



**Informe de AUDITORIA (Art. 96 R.D. 1720/2007) de
PROTECCIÓN DE DATOS
DE CARÁCTER PERSONAL PARA
COVIAR**

Auditado por:

:

Juan Carlos Serrano
Auditor de Protección de Datos
Lead auditor ISO 27001, ISO 20000, ISO 9001
BUREAU VERITAS CERTIFICATION

INDICE

INDICE	2
INTRODUCCION.....	3
FASES EN LA REALIZACIÓN DE LA AUDITORÍA	4
PLAN DE TRABAJO	5
1. REVISIÓN DEL DOCUMENTO DE SEGURIDAD	6
2. ANÁLISIS DE LOS SISTEMAS DE INFORMACIÓN DE LA EMPRESA.....	9
3. IDENTIFICACIÓN, AUTENTICACIÓN Y CONTROLES DE ACCESO	10
4. FUNCIONES DEL RESPONSABLE DE SEGURIDAD	11
5. SOPORTES DE DATOS	12
6. PRUEBAS CON DATOS REALES	14
7. COPIAS DE SEGURIDAD	15
8. REGISTRO DE INCIDENCIAS.....	16
9. CONTROL DE ACCESO FÍSICO A LA SALA DE SERVIDORES	17
10. REGISTRO DE ACCESOS	18
11. TRANSMISIONES.....	19
RECOMENDACIONES.....	20
CONCLUSIÓN FINAL	24

INTRODUCCION

El Reglamento de Medidas de Seguridad de los ficheros de carácter personal establece, cuando existen ficheros de nivel medio o alto:

“Artículo 96. Auditoría.

1.- A partir del nivel medio, los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa, que verifique el cumplimiento del presente título.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el apartado anterior.

Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.

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 Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.”

FASES EN LA REALIZACIÓN DE LA AUDITORÍA

La auditoría obligada por el Reglamento del R.D. 1720/2007 se ha realizado durante el día 23 de julio de 2007 y ha constado de las siguientes fases:

- Conocimiento genérico de la empresa, su ámbito de negocio, los sistemas de información de que disponen, su estructura administrativa, sus relaciones con organismos oficiales, asociaciones, instituciones y otras empresas.
- Elaboración de un programa de trabajo en el que se detallan las actividades o tareas a auditar, teniendo para ello en cuenta, por un lado, los requisitos de revisión impuestos por el Reglamento en relación con la auditoría, y por el otro, el ámbito de negocio y sistemas de la empresa.
- Realización del trabajo de campo, esto es, la revisión práctica de las actividades incluidas en el plan de trabajo.
- Análisis de los puntos débiles y obtención de conclusiones y recomendaciones.
- Elaboración del informe.

PLAN DE TRABAJO

A partir del hecho de que la auditoría debe verificar el cumplimiento del Reglamento, el Plan de Trabajo deberá incluir específicamente la comprobación de todos los artículos de aquel que sean de aplicación a tenor del tipo de ficheros de que disponga la empresa (medio, alto).

Para la realización organizada de esta auditoría se ha preparado una tabla de control o de “checklist”. Esta tabla esta dividida en once áreas de manera que se puedan identificar aquellos ítems a auditar de una manera lógica. De esta manera las áreas serán las siguientes:

- 1 Revisión del documento de seguridad
- 2 Análisis de los sistemas de información de la empresa.
- 3 Identificación, autenticación y controles de acceso
- 4 Funciones del responsable de seguridad
- 5 Soportes de datos
- 6 Pruebas con datos reales
- 7 Copias de seguridad
- 8 Registro de incidencias
- 9 Control de acceso físico a la sala
- 10 Registro de accesos
- 11 Transmisiones

A continuación se incluye la tabla “checklist” de los puntos auditados de las áreas anteriormente mencionadas, así como los resultados obtenidos para cada apartado.

1. REVISIÓN DEL DOCUMENTO DE SEGURIDAD

El objetivo de la revisión del Documento de Seguridad, del que toda empresa con ficheros de datos personales debe disponer es doble. Por un lado, el auditor analiza que su contenido cumple con los requisitos establecidos en el Reglamento para el mismo. En segundo lugar, permite al auditor identificar los procedimientos y controles de seguridad definidos en la instalación, para posteriormente verificar su cumplimiento.

Además de la revisión del contenido del Documento de Seguridad, se han auditado aquellos procedimientos que afectan tanto a su desarrollo, mantenimiento y actualización.

En el caso de esta auditoría, se comprueba la existencia de un único documento de seguridad y procedimientos para todos los ficheros. La denominación de este documento de seguridad es "R70. Documento de Seguridad" y está actualizado el 2 de junio de 2008. Esto obliga a suponer que las medidas de seguridad deben ser comunes a todos los ficheros, aunque posteriormente se individualizan los registros de incidencias, usuarios, etc.

A continuación se exponen todos estos aspectos auditados.

1.1 Comprobación del contenido y alcance del Documento de seguridad:

Punto auditado	Conclusión
Medidas, controles, procedimientos, normas y estándares de seguridad.	Satisfactorio. El Documento de Seguridad incluye todos los apartados exigidos por el Reglamento.
Relación de las funciones y obligaciones del personal.	Satisfactorio. Se incluyen las figuras, funciones y responsabilidades que parecen las lógicas para la coordinación de la seguridad y gestión de los ficheros
Estructura de los ficheros con datos personales y descripción de los sistemas de información que los tratan	Satisfactorio. Se presenta como Anexo al Documento de Seguridad
Procedimientos de notificación y gestión de incidencias.	Satisfactorio. Este procedimiento está incluido dentro del Sistema de Gestión de la Calidad "P02. Gestión de la mejora" y utiliza el formato de comunicación de incidencias "R46. Formato de incidencias"
Procedimientos de realización de copias de seguridad y de recuperación de datos.	Satisfactorio. Sistema RAID1 y copias de seguridad en cintas de Backup a diario.
Relación de personal autorizado a conceder, alterar o anular el acceso sobre datos y recursos.	Satisfactorio. Incluido en el Documento de Seguridad.
Identificación del responsable o responsables de seguridad.	Satisfactorio. Incluido en el Documento de Seguridad.

Relación de controles periódicos a realizar para verificar el cumplimiento del documento.	Satisfactorio
Medidas a adoptar cuando un soporte vaya a ser desechado o reutilizado	Satisfactorio. Se recomienda incluir dentro del Procedimiento de gestión de soportes las buenas prácticas recogidas en la ISO 27002:2007 sobre eliminación de soportes.
Relación de personal autorizado a acceder a los locales donde se encuentren ubicados los sistemas que tratan datos personales.	Satisfactorio. El personal que accede es todo de plantilla
Relación de personal autorizado a acceder a los soportes de datos.	Satisfactorio. Incluido en los Anexos.
Período máximo de vida de las contraseñas.	Satisfactorio. Se recomienda actualizar a las buenas prácticas de vida y uso de contraseñas de la ISO 27002:2007

1.2 Revisión de las políticas relacionadas con el documento de seguridad:

Difusión del documento entre empleados y colaboradores externos	Satisfactorio. Última realizada el 2/6/2008. A todo el personal y por intranet. Personal externo no accede al documento.
Procedimientos para la revisión y actualización del documento.	Satisfactorio. Se encuentran incluido dentro del Sistema de Gestión de la Calidad y LOPD
Procedimientos de comunicación a empleados y colaboradores externos de las actualizaciones del documento.	Satisfactorio. Procedimiento dentro del sistema de Gestión de la Calidad. "4.6. Requisitos de documentación"

1.3 Revisión del conocimiento práctico de las normas de seguridad por parte del personal.

Realización de entrevistas a una muestra de usuarios que incluya todos los estamentos y funciones	<p>El resultado de las diferentes entrevistas deja de manifiesto las buenas prácticas descritas en el Documento de Seguridad. Existen normas internas como compromisos de confidencialidad.</p> <p>Es de interés, una formación por medio de charlas, recordatorios, folletos, etc.</p>
---	---

1.4 Revisión del grado de actualización del documento.

Este punto se ha cumplimentado al final de la auditoría, una vez ha sido analizada la adecuación y efectividad de los controles en la práctica existentes y contrastada su aplicación con los controles incluidos en el documento de seguridad.

El documento de seguridad es un documento vivo y que evoluciona a lo largo del tiempo, tanto en los procedimientos y políticas como en los registros que



23 de julio de 2007

acompañan al documento. Por esto se ha realizado una comprobación de la una evolución en los contenidos del documento de seguridad.

La conclusión es que el Documento de Seguridad y procedimientos para todos los ficheros registrados es revisada, encontrándose el documento de seguridad en su versión del 2 de junio de 2008.

2. ANÁLISIS DE LOS SISTEMAS DE INFORMACIÓN DE LA EMPRESA.

El objetivo de este apartado es determinar 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 sólo 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 tienen un alto grado de descentralización y la aplicación de las medidas supone la realización de una inversión.

En segundo lugar, este análisis de los sistemas de información permite al auditor centrar la revisión de algunos de los controles exclusivamente en aquellos sistemas y ficheros para los que, en función de su nivel, el Reglamento exige su aplicación.

Para la realización de 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, probablemente con ocasión de la elaboración del documento de seguridad.

Determinar los campos (de los ficheros) que reflejan datos de nivel medio o alto.	Cumplimentado y satisfactorio.
Detectar todos los ficheros que incluyen alguno de esos campos y además algún otro que permita identificar a la persona.	Satisfactorio
Detectar todos los ficheros que incluyen algún dato identificativo de la persona.	Satisfactorio
Con los ficheros así clasificados en niveles, verificar que la estructura de esos ficheros está incluida en el Documento de Seguridad.	Satisfactorio

3. 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.

El resultado auditado de esta es el siguiente:

Comprobar que existe una relación de usuarios autorizados a acceder a los sistemas y que incluye los tipos de acceso permitidos	Satisfactorio. La relación de usuarios se encuentra en la ficha del fichero.
Verificar que en la práctica los usuarios dados de alta en los sistemas y los tipos de accesos a ellos concedidos son coherentes con los establecidos en el Documento de Seguridad.	Por muestreo los accesos parecen coherentes.
Comprobar que los derechos de acceso concedidos a los usuarios son los necesarios y suficientes para el ejercicio de las funciones que tienen encomendadas, las cuales a su vez se encuentran –o deben estar- documentadas en el Documento de Seguridad.	Satisfactorio. Los derechos de acceso son suficientes y correctos y están documentados en el Documento de Seguridad.
Verificar que no hay dadas de alta en el sistema cuentas de usuario genéricas, es decir, utilizadas por más de una persona, no permitiendo por tanto la identificación de la persona física que las ha utilizado.	No existen cuentas genéricas
Comprobar que en la práctica las personas que tienen atribuciones y privilegios dentro del sistema para conceder derechos de acceso son las autorizadas e incluidas en el Documento de Seguridad.	Las personas que autorizan son los que tienen esa funcionalidad. (Javier Povedano)
Verificar que el sistema de autenticación de usuarios guarda las contraseñas encriptadas.	Satisfactorio. Windows 2003 Server
Comprobar que en el sistema están habilitadas para todas las cuentas de usuario las opciones que permiten establecer un número máximo de intentos de conexión y un período máximo de vigencia para la contraseña, coincidente con el establecido en el Documento de Seguridad	Está habilitadas
Analizar los procedimientos de asignación y distribución de contraseñas.	Los procedimientos son coherentes

4. FUNCIONES DEL RESPONSABLE DE SEGURIDAD

El Reglamento obliga a nombrar uno o más responsables de seguridad por la mera existencia de ficheros de nivel medio o 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.

El resultado es el que a continuación se detalla:

Estudiar y analizar las funciones encomendadas a cada uno de los responsables de seguridad	Existen funciones específicas y detalladas en el Documento de Seguridad
Determinar si entre ellas se encuentran aquellas especificadas en el Reglamento para los ficheros de Nivel Alto	Satisfactorio
Revisar los procedimientos asociados con las funciones encomendadas	Satisfactorio
Analizar el grado de cumplimiento de las funciones encomendadas	Satisfactorio
Estudiar y analizar los controles definidos para su realización por parte de los responsables de seguridad y comprobar su operatividad y grado de adecuación	Satisfactorio aunque puede ser necesaria una revisión de las funciones del responsable de seguridad de manera que se defina en el tiempo.

5. SOPORTES DE DATOS

En relación con los soportes de datos, el auditor ha revisado varios aspectos relativos a:

- Identificación de los soportes
- Inventario de soportes
- Registro de entrada/salida de soportes

Verificar que existe un inventario de los soportes existentes(5.1)	Existe inventario de soportes. Son 5 cintas
Comprobar que dicho inventario incluye las copias de seguridad.	Son las copias de seguridad en exclusiva
Determinar si las copias de seguridad, o cualquier otro soporte, se almacenan fuera de la instalación	Se realizan copias `por medio de VPN en Bilbao.
Analizar los procedimientos de actualización de dicho inventario.	Están definidos en el Documento de Seguridad
Analizar los procedimientos de etiquetado e identificación del contenido de los soportes.	Cumplido.
Verificar los accesos a los posibles almacenamientos de soportes y comprobar que exclusivamente pueden acceder a ellos las personas autorizadas en el Documento de Seguridad	Cumple ya que sólo accede el personal de sistemas.
Analizar los procedimientos en relación con la salida de soportes fuera de su almacenamiento habitual.	No salen soportes
Evaluar los estándares de distribución y envío de estos soportes.	Positivo. El funcionamiento es seguro
Obtener una relación de los ficheros que se envían fuera de la empresa, en la que se especifique el tipo de soporte, la forma de envío, el estamento que realiza el envío y el destinatario. Comprobar que todos los soportes incluidos en esa relación se encuentran también en el inventario de soportes del punto 5.1.	No se envían ficheros
Obtener una copia del Registro de Entrada y Salida de Soportes y comprobar que en él se incluyen los soportes del punto anterior y los desplazamientos que realizan.	Satisfactorio
Verificar que el Registro de Entrada y Salida refleja la información requerida por el Reglamento	Cumple



Analizar los procedimientos de actualización del Registro de Entrada y Salida en relación con el movimiento de soportes.	Cumple
Analizar los controles para detectar la existencia de soportes recibidos/enviados que no se inscriben en el Registro de Entrada/Salida.	No aplica
Comprobar, en el caso de que el Inventario de Soportes y/o el Registro de Entrada/Salida estén informatizados, que se realizan copias de seguridad de ellos, al menos, una vez a la semana.	No aplica. No está informatizado
Cotejar la relación de soportes enviados fuera de la empresa y la relación de ficheros de nivel alto obtenida en el Apartado 2. Comprobación además del cifrado (nivel alto) si salen al exterior.	Cumple

6. PRUEBAS CON DATOS REALES

El auditor ha comprobado, en primer lugar, cual es la política de la empresa en cuanto a la realización de pruebas con datos reales, para a continuación analizar, en función de esa política, las normas y procedimientos definidos y verificar su cumplimiento.

En este caso no se realizan pruebas con datos reales y se han verificado los siguientes requisitos.

<p>Verificar que los controles y normas que están operativos para los ficheros en producción lo están también para los ficheros del entorno de pruebas.</p>	<p>No se realizan pruebas con datos reales</p>
<p>Analizar los procedimientos para el entorno de pruebas en relación con: Identificación y autenticación de usuarios, control de accesos, políticas de contraseña y número máximo de intentos de conexión, inventario de soportes, registro de E/S de soportes, copias de seguridad, ficheros de soporte enviados fuera de las instalaciones y transmisiones cifradas, registro de incidencias, registro de acceso...</p>	<p>No se realizan pruebas con datos reales</p>

7. COPIAS DE SEGURIDAD

Los procedimientos respecto a las copias de seguridad y restauración del sistema son el punto crítico en cualquier sistema informático.

Para este apartado el auditor ha comprobado los siguientes aspectos:

Analizar los procedimientos para la realización de las copias de seguridad.	Los procedimientos son válidos y adecuados.
Verificar que los procedimientos aseguran que, de todos los ficheros con datos de carácter personal, se realiza copia al menos una vez cada semana.	Satisfactorio. Se realizan a diario.
Comprobar que los procedimientos aseguran la realización de copias de todos aquellos ficheros que han experimentado algún cambio en su contenido.	Satisfactorio. Se realiza copia integra
Analizar los controles existentes para la detección de incidencias en la realización de las pruebas.	Satisfactorio
Evaluar los controles sobre el acceso físico a las copias de seguridad.	Solamente puede acceder personal autorizado
Verificar que sólo las personas con acceso autorizado en el documento de seguridad tienen acceso a los soportes que contienen las copias de seguridad.	Satisfactorio
Comprobar que las copias de seguridad de ficheros de nivel alto incluyen los ficheros cifrados si estas copias se transportan fuera de las instalaciones.	Satisfactorio
Verificar que las copias de seguridad de los ficheros de nivel alto se almacenan en lugar diferente al de los equipos que las procesan	Satisfactorio

8. REGISTRO DE INCIDENCIAS

El registro de incidencias es la parte del Documento de Seguridad que permitirá la realización de estudios e informes que permitan evolucionar la seguridad dentro del sistema informático de la organización. Una incidencia será todo aquel evento que ponga en peligro la integridad física y/o lógica del fichero.

Los aspectos auditados son:

Comprobar que está claramente especificado que tipos de sucesos se consideran incidencia de acuerdo con la definición que del término realiza el Reglamento.	Satisfactorio y perfectamente documentado. El documento es el "P02. Gestión de la mejora" y queda registrado en el documento "R46. Registro"
Comprobar que los usuarios conocen que tipo de situaciones deben reportar como incidencia.	Conocen las principales
Analizar los procedimientos para la notificación de incidencias, ver que están operativos y comprobar que son conocidos por todos los usuarios.	Los procedimientos son válidos.
Analizar los procedimientos para la resolución de incidencias y comprobar que están operativos.	Se ha rellenado 1 incidencia. Se ha realizado una buena gestión para su resolución
Evaluar si los procedimientos seguidos en la práctica se corresponden con aquellos definidos en el Documento de Seguridad.	Satisfactorio
Verificar que la información guardada en el Registro de Incidencias cumple los requisitos establecidos por el Reglamento	Satisfactorio. Puede completarse con datos sobre la restauración en el caso que fuera necesaria
Analizar los procedimientos de inscripción en el Registro de Incidencias.	Satisfactorio.
Analizar los controles de detección de incidencias no inscritas en el Registro.	Satisfactorio
Si el registro está informatizado, comprobar que se realiza copias de seguridad de él	No está informatizado. No aplica aunque se realiza copia integra

9. 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 (medidas lógicas), el acceso físico a la sala de servidores debe estar restringido exclusivamente a personal autorizado.

Durante la auditoría se ha realizado las siguientes verificaciones:

Comprobar la existencia, como parte del Documento de Seguridad, de una relación de usuarios con acceso autorizado a la sala (9.1)	No existe relación de usuarios personalizada pero solamente pueden acceder los autorizados
Verificar que la inclusión del personal en la relación anterior es coherente con las funciones que tienen encomendadas.	Satisfactorio
Comprobar que la relación es lógica (personal de limpieza, seguridad)	Satisfactorio. Solamente accede personal propio
Analizar las políticas de la instalación en relación con los accesos ocasionales a la sala.	Satisfactorio
Determinar que personas tienen llaves de acceso, tarjetas, etc. de acceso a la sala y cotejar con la relación del punto 9.1.	Satisfactorio

10. REGISTRO DE ACCESOS

El registro de acceso, tal como obliga el R.D.: 994/1999, debe contener aquella información que luego permita al responsable de seguridad con el apoyo de los administradores del sistema evaluar la integridad en el tiempo del fichero.

Así se han realizado las siguientes comprobaciones:

Verificar que la información incluida en el Registro de Accesos cumple los requisitos del Reglamento	Cumple gracias a utilidades de monitorización de los sistemas operativos.
Comprobar que están activados los parámetros de activación del Registro para todos los ficheros de Nivel Alto.	Satisfactorio. Son realizados por aplicación
Analizar los procedimientos de descarga a cinta o a otro soporte de este Registro de Accesos y el período de retención de este soporte.	Copia de seguridad
Analizar los procedimientos de realización de copias de seguridad del Registro de Accesos y el período de retención de las copias.	Copia de seguridad
Verificar la asignación de privilegios que permitan activar/desactivar el Registro de Accesos para uno o más ficheros.	No aplica. Aplicación cerrada
Comprobar que el Registro de Accesos se encuentra bajo el control directo del Responsable de Seguridad pertinente.	Satisfactorio

11. TRANSMISIONES

Uno de los puntos más delicados por su potencialidad peligrosidad de crear una incidencia al fichero y a la vez necesario en un sistema de información es el 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.

En este caso se ha auditado:

Analizar los sistemas utilizados para la transmisión de datos (FTP, Editran, E-mail...)	VPN con Bilbao. Y sólo es un fichero
Comprobar que todos los ficheros de nivel alto se cifran antes de su transmisión. Para ello, hacer uso de la relación de ficheros cedidos del apartado 5, y de la relación de ficheros clasificados por niveles que se realizó en el punto 2.4. -.	No procede
Analizar las normas y controles establecidos acerca de la transmisión por parte de usuarios de ficheros, cartas, e-mails, etc. con información de nivel Alto.	No procede

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. “*

En los puntos anteriores se han incluido los datos, hechos y observaciones en los que se basa el auditor para proponer medidas correctoras. A continuación se exponen para cada uno de los apartados que propuestas recomienda el auditor. Respecto a los datos hechos y observaciones han sido enumerados a lo largo de este documento.

1. Revisión del documento de seguridad

El documento de seguridad ha sido revisado y es apreciable el alto compromiso para avanzar la gestión del mismo.

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

Pasamos a realizar recomendaciones para cada uno de los puntos auditados:

1.1 Comprobación del contenido y alcance.

- Debe tener una mayor difusión entre los usuarios del fichero de forma que para cada empleado y usuario sea una herramienta más en su que hacer diario
- 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, periodos de contraseñas, etc.

1.2 Revisión de las políticas relacionadas con el Documento de seguridad

- El documento debe tener una mayor difusión entre los empleados y debe ser actualizado si redescubre una buena práctica mejor que la que se está realizando.
- El documento debe tener difusión entre los diferentes proveedores y colaboradores externos como Informática externa.

1.3 Conocimiento práctico entre los empleados

- Los empleados deben no sólo 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, atención telefónica, etc.

1.4 Revisión del documento

- El documento ha sido revisado y se recomienda su evolución continua. También se recomienda que se eviten los procedimientos que son técnicos y son responsabilidad de sistemas haciendo mención a ellos según sea necesario.

2. Análisis de los sistemas de información de la empresa.

Este apartado de la auditoría es correcto y está bien documentado.

3. Identificación, autenticación y controles de acceso

Puesto que es utilizado un Sistema Operativo Windows 2003 Server, debiera de nombrarse en el documento de seguridad ya que su utilización permite dar mayores garantías de cumplimiento de la materia de Protección de datos

Los controles de accesos a los sistemas son adecuados y están bajo la responsabilidad de personas con la formación suficiente. Además están implantadas medidas de control que permiten observar las actividades que desarrollan los diferentes usuarios.

4. Funciones del responsable de seguridad

El resultado de la auditoría de este apartado descubre oportunidades de mejora. De esta manera se recomienda lo siguiente:

- Elaborar un cuadro de controles en el tiempo del sistema y en la documentación que deberá revisar el responsable de seguridad
- Conservar los informes que elabore el responsable de seguridad para poder hacer evolucionar al sistema informático
- Definir en el tiempo las revisiones a realizar

5. Soportes de datos

Respecto al uso y tratamiento que de los soportes de datos, se obtienen las siguientes conclusiones y recomendaciones.

- Debe ser actualizado el procedimiento de salida de datos, de manera que recoja el funcionamiento habitual de las copias bajo una línea VPN.

6. Pruebas con datos reales

Al no realizarse pruebas con datos reales, no existe mayor problema en este apartado.

De todas formas se debe considerar que si en un futuro se hicieran pruebas con datos reales, las medidas de seguridad que se aplican a producción deben ser aplicadas a pruebas

Por otra parte, sería necesario documentar en este procedimiento como se cargarán los ficheros de prueba y detallar el algoritmo de separación de identidad.

7. Copias de seguridad

La metodología empleada para la realización de las copias de seguridad es adecuada.

Las copias es interesante que se encuentren cifradas para evitar que puedan ser recuperadas por personal no autorizado y en otros sistemas.

8. Registro de incidencias

Toda la documentación sobre el registro y control de las incidencias es adecuada a la Protección de Datos. También se dispone de unas claves que codifican cualquier incidencia. Se dispone de los modelos de notificación para poder registrar todo evento que haga peligrar la integridad de la base de datos.

Las recomendaciones que se proponen son las siguientes:

- Se sugiere una formación a los usuarios de los diferentes ficheros sobre la gestión y reconocimiento de una incidencia, recordatorios del cumplimiento de la LOPD, etc.

9. Control de acceso físico a la sala

El acceso a la sala está restringido al personal de autorizado por lo que en un principio parece que la seguridad física de los servidores es la correcta.

Tras el examen de los diferentes puntos de la L.O. 15/99 y R.D. 1720/2007 que afectan a este punto, no se realiza ninguna recomendación especial pero se recuerda que el tratamiento informático se encuentra, en líneas generales, al máximo de lo exigible por lo recursos que posee.

10. Registro de accesos

La monitorización de los accesos que se tiene activada en la actualidad es suficiente para el cumplimiento de la Ley.

Este auditor recomienda:

- Debe incluirse en el procedimiento de las copias de seguridad su periodo de conservación y retención en Bilbao

11. Transmisiones

La transmisión de datos en la red local está controlada mediante switches



23 de julio de 2007

- Debe incluirse una política sobre el acceso a Internet.

CONCLUSIÓN FINAL

En opinión del auditor, la evolución de la implantación realizada en esta materia en la que se funden aspectos tanto informáticos como jurídicos, se ha realizado de una manera acertada.

Debe evitarse la asociación que en el día a día hacemos de la palabra “dato” con sistemas informáticos y por derivación con la informática. En realidad estamos hablando de información sin importarnos el soporte ya sea mecanizado o no

En este punto debe leerse la definición que nos da la L.O. 15/99 y en este caso aplicar el Art. 3 “a) *Datos de carácter personal: cualquier **información** concerniente a personas físicas identificadas o identificables*”.

Parece quedar claro que hablamos de información y deben ser los diferentes departamentos propietarios de la misma los encargados de protegerla, exigiendo al Dpto. de informática la colaboración total y absoluta en el tema.

Por supuesto que Sistemas tiene responsabilidad en la protección de datos de carácter personal de cualquier organización, pero ésta se centra más en la aplicación técnica de las herramientas, recursos y conocimientos que poseen para garantizar tanto la integridad física y lógica de las bases de datos como las de las comunicaciones. El resto de los departamentos que utilizan datos de carácter personal son los responsables de la información que les fue proporcionada o cedida por las personas físicas.

Centrándonos en esta auditoría:

- Deben verificarse cada cierto tiempo el cumplimiento de los contratos con los diferentes proveedores y clientes para que se ajusten al Art. 12 de la L.O. 15/99 y no incurrir en cesión no autorizada de información de carácter personal. La sanción mínima para esta infracción asciende a 300.507 € (50.000.000 ptas.)
- Debieran crearse normas de actuación, de aplicación por parte del personal, cuando se realice una llamada telefónica o una visita a un cliente de manera que no se vulneren los derechos que otorga la L.O. 15/99, a la vez que marca un guión de actuación y funde aspecto de la confidencialidad y de la protección de datos.
- Cuando se comunica a un cliente información personal sobre los vigilantes debe tenerse en cuenta el punto 4 Art5 de la L.O 15/1999, es decir, recordad al cliente que dispone de tres meses para informar de forma expresa, precisa e inequívoca del tratamiento de la información que va a realizar, de la procedencia de los datos, de la existencia de un fichero o tratamiento, finalidad y destinatarios, de la posibilidad de ejercer sus derechos, de la identidad y dirección del responsable del tratamiento...
- También debe tener en consideración aquellas recomendaciones que han sido reflejadas en el apartado Recomendaciones de este mismo documento.

También es posible destacar puntos fuertes.

- Dedicación de recursos específicos a la aplicación de la LOPD y conviviendo con el sistema de Gestión de la Calidad.



23 de julio de 2007

- Concienciación de los Responsables directos
- Garantía del cumplimiento y respeto, respecto a los derechos de las personas (acceso, rectificación., cancelación y oposición)