RELACIÓN DE MEDIDAS DE SEGURIDAD APLICABLES EN LA EMPRESA

Objetivo

El objetivo de este documento es servir de guión para verificar el cumplimiento de los procedimientos e instrucciones que la normativa vigente en materia de protección de datos hace de obligado cumplimiento por parte del Responsable del Fichero.

A través de la relación de Medidas de Seguridad que son aplicativas según los niveles de datos de carácter personal tratados por la empresa, así como la distinción de los soportes informatizados o documentales, este documento será de ayuda para la adecuación de dichas medidas y controles de seguridad obligatorios, se definirán posibles **deficiencias a fin que el Responsable del Fichero y el Responsable de Seguridad identifiquen los problemas detectados en la empresa y a través de propuestas y explicaciones prácticas, será de fácil aplicación las correcciones o implementaciones de estas medidas de seguridad.**

La obligación general de adoptar las medidas de seguridad necesarias para garantizar que los datos están protegidos frente a posibles incidencias viene dada por el artículo 9 de la L.O.P.D., que obliga al responsable del fichero a adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado. Esta distinción entre medidas de índole técnica y organizativa nos hace pensar en que la implantación real de un sistema de protección de datos afectará tanto a los sistemas de información utilizados en el tratamiento de información como la organización del personal en el uso de esa información para el desarrollo de las funciones de su cargo.

Las obligaciones concretas vienen definidas a partir de Real Decreto 1720/2007 de 21 de diciembre, mediante el que se aprueba el **Reglamento de Medidas de Seguridad aplicables a Ficheros Automatizados y No Automatizados** que Contengan Datos de Carácter Personal (el llamado Reglamento de Seguridad). El Reglamento de Seguridad tiene por objeto establecer estas 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.

Niveles de seguridad

Las medidas de seguridad se clasifican en **tres niveles** dependiendo del tipo de datos que traten: *básico, medio y alto*.

Dichos niveles se establecen atendiendo a la naturaleza de la información tratada y en su caso, de las finalidades de los ficheros o tratamientos de datos de carácter personal en relación con la mayor o menor necesidad de garantizar la confidencialidad, integridad y/o disponibilidad de la información.

Cada uno de los niveles descritos tiene una condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el Responsable de Fichero.

Además, dichas medidas son acumulativas, es decir, los ficheros que contengan datos de nivel alto deberán cumplir las medidas de nivel alto además de las de nivel medio y bajo.

Definiciones previas

A efectos de este reglamento, se entenderá por:

a) ***Sistema de información:*** conjunto de ficheros, tratamientos, programas, soportes y en su caso equipos empleados para el tratamiento de datos de carácter personal.

b) ***Sistema de tratamiento:*** modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

c) ***Recurso:*** cualquier parte componente de un sistema de información.

d) ***Usuario:*** sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

e) ***Accesos autorizados:*** autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.

f) ***Perfil de usuario:*** accesos autorizados a un grupo de usuarios.

g) ***Identificación:*** procedimiento de reconocimiento de la identidad de un usuario.

h) ***Autenticación:*** procedimiento de comprobación de la identidad de un usuario.

i) ***Control de acceso:*** mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

j) ***Ficheros temporales:*** ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

k) ***Contraseña:*** información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.

l) ***Incidencia:*** cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

m) ***Soporte:*** objeto físico que almacena o contiene datos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

n) ***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.

o) ***Copia de respaldo:*** copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

p) ***Documentación:*** todo escrito, señal, grafico, sonido, dibujo, película, fotografía, cinta magnética, cinta mecanográfica, casete, disco, CD, DVD, dispositivos externos de almacenamiento u otro medio físico en el que se haya registrado información.

q) ***Transmisión de documentos:*** cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

Destinatario

El presente documento deberá ser estudiado e implantado por el Responsable de Fichero o Tratamiento y el Responsable de Seguridad para que se adopten las medidas correctoras adecuadas, ya que en virtud del artículo 9 de la Ley Orgánica 15/99 de Protección de datos, *"El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias 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".*

Niveles de Seguridad

Lo primero que deberá hacer el Responsable del Fichero y el de Seguridad, es conocer qué nivel de seguridad es el aplicativo según los datos de carácter personal que se traten en la empresa.
Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.

1. DATOS DE NIVEL BÁSICO: Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico. Es decir, por el mero hecho de ser un dato que identifica o puede identificar a una persona física ya le serán de aplicación las medidas descritas para el nivel básico de seguridad. Cualquier dato quedará incluido: nombre, apellido, teléfono, dirección, matrícula de vehículo, números de cuenta, números de referencia en un expediente, imagen, voz, huella dactilar, correo electrónico que puede identificarle, etc.

2. DATOS DE NIVEL MEDIO: Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:

- Los relativos a la comisión de infracciones administrativas o penales.
- Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre, es decir, los destinados a una prestación de servicios de información sobre solvencia patrimonial y crédito.
- Los datos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.
- De los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.
- De los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias.
- De los que sean responsables las Mutuas de Accidentes de Trabajo y enfermedades profesionales de la Seguridad Social.

- Los conjuntos de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

3. DATOS DE NIVEL ALTO: Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

- Los datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
- Los datos recabados para fines policiales sin consentimiento de las personas afectadas.

Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

También es necesario remarcar que en el caso de que en un sistema de información existan ficheros o tratamientos que requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación el nivel de medidas de seguridad correspondiente siempre que puedan delimitarse los datos y los usuarios que tengan acceso a los mismos. Si no fuera así, será de aplicación el sistema de seguridad del nivel más elevado.

A continuación citamos cada una de las medidas que establece el Reglamento de Seguridad, distinguiendo entre las medidas que afectan al tratamiento automatizado de información de las que afectan al tratamiento no automatizado o documental de la información, y dentro de las mismas, los tres niveles de seguridad existentes.

MEDIDAS DE SEGURIDAD OBLIGATORIAS PARA FICHEROS AUTOMATIZADOS

NIVEL BASICO

Documento de Seguridad

El Documento de seguridad tendrá el carácter de documento interno de la organización. 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.

Funciones y obligaciones del personal

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.

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.

Las obligaciones de los usuarios están recogidas en el Documento de seguridad. Además, se distribuye a todos los usuarios con acceso a datos, la normativa de la empresa, ***Usos y Recomendaciones***, que comprende todas las obligaciones que les pueden afectar.

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.

RESPONSABLE DEL FICHERO, dispone de los formularios para el caso de incidencias en el sistema de tratamiento de la información, a través del **Anexo F de *Procedimiento de Notificación y gestión de incidencias.***

Control de acceso

Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones. 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. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

Se aconseja, a fin de mantener una política de accesos a la información correcta, lo siguiente:

- Fijar control de accesos, autenticación y validación para el servidor. De esta manera, se impedirán los accesos no consentidos al servidor y se protegerá de manipulaciones la configuración de la red, en la cual se habrán determinado diferentes accesos dependiendo de los perfiles del personal.
- Además, debe fijarse un control de entrada a los equipos, para que cada usuario valide su entrada en su PC o en aquellos equipos de uso compartido.

En definitiva, dependiendo del usuario y su contraseña, se tendrá acceso a una determinada información, de manera que si toda la gestión de la información se almacena en la red, ya se habrán controlado los accesos mediante el servidor, pero di además, cada usuario mantiene información confidencial en su PC, se deberá llevar una política de passwords también en estos.

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, que es el supuesto en el que nos encontramos en RESPONSABLE DEL FICHERO.

Gestión de soportes y documentos

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. 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.

Identificación y autenticación

El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios. 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. 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.

Deber reproducirse aquí lo mencionado en el apartado **Control de acceso** en cuanto al sistema de identificación y autenticación correcto en cuanto a la información contenida en el servidor y en los PC's, pero también pueden existir otras formas de autenticación, como puede ser el uso de datos biométricos.

Debe tenerse en cuenta también una correcta política de actualización de contraseñas y de bloqueo de salvapantallas que no permita los accesos por personas distintas al usuario de del PC.

Copias de respaldo y recuperación

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. 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.

En el **Anexo G** encontramos las herramientas suficientes e idóneas para instrumentalizar toda la información necesaria para el correcto registro del Procedimiento de Respaldo y Recuperación y del Procedimiento de gestión de copias de seguridad y soportes.

NIVEL MEDIO

Responsable de Seguridad

En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciado según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad. En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

En el **Anexo E** ***Nombramientos y Autorizaciones*** han quedado nombrados todos los responsables que en materia de Protección de datos existen en la empresa. Una persona puede ostentar más de una responsabilidad, así como alguna de ellas puede quedar repartida entre dos o más personas.

Auditoría

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. 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.

En la Implantación encontramos un apartado diferenciado y autónomo para el control de Auditorías y modificaciones instrumentalizadas a través de las mismas.

Gestión de soportes y documentos

En virtud del Reglamento de seguridad, se deberá establecer un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo 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 entrada y salida de soportes informáticos que deberán estar previamente inventariados a fin de controlar las entradas y salidas de soportes, debiendo estar, en todo caso, identificados así como autorizado cualquier flujo de información por parte del Responsable del fichero.

En el RESPONSABLE DEL FICHERO cualquier salida de datos en soporte automatizado se registra en los formularios que se entregan junto con el resto de documentación de la Implantación de protección de datos llevada a cabo, estos formularios se procuran a través de los **Anexos G.3 y G. 4.**

Igualmente, se dispone de un inventario de todos los soportes técnicos que existen en la empresa, que se irá actualizando anualmente o bien, cuando lo estime pertinente el Responsable de Seguridad por haber introducido modificaciones sustanciales en la empresa. El **Anexo B de *Estructura informática y equipamiento* nos facilita este registro y control.**

Identificación y autenticación

El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Además de lo señalado para el Nivel Básico en cuanto a Control de Accesos y Control de Identificación y autenticación, en el Nivel Medio el RESPONSABLE DEL FICHERO debe tener configurado el bloqueo de cuenta en caso de reiterados intentos de acceso erróneos, a fin de preservar el sistema de contraseñas para la entrada en los equipos y sistemas informáticos e impedir la entrada aleatoria a los mismos. Se propone el bloqueo a los 5 intentos.

Control de acceso físico

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de Información. En el caso en que el personal de visita no sea el autorizado, se llevará un libro de registro de visitas en el que se legitima el acceso a los lugares donde existen datos.

La norma fundamental es que personal no autorizado pueda acceder a los sistemas o los equipos pudiendo dañarlos o manipularlos externamente. Por eso, debe controlarse que las personas ajenas a la empresa puedan entrar en los lugares de trabajo donde se encuentran los equipos informáticos, sin ir acompañadas de personal autorizado.

Registro de Incidencias

En el registro regulado en el artículo 90 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

En la Implantación se contempla esta opción en las hojas de incidencias existentes para los datos de nivel Medio.

NIVEL ALTO

Gestión y distribución de soportes

Los soportes que almacenen datos de carácter personal de nivel alto, se deberán identificar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a identificar su contenido, y dificultando la identificación para el resto

de personas. Asimismo, cuando dichos soportes se tengan que distribuir o cambiar de lugar, deberán cifrarse los datos para que estos no sean accesibles ni manipulados.

Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.

Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

Copias de respaldo y recuperación

Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

La empresa debe mantener una política de copias de seguridad sobre toda la información, incluyendo la de nivel alto, para garantizar su conservación. Esta política quedará fijada en el **Anexo G.1 y G.2** dentro de los ***Procedimientos de Control y Seguridad*.**

Registro de Accesos

De cada intento de acceso o acceso autorizado deberá guardarse, 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.

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. Dichos mecanismos permitirán la conservación de los datos registrados de dos años, como mínimo.

Telecomunicaciones

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

MEDIDAS DE SEGURIDAD OBLIGATORIAS PARA FICHEROS DOCUMENTALES

NIVEL BASICO

Criterios de archivo

Los criterios del archivo 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.

El RESPONSABLE DEL FICHERO, debe cumplir con las medidas de seguridad en el control de los accesos a los archivos documentales, independientemente de si existe un único archivo para todos los departamentos de la empresa, ubicado en un despacho diferenciado o bien esté desgranado en diferentes departamentos o salas.

La norma básica es que la documentación almacenada en cada uno de los despachos o departamentos se corresponda con la necesaria para las funciones del personal de ese departamento, sólo el personal autorizado debe acceder a la documentación.

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.

Para los archivos en papel debe disponerse de armarios archivadores y cajones que se puedan cerrar bajo llave. En el caso de los expedientes de trabajo diario, que se encuentre en los departamentos en horario laboral, es recomendable evitar que queden expedientes documentales fuera de los armarios de los despachos al final de la jornada, volviendo a estar todo dentro de armarios y bajo llave.

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.

Se recomienda tener en cuenta los siguientes aspectos:

a. Proteger la información en papel cuando se abandona el puesto de trabajo.
b. Proteger los puntos de correo, envío de fax, fotocopiadoras, escáner, etc.
c. Recoger de forma inmediata los documentos impresos o enviados por fax confidenciales y con información personal.

Esta serie de medidas figuran en la normativa que se distribuye entre los empleados.

NIVEL MEDIO

Responsable de seguridad: ídem que en el tratamiento automatizado

Auditoria: ídem que en el tratamiento automatizado

NIVEL ALTO

Almacenamiento de la información

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.

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.

Esta medida se debe intensificar a la finalización de la jornada laboral diaria.

Copia o reproducción

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 o, en su defecto, por el Responsable de Seguridad. No deben permitirse las copias no autorizadas e indiscriminadas de expedientes con información de nivel alto.

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, por algún método que nos certifique su inexistencia o imposibilidad de recuperación. Esto puede ser desde una máquina destructora de papel, para pequeños volúmenes, o bien mediante la contratación con alguna empresa de recogida y destrucción de documentos, que nos certifican su efectiva destrucción.

Acceso a la documentación

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

Traslado de la 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.

MEDIDAS ADICIONALES RECOMENDADAS (derivadas de resoluciones AGPD)

Muchas de ellas ya serán, seguramente, tenidas en cuenta en el RESPONSABLE DEL FICHERO, y, si bien, no son exigidas expresamente por la normativa vigente, son rutinas o sistemas que favorecen a la confidencialidad de los datos y al tratamiento legítimo de los mismos, o bien son una plasmación práctica de las normas.

- Protección servidores

El acceso al/los despacho/s donde se encuentran los servidores, deberá estar restringido exclusivamente al personal autorizado, así como aquel que deba realizar labores de mantenimiento del mismo. La estancia de los servidores debería estar cerrada y sólo debería tener acceso al mismo el departamento de sistemas.

- Bloqueo estaciones

Se deberá garantizar que la información que puede mostrarse desde los puestos de trabajo no podrá ser vista por personas no autorizadas. Cuando el responsable de un puesto de trabajo deba abandonarlo, aunque sea temporalmente, deberá dejarlo de forma que quede completamente impedida la visualización, extracción o manipulación de los datos protegidos. Las estaciones deberían estar configuradas de forma que se bloquean automáticamente pasado un periodo de inactividad teniendo que reanudar la sesión mediante validación con contraseña.

- Antivirus

Todos los ordenadores deberán tener instalados programas antivirus residentes en memoria que deberán, asimismo, estar actualizados diariamente, para así garantizar la protección y detección inmediata de la posible entrada de virus informáticos en el sistema. Deberá anotarse la entrada o detección de uno de ellos en el libro de incidencias.

- Configuración fija aplicaciones

Los puestos de trabajo desde los que se tenga acceso a los ficheros tendrán una configuración fija en sus aplicaciones y sistemas operativos, que sólo podrá ser cambiada bajo la autorización del Responsable de Seguridad o administradores autorizados. Ningún usuario podrá instalar una aplicación sin autorización del Administrador de Sistemas, quien analizará si dicha aplicación puede perjudicar otras que traten datos de carácter personal. Éste decidirá respetando las normas establecidas en el presente documento. Los usuarios reciben normativa al respecto para que en caso de querer instalar cualquier tipo de aplicación pidan autorización al departamento de sistemas.

- Dispositivos de red

Cualquier dispositivo que sirva de protección entre la red local e Internet, estará programado para que en todo momento realice correctamente su función de filtrado con la misión de permitir o denegar el paso de determinados servicios y programas en ambas direcciones. Desde el departamento de sistemas se deberán revisar periódicamente las reglas establecidas en dispositivos tipo firewall para que en todo momento actúen de acuerdo a las políticas internas definidas.

- Ficheros ubicados en el servidor

Para los ficheros creados mediante aplicaciones ofimáticas que contengan datos de carácter personal, el Responsable de Fichero decidirá, junto con el Responsable de Seguridad, qué estructura de directorios deberá existir en el servidor central para su almacenamiento y cada directorio se protegerá de forma que sólo accedan los usuarios autorizados, definiéndose así perfiles de usuarios para el acceso a directorios.

Todo documento ofimático generado por los usuarios que pueda contener datos de carácter personal deberá ubicarse en el servidor de ficheros. En este servidor habrá una estructura de

carpetas personalizada para cada usuario además de carpetas compartidas para los diferentes departamentos.

- Procedimientos alta/baja usuarios

Cuando se produzca una alta de un nuevo usuario, el Responsable de Seguridad deberá decidir a qué recursos y datos podrá acceder y el administrador de sistemas preparará el ordenador de acuerdo con lo decidido. De la misma forma, cuando se produzca una baja de un usuario, se deberán aplicar mecanismos de desinstalación de software y hardware al ordenador que utilizaba para evitar cualquier intento de acceso a datos desde el mismo. El departamento de sistemas tiene procedimientos establecidos para las bajas y altas en los puestos de trabajo (limpieza disco duro, ficheros temporales, perfil usuario, cuenta correo, etc.). Asimismo, se procederá a la modificación del Documento de seguridad, a la firma del debido consentimiento y obligada confidencialidad y se le instruirá sobre la normativa en la empresa de protección de datos.

Finalmente, en el supuesto de cambios importantes en las medidas de seguridad empleadas, en los ficheros, en las finalidades del tratamiento de los datos, el Responsable del fichero consultará con los auditores externos para saber cómo actuar en cada caso. El Reglamento de seguridad dispone en su artículo 96 que *"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"*, siendo recomendable que se realice anualmente. Añade este precepto, que 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.