓN	
SISTEMA DE TRATAMIENTO	AUTOMATIZADO
COMPROBACIONES A REALIZAR	- 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 periodo? - ¿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?
NIVEL	BÁSICO
SISTEMA DE TRATAMIENTO	AUTOMATIZADO
COMPROBACIONES A REALIZAR	- ¿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?
NIVEL	ALTO

REGISTRO DE ACCESOS	
SISTEMA DE TRATAMIENTO	AUTOMATIZADO
COMPROBACIONES A REALIZAR	- ¿Existe el registro de accesos? En caso negativo ¿concurren en el responsable alguna de las circunstancias que le eximen de este requisito? ¿Se ha hecho constar en el Documento de Seguridad? - ¿Se está recogiendo en este registro la información mínima exigida en el Reglamento? - ¿Los mecanismos que permiten el registro de estos accesos están directamente bajo control del responsable de seguridad? - ¿Existe la posibilidad de desactivar estos mecanismos? - ¿Se conservan los datos registrados por un periodomínimo de dos años? - ¿Revisa el responsable de seguridad periódicamente la información registrada? - ¿Realiza el responsable de seguridad un informe, al menos mensualmente, con el resultado de las revisiones realizadas y los problemas detectados?
NIVEL	ALTO
SISTEMA DE TRATAMIENTO	NO AUTOMATIZADO
COMPROBACIONES A REALIZAR	- ¿El acceso a la documentación se realiza exclusivamente por personal autorizado? - ¿Existen mecanismos para identificar los accesos realizados cuando los documentos son utilizados por múltiples usuarios? - ¿Se ha establecido un procedimiento para registrar el acceso de personas no incluida en el caso anterior? ¿Es adecuado?
NIVEL	ALTO

TELECOMUNICACIONES	
SISTEMA DE TRATAMIENTO	AUTOMATIZADO
COMPROBACIONES A REALIZAR	- ¿La transmisión de datos a través de redes se realiza de forma cifrada (o por cualquier otro mecanismos que garantice que la información no sea inteligible ni manipulada por terceros)? ¿Este mecanismo de cifrado es eficaz?
NIVEL	ALTO

AUDITORÍA	
SISTEMA DE TRATAMIENTO	TODOS
COMPROBACIONES A REALIZAR	- ¿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 auditorias anteriores? ¿Han sido eficaces y han corregido las deficiencias encontradas?
NIVEL	MEDIO

CRITERIOS DE ARCHIVO	
SISTEMA DE TRATAMIENTO	NO AUTOMATIZADO
COMPROBACIONES A REALIZAR	- ¿Existe la legislación específica con criterios para el archivo de soportes o documentos?¿Garantizan estos criterios la conservación de documentos, la localización y consulta de la información? ¿Posibilitan el ejercicio de los derechos de oposición, acceso, rectificación y cancelación? - En caso de no existir legislación específica ¿ha establecido el responsable del fichero los criterios y procedimientos de actuación para el archivo de documentos? ¿Es adecuado este procedimiento?
NIVEL	BÁSICO

DISPOSITIVOS DE ALMACENAMIENTO	
SISTEMA DE TRATAMIENTO	NO AUTOMATIZADO
COMPROBACIONES A REALIZAR	¿Los dispositivos de almacenamiento de documentos disponen de mecanismos que obstaculicen su apertura? Si sus características físicas no permiten adoptar esta medida ¿ha adoptado el responsable medidas que impidan el acceso de personas no autorizadas?
NIVEL	BÁSICO

CUSTODIA DE SOPORTES	
SISTEMA DE TRATAMIENTO	NO AUTOMATIZADO
COMPROBACIONES A REALIZAR	¿Se custodia correctamente la documentación cuando esta no se encuentra archivada en los dispositivos de almacenamiento por estar en revisión o tramitación? ¿Se impide en todo momento que sea accedida por persona no autorizada?
NIVEL	BÁSICO

4. Supuesto práctico. Auditoría de una clínica de cirugía estética

Esta auditoría se basa en un supuesto ficticio y concreto, y no debe ser tomada como modelo para evaluar el cumplimiento de ninguna clínica real. El objeto de dicho ejemplo práctico es difundir, ilustrar y poner de manifiesto aspectos de cumplimiento legal, así como un acercamiento a las metodologías de auditoría para arrojar un poco de transparencia y desmitificar su complejidad.

Recuerde

Una auditoría real siempre es única y diseñada específicamente para la organización que se audita.

Doña María Navarrete Luces dirige una clínica de cirugía estética denominada "Clínicas Navarrete Luces S. L." y hace dos años implantó la ley de protección de datos en su empresa, estableciendo las medidas de seguridad oportunas. La ley le exige que realice una auditoría cada dos años, ya que tiene ficheros de nivel alto al incluir en sus bases de datos el historial clínico de sus pacientes, por lo que decide contratar a un auditor externo para que verifique el cumplimiento de la Ley Orgánica de Protección de Datos.

Este auditor externo tendrá que tener al menos un conocimiento genérico de la empresa, de su ámbito de negocio, de los sistemas de información de que disponen, de su estructura administrativa, y de sus relaciones con otras empresas o instituciones.

El auditor deberá realizar un programa de trabajo en el que detallará las actividades o tareas a auditar, teniendo en cuenta los requisitos de revisión exigidos o impuestos por el reglamento con relación a la auditoría y por otro lado, el ámbito de negocio y sistemas de la empresa.

El auditor deberá solicitar a la empresa auditada toda la documentación necesaria para verificar el cumplimiento de la normativa vigente en materia de protección de datos, así como la realización de entrevistas con el personal e inspección visual del centro auditado para ver *in situ* si se aplican las medidas de seguridad reflejadas en el documento de seguridad.

Deberá realizar un análisis de toda la documentación e información que ha recabado para establecer los puntos débiles existentes en la empresa en materia de protección de datos, así como exponer las conclusiones a las que ha llegado y en su caso establecer las medidas correctoras ante un deficiente cumplimiento de la normativa vigente, como de las posibles recomendaciones para mejorar la seguridad de la empresa en protección de datos.

Por último, el auditor deberá realizar un informe donde se refleje todo lo mencionado anteriormente.

En este supuesto, el auditor externo "Auditoría LOPD Méndez Vila S.L.", después de haber analizado toda la documentación y de realizar la inspección visual de las instalaciones y funcionamiento de la empresa presenta el siguiente informe en el que se expone lo siguiente:

MODELO DE INFORME DE AUDITORÍA

En Málaga a 29 de Mayo de 2012

1. Entidad auditada.

Nombre	Clínica Navarrete Luces S. L
CIF	B-92305062
Domicilio Social	C/ Santa Clara Nº 4
Actividad	Cirugía estética
Responsable de Contacto	María Navarrete Luces
Centros de Trabajo: Clínicas Navarrete Luces S. L	

2. Auditor externo.

Nombre	Don Gonzalo Méndez Vila
NIF	25910730-V
Auditores que han participado: Carmen Paradas Navas y Rodrigo Vela Núñez.	

3. Objetivos de la auditoría.

El objeto del presente informe es la realización de una auditoría de los procedimientos e instrucciones vigentes en materia de seguridad de datos de carácter personal, de con-

Continúa en página siguiente >>

<< Viene de página anterior

formidad con lo establecido en los artículos 96 y 100 del Real Decreto 1720/2007, de 21 de diciembre, reglamento de desarrollo de la LOPD. Dicha auditoría verificará, respecto de los ficheros incluidos en este documento, el grado de cumplimiento de las medidas de seguridad del nivel correspondiente establecidas en el citado reglamento.

4. Ficheros y tratamientos auditados.

Nombre fichero o tratamiento	Tipo de fichero (manual, automatizado o mixto)	Código de inscripción	Nivel de seguridad	Descripción
Pacientes	Mixto	2070052613	Alto	Gestión de los datos de los pacientes y de su historia clínica y de las tareas administrativas derivadas de la prestación asistencial.

5. Centro de trabajo auditado.

Nombre	Clínicas Navarrete Luces S. L
Dirección	C/ Santa Clara Nº 4
Actividad del centro	Cirugía Estética

Continúa en página siguiente >>

<< Viene de página anterior

6. 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 señalada.

7. Entrega del informe.

Se entregará ejemplar de este informe a:

Nombre y apellidos	Cargo o Departamento
María Navarrete Luces	Directora. (Departamento de dirección)
Mario Dávila Barquero	Jefe de cirugía.
Luisa Galindo Robles	Médico titular.

8. 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 se realiza la siguiente valoración:

Continúa en página siguiente >>

<< Viene de página anterior

Fichero o tratamiento	Nivel asignado por el responsable del fichero o tratamiento	Nivel que corresponde según el auditor
Fichero personal	Nivel básico	Nivel básico
Fichero pacientes	Nivel alto	Nivel alto
Fichero videovigilancia	Nivel básico	Nivel básico
Comentarios: los niveles están establecidos correctamente. Del fichero de personal y de videovigilancia no se debe realizar auditoría, porque son de nivel básico, por lo que la auditoría se centra en el fichero de pacientes.		

9. Resultados de la auditoría.

FICHEROS AUTOMATIZADOS		
NIVEL	**MEDIDA**	**CUMPLIMIENTO**
Obligaciones comunes a todos los niveles	Aplicación de niveles de seguridad (artículo 81)	SATISFACTORIO

Continúa en página siguiente >>

Continúa en página siguiente >>

<< Viene de página anterior

<< Viene de página anterior

FICHEROS AUTOMATIZADOS		
NIVEL	**MEDIDA**	**CUMPLIMIENTO**
Obligaciones comunes a todos los niveles	Acceso a datos a través de redes de comunicaciones (artículo 85)	Cumplimiento normal, aunque con recomendación.
Obligaciones comunes a todos los niveles	Régimen de trabajo fuera de los locales de la ubicación del fichero (artículo 86)	SATISFACTORIO
Obligaciones comunes a todos los niveles	Ficheros temporales (artículo 87)	SATISFACTORIO
Obligaciones comunes a todos los niveles	Documento de seguridad (artículo 88)	SATISFACTORIO
Básico	Funciones y obligaciones del personal (artículo 89)	Cumplimiento normal aunque con recomendaciones.
Básico	Registro de incidencias (artículo 90)	SATISFACTORIO
Básico	Control de acceso (artículo 91)	SATISFACTORIO
Básico	Gestión de soportes y documentos (artículo 92)	SATISFACTORIO

Continúa en página siguiente >>

Continúa en página siguiente >>

<< Viene de página anterior

FICHEROS AUTOMATIZADOS		
NIVEL	**MEDIDA**	**CUMPLIMIENTO**
Básico	Identificación y autenticación (artículo 93)	SATISFACTORIO
Básico	Copias de respaldo y recuperación (artículo 94)	SATISFACTORIO
Medio	Responsable de seguridad (artículo 95)	SATISFACTORIO
Medio	Auditoría bienal (artículo 96)	SATISFACTORIO
Medio	Gestión de soportes y documentos (características adicionales ficheros de nivel medio) (artículo 97)	SATISFACTORIO
Medio	Identificación y autenticación (características adicionales ficheros de nivel medio) (artículo 98)	CUMPLIMIENTO DEFICIENTE. (Medida correctora)

Continúa en página siguiente >>

Continúa en página siguiente >>

<< Viene de página anterior

<< Viene de página anterior

FICHEROS AUTOMATIZADOS		
NIVEL	**MEDIDA**	**CUMPLIMIENTO**
Medio	Control de acceso físico (artículo 99)	SATISFACTORIO
Medio	Registro de incidencias (características adicionales ficheros de nivel medio) (artículo 100)	SATISFACTORIO
Alto	Gestión y distribución de soportes (características adicionales ficheros de nivel alto) (artículo 101)	SATISFACTORIO
Alto	Copias de respaldo y recuperación (características adicionales ficheros de nivel alto) (artículo 102)	SATISFACTORIO
Alto	Registro de accesos (artículo 103)	SATISFACTORIO
Alto	Cifrado de datos en telecomunicaciones (artículo 104)	SATISFACTORIO

Continúa en página siguiente >>

<< Viene de página anterior

FICHEROS NO AUTOMATIZADOS (PAPEL)		
NIVEL	**MEDIDA**	**CUMPLIMIENTO**
Básico	Obligaciones comunes (se cumplimentarán las que correspondan en el apartado de ficheros automatizados) (artículo 105)	SATISFACTORIO
Básico	Criterios de archivo (artículo 106)	SATISFACTORIO
Básico	Dispositivos de almacenamiento (artículo 107)	SATISFACTORIO
Básico	Custodia de los soportes (artículo 108)	SATISFACTORIO
Medio	Responsable de seguridad (artículo 109)	SATISFACTORIO
Medio	Auditoría bienal (artículo 110)	SATISFACTORIO
Alto	Almacenamiento de la información (artículo 111)	SATISFACTORIO
Alto	Copia o reproducción (artículo 112)	SATISFACTORIO
Alto	Acceso a la documentación (artículo 113)	SATISFACTORIO
Alto	Traslado de documentación (artículo 114)	SATISFACTORIO

Continúa en página siguiente >>

<< Viene de página anterior

OTRAS MEDIDAS A ADOPTAR	CUMPLIMIENTO SI/NO
¿Se solicita el consentimiento del titular de los datos para la cesión de los mismos a terceros?	SI
¿Se regula mediante contrato la relación entre el responsable del fichero y el encargado del tratamiento?	SI
¿La empresa pone a disposición de los usuarios los medios necesarios para poder ejercitar sus derechos? (acceso, rectificación, cancelación y oposición)	SI
¿Se informa en la recogida de los datos a sus titulares de la finalidad y uso de los mismos? (a través de formularios, e-mail, por teléfono).	SI
¿Se adoptan las medidas de seguridad para el control de las cámaras de videovigilancia que captan imágenes? (Dcho. información al titular, inscripción de fichero a la AGPD, y conservación de las imágenes, etc.)	SI

Continúa en página siguiente >>

<< Viene de página anterior

10. Medidas correctoras.

Fichero	Art.	Nivel de medidas	Deficiencia	Medida correctora
Fichero pacientes (nivel alto)	Arts. 93 y 98 del Reglamento 1720/2007, de 21 de diciembre.	Medidas de nivel medio	Identificación y autenticación. No se ha procedido al cambio de las contraseñas de los usuarios en los dos años desde que se realizó la protección de datos.	El responsable de seguridad debe cambiar las contraseñas de los usuarios o informarles para que la cambien como mínimo cada año. El tiempo que transcurra desde que se atribuye una contraseña a los usuarios hasta que la cambian no puede superar el año.

11. Recomendaciones.

Fichero	Nivel	Medidas	Recomendación
Fichero pacientes	Alto	Funciones y obligaciones del personal	Revisión del conocimiento práctico de las normas de seguridad por parte del personal. Establecer normas internas como compromisos de confidencialidad, formar al trabajador por medio de charlas, recordatorios, folletos, etc.
		Transmisiones: Telecomunicaciones	Debe incluirse una política sobre el acceso a Internet.

Continúa en página siguiente >>

<< Viene de página anterior

Conclusiones específicas:

1. **Documento de seguridad.** El documento de seguridad ha sido revisado, por lo que se puede acreditar que se encuentra totalmente al día, mostrando en todo momento la realidad de la empresa.

   Por otro lado se ha dotado a la empresa de las herramientas técnicas para que pueda ser actualizado periódicamente por personal con formación acreditada en la materia.

   El sistema informático y de ficheros revisados mantienen las medidas de seguridad que en principio pudieran ser suficientes y lógicas para preservar la información vital de la empresa.

2. **Ficheros inscritos.** La empresa tiene tres ficheros que acreditan el tipo de datos manejados por la empresa. El nivel de seguridad de cada uno de ellos ha sido revisado para adaptarlo tanto a la legislación vigente como a la efectiva realidad de la empresa.

3. **Análisis de los sistemas de información de la empresa.** Este apartado de la revisión es correcto y está bien documentado.

4. **Identificación, autentificación y controles de acceso.** Los sistemas de identificación y autentificación cumplen de forma deficiente los mandatos del R. D. 1720/2007, de 21 de diciembre. En las medidas de seguridad de los ficheros automatizados de nivel básico existe una relación de usuarios con acceso autorizado. Esta se mantiene actualizada y los procedimientos de identificación y autenticación para dicho acceso garantizan la identificación del usuario de una forma correcta, ya que existe un procedimiento de asignación de contraseñas que garantiza la confidencialidad, pero se encuentran algunas deficiencias ya que no se produce el cambio de estas de forma anual.

   Respecto a las medidas de seguridad en los ficheros automatizados de nivel medio se limita el intento reiterado de acceso no autorizado al sistema y se anotan en el registro de incidencias.

Continúa en página siguiente >>

<< Viene de página anterior

Con respecto al control de acceso las medidas adoptadas son las correctas. Se ha restringido el acceso a los locales donde se encuentran ubicados los sistemas de información que se realizan exclusivamente por el personal autorizado en el documento de seguridad.

En cuanto a las medidas adoptadas en los ficheros no automatizados de nivel alto, los archivadores u otros elementos de almacenamiento están en áreas de acceso restringido, dotados de sistemas de apertura mediante llave u otro dispositivo, y están cerradas mientras no sea preciso acceder a los documentos incluidos en el fichero.

5. **Funciones del responsable de seguridad.** Se han establecido funciones específicas y detalladas para el responsable de seguridad en el documento de seguridad, además se ha especificado las funciones propias para los ficheros de nivel alto y se ha comprobado el cumplimiento de las tareas encomendadas al responsable de seguridad.
6. **Soporte de datos.** El soporte de los datos es correcto y adecuado a tenor del análisis efectuado.

   Medidas de seguridad en ficheros automatizados y no automatizados, en el nivel básico.

   Está identificado el tipo de información contenida en el soporte o documento. Existe y se mantiene un inventario de soportes, se almacenan en lugar de acceso restringido, y acceden solo personas autorizadas en el documento de seguridad. Si se trasladasen documentos o soportes existen medidas para evitar la sustracción o pérdida. También hay un inventario donde se dan de baja los documentos desechados, y un sistema de etiquetado que permite identificar el contenido de soportes con datos de carácter personal, considerados especialmente sensibles por la organización y que dificultan su identificación al resto de personas que no están autorizadas para su identificación.

Continúa en página siguiente >>

<< Viene de página anterior

Medidas de seguridad en ficheros automatizados y no automatizados, en el nivel medio.

Existe un registro de entrada de soportes y un registro de salida y otro registro de las personas encargadas de la recepción y entrega de soportes que están autorizadas. En el documento de seguridad se han anotado todas las entradas y salidas de soportes.

Medidas de seguridad en ficheros automatizados y no automatizados, en el nivel alto. Se utilizan sistemas de etiquetado que son adecuados y cumplen su finalidad.

La distribución de soportes se realiza de forma cifrada, garantizando un transporte seguro, se cifran los datos en los dispositivos portátiles cuando salen fuera de las instalaciones del responsable del fichero y se han adoptado medidas para minimizar los riesgos derivados del tratamiento en entornos desprotegidos. El traslado físico de la documentación contenida en el fichero, la realización de copias, o la reproducción de documentos se realiza por personas autorizadas para ello en el documento de seguridad y se destruyen las copias o reproducción desechables de forma que no se puede acceder a la información contenida en las mismas.

7. **Copias de seguridad.** La metodología empleada para la realización de las copias de seguridad es adecuada. Las copias se encuentran cifradas para evitar que puedan ser recuperadas por personal no autorizado. Se conserva una copia de respaldo y de los procedimientos de recuperación de datos en lugar diferente al de los equipos que los tratan, y este lugar cumple las medidas de seguridad exigidas en el reglamento.
8. **Registro de incidencias.** Toda documentación sobre el registro y control de incidencias es adecuada a la protección de datos. Se dispone de los modelos de notificación para poder registrar todo evento que haga peligrar la integridad de la base de datos.

Continúa en página siguiente >>

<< Viene de página anterior

9. **Control de acceso físico a la sala del servidor.** El acceso a la sala está restringido al personal autorizado por lo que, en principio, parece que la seguridad física de los servidores es la correcta.
10. **Registro de accesos.** La monitorización de los accesos que tiene activada es suficiente para el cumplimiento de la ley.

    En la parte automatizada del fichero de nivel alto existe el registro de acceso y se ha hecho constar en el documento de seguridad. En este registro se recoge la información mínima exigida en el reglamento. Los mecanismos de registro de acceso están bajo el control del responsable de seguridad, también existe posibilidad de desactivar estos mecanismos. Se conservan los datos registrados por un periodo mínimo de dos años, y el responsable de seguridad revisa periódicamente la información. Se realiza una vez al mes un informe con el resultado de las revisiones efectuadas y los problemas detectados.

    En la parte no automatizada de nivel de seguridad alto, el acceso a la documentación se realiza por el personal autorizado, también existen mecanismos para identificar los accesos efectuados cuando los documentos son utilizados por múltiples usuarios. El procedimiento para registrar el acceso de personas no incluidas en el caso anterior es adecuado.
11. **Pruebas con datos reales.** Se ha comprobado que la empresa no realiza pruebas con datos reales. De todas formas se debe considerar que si en un futuro se hicieran pruebas con datos reales se adoptarán las medidas oportunas para su protección.
12. **Transmisiones.** Uno de los puntos más delicados por su potencial peligrosidad es la de los sistemas de transmisión o de telecomunicaciones.

    En este apartado deben tenerse en cuenta tanto las redes locales como las conexiones externas que puedan afectar a la integridad del fichero. Se ha podido comprobar que los sistemas utilizados para la transmisión de datos (FTP, e-mail,

Continúa en página siguiente >>

<< Viene de página anterior

etc.) cumplen las medidas de seguridad oportunas para la protección de los datos pero se pueden adoptar medidas adicionales que se han reflejado anteriormente.

13. **Cumplimiento de las medidas jurídicas.** Queda acreditado que se llevan a cabo las cláusulas legales, contratos, informes, avisos legales, etc. requeridos en esta materia con los diferentes pacientes, proveedores y trabajadores y que se ajustan a los establecido por la Ley Orgánica de Protección de Datos 15/1999 de 13 diciembre, no incurriendo en cesión no autorizada de información de carácter personal.

    Además existe un cumplimento y respeto a los derechos de las personas (acceso, rectificación, cancelación y oposición).

Conclusiones finales:

Se ha realizado una auditoría externa de los sistemas de información e instalaciones de tratamiento y almacenamiento de datos de carácter personal de la entidad "Clínicas Navarrete Luces S.L." 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 la valoración efectuada, se puede establecer que los sistemas de información e instalaciones de tratamiento y almacenamiento de la entidad "Clínicas Navarrete Luces" 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 incluyen las correspondientes medidas correctoras o complementarias.

Continúa en página siguiente >>

<< Viene de página anterior

Por último, se recuerda a la entidad "Clínica Navarrete Luces" 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.

Auditor: Don Gonzalo Méndez Vila

FDO:

Director del Departamento Jurídico de Auditoría LOPD Méndez Vila S. L.