



REGLAMENTO DE MEDIDAS DE SEGURIDAD DE LOS FICHEROS AUTOMATIZADOS QUE CONTENGAN DATOS DE CARACTER PERSONAL DEL ILMO. AYUNTAMIENTO DE PINTO.

1.- EXPOSICION DE MOTIVOS.

1.1.- JUSTIFICACION /ADECUACION LEGAL.

El art. 18.,4 de la Constitución Española establece que "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

La Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de carácter personal prevé en su art. 9, la obligación del responsable del fichero de adoptar las medidas de índole técnica y organizativas que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural, estableciéndose en el artículo 43.3 h) que mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen, constituyen infracción grave en los términos previstos en la propia Ley.

1.2.- OBJETO.

El presente documento de Seguridad tiene por objeto el desarrollo de lo dispuesto en el art. 9 de la Ley Orgánica y el art. 10 del Reglamento de Medidas de Seguridad de la Agencia de Protección de Datos, determinando las medidas de índole técnica y organizativa que garanticen la confidencialidad e integridad con la finalidad de preservar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos personales. De acuerdo con éste criterio, no se tratan las medidas relativas a la pérdida de los datos de carácter personal en tanto no supongan un menoscabo de los derechos constitucionalmente protegidos.

Las medidas de seguridad que se establecen se configuran como las básicas de seguridad que han de cumplir todos los ficheros que contengan datos de carácter personal, estableciendo también las medidas especiales de nivel medio y alto, para ficheros que por la especial naturaleza de los datos que contienen o por las propias características de los mismos exigen un grado de protección mayor.





2.- DISPOSICIONES GENERALES.-

2.1.- AMBITO DE APLICACION Y FINES.

El presente documento tiene por objeto establecer las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los Centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal sujetos al régimen de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

2.2.. DEFINICIONES.-

A efectos del presente documento, se entenderá que las definiciones a los siguientes conceptos son:

SISTEMA DE INFORMACION: Conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

USUARIO: sujeto o proceso autorizado para acceder a datos o recursos.

RECURSO: Cualquier parte componente de un sistema de información.

ACCESOS AUTORIZADOS: Autorizaciones concedidas a un usuario para la utilización de los diversos recursos.

IDENTIFICACION: Procedimiento de reconocimiento de la identidad de un usuario.

AUTENTICACION: Procedimiento de comprobación de la identidad de un usuario.

CONTROL DE ACCESO: Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

CONTRASEÑA: Información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.

INCIDENCIA: Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.





SOPORTE: Objeto físico susceptible de ser tratado en un sistema informático y sobre el cual se puede grabar o recuperar datos.

RESPONSABLE DE SEGURIDAD: Persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

COPIA DE RESPALDO: Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

2.3.- NIVELES DE SEGURIDAD. GENERALIDADES.-

Las medidas de seguridad exigibles se clasifican en tres niveles: básico, medio y alto .

Dichos niveles se establecen atendiendo a la naturaleza de la información tratada , en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

a. APLICACION DE LOS NIVELES DE SEGURIDAD.

Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico.

Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos ficheros cuyo funcionamiento se rija por el artículo 28 de la Ley Orgánica 5/1992, deberán reunir , además de las medidas de nivel básico , las calificadas como de nivel medio.

Los ficheros que contengan datos de ideología, religión, creencias. origen racial, salud o vida sexual así como los que contengan los datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas como de nivel alto.

Cuando los ficheros contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo deberán garantizar las medidas de nivel medio establecidas en el apartado 2.3.2. del presente Documento.

Cada uno de los niveles descritos anteriormente tiene la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes.





b. ACCESO A DATOS A TRAVES DE REDES DE COMUNICACION.

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

c. REGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACION DEL FICHERO.

La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por el responsable del fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

d. FICHEROS TEMPORALES.

Los ficheros temporales deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios establecidos en el presente Documento.

Todo fichero temporal será borrado una vez que haya dejado de ser necesario para los fines que motivaron su creación.

2.3.1.- MEDIDAS DE SEGURIDAD DE NIVEL BASICO.

a.- DOCUMENTO DE SEGURIDAD.

El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

El contenido del documento deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

b. FUNCIONES Y OBLIGACIONES DEL PERSONAL.

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas de acuerdo con lo previsto en el artículo 8.2.c).





Será obligación del personal:

1. Cambiar la clave de acceso al sistema , según los plazos establecidos o cuando lo requiera el Departamento de Informática.

2.- No se realizará copias ni notificaciones de los datos con los que el personal trabaja.

3.- Comunicará todas las incidencias con los ficheros automatizados al Departamento de informática.

4.- No deberá comunicar la clave de acceso a ninguna persona.

5.- No deberá instalar ningún tipo de software que no haya sido autorizado previamente por el Departamento de Informática.

El responsable del fichero adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

c. REGISTRO DE INCIDENCIAS.

El procedimiento de notificación y gestión de incidencias contendrá necesariamente un registro en el que se haga constar el tipo de incidencia , el momento en que se ha producido, la persona que realiza la notificación , a quien se le comunica y los efectos que se han derivado de la misma.

d. IDENTIFICACION Y AUTENTICACION.

El responsable del fichero se encargará de que exista una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso.

Cada usuario dispondrá de un login de entrada al sistema con una contraseña asociada.

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.





Las contraseñas se cambiarán mensualmente y mientras estén vigentes se almacenarán de forma ininteligible.

Se limitará a tres veces la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

e. CONTROL DE ACCESO.

Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a información o recursos con derechos distintos de los autorizados.

Existirá una relación de usuarios que contendrá el acceso autorizado para cada uno de ellos.

Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos conforme a los criterios establecidos por el responsable del fichero.

f. GESTION DE SOPORTES.

Los soportes informatizados que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.

La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizada por el responsable del fichero previa consulta y autorización del Secretario, Comisión de Gobierno o Alcalde.

g. COPIAS DE RESPALDO Y RECUPERACION.

El responsable del fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.





Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberán garantizar su reconstrucción en el estado en el que se encontraban al tiempo de producirse la pérdida o destrucción.

Deberán realizarse copias de respaldo:

1. Diariamente
2. Mensualmente
3. Anualmente
4. Cuando se produzca un cierre o apertura contable
5. En cualquier momento en que el responsable del sistema considere oportuno.

h. AUDITORIA INTERNA.

Existirá un fichero de incidencias que reflejará el día, hora y usuario que realizó la operación.

i. PROTECCION DE FICHEROS Y SERVIDORES.

Los ficheros y soportes magnéticos estarán protegidos con armarios ignífugos. La sala donde se encuentran los servidores y equipos informáticos estará protegida con cámara de seguridad.

2.3.2. MEDIDAS DE SEGURIDAD DE NIVEL MEDIO.

a. RESPONSABLE DE SEGURIDAD

El responsable del fichero asignará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero de acuerdo con este Documento.

b. AUDITORIA.

Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del presente Documento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos cada dos años.

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente Documento, identificar sus deficiencias y proponer las medidas





correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basan los dictámenes alcanzados y recomendaciones propuestas.

Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedarán a disposición de la agencia de Protección de Datos.

c. CONTROL DE ACCESO FISICO.

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal.

d. GESTION DE SOPORTES.

Deberá establecerse un sistema de registro de entrada de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

Igualmente se dispondrá de un sistema de registro de salida de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes, el tipo de información que contiene, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán, las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario.

Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

e . REGISTRO DE INCIDENCIAS.

Deberá especificarse los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en si caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.





Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

f. PRUEBAS CON DATOS REALES.

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 tipo de fichero tratado.

2.3.3.- MEDIDAS DE SEGURIDAD DE NIVEL ALTO.

a. DISTRIBUCION DE SOPORTES.

La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

b. REGISTRO DE ACCESOS.

De cada 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.

En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

Los mecanismos que permiten el registro de los datos detallados en los párrafos anteriores, estarán bajo el control directo del responsable de seguridad competente sin que se deba permitir, en ningún caso, la desviación de los mismos.

El periodo mínimo de conservación de los datos registrados será de dos años.

El responsable de seguridad competente se encargará de revisar periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes.

c. COPIAS DE RESPALDO Y RECUPERACION.

Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquel en que se encuentren los equipos informáticos





que los tratan, cumpliendo en todo caso, las medidas de seguridad exigidas en éste Documento.

d. TELECOMUNICACIONES.

La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

3.- INFRACCIONES Y SANCIONES.

El incumplimiento de las medidas de seguridad descritas en el presente Documento será sancionado de acuerdo a lo establecido en los artículos 43 y 44 de la Ley orgánica 5/1992, cuando se trate de ficheros de titularidad privada.

El procedimiento a seguir para la imposición de la sanción a la que se refiere el párrafo anterior será el establecido en el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

Cuando se trate de ficheros de los que sean responsables las Administraciones Públicas se estará, en cuanto al procedimiento y las sanciones, a lo dispuesto en el artículo 45, de la Ley Orgánica 5/1992.

3.1.- RESPONSABLES.

Los responsables de los ficheros, sujetos al régimen sancionador de la Ley Orgánica 5/1992, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos con carácter personal en los términos establecidos en el presente documento.

4.- COMPETENCIAS DEL DIRECTOR DE LA AGENCIA DE PROTECCION DE DATOS.

El Director de la Agencia de Protección de datos, de conformidad con lo establecido en el artículo 36 de la Ley Orgánica 5/1992, podrá:





- Dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos automatizados a los principios de la Ley Orgánica 5/1992.

- Ordenar la cesación de los tratamientos de datos de carácter personal y la cancelación de los ficheros cuando no se cumplan las medidas de seguridad previstas en el presente documento.

4.1.- PLAZOS DE IMPLANTACION DE LAS MEDIDAS.

En el caso de sistemas de información que se encuentren en funcionamiento a la entrada en vigor del presente Documento, las medidas de seguridad de nivel básico previstas en el presente Documento deberán implantarse en el plazo de seis meses desde la entrada en vigor, las del nivel medio en el plazo de un año y las del nivel alto en el plazo de dos años.

Cuando los sistemas de información que se encuentren en funcionamiento no permitan tecnológicamente la implantación de algunas de las medidas de seguridad previstas en el presente Documento, la adecuación de dichos sistemas y la implantación de las medidas de seguridad deberán realizarse en el plazo máximo de tres años a contar desde la entrada en vigor del presente Documento.

5.- REFERENCIA A TEXTOS LEGALES.

Ley Orgánica 5/1992 de 29 de octubre, de Regulación del Tratamiento automatizado de Datos de carácter personal (LORTAD).

Real Decreto 994/1999 de 11 de Junio por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

NOTAS.-

APROBADO PROVISIONALMENTE EN PLENO 26.1.2000

PUBLICADO ANUNCIO EN BOCM EL 21.2.2000

PUBLICACION INTEGRAL BOCM 13.4.2000

ENTRADA EN VIGOR 29.4.2000



