INFORME DE AUDITORIA EN EL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS

" AMICA ”

OBJETO DE LA AUTITORIA
FASES EN LA REALIZACIÓN DE LA AUDITORÍA
PLAN DE TRABAJO

1. DELIMITACION DE LOS FICHEROS
2. REVISIÓN DEL DOCUMENTO DE SEGURIDAD
3. ENCARGADOS DE TRATAMIENTO
4. PRESTACIONES DE SERVICIO SIN ACCESO A DATOS PERSONALES
5. DELEGACION DE AUTORIZACIONES
6. REGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL FICHERO
7. FICHERO TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS
8. FUNCIONES Y OBLIGACIONES DEL PERSONAL
9. REGISTRO DE INCIDENCIAS
10. CONTROL DE ACCESO
11. GESTION DE SOPORTES Y DOCUMENTOS
12. IDENTIFICACION Y AUTENTIFICACION
13. COPIAS DE RESPALDO Y RECUPERACION
14. REGISTRO DE ACCESOS
15. ACCESO A TRAVES DE REDES DE COMUNICACIONES
16. AUDITORIA
17. MEDIDAS APLICABLES A FICHEROS NO AUTOMATIZADOS
18. CALIDAD DE LOS DATOS
19. INFORMACION A LOS INTERESADOS
20. OBTENCION DEL CONSENTIMIENTO

CONCLUSIÓN FINAL

OBJETO DE LA AUDITORIA

El presente documento tiene por objeto comprobar el grado de adecuación de la entidad al Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal y que contempla las medidas de seguridad necesarias en el tratamiento de datos de carácter personal y también a lo establecido en la Ley Orgánica 15/ 1999 de protección de datos de carácter personal

Concretamente se pretende dar cumplimiento a lo dispuesto en los artículos 96 y 110 del citado reglamento que establecen la obligación de someter todos los sistemas de información e instalaciones de tratamiento y almacenamiento de datos a una auditoria interna o externa con el objetivo de verificar el cumplimiento de todas las obligaciones impuestas a este respecto por el RD 1720/2007 y por los procedimientos e instrucciones vigentes en materia de seguridad.

El objetivo final de la auditoria es verificar el grado de adecuación de la entidad a las medidas y controles de la Ley de Protección de Datos y su normativa de desarrollo, identificando sus deficiencias y proponiendo las medidas correctoras o complementarias necesarias. A su vez, incluye los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

Los puntos básicos a revisar en este documento:

- **Aspecto Técnico:** se revisa el cumplimiento de las medidas de seguridad que deben reunir los ficheros automatizados.
- **Aspecto Organizativo:** se revisan los procedimientos normativos y reglas de seguridad elaborados e implantados por la entidad.
- **Aspecto Jurídico:** se revisa la tipología de los datos almacenados en los sistemas de información y aplicaciones informáticas, y la calificación de los ficheros como de nivel básico, medio o alto

FASES EN LA REALIZACIÓN DE LA AUDITORÍA

La auditoría obligada por el Reglamento del R.D. 1720/2007 se ha realizado con visitas presenciales del auditor y ha constado de las siguientes fases:
-Conocimiento genérico de la entidad, su ámbito de negocio, los sistemas de información de que disponen, su estructura administrativa y el organigrama de sus trabajadores, sus relaciones con organismos oficiales, asociaciones, instituciones y 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 entidad.
-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 y la LOPD , 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 AMICA (básico, medio, alto).
Para la realización organizada de esta auditoría se ha preparado una tabla de control o de "checklist".
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. DELIMITACION DE LOS FICHEROS
2. REVISIÓN DEL DOCUMENTO DE SEGURIDAD
3. ENCARGADOS DE TRATAMIENTO
4. PRESTACIONES DE SERVICIO SIN ACCESO A DATOS PERSONALES
5. DELEGACION DE AUTORIZACIONES
6. REGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL FICHERO
7. FICHERO TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS
8. FUNCIONES Y OBLIGACIONES DEL PERSONAL
9. REGISTRO DE INCIDENCIAS
10. CONTROL DE ACCESO
11. GESTION DE SOPORTES Y DOCUMENTOS
12. IDENTIFICACION Y AUTENTIFICACION
13. COPIAS DE RESPALDO Y RECUPERACION
14. REGISTRO DE ACCESOS
15. ACCESO A TRAVES DE REDES DE COMUNICACIONES
16. AUDITORIA
17. MEDIDAS APLICABLES A FICHEROS NO AUTOMATIZADOS
18. CALIDAD DE LOS DATOS
19. INFORMACION A LOS INTERESADOS
20. OBTENCION DEL CONSENTIMIENTO

1.-DELIMITACION DE LOS FICHEROS

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

- **¿**Es adecuado el número y la definición de los ficheros actuales**? SI**

- **Ficheros actuales**

  Se encuentran descritos en el documento de seguridad actualizado a fecha Noviembre de 2014

NIVEL DE CUMPLIMIENTO

Satisfactorio. Corresponden los ficheros inscritos a los realmente tratados por la entidad

RECOMENDACIONES

Se procederá a la inscripción de nuevos ficheros en caso de necesitarse con carácter previo al tratamiento de los datos de carácter personal

LEGISLACION

Artículo 55. Notificación de ficheros.

1. Todo fichero de datos de carácter personal de titularidad pública será notificado a la Agencia Española de Protección de Datos por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, en el plazo de treinta días desde la publicación de su norma o acuerdo de creación en el diario oficial correspondiente.

2. Los ficheros de datos de carácter personal de titularidad privada serán notificados a la Agencia Española de Protección de Datos por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación. La notificación deberá indicar la identificación del responsable del fichero, la identificación del fichero, sus finalidades y los usos previstos, el sistema de tratamiento empleado en su organización, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, la indicación del nivel de medidas de seguridad básico, medio o alto exigible, y en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales de datos.

Artículo 58. Notificación de la modificación o supresión de ficheros.

1. La inscripción del fichero deberá encontrarse actualizada en todo momento. Cualquier modificación que afecte al contenido de la inscripción de un fichero deberá ser previamente notificada a la Agencia Española de Protección de Datos o a las autoridades de control autonómicas competentes, a fin de proceder a su inscripción en el registro correspondiente, conforme a lo dispuesto en el artículo 55.

2. Cuando el responsable del fichero decida su supresión, deberá notificarla a efectos de que se proceda a la cancelación de la inscripción en el registro correspondiente.

2.-REVISION DEL DOCUMENTO DE SEGURIDAD

- ¿Ha elaborado el responsable del fichero el Documento de Seguridad? **SI**
- ¿Contiene los aspectos mínimos exigidos por el Reglamento? **SI**
- ¿Está el documento actualizado? **SI**
- Fecha de la última actualización: **DICIEMBRE 2014**
- Motivo de la última actualización: **AUDITORIA PERIODICA INCORPORACION DE ANEXOS, CAMBIO RESPONSABLES FICHERO DE VIDEOVIGILANCIA Y ACTUALIZACION DE DATOS NO RELEVANTES, QUE NO MODIFICAN SUSTANCIALMENTE EL CONTENIDO.**
- ¿Se ha revisado cuando se han producido cambios relevantes desde la auditoría anterior? **SI**
- ¿Está su contenido adecuado a la normativa vigente en el momento presente en materia de seguridad de los datos de carácter personal? **SI**
- ¿Se ha indicado con qué periodicidad se deben cambiar las contraseñas? **SI**
- ¿Es inferior o igual a un año? **SI**
- ¿Se especifica cuál es el personal autorizado para la concesión, alteración o anulación de accesos autorizados sobre datos o recursos? **SI.**
- ¿Se especifica cuál es el personal autorizado para acceder a los lugares donde se almacenan los soportes informáticos? **SI**
- 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**? SI**
- ¿Se ha reflejado en el Documento de Seguridad si los datos personales se incorporan y tratan exclusivamente en los sistemas del encargado? **SI**
- ¿Se ha delegado en el encargado del tratamiento la llevanza del Documento de Seguridad para los ficheros objeto del contrato? **NO**
- ¿Se ha reflejado esta circunstancia en el contrato? **SI**
- ¿Establece la identidad del responsable o responsables de seguridad? **SI. SE HA DESIGNADO A VARIOS CO-RESPONSABLES.**
- ¿Se especifica si la designación es única para todos los ficheros o está diferenciada según el sistema de tratamiento utilizado? **ESTA DIFERENCIADA POR FICHEROS**
- Persona o personas designadas como responsables de seguridad: **ESTAN DETERMINADAS EN EL DOCUMENTO DE SEGURIDAD.**
- ¿Contiene los procedimientos y controles periódicos a realizar para

verificar el cumplimiento de lo dispuesto en el propio documento? **SI**

35 17 ¿Especifica qué medidas hay que adoptar en caso de desechado o reutilización de soportes? **SI**

35 17 ¿Relaciona las personas que están autorizadas a acceder físicamente a los locales donde se ubican los sistemas de información? **SI EN EL DOCUMENTO DE SEGURIDAD.**

NIVEL DE CUMPLIMIENTO

Satisfactorio. El documento de seguridad tiene el contenido establecido por la ley y el reglamento

RECOMENDACIONES

El documento de seguridad debe de estar permanentemente actualizado describiendo la realidad de AMICA

LEGISLACION

Del documento de seguridad

Artículo 88. El documento de seguridad.

1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.
2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.
3. El documento deberá contener, como mínimo, los siguientes aspectos:
a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.
c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.
d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
e) Procedimiento de notificación, gestión y respuesta ante las incidencias.
f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.
g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.
4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:
a) La identificación del responsable o responsables de seguridad.
b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.
5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.
6. En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento

de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados.
En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento.
7. El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.
8. El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

3.- ENCARGADOS DE TRATAMIENTO

- ¿Se realiza el tratamiento por persona distinta al responsable del fichero?

  SI

- ¿se ha formalizado mediante contrato conforme a lo establecido en el artículo 12 de la LOPD y artículos 20 a 22 del RLOPD?

  SI

- Si la realización de este encargo se realiza en los locales del responsable ¿se ha hecho constar esta circunstancia en el Documento de Seguridad?,

  SI

- ¿Consta por escrito en el contrato el compromiso del personal del encargado de tratamiento respecto al cumplimiento de las medidas de seguridad recogidas en el Documento de Seguridad del responsable?

  SI

- Cuando el tratamiento se realiza mediante acceso remoto a los sistemas del responsable
  - ¿Se ha establecido alguna limitación a la incorporación de los datos a sistemas o soportes distintos de los del responsable? **SI**

  - ¿se ha hecho constar tal circunstancia en el Documento de Seguridad del responsable?

    SI

- 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?, **ASI SE AFIRMA EN LOS CONTRATOS SE PRESTACION DE SERVICIOS SUSCRITOS CON LOS MISMOS**
  - ¿identifica el fichero o tratamiento y el responsable del mismo?,

    SI
  - ¿detalla las medidas de seguridad a implementar en relación con su tratamiento?

    SI

NIVEL DE CUMPLIMIENTO

Satisfactorio. Se tienen firmados contratos de prestación de servicios que incluyen el contenido establecido en la normativa en cuanto a los accesos por cuenta de terceros.

RECOMENDACIONES

Se recomienda firmar contratos que recojan las obligaciones legales en materia de protección de datos con toda organización externa que tenga acceso a las instalaciones para la prestación de cualquier tipo de servicio. Con aquellos encargados que tengan un acceso a los sistemas informáticos de la entidad o que presten algun tipo de servicios en " la nube" se ha de tener un celo especial a la hora de establecer las obligaciones que deben de cumplir .

LEGISLACION

Artículo 12. Acceso a los datos por cuenta de terceros

1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.
2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.
En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.
3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.
4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

4.-PRESTACIONES DE SERVICIO SIN ACCESO A DATOS PERSONALES

- 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**
- 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 **SI**

NIVEL DE CUMPLIMIENTO

Satisfactorio. Se tienen firmado contratos de prestación de servicios con el contenido establecido en la normativa con aquellas entidades que acceden a las instalaciones para efectuar tareas que no implican acceso a datos personales.

RECOMENDACIONES

Se recomienda firmar contratos que recojan las obligaciones legales en materia de protección de datos con toda organización externa que tenga acceso a las instalaciones para la prestación de cualquier tipo de servicio.

LEGISLACION

Artículo 83. Prestaciones de servicios sin acceso a datos personales.

El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.

Cuando se trate de personal ajeno, **el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto** respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

5.- DELEGACION DE AUTORIZACIONES

- ¿Se han delegado las autorizaciones que el Reglamento atribuye al responsable en otras personas?, **SI**
- ¿se ha hecho constar en el Documento de Seguridad las personas habilitadas para otorgar estas autorizaciones y las personas en quienes recae dicha delegación? **SI**

NIVEL DE CUMPLIMIENTO

Satisfactorio

RECOMENDACIONES

El documento de seguridad debe de recoger los nombres de las personas a las que se les delegan las autorizaciones.

LEGISLACION

Artículo 84. Delegación de autorizaciones.

Las autorizaciones que en este título se atribuyen al responsable del fichero o tratamiento podrán ser delegadas en las personas designadas al efecto. En el documento de seguridad deberán constar las personas habilitadas para otorgar estas autorizaciones así como aquellas en las que recae dicha delegación. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero.

6.-REGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL FICHERO

- El almacenamiento de datos personales en dispositivos portátiles o lo tratamientos fuera de los locales del responsable o del encargado ¿han sido autorizados expresamente por el responsable del fichero?, **SI**
- ¿consta dicha autorización en el Documento de Seguridad? **SI**
- ¿Se garantiza el nivel de seguridad correspondiente al tipo de fichero tratado? **SI**

NIVEL DE CUMPLIMIENTO

Satisfactorio

RECOMENDACIONES

Los dispositivos portátiles deben de contar con contraseñas para proteger la integridad de los datos que guarden.

LEGISLACION

Artículo 86. Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.

1. Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.
2. La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.

7.-FICHEROS TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS

35 17 ¿Cumplen el nivel de seguridad correspondiente? **SI**

35 17 ¿Se han destruido o borrado cuando ya no han sido necesarios para los fines que motivaron su creación? **SI**

NIVEL DE CUMPLIMIENTO

Satisfactorio

RECOMENDACIONES

Las copias de trabajo deben de ser destruidas o borradas tan pronto dejen de ser necesarias

LEGISLACION

Artículo 87. Ficheros temporales o copias de trabajo de documentos.

1. Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda conforme a los criterios establecidos en el artículo 81.
2. Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

8.-FUNCIONES Y OBLIGACIONES DEL PERSONAL

- ¿Están las funciones y obligaciones del personal con acceso a datos de carácter personal y los sistemas de información claramente definidos? **SI**
- ¿Están documentadas y reflejadas en el Documento de Seguridad? **SI**
- ¿Se han definido las funciones de control o autorizaciones delegadas por el responsable del fichero? **SI**
- ¿Están definidas las personas que dentro de la organización se responsabilizan de la política de protección de datos? **SI**
- ¿Conoce el personal las medidas de seguridad que afectan al desarrollo de sus funciones? **SI**
- ¿Conoce las consecuencias de su incumplimiento? **SI**
- ¿El personal de nueva incorporación es formado en esta materia? **SI**
  - Modo **SE LES HACE ENTREGA DE UN COMPROMISO DE CONFIDENCIALIDAD DENTRO DE LOS DOCUMENTOS DE BIENVENIDA A AMICA EN EL QUE SE INFORMA ASI MISMO DE SUS OBLIGACIONES EN LA MATERIA Y DE LA POLITICA EN MATERIA DE SEGURIDAD Y PROTECCION DE DATOS DE LA ENTIDAD.**

NIVEL DE CUMPLIMIENTO

Satisfactorio

RECOMENDACIONES

El personal debe de ser permanentemente formado en esta materia. Se recomienda la realizacion de charlas de refresco entre todo el personal y especialmente en los que tienen acceso a datos a los que deban de aplicarse medidas de seguridad de nivel alto

LEGISLACION

Artículo 89. Funciones y obligaciones del personal.
1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.

También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.
2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

9.-REGISTRO DE INCIDENCIAS.

- ¿Se ha creado un registro de incidencias? **SI**
- ¿Se reflejan en él los siguientes conceptos?: Tipo de incidencia, fecha y hora en que se produjo, persona que notifica la incidencia, persona a quien se le comunica, efectos' derivados de dicha incidencia, procedimientos realizados para anular sus efectos, medidas correctoras adoptadas, persona que ejecuta o supervisa la ejecución del procedimiento, datos restaurados, detalle de los datos recuperados manualmente y otros. Especificar. **SI**
- ¿Existe un procedimiento de notificación y gestión de incidencias de seguridad? **SI**
- ¿El procedimiento está bien diseñado y es eficaz? **SI**
- ¿Conoce todo el personal afectado dicho procedimiento? **SI**
- ¿Existe un registro de incidencias donde se reflejen todos los datos exigidos en el reglamento? **SI**
- ¿Se han registrado todas las incidencias ocurridas? **SI**
- ¿Se revisa periódicamente el registro de incidencias para su análisis y adopción de medidas correctoras de las incidencias anotadas? **SI**
- ¿Se han anotado las ejecuciones de los procedimientos de recuperación de datos realizados? **NO HA SIDO NECESARIO**
- ¿Figuran en estas anotaciones los datos exigidos por el Reglamento? **SI. CUANDO SEA NECESARIO.**
- ¿Existe la autorización por escrito del responsable del fichero para la ejecución de procesos de recuperación de datos? **SI. EXISTE LA PREVISION POR SI RESULTA NECESARIO.**

NIVEL DE CUMPLIMIENTO

Satisfactorio

RECOMENDACIONES

Siempre que se produzca una incidencia debe de documentarse.

LEGISLACION

Artículo 90. Registro de incidencias.

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga 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.

10.-CONTROL DE ACCESO

- ¿Los accesos autorizados de los usuarios se corresponden exclusivamente a los datos y recursos que precisan para el desarrollo de sus funciones? **SI**
- ¿Existen mecanismos que impidan que los usuarios accedan a datos o recursos distintos de los autorizados? **SI**
- ¿Existe una relación de usuarios**? SI**
- ¿Especifica el documento de seguridad que datos y recursos tiene autorizados cada uno de los usuarios**? SI**
- ¿Está actualizada y se mantiene permanentemente actualizada? **SI**
- ¿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? **SI**
- ¿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? **SI**
- El personal ajeno al responsable que tiene acceso a los datos y recursos de éste ¿Se encuentra sometido a las mismas condiciones y obligaciones que el personal propio? **SI**
- ¿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? **SI**
- ¿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? **SI**
- ¿Están cerradas estas áreas mientras no sea preciso el acceso a los documentos incluidos en el fichero? **SI**
- Si los locales del responsable no permiten disponer de un área de acceso restringido ¿Ha adoptado el responsable medidas alternativas? **SI**
- ¿Se ha hecho constar esta circunstancia en el Documento de Seguridad? **SI**
- ¿Se han motivado adecuadamente? **SI**

NIVEL DE CUMPLIMIENTO

Satisfactorio

RECOMENDACIONES

Se han de establecer mecanismos que impidan el acceso por parte de los usuarios a recursos no autorizados. Se ha de ser tan restrictivo como sea posible a la hora de configurar los accesos habida cuenta de que en Amica son muchas las personas con acceso a los sistemas y recursos informaticos, Periodicamente se habrían de delimitar los usuarios y sus perfiles.

LEGISLACION

Artículo 91. Control de acceso.

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.
2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.
5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

11.-GESTION DE SOPORTES Y DOCUMENTOS

- ¿Está identificado el tipo de información contenido en el soporte o documento? **SI**
- ¿Existe un inventario de soportes de salida/entrada de soportes o documentos externos? **SI**

  - ¿Se reflejan los siguientes conceptos para la salida**?: SI**
  - Tipo de soporte o documento
  - fecha y hora en que se produjo
  - el destinatario
  - el número de soportes o documentos
  - el tipo de información que contienen
  - la forma de envío
  - la persona responsable del envío
  - la persona responsable de la entrega (autorizada).
  - ¿Se reflejan los siguientes conceptos para la entrada?: **SI**
  - Tipo de soporte o documento
  - fecha y hora en que se produjo
  - el remitente o emisor
  - el número de soportes o documentos
  - el tipo de información que contienen
  - la forma de envío
  - la persona responsable de la recepción (autorizada).

- ¿Se almacenan los soportes o documentos en lugares de acceso restringido? **SI**
- ¿Existen mecanismos por los que solamente puedan acceder las personas autorizadas en el Documento de Seguridad? **SI**
- ¿Funcionan adecuadamente estos mecanismos? **SI**
- ¿Se ha dejado constancia en el Documento de Seguridad, si fuera el caso de la imposibilidad de cumplir con las obligaciones establecidas en el Reglamento sobre identificación, inventariado y acceso a los soportes dadas sus características físicas? **SI**
- ¿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? **SI**
- ¿Se están tomando las medidas adecuadas en el traslado de documentación para evitar la sustracción, pérdida o acceso indebido durante su transporte? SI
- 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**?** **SI**
- ¿Son adecuadas estas medidas? **SI**

- ¿Se dan de baja en el inventario estos soportes o documentos desechados**? SI**
- 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? **SI**
- ¿Son adecuados y cumplen su finalidad**? SI**
- ¿Se utilizan sistemas de etiquetado que permitan la identificación de su contenido a las personas autorizadas y dificulten su identificación al resto? **SI**
- ¿Son adecuadas y cumplen su finalidad? **SI**
- ¿La distribución de soportes se realiza de forma cifrada o por otro mecanismo que garantice que no sea inteligible o manipulable durante el transporte? **SI**
- ¿Se cifran los datos en los dispositivos portátiles cuando estos salen de las instalaciones del responsable del fichero? **SI**
- 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? **SI**
- ¿Se han adoptado las medidas para minimizar los riesgos derivados de este tratamiento en entornos desprotegidos**? SI**
- ¿Son adecuadas? **SI**
- ¿Se adoptan las medidas que impidan el acceso o manipulación de la información en los casos de traslado físico de la documentación contenida en un fichero? **SI**
- ¿Son apropiadas estas medidas? SI
- La generación de copias o reproducción de documentos ¿Se realiza exclusivamente por el personal autorizado en el documento de seguridad? SI
- ¿Se destruyen las copias o reproducciones desechadas? **SI**
- ¿Se reciben datos a través de soportes informáticos? **SI**
- ¿Son sometidos sistemáticamente a controles antivirus? Especificar procedimiento. **SI. EL ANTIVIRUS LES ANALIZA DE MANERA AUTOMATICA**

NIVEL DE CUMPLIMIENTO

Satisfactorio

RECOMENDACIONES

Deben de adoptarse todo tipo de medidas tendentes a evitar accesos no autorizados en la manipulación de soportes y documentos. Se recomienda el uso de sobres cerrados en el traslado de documentacion.

LEGISLACION

Artículo 92. Gestión de soportes y documentos.

1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad. Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.
2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.
3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.
4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.
5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

12.-IDENTIFICACION Y AUTENTIFICACION

- ¿Existe una relación de usuarios con acceso autorizado? **SI**
- ¿Se mantiene actualizada? **SI**
- ¿Existen procedimientos de identificación y autentificación para dicho acceso**? SI**
- ¿Garantiza la correcta identificación del usuario? **SI**
- El mecanismo de acceso y verificación de autorización de los usuarios ¿Les identifica de forma inequívoca y personalizada**? SI**
- ¿Existe un procedimiento de asignación, distribución y almacenamiento de contraseñas? SI
- ¿Garantiza su confidencialidad e integridad? **SI**
- ¿Se cambian las contraseñas con la periodicidad establecida en el Documento de Seguridad? SI
- ¿Se almacenan las contraseñas de forma ininteligible mientras están en vigor? **SI**
- ¿Se limita el intento reiterado de acceso no autorizado al sistema**? SI**
- ¿Se anotan estos intentos en el registro de incidencias? **SI. SE BLOQUEAN AL QUINTO INTENTO FALLIDO**
- ¿Existe alguna política de creación de contraseñas o se deja a la elección del usuario? **SI SE ESTABLECE UN NUMERO MINIMO DE CARACTERES**

NIVEL DE CUMPLIMIENTO

Satisfactorio

RECOMENDACIONES

El listado de usuarios se ha de mantener permanentemente actualizado. Es conveniente establcer que la duracion de las contraseñas sea inferior a un a.o

LEGISLACION

Artículo 93. Identificación y autenticación.

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.
2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.
3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.

13.-COPIAS DE RESPALDO Y RECUPERACION

- ¿El responsable del fichero ha definido los procedimientos de realización de copias de respaldo y recuperación de los datos**? SI**
- ¿Es adecuada esta definición? **SI**
- ¿Están reflejados estos procedimientos en el Documento de Seguridad? **SI**
- ¿Ha verificado el responsable del fichero la correcta aplicación de estos procedimientos? **SI**
- ¿Realiza esta verificación cada 6 meses? **SE HACE EN CADA COPIA. EL SERVIDOR EMITE UN INFORME Y SE REVISA DIARIAMENTE.**
- ¿Garantizan los procedimientos establecidos la reconstrucción de los datos al estado en que se encontraban antes de producirse la pérdida o destrucción? **SI**
- Si esta pérdida o destrucción afecta a ficheros parcialmente automatizados ¿Se ha procedido a grabar manualmente los datos**? NO HA SIDO NECESARIO**
- ¿Queda constancia motivada de este hecho en el Documento de Seguridad? **SI**
- ¿Se realizan copias de respaldo al menos semanalmente? **SI**
- ¿Las pruebas previas a la implantación o modificación de los sistemas de información se realizan con datos reales**? NO HA SIDO NECESARIO**
- ¿Se hacen copias de seguridad previas a la realización de pruebas con datos reales? **SI**
- ¿Se conserva una copia de respaldo y de los procedimientos de recuperación de datos en lugar diferente al de los equipos que los tratan? **SI**
- ¿Cumple este lugar con las medidas de seguridad exigidas en el reglamento**? SI**

NIVEL DE CUMPLIMIENTO

Satisfactorio

RECOMENDACIONES

Las copias de respaldo deben de realizarse en un soporte extraíble al menos semanalmente y guardarse en lugar distinto a aquel donde se encuentran los sistemas informáticos. Al menos semestralmente se debe comprobar la correcta realización de las mismas. Se recomienda la realizacion de planes de contingencia en los que se lleve a cabo una restauracion completa del sistema, para prevenir errores o fallos de configuracion.

LEGISLACION

Artículo 94. Copias de respaldo y recuperación.

1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.
2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.
3. El responsable del fichero se encargará de 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.
4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad. Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

14.-REGISTRO DE ACCESOS

- ¿Existe el registro de accesos? **NO**
- En caso negativo ¿concurren en el responsable alguna de las circunstancias que le eximen de este requisito? **NO**
- ¿se ha hecho constar en el Documento de Seguridad? **SI**
- ¿Se está recogiendo en este registro la información mínima exigida en el Reglamento? **NO**
- ¿Los mecanismos que permiten el registro de estos accesos están directamente bajo el control del responsable de seguridad? **SI**
- ¿Existe la posibilidad de desactivar estos mecanismos? **NO**
- ¿Se conservan los datos registrados por un período mínimo de dos años? **NO**
- ¿Revisa el responsable de seguridad periódicamente la información registrada? **NO**
- ¿Realiza el responsable de seguridad un informe, al menos mensualmente, con el resultado de las revisiones realizadas y los problemas detectados? **NO**
- ¿El acceso a la documentación se realiza exclusivamente por personal autorizado? **SI**
- ¿Existen mecanismos para identificar los accesos realizados cuando los documentos son utilizados por múltiples usuarios? **NO. ESTAN DEFINIDOS LOS PERFILES CON ACCESO**
- ¿Se ha establecido un procedimiento para registrar el acceso de personas no incluidas en el caso anterior?, **NO SE LES PERMITE EL ACCESO**

NIVEL DE CUMPLIMIENTO

Mejorable. Es recomendable que en tanto sea posible económicamente, que se cambie la aplicación informática actual por otra en la que se establezca un registro de accesos a los datos a los que se les deben de aplicar medidas de seguridad de nivel alto. No obstante se ha sido muy riguroso en la determinación de los perfiles de los usuarios con acceso de modo que solo tienen posibilidad de lectura y modificación un número limitado de personas y lo tienen en función de las necesidades específicas de su puesto de trabajo. Se tiene usar el criterio mas restrictivo posible respecto a la asignacion de perfiles, especialmente para los usuarios que tengan acceso a datos a los que se deban de aplicar medidas de seguridad de nivel alto.. En tanto no se disponga de otra aplicación se velará porque todo el personal con acceso tenga suscritos contratos de confidencialidad y esté obligado por el secreto profesional.

RECOMENDACIONES

Cuando se tratan de manera automatizada datos de carácter personal a los que deben de aplicarse medidas de nivel alto debe de crearse un sistema que registre los accesos en la forma legal y reglamentariamente determinada

LEGISLACION

Artículo 103. Registro de accesos.

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.
6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:
a) Que el responsable del fichero o del tratamiento sea una persona física.
b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.
La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.

15.-ACCESO A TRAVES DE REDES DE TELECOMUNICACIONES

Los accesos a datos mediante redes de comunicaciones ¿garantizan un nivel de seguridad equivalente a los accesos en modo local?

ACCESO A DATOS A TRAVÉS DE REDES EXTERNAS A LA LAN (Internet, VPN u otras WAN)

- ¿Hay accesos a los datos a través de redes de comunicaciones externas a la LAN? **S**I
- Si es afirmativo:
- ¿Se autentica al usuario en el acceso? **SI CON LAS MISMAS GARANTIAS QUE CUANDO EXISTEN ACCESOS LOCALES.**
- ¿Se transmiten datos personales a través de redes de telecomunicaciones? **NO ES FRECUENTE**
- En caso afirmativo: ¿se cifran los datos o se utiliza un mecanismo que garantice que la información no sea inteligible ni manipulable por terceros? **SOLAMENTE SE CIFRAN SI A ESTOS DATOS SE LES DEBEN APLICAR MEDIDAS DE SEGURIDAD DE NIVEL ALTO Y SIEMPRE QUE TECNICAMENTE EXISTA ESA POSIBILIDAD SE ENVIAN ENCRIPTADOS CON CONTRASEÑA.**

TRANSMISIÓN DE DATOS A TRAVÉS DE REDES DE TELECOMUNICACIONES

- ¿Se utiliza algún otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros? **SI**
- En caso afirmativo, descripción de los mecanismos. **SOLAMENTE SE CIFRAN SI A ESTOS DATOS SE LES DEBEN APLICAR MEDIDAS DE SEGURIDAD DE NIVEL ALTO Y SIEMPRE QUE TECNICAMENTE EXISTA ESA POSIBILIDAD**

ACCESO A INTERNET

- ¿Existe conexión a Internet? Analógica, ADSL, RDSI, cable módem, inalámbrica (satélite, otros). **SI**
- ¿Tienen todos los usuarios acceso a Internet? **SI**
- ¿Es un acceso restringido? **SI**
- ¿Existe política de seguridad para el uso de Internet? **SI**
- ¿Son conocidas por el personal? ¿De qué manera se difunde? **SI SE ENTREGO UN DOCUMENTO EN EL QUE SE PROHIBE EL USO DE ESTA HERRAMIENTA PARA FINES PARTICULARES O NO RELACIONADOS CON EL TRABAJO**
- ¿Existen sanciones ante su incumplimiento? **SI**
- ¿Se imparte periódicamente formación al respecto? **SI**
- ¿Tienen acceso a Internet los equipos que almacenan información de carácter personal? **SI**

NIVEL DE CUMPLIMIENTO

Satisfactorio

RECOMENDACIONES

El uso de las herramientas informáticas debe de circunscribirse a temas laborales.

LEGISLACIONI

Artículo 85. Acceso a datos a través de redes de comunicaciones.

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 80.

16.-AUDITORIA.

I

- ¿Se realiza la actual auditoría en el plazo establecido desde la anterior? **SI**
- 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? **SI**
- ¿Los informes de las auditorías anteriores incluían los datos, hechos y observaciones en los que se basaban sus dictámenes**? SI**
- ¿Se han implementado las medidas correctoras propuestas por auditorías anteriores? **SI**
- ¿Han sido eficaces y han corregido las deficiencias encontradas? **SI**

NIVEL DE CUMPLIMIENTO

Satisfactorio

RECOMENDACIONES

Se ha de realizar auditoría con la periodicidad establecida en la norma o siempre que se produzcan cambios sustanciales

LEGISLACION

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 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 señalado en el párrafo anterior.
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 las 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.

17.- MEDIDAS APLICABLES A LOS FICHEROS NO AUTOMATIZADOS.

El presente cuestionario tiene por objeto recabar información sobre las medidas de seguridad aplicables específicamente para ficheros no automatizados.

1. CRITERIOS DE ARCHIVO .
   - ¿Qué legislación es aplicable? **NO EXISTE UNA LEGISLACION ESPECIFICA, SALVO POR AFINIDAD LA SANITARIA**
   - En caso de que no sea aplicable ninguna legislación referente al archivo de la documentación, ¿cuál es el criterio y procedimiento de actuación que sigue? **LA DOCUMENTACION SE ARCHIVA SIGUIENDO CRITERIOS CONTABLES , Y DE MANERA CRONOLOGICA Y ALFABÉTICA**

2. DISPOSITIVOS DE ALMACENAMIENTO
   - ¿Qué mecanismos impiden el acceso a la documentación y garantizan la imposibilidad de acceso al lugar de archivo? **SALAS, FICHEROS Y ARCHIVADORES CERRADOS CON LLAVE A LAS QUE SOLO TIENEN ACCESO UN NUMERO CONOCIDO Y LIMITADO DE PERSONAS AUTORIZADAS.**

3. CUSTODIA
   - Con carácter previo al archivo de la documentación, ¿qué medidas se toman para evitar que personas sin autorización puedan acceder a dichos documentos? **LOS DOCUMENTOS SIEMPRE PERMANECEN BAJO CUSTODIA DE PERSONAL AUTORIZADO**

4. ALMACENAMIENTO DE LA INFORMACIÓN

   Los armarios, archivadores u otros mecanismos que se utilicen para el archivo:
   - ¿están situados en áreas de acceso protegido**?, SI**
   - ¿cuentan con sistema de apertura con llave o dispositivos equivalentes?, **SI**
   - ¿están cerradas mientras no es necesario el acceso? **SI**

5. COPIA O REPRODUCCIÓN
   - ¿Se controla la realización de copias de la documentación? **SI**
   - ¿Cómo? **SE HA PROHIBIDO AL PERSONAL LA REALIZACION DE COPIAS NO AUTORIZADAS**
   - ¿Qué mecanismos se utilizan para la destrucción de las copias una vez que han sido utilizadas de tal forma que se impida su recuperación posterior? **DESTRUCTORA DE PAPEL**

6. ACCESO A LA DOCUMENTACIÓN
   - ¿Existe un listado de personas autorizadas a acceder a la información? **SI**

7. TRASLADO DE LA DOCUMENTACIÓN
   - ¿Qué medidas se adoptan para evitar la pérdida, alteración o acceso no autorizado durante el traslado de documentos? **CUSTODIA DE LA DOCUMENTACION EN DISPOSITIVOS CERRADOS.**

NIVEL DE CUMPLIMIENTO

Satisfactorio

RECOMENDACIONES

Se debe de instruir a todo el personal que tenga acceso a documentos que contengan datos de carácter personal en que debe de adoptar medidas que eviten la alteración, perdida o acceso no autorizado a los mismos.

LEGISLACION

Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados
SECCIÓN 1. ª MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO

Artículo 105. Obligaciones comunes.
1. Además de lo dispuesto en el presente capítulo, a los ficheros no automatizados les será de aplicación lo dispuesto en los capítulos I y II del presente título en lo relativo a: a) Alcance. b) Niveles de seguridad. c) Encargado del tratamiento.
d) Prestaciones de servicios sin acceso a datos personales. e) Delegación de autorizaciones. f) Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento. g) Copias de trabajo de documentos. h) Documento de seguridad.
2. Asimismo se les aplicará lo establecido por la sección primera del capítulo III del presente título en lo relativo a:
a) Funciones y obligaciones del personal. b) Registro de incidencias. c) Control de acceso) Gestión de soportes.

Artículo 106. Criterios de archivo.
El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.
En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

Artículo 107. Dispositivos de almacenamiento.
Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura.
Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

Artículo 108. Custodia de los soportes.
Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

SECCIÓN 2. ª MEDIDAS DE SEGURIDAD DE NIVEL MEDIO

Artículo 109. Responsable de seguridad.

Se designará uno o varios responsables de seguridad en los términos y con las funciones previstas en el artículo 95 de este reglamento.

Artículo 110. Auditoría.

Los ficheros comprendidos en la presente sección se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

SECCIÓN 3. ª MEDIDAS DE SEGURIDAD DE NIVEL ALTO

Artículo 111. Almacenamiento de la información.

1. Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.
2. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.

Artículo 112. Copia o reproducción.

1. La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.
2. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Artículo 113. Acceso a la documentación.

1. El acceso a la documentación se limitará exclusivamente al personal autorizado.
2. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.
3. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

Artículo 114. Traslado de documentación.

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

18 CALIDAD DE LOS DATOS

¿Solamente se recogen de los interesados los datos pertinentes, necesarios y no excesivos? **SI**
¿Los datos recogidos únicamente se usan para finalidades determinadas, explicitas y legitimas? **SI**
¿Los datos recogidos son permanentemente actualizados? **SI**
¿Responden los datos almacenados a la situación actual del interesado? **SI**
¿Se cancelan los datos cuando dejan de ser necesarios, pertinentes u oportunos? **SI**
¿Qué procedimientos de cancelación se emplean? **DESTRUCCION FISICA DE LA DOCUMENTACION EN FORMATO PAPEL Y BORRADO DE ALTO NIVEL PARA LOS DATOS ALMACENADOS EN SOPORTES AUTOMATIZADOS**
¿Se almacenan los datos de manera que se permitan los ejercicios de los derechos de acceso, rectificación, cancelación y oposición dentro de los plazos legalmente establecidos? **SI**
¿Se recogen datos por medios fraudulentos? **NO**

NIVEL DE CUMPLIMIENTO

Satisfactorio

RECOMENDACIONES

Se deben de mantener los datos siempre que sea pertinente, procediendo a su cancelación al término de los plazos legal o reglamentariamente establecidos. Nunca se deben de emplear los datos para finalidades distintas y se deberán de mantener permanentemente actualizados.

LEGISLACION

Artículo 4. Calidad de los datos.
1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.
2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.
3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.
4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.
5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.
Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los

valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.
6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.
7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

19 INFORMACION A LOS INTERESADOS

¿Se informa a los interesados conforme establece el artículo 5 de la LOPD? **SI**
¿Se incluyen en los formularios clausulas de información al interesado? **SI**
¿Si no existen formularios u otros documentos se informa al interesado por otros medios? **SI**

NIVEL DE CUMPLIMIENTO

Satisfactorio

RECOMENDACIONES

Siempre que existan formularios o documentos que se entreguen a los interesados o deban ser firmados por ellos deberán de incluirse clausulas con el contenido mínimo establecido en la LOPD

Se establece como recomendacion la obligacion de revisar las condiciones de la página web y la politica de cookies. Se revisaran tambien las clausaulas para la solicitud de contacto, y en las ofertas de empleo.

LEGISLACION

Artículo 5. Derecho de información en la recogida de datos.
1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:
a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.
....
2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.
3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.
4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.
5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.
Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

20 OBTENCION DEL CONSENTIMIENTO

¿Es correcta la obtención del consentimiento de los interesados al tratamiento de sus datos personales? **SI**
¿Se guarda prueba de la existencia de dicho consentimiento? **SI**
¿Los formularios u otros documentos incorporan clausulas especificas para obtener el tratamiento de los datos personales de los interesados, si es necesario? **SI**

NIVEL DE CUMPLIMIENTO

Satisfactorio

RECOMENDACIONES

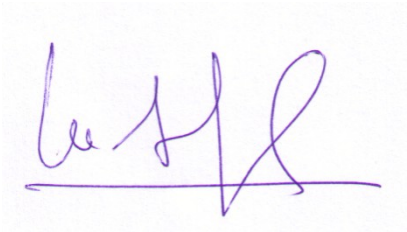
Siempre que existan formularios o documentos que se entreguen a los interesados o deban ser firmados por ellos deberán de incluirse clausulas para obtener el consentimiento de los mismos.

LEGISLACION

Artículo 6. Consentimiento del afectado.
1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.
2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.
3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.
4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado

CONCLUSION FINAL

Conforme a la información facilitada por la entidad AMICA y en los puntos que se mencionan en este informe de auditoría se concluye que esta cumple con la normativa de protección de datos establecida en la Ley 15/1999 de protección de datos de carácter personal y el reglamento RD 1720/2007 de desarrollo de la misma



Fdo.: Luis Ángel González Pérez
Abogado
Auditor LOPD

En Torrelavega a 3 de Enero de 2015