



SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

audedatos
CONSULTORÍA EN PROTECCIÓN
DE DATOS DE CARÁCTER PERSONAL

RESUMEN EJECUTIVO DEL INFORME DE AUDITORÍA EXTERNA SOBRE CUMPLIMIENTO DE LA LOPD

(Medidas de seguridad de ficheros
automatizados)

Conforme al RD 1720/2007

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

ÍNDICE

1. INTRODUCCIÓN.....	3
2. CONCLUSIONES.....	3
3. CUADRO SINÓPTICO	17
3.1. DEFINICIÓN DE NIVELES DE CUMPLIMIENTO	17
3.2. ICONOS	17
3.3. TABLAS.....	17

1.INTRODUCCIÓN

Se ha realizado una auditoría en materia de protección de datos en la que se ha analizado el cumplimiento de las medidas de seguridad relativas a ficheros automatizados contempladas en el RD 1720/2007.

Sin perjuicio de la existencia del preceptivo informe de auditoría, se entrega el presente informe ejecutivo que contiene las conclusiones relevantes de la misma.

2. CONCLUSIONES

En lo relativo a las conclusiones de la auditoría hay que manifestar en primer lugar que aunque el alcance de la auditoría al que se refiere este informe se refiere - en principio - exclusivamente al principio de seguridad y las medidas que para su desarrollo son contempladas en el RD 1720/2007 para los ficheros automatizados y no - por tanto - al cumplimiento de todos los principios y obligaciones de la LOPD y desarrollados en el RD 1720/2007 se realizan algunas consideraciones al respecto que hemos detectado en el marco de la auditoría por su especial importancia, pero no aparecen detalladas las deficiencias en los ANEXOS correspondientes, a diferencia de las deficiencias relativas a las medidas de seguridad relativas a los ficheros automatizados.

A. CUMPLIMIENTO DE OBLIGACIONES RELATIVAS A PRINCIPIOS Y OBLIGACIONES DISPUESTOS EN LA LOPD.

La LOPD dispone una serie de principios y obligaciones que el RD 1720/2007 desarrolla.

Un somero análisis, derivado de las entrevistas realizadas, evidencia lo siguiente:

1. CALIDAD DE DATOS

Pertinencia: De la auditoría se deriva que - en general - los datos que se tratan son pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se obtuvieron.

Finalidad compatible: De la auditoría se deriva que las finalidades para las que se utilizan los datos son compatibles con las finalidades para las que fueron recogidos.

Límite Temporal: De la auditoría se deriva que - por lo general - los datos no suelen ser eliminados, aspecto que debe ser analizado caso por caso estableciendo procedimientos de control de este límite temporal en relación con los diversos tratamientos.

2. DEBER DE INFORMACIÓN

En relación con el cumplimiento del deber de información (art. 5 de la LOPD), de la auditoría se deriva que:

a) Se ha generalizado la incorporación de cláusulas o leyendas para cumplir con esta obligación.

b) Y otros tratamientos en los que no se cumple con esta obligación, como en el Diario Oficial de este año, donde se especifican las bases y la información a aportar para los candidatos a las oposiciones, pero no se les informa de qué se va a hacer con sus datos.

Se recomienda que cuando se publiquen los listados con los candidatos admitidos, se adjunte una cláusula que permita que se cumpla con el deber de informar.

3. SEGURIDAD DE LOS DATOS

Dado que el cumplimiento del principio de seguridad (art. 9 LOPD) es objeto de desarrollo a lo largo de este informe (en lo relativo a los ficheros automatizados) y de un estudio específico relativo a tres tratamientos en el caso de ficheros no automatizados, nos remitimos a las conclusiones que allí se consignan.

4. DEBER DE SECRETO

Dado que el deber de secreto (art. 10 LOPD) se ha de poner en relación con el conocimiento por parte de los usuarios de sus funciones y obligaciones y este aspecto se aborda en las conclusiones posteriores de la auditoría de ficheros automatizados y en el estudio específico de ficheros no automatizados respectivamente, nos remitimos a las recomendaciones realizadas en las mismas.

6. ACCESO A DATOS POR TERCEROS

A lo largo de la auditoría se ha detectado la existencia de numerosos supuestos de encargados del tratamiento en los diferentes servicios de la Sindicatura de Comptes de la Comunitat Valenciana. Se ha evidenciado la firma generalizada de estos contratos pero en algunos casos se ha evidenciado mediante declaraciones admisibles de los propios entrevistados la inexistencia del contrato firmado en ese sentido, como por ejemplo con el encargado de la realización de las copias de seguridad CETESI (Centro de Telecomunicaciones y Sistemas de Información de la Generalitat Valenciana).

No se han evidenciado supuestos de subcontratación.

Asimismo, y en relación con la limitación en la conservación de los datos por parte de los encargados y aunque tampoco se ha evidenciado que se incumpla esta medida y se conserven datos más allá de lo establecido en estos preceptos, debe velarse por ello.

Para habilitar la posibilidad de control por parte de la Sindicatura de Comptes de la Comunitat Valenciana de los encargados del tratamientos, atendiendo al deber de diligencia in iligendo e in vigilando de los proveedores impuesto en el RD 1720/2007 deben articularse cláusulas que habiliten la posibilidad de solicitar información/documentación a los proveedores con el objeto de acreditar el cumplimiento de sus obligaciones en materia de protección de datos por parte estos. La información/documentación exigida podrá ser mayor o menor y diferente en función de los servicios prestados por el encargado. En algunos casos esta exigencia puede aconsejar no sólo la solicitud de información sino cláusulas que habiliten auditar al encargado. Y en todo caso los contratos deben permitir activar mecanismos de resolución basados en el incumplimiento de las obligaciones derivadas del cumplimiento de las medidas derivadas de sus obligaciones como encargados del tratamiento; y en caso de incumplimiento adoptarlas efectivamente.

7. DERECHO DE LAS PERSONAS

Los interesados tienen un haz de derechos que les permiten el control del tratamiento que se realiza de sus datos. Se trata de los derechos de acceso, rectificación, cancelación y oposición (conocidos como derechos ARCO). El procedimiento para la solicitud de estos derechos está sometido a un procedimiento que está regulado en el RD 1720/2007.

De la auditoría se ha evidenciado que:

1. No se ha detectado la existencia de supuestos de peticiones de estos derechos.
2. Se ha evidenciado que existe un procedimiento formal descrito de cómo proceder en el caso de que un interesado solicite la atención de sus derechos ARCO, que contempla tanto los puntos de recogida de solicitudes como los de atención de las mismas

Hay que tener en cuenta a la hora de articular el procedimiento un aspecto que se ha evidenciado como crítico:

Los usuarios de atención nombrados para poder atender las peticiones de ejercicio de derechos, desconocen qué son los Derechos Arco y cómo proceder para notificarlas al Responsable de Seguridad encargado de atender dichas peticiones.

8. TRANSFERENCIAS INTERNACIONALES DE DATOS

No se producen transferencias internacionales de datos por lo que no se analiza ni se aportan conclusiones sobre esta obligación.

B. CUMPLIMIENTO DE LAS MEDIDAS DERIVADAS DEL PRINCIPIO DE SEGURIDAD (ART. 9 LOPD) RELATIVAS A FICHEROS AUTOMATIZADOS.

Las conclusiones del informe de auditoría en relación con el cumplimiento del principio de seguridad, en lo relativo a las medidas de seguridad respecto de ficheros automatizados dispuestas en el RD 1720/2007 son las siguientes:

1. IDENTIFICACIÓN DE FICHEROS

Existe una relación detallada de los ficheros inscritos en la AEPD, que se encuentra en el Documento de Seguridad de la Sindicatura de Comptes de la Comunitat Valenciana.

En dicho documento se recogen todos los campos necesarios para identificar: la descripción y finalidad de cada fichero, la disposición general de creación, modificación o supresión, el origen y procedencia de los datos, los tipos de datos y estructura del fichero, el nivel de seguridad del mismo, si existen encargados de tratamiento, la cesión o comunicación de los datos del fichero y donde atender los Derechos Arco.

Existe también una relación de los ficheros físicos automatizados y su correspondencia directa con cada fichero jurídico.

2. NIVEL DE SEGURIDAD DE LOS FICHEROS INSCRITOS

El nivel de seguridad de los ficheros inscritos es correcto puesto que se ha adecuado a lo dispuesto en el RD 1720/2007.

3. DOCUMENTO DE SEGURIDAD

Se evidencia la existencia de un Documento de Seguridad de nivel alto, gestionado con la aplicación "Gesdatos".

Se ha constatado mediante revisión del Documento de Seguridad, que todos y cada uno de los apartados del artículo 88- punto 2, están incluidos en el Documento de Seguridad.

En la actualidad, y tras entrevistas con los Responsables de Seguridad, se constata que el Documento de Seguridad está correctamente actualizado según la estructura y organización actual de la Sindicatura de Comptes de la Comunitat Valenciana.

4) El Documento de Seguridad está adecuado, a día de hoy, a las disposiciones vigentes en materia de seguridad de protección de datos de carácter personal al RD1720/2007.

La última copia guardada del Documento de Seguridad en el apartado "Recursos" de GESDATOS es de fecha 10_07_09.

Se recomienda guardar una copia periódica del documento de seguridad para llevar un control de versiones.

En el Documento de Seguridad de la organización se contempla la identificación de las figuras de Responsables de Seguridad para cada uno de los ficheros inscritos.

Se recomienda que todo lo especificado en el Documento de Seguridad de LOPD concuerde con el Documento de "Política de Seguridad" de Sindicatura de Comptes de la Comunitat Valenciana, actualizando este último documento, en caso de ser necesario, puesto que es imprescindible de cara a optar a posibles certificaciones futuras, tales como ISO/IEC 27001 (Sistema de Gestión de Seguridad de la Información), etc.

4. ENCARGADOS DE TRATAMIENTO

Además de los aspectos jurídicos a los que ya hemos referencia anteriormente, en relación con los encargados del tratamiento y de conformidad con el artículo 12 de la LOPD deberían formalizarse los correspondientes contratos con cada uno de los colaboradores externos a los que se les da acceso a información de carácter personal.

5 FUNCIONES Y OBLIGACIONES DEL PERSONAL

5.1. USUARIOS.

De las entrevistas realizadas con el objeto de conocer el estado real de conocimiento por parte de los usuarios de sus funciones y obligaciones cabe concluir que se conocen de forma generalizada sus funciones y obligaciones,.

Todos los usuarios firman su "Alta de Usuario" al Sistema de Información nada más llegar a la organización, a la vez que reciben un "Manual de Formación" en materia de protección de datos.

A su vez, se les ha creado una carpeta común en la Intranet llamada "Protección de Datos", donde disponen de manuales personalizados para el cumplimiento de sus obligaciones.

Las autorizaciones delegadas por el responsable del fichero o tratamiento se encuentran documentadas en el Documento de Seguridad.

El Responsable del Fichero ha tomado las medidas necesarias para que el personal conozca dichas normas ya que existe constancia de la firma por parte de los usuarios del Sistema de Información de un acuerdo de confidencialidad, que recoge los requerimientos establecidos por el RDLOPD, aun así, existen algunos usuarios que desconocen ciertas obligaciones en materia de protección de datos.

No obstante existen usuarios del sistema de información que, pese a haber recibido

formación en materia de protección de datos y haber firmado su alta de usuario, desconocen parte de sus obligaciones respecto a los procedimientos a la hora de notificación de incidencias (desconocen que existe una aplicación para notificar al Departamento de Informática las incidencias, donde se les obliga a detallar una serie de campos imprescindibles para cumplir con dicho registro) y el procedimiento de entradas/salidas de soportes.

Desde Recepción (más concretamente los ordenanzas), que actúan como "Usuarios de Atención" y, por lo tanto, están expuestos a recibir una petición de Ejercicio de Derechos, desconocían qué son los Derechos Arco y que debían notificar y llevar dichas solicitudes al Responsable de Seguridad Roberto Pere Cortell.

Todos los usuarios del Sistema de Información deben conocer la existencia de los procedimientos de notificación de incidencias y de registro de entrada/salida de soportes así como el procedimiento para atender o notificar al responsable oportuno las Peticiones de Ejercicio de Derechos.

Se recomienda promover la formación continua y los conocimientos relativos a la Seguridad de la Información de todos los usuarios del sistema que accedan o traten datos de carácter personal.

Se recomienda que se definan y documenten los roles y responsabilidades de los empleados, contratistas y terceros en concordancia con la Política de Seguridad de la Información.

Los roles y responsabilidades debieran incluir requerimientos para:

- a) implementar y actuar en concordancia con las políticas de seguridad de la información de la organización;
- b) proteger los datos de carácter personal contra el acceso, divulgación, modificación, destrucción o interferencia no autorizada;
- c) ejecutar procesos o actividades de seguridad particulares;
- d) asegurar que se asigne a la persona la responsabilidad por las acciones tomadas.

A su vez, debiera existir un proceso disciplinario para los empleados que hayan cometido un incumplimiento respecto de sus obligaciones como usuarios del Sistema de Información y haya afectado a la seguridad, confidencialidad e integridad de los datos.

5.2. RESPONSABLES DE SEGURIDAD

En el Documento de Seguridad se designan los Responsables de Seguridad encargados de coordinar y controlar las medidas definidas en el mismo.

Los Responsables de Seguridad han firmado su "nombramiento" que le otorga el cargo asignado y en la totalidad conocen las funciones que han sido delegadas por el Responsable del fichero.

Los Responsables de Seguridad no han firmado el Alta de sus obligaciones y tareas asignadas.

Los Responsables de Seguridad han visto aconsejable la delegación de determinados aspectos esenciales de sus funciones en personas próximas física y/o funcionalmente a algunos ficheros concretos, tales como "Expedientes de Personal", "Documentación de Archivo" y "Documentación de Archivo de Fiscalizaciones", asignándoles el perfil de "Gestor de Fichero Concreto".

El Gestor de fichero concreto, es una figura que se ubica en una situación intermedia entre el Responsable de Seguridad y los usuarios del sistema.

En el Gestor se han delegado actividades de control y ejecución de medidas de seguridad relacionadas con los ficheros concretos anteriormente mencionados. Esto ha permitido una adecuada colaboración con las tareas del Responsable de Seguridad debido a su relación directa con el fichero y a su cercanía con los usuarios.

Se recomienda la formación continua de los Responsables de Seguridad en materia de protección de datos.

Se recomienda que, conforme vaya cambiando la estructura de la organización, se realicen controles para determinar si es necesario nombrar a más Responsables de Seguridad o Gestores de Fichero Concreto o, a redistribuir las tareas asignadas entre los mismos.

6. GESTIÓN DE SOPORTES

6.1. INVENTARIO Y ALMACENAMIENTO

Los soportes de la organización que contienen datos de carácter personal, en concreto las copias de seguridad (cintas y discos duros), están correctamente inventariados, permiten identificar el tipo de información que contienen y se encuentran almacenados en un lugar con acceso restringido a terceros. Sólo son accesibles, por el personal autorizado para ello en el Documento de Seguridad (en este caso, el Departamento de Sistemas).

Existen dos ubicaciones para el almacenamiento de los soportes:

-Una caja ignífuga ubicada en el Departamento de Sistemas.

-Una sala ubicada en la quinta planta donde, a su vez, se almacena el robot de cintas. Dicha sala permanece cerrada bajo llave y únicamente tiene acceso el personal autorizado.

Por otra parte, respecto a los ficheros de nivel alto, la codificación de las cintas utilizadas para la realización de copias de seguridad por el robot de copias es realizada automáticamente por éste, de forma que las identifica unívocamente, y las indexa debidamente, permitiendo conocer su contenido únicamente a los operadores de copia autorizados.

6.2. SALIDA DE SOPORTES

Todas las salidas de soportes deberían estar debidamente registradas y controladas.

Se ha comprobado que en el caso de que se produzca una salida de soportes, ésta será autorizada por el Responsable de Seguridad quién dará su autorización por escrito respecto a la salida del mismo.

Se producen salidas con periodicidad diaria/mensual de los equipos portátiles de los auditores que, por cuestiones de trabajo, se llevan el equipo fuera de las instalaciones de la organización.

Dicha entrada/salida periódica está aprobada formalmente por el Responsable de Fichero y se encuentra registrada en Gesdatos.

Las autorizaciones para las salidas de soportes pueden ser específicas para cada salida o realizarse de forma general siempre que de las autorizaciones generales se deduzca de forma inequívoca las salidas concretas en que se plasmen.

Se recomienda que previamente a toda autorización de salida de soportes se proceda a validar que la salida es legítima por lo que al menos en el momento inicial en el caso de las salidas periódicas y cada vez en las puntuales, debería existir un sistema de chequeo que permita garantizar que la misma está habilitada legalmente (en Gesdatos se disponen de un test para verificar que la misma se encuentra legitimizada).

6.3. OTRAS MEDIDAS RELATIVAS A LA GESTIÓN DE SOPORTES: RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL FICHERO.

Se ha evidenciado la utilización de equipos portátiles de los auditores que almacenan datos de carácter personal de nivel alto, fuera de las instalaciones de la organización.

Este hecho es conocido por el Responsable del Fichero y por los Responsables de Seguridad y ha sido aprobado formalmente debido a que dicha salida de equipos es indispensable para que los auditores puedan realizar sus tareas laborales.

Existe una relación detallada de qué equipo custodia qué persona.

Se lleva un control de acceso de los periodos de tiempo en los que los auditores se encuentran fuera de las instalaciones con el equipo portátil trabajando.

No todos los equipos se encuentran cifrados o encriptados, por lo tanto, son vulnerables en caso de pérdida de los mismos, robo, etc., a que terceros no autorizados puedan llegar a tener acceso a la información, aunque sí que se encuentran protegidos mediante control de acceso lógico por usuario y contraseña, y la aplicación de TeamMate, que es donde todos los auditores guardan sus informes de auditoría, dispone a su vez de contraseña.

Los equipos portátiles disponen de sistema de autenticación biométrico basado en huella dactilar.

A su vez, existen usuarios que utilizan pen drives personales para guardar información sensible que se llevan fuera de las instalaciones, sin ningún tipo de autorización por parte de los Responsables de Seguridad, y sin ninguna medida de

seguridad adicional para evitar que la información pueda ser accedida por terceros no autorizados en caso de pérdida o robo de los mismos.

Se deben cifrar/criptar los equipos portátiles de los auditores, los cuáles almacenan información sensible, como medida de seguridad en caso de pérdida, robo de equipo, etc., consiguiendo evitar así que terceros no autorizados pudiesen tener acceso a la información que almacenan.

Se debe prohibir el uso de pen drives y otros soportes de almacenamiento externos sin autorización de los Responsables de Seguridad.

En caso de autorizar dichos soportes, los Responsables de Seguridad deberán aplicar las medidas de seguridad oportunas a dichos dispositivos para proteger la integridad y la confidencialidad de la información contenida en los mismos.

Se recomienda adoptar medidas técnicas y organizativas tendente a evitar el tratamiento de datos personales en soportes (entre otros portátiles y pen drives) sin adoptar las correspondientes medidas de seguridad.

7. COPIAS DE RESPALDO Y RECUPERACIÓN

Los procedimientos de copia de seguridad actuales cubren la copia de seguridad tanto de los datos como de las aplicaciones que se utilizan para el acceso a los mismos.

Debería verificarse que la copia de seguridad almacene información suficiente acerca de la configuración de las aplicaciones y otro software de infraestructura (como bases de datos, sistema operativo, etc.) que permita minimizar el tiempo de restauración del servicio ante la pérdida completa del hardware ubicado en ella. En este caso, no se trataría únicamente de permitir recuperar la información, sino de permitir restaurar el servicio con la menor interrupción posible. Por lo anterior, se recomienda la utilización, en la medida de lo posible, de herramientas que permitan almacenar imágenes virtuales de los sistemas informáticos críticos, de forma que sea posible una restauración rápida de los mismos en un hardware similar.

Se debe verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

8. CONTROL DE ACCESO

8.1. CONTROL DE ACCESO LÓGICO

Los usuarios de la organización acceden únicamente a aquellos datos y recursos que precisan para el desarrollo de su trabajo.

Existe una relación actualizada de usuarios que contiene el acceso autorizado de cada uno de ellos.

Sólo los Responsables de Seguridad pueden conceder, alterar o anular accesos.

8.2. CONTROL DE ACCESO FÍSICO

Exclusivamente el personal autorizado en el Documento de Seguridad, tiene acceso a los lugares donde se hayan instalados los equipos físicos (en este caso el CPD, Centro de Proceso de Datos, situado en la planta baja) que dan soporte a los sistemas de información.

El CPD de Sindicatura de Comptes se encuentra protegido mediante un sistema de cierre mediante llave, dispone de sistema de sensor de temperatura y un extintor contra incendios.

Únicamente el personal de Seguridad, son las personas encargadas de la custodia de las llaves de acceso.

Se dispone a su vez, de un sistema de Videovigilancia, controlado en todo momento por personal de Seguridad las 24 horas, que cubre la seguridad de distintas zonas de la organización incluyendo el CPD.

La sala en la que se encuentran ubicados los servidores contiene también otro tipo de dispositivos electrónicos (concentradores informáticos, centralita telefónica, comunicaciones informáticas en general,...) que ocasiona que personal técnico de las compañías suministradoras o de mantenimiento (como por ejemplo Telefónica, personal de limpieza, mantenimiento de aire acondicionado, etc.) pueda tener acceso al mismo.

El Responsable de Seguridad de Informática, supervisa al personal técnico durante su visita.

Se debería hacer entrega al personal de Seguridad de un listado de personas autorizadas a acceder a determinadas salas, despachos, etc., donde se almacenan datos de carácter personal, tal como el CPD (Centro de Proceso de Datos). De forma que no cedan las llaves de acceso a cualquier usuario de la organización que se las pida.

A su vez, debería haber un control de dichas llaves, controlando en todo momento quién las tiene, a qué hora se las lleva y cuándo las devuelve.

Se debería mantener listas de acceso autorizado de forma documentada y actualizada de todos aquellos con acceso. Dichas listas deberían ser revisadas periódicamente.

Debería procederse a establecer un plan de revisiones periódicas de los servidores como medida de mantenimiento preventivo, realizado bien por personal interno, bien por externo, contratándolo específicamente a compañías especializadas en ello.

9. IDENTIFICACIÓN Y AUTENTICACIÓN

Existe una relación actualizada de usuarios con acceso autorizado al sistema de información, así como un procedimientos de identificación y autenticación para dichos accesos.

Al basarse el mecanismo de autenticación en nombre de usuario y contraseña, existe un procedimiento de asignación, distribución y almacenamiento que garantiza su integridad.

Para acceder a la red es necesario disponer de usuario y contraseña y validarse correctamente en el directorio activo de Windows.

La validación en la red dará acceso a las carpetas del servidor de ficheros a las que esté autorizado. Para acceder a las aplicaciones, además, hay que validarse correctamente mediante usuario y contraseña. En este último caso, el perfil de usuario asignado determinará el nivel de acceso dentro del sistema de gestión integral. Los accesos a estos ficheros están controlados por un administrador (Responsable de Seguridad).

También se dispone de la opción de un sistema biométrico mediante huella, para la validación de acceso al sistema de los usuarios.

Los usuarios cambian la contraseña según lo establecido en el Documento de Seguridad, actualmente cada dos meses.

A su vez, se dispone de un número limitado de cinco reintentos fallidos a nivel de sistema operativo (Windows 2000/2003 Server / XP/Vista/Windows 7) que dan lugar al bloqueo de la cuenta. Una vez el sistema se bloquea, es necesario que el Administrador de Sistemas proceda al desbloqueo

10. GESTIÓN DE INCIDENCIAS

Existe un procedimiento de notificación y gestión de las incidencias que afecta a los datos de carácter personal y se haya establecido un registro en la aplicación Gesdatos, en el que se hace constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

A su vez, existe un registro de incidencias, habilitado a través de un módulo de la Intranet para los usuarios del sistema de información, en el que consta el tipo de incidencia y la persona que realiza la notificación.

Muchos usuarios desconocen dicho módulo, por lo que notifican las incidencias al departamento de Informática vía llamada telefónica.

Se recomienda la notificación mediante charlas, o bien, vía correo electrónico a los usuarios del sistema de información de dicho módulo para la notificación de incidencias.

Además de la información que consta en el registro de incidencias relativo al nivel básico, en el mismo se consignan los procedimientos realizados de la recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados, y si fuera el caso, qué datos ha sido necesario grabar manualmente en el proceso de restauración.

Se ha evidenciado que, en los casos en los que se ha tenido que proceder a la recuperación de datos, el Responsable de Seguridad Informática se encarga previamente de autorizar por escrito la recuperación de la información

12.2. FICHEROS TEMPORALES

En determinados equipos, se generan ficheros temporales que no son eliminados en una vez dejan de ser utilizados para los fines que motivaron su creación y no se controla la aplicación de las medidas de seguridad que les corresponde según la naturaleza de la seguridad que contienen, sobretodo documentos de tablas en excel y documentos en word.

Como su almacenamiento se realiza, generalmente, en las mismas carpetas en las que se almacena la documentación que tiene carácter permanente, no pueden distinguirse fácilmente y permanecen sine die en los sistemas informáticos, pudiendo tratarse, con el tiempo, de datos no actualizados, incompletos o inexactos.

Se recomienda adoptar medidas técnicas y organizativas tendentes a evitar la creación y uso de ficheros temporales sin adoptar las correspondientes medidas de seguridad.

12.3. PRUEBAS CON DATOS REALES

Los Responsables de Seguridad afirman que no se realizan pruebas con datos reales.

13. AUDITORÍA

13.1. ORDINARIA

Los Responsables de Seguridad afirman que ésta es la primera auditoría que han tenido con respecto al R.D. 1720/2007.

A su vez, se ha evidenciado la realización de auditorías de los sistemas de información y de certificaciones de la red de la organización por encargados de tratamiento contratados a tal efecto.

Deben realizarse las auditorías ordinarias dentro del plazo máximo legalmente establecido de dos años y abordarse el plan de acciones correctoras correspondiente derivado de las deficiencias detectadas en las mismas y medidas correctoras y recomendaciones propuestas.

13.2. EXTRAORDINARIA

De la auditoría se desprende que no se han realizado modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas, por lo que no ha sido necesario realizar una auditoría con carácter extraordinario.

14. CONTROLES PERIÓDICOS

Se ha definido un sistema de controles periódicos con el objeto de comprobar el efectivo cumplimiento de las medidas dispuestas en el Documento de Seguridad.

El sistema de controles periódicos cumple con los siguientes principios exigidos:

- a. Segregación de funciones: existe una segregación de funciones de forma tal que se garantiza la efectividad e independencia de los controles.
- b. Documentación de tareas pendientes: dicho sistema de controles permite documentar los controles realizados, los controles superados y las tareas pendientes derivadas de los mismos.

Los Responsables de Seguridad realizan sus respectivos controles periódicos con la aplicación Gesdatos, creando posteriormente un listado de tareas pendientes para cada uno de ellos.

15. DESECHADO Y REUTILIZACIÓN DE SOPORTES

Existen soportes físicos de almacenamiento, como discos duros, que actualmente no están siendo utilizados, ni serán utilizados en un futuro y que permanecen guardados en el departamento de sistemas en un armario cerrado bajo llave.

Se debe desechar los soportes que, una vez concluida su vida útil, ya no se vayan a volver a utilizar, para evitar que los mismos sean manipulados o accedidos por terceros no autorizados.

Se debería de proceder a la destrucción física de los mismos.

Se recomienda realizar una evaluación de riesgos en aquellos equipos y soportes que almacenan información de carácter personal para determinar si los mismos debieran ser físicamente destruidos en lugar de ser enviados a reparar o descartar.

16. REGISTRO DE ACCESOS

Las aplicaciones que tratan ficheros físicos de nivel alto, no disponen de un Registro de Accesos que cumpla con los requisitos que nos marca el artículo 103 del RDLOPD.

Aunque desde el Departamento de Sistema de ha intentado suplir dicha carencia con la herramienta que nos brinda Windows para el registro de los logs de determinados accesos, no se cumple con todos los campos que dicho registro debe tener, puesto

que no se puede saber si un usuario ha accedido a un fichero en modo lectura, o ha modificado el mismo.

No se realizan revisiones al menos una vez al mes de la información de control registrada y no se elaboran un informes de las revisiones realizadas y los problemas detectados.

Las aplicaciones que tratan con datos de nivel alto deben de tener implementado un Registro de Accesos de modo que:

1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.
2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.
3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.
4. El período mínimo de conservación de los datos registrados será de dos años.
5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

Se debería implementar un proceso que permita detectar desviaciones con respecto a comportamientos esperados, o bien patrones de conducta sospechosos o de consulta a datos sensibles, para disminuir la necesidad de consultar individualmente todos los registros de accesos para detectar comportamientos anómalos.

3. CUADRO SINÓPTICO

En las siguientes tablas, y de forma sinóptica, se detallan el nivel de cumplimiento de las diferentes obligaciones y medidas.

3.1. DEFINICIÓN DE NIVELES DE CUMPLIMIENTO

La definición de niveles de cumplimiento en una materia sometida a una normativa, como es el caso de la protección de datos, es discutible, puesto que los principios y las obligaciones legales, así como las medidas, se cumplen o no se cumplen.

Ello nos lleva a entender que, en principio, todos los principios, obligaciones y medidas dispuestos en la legislación: bien se cumplen; bien no.

No obstante ello es posible entender, que existen supuestos en los que el cumplimiento o el incumplimiento no es total por lo que se ha optado por una definición de niveles de cumplimiento pedagógica que contemple estos tres escenarios: cumplimiento total (ausencia de deficiencia); incumplimiento total (existencia de deficiencias mayores o graves); y cumplimiento o incumplimiento parcial (existencia de deficiencias pero que no se consideran graves).

3.2. ICONOS





Para que dichos niveles sean gráficos se han establecido los siguientes iconos:

SIGNIFICADO	ICONO
Cumplimiento total	
Cumplimiento/Incumplimiento parcial	
Incumplimiento total	

3.3. TABLAS

3.3.1 CUMPLIMIENTO DE OBLIGACIONES RELATIVAS A PRINCIPIOS Y OBLIGACIONES DISPUESTOS EN LA LOPD

MATERIA	MEDIDA DE SEGURIDAD	NIVEL DE CUMPLIMIENTO
Inscripción, modificación y supresión de ficheros	Inscripción, modificación y supresión de ficheros	
Deber de información al interesado	Deber de información	
Deber de secreto	Deber de secreto	

Comunicación de datos	Comunicación de datos	
Acceso a datos por cuenta de terceros	Acceso a datos por cuenta de terceros	
Prestación de servicio sin acceso a datos	Prestación de servicios sin acceso a datos (art. 83 RD 1720/2007)	
Derechos de las personas	Impugnación de valoraciones Derechos de acceso, rectificación, cancelación, oposición	
Transferencias internacionales de datos	Trasferencias internacionales de datos	No aplica

3.3.2 CUMPLIMIENTO DE MEDIDAS DERIVADAS DEL PRINCIPIO DE SEGURIDAD (ART. 9) RELATIVAS A FICHEROS AUTOMATIZADOS.

MATERIA	MEDIDA DE SEGURIDAD	NIVEL DE CUMPLIMIENTO
Documento de seguridad	Contenido del documento de seguridad de nivel Básico	
	Documento de seguridad de nivel Medio	
Ficheros	Nivel de Seguridad	
	Identificación	
Funciones y obligaciones del personal	Funciones y obligaciones del personal	
	Responsables de seguridad	
Gestión de soportes	Inventario y almacenamiento de soportes	
	Autorización para la salida de soportes	
	Registro de salida de soportes	
	Registro para la entrada de soportes	
	Desechado o reutilización de soportes	
	Cifrado en la distribución de soportes	
Copias de respaldo y recuperación	Copias de respaldo y recuperación	
	Copias de respaldo y de los procedimientos de recuperación en nivel alto	
Control de acceso	Control de acceso lógico	
	Control de acceso físico	
	Registro de accesos	
Identificación y autenticación	Identificación y autenticación	
Gestión de incidencias	Registro de Incidencias de nivel Básico	
	Registro de incidencias de nivel Medio	
Telecomunicaciones	Acceso a datos a través de redes de comunicaciones	
	Transmisión de datos a través de redes de telecomunicaciones	
Tratamientos especiales	Régimen de trabajo fuera de los locales de la ubicación del fichero	
	Ficheros temporales	
	Pruebas con datos reales	
Auditoría	Auditoría ordinaria	
	Auditoría extraordinaria	

4. OPINIÓ

En nuestra opinión profesional la entidad auditada tiene un cumplimiento **SUFICIENTE** de las medidas que exige el RD 1720/2007 en relación con los ficheros automatizados que supone que este informe sea **FAVORABLE** pero con Salvedades. En el informe se consignan deficiencias y las correspondientes medidas correctoras o complementarias.

Adicionalmente, se han propuesto una serie de recomendaciones que, si bien no son de obligado cumplimiento, recomendamos que sean valoradas.

Por último, se recuerda a la entidad auditada, que sus Responsables de Seguridad deben analizar el presente informe de auditoría y elevar al Responsable del Fichero las conclusiones que resulten para que ésta adopte las medidas correctoras adecuadas.

En Valencia, a 17 de Diciembre de 2009

Auditor/es:

Entidad Auditora:

Eduard Chaveli Donet
(Auditor Jefe)

Elísabeth Iglesias Domínguez
(Asistente Técnico)

Ace&Niu Consulting S.L.
(AUDEDATOS)