Tema 7: Ley Orgánica de Protección de datos.

Grupo: Appay.

Emilio Maestre Hortal
Jose Fco Moreno Fernández
Pablo López Riquelme
Sergio Pérez Seré
Jose Manuel Palau Alegría

Índice

1.- La Agencia de Protección de Datos.

La agencia de protección de datos es la autoridad estatal de control independiente encargada de velar por el cumplimiento de las normativas sobre protección de datos. Garantiza y tutela el derecho fundamental de la protección de datos de carácter personal de los ciudadanos.

Es un ente de derecho púbico, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones. Se relaciona con el Gobierno a través del Ministerio de Justicia.

Agencia Española de Protección de Datos.

Las funciones de la Agencia en relación a los actos/actores involucrados:

1. En relación a los afectados:

- Atender a sus peticiones y reclamaciones.
- Informar de los derechos de la Ley.
- Promover campañas de difusión.
- Velar por la publicidad de los dicheros de datos de carácter personal.

2. En relación con quienes tratan datos:

- Emitir las autorizaciones pertinentes.
- Requerir medidas de corrección.
- En caso de ilegalidad, ordenar el cese en el tratamiento y la cancelación de los datos.
- Ejercer la potestad sancionadora en los términos previstos en el Título VII de la Ley Orgánica de Protección de Datos.
- Recabar de los responsables de los ficheros la ayuda e información que precise para el ejercicio de sus funciones.
- Autorizar las transferencias internacionales de datos.

3. En la elaboración de normas:

- Informar preceptivamente los Proyectos de normas de desarrollo de la Ley Orgánica de Protección de Datos.
- Informar los Proyectos de normas que incidan en materia de protección de datos.
- Dictar las instrucciones y recomendaciones precisas para adecuar los tratamientos automatizados a los principios de la Ley Orgánica de Protección de Datos.
- Dictar recomendaciones de aplicación de las disposiciones legales y reglamentarias en materia

de seguridad de los datos y control de acceso a los ficheros.

4. En materia de telecomunicaciones:

- Tutelar los derechos y garantías de los abonados y usuarios en el ámbito de las comunicaciones electrónicas, incluyendo el envío de comunicaciones comerciales no solicitadas (spam).
- Recibir las notificaciones de las eventuales quiebras de seguridad que se produzcan en los sistemas de los proveedores de servicios de comunicaciones electrónicas.

5. Otras funciones:

- Cooperación con diversos organismos internacionales y con los órganos de la Unión Europea en materia de protección de datos.
- Representación de España en los foros internacionales de la materia.
- Control y observancia de los dispuesto en la Ley reguladora de la Función Estadística Pública.
- Elaboración de una Memoria Anual, que es presentada por el Directos de la Agencia ante las Cortes.

Organización.

1.- Directora: **Doña Mar España Martí.**

La representa a la Agencia y sus actos se consideran como actos de la Agencia. Sus resoluciones ponen fin a la vía administrativa y son recurribles ante la Sala de lo Contencioso de la Audiencia Nacional.

Su nombramiento lo realiza el Gobierno mediante Real Decreto por el Consejo Consultivo y a propuesta del Ministro de Justicia. Su mandato es de cuatro años.

La directora no puede recibir instrucciones de ningun poder o autoridad y ejerce sus funciones con plena independencia y objetividad.

2. Consejo Consultivo:

Es el órgano de asesoramiento del Director, siendo este elegido entre sus miembros, está compuesto por 10 miembros nombrados por un periodo de cuatro años. Es presidido por el director de la Agencia.

El Consejo Consultivo se reúne cuando lo convoca el director y, como mínimo, cada seis meses. Emite informes en todas las cuestiones que le someta el director, pudiendo realizar propuestas relacionadas con la protección de datos.

3.- Inspección de datos:

Subdirector general de inspección de datos: Pedro Colmenares Soto.

Se encarga de tramitar los procedimientos relativos al ejercicio de la potestad sancionadora que tiene a cargo la Agencia sobre protección de datos, spam y cookies y llamadas automáticas sin intervención humana o mensajes de fax con fines comerciales. Sintetizando, ejerce la función inspectora.

También tutela los derechos de acceso, rectificación, cancelación y oposición de los ciudadanos (ARCO).

4.- Secretaría general.

Subdirectora general, secretaría general: Elena Azpiazu Garrido

Se encarga de dar soporte y apoyo al funcionamiento de las diferentes unidades de la Agencia, de elaborar informes y propuestas y de la secretaría del Consejo Consultivo.

5.- Registro general de protección de datos.

Subdirector general del Registro General de Protección de datos: Julián Prieto Hergueta

- Velar por la publicidad de los tratamientos de datos.
- Inscribir los ficheros de los que sean titulares las Administraciones públicas y los de
- titularidad privada.
- Las autorizaciones de transferencias internacionales de datos y los códigos de conducta.

2.- Registro de ficheros.

La LOPD define al responsable del fichero o tratamiento como la "persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no la realice materialmente. Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

La Ley Orgánica de Protección de Datos entiende por fichero a "todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso".

Por otro lado, entiende por tratamiento "cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, cancelación, bloqueo o supresión, asó como las cesiones de datos que resulten de comunicaciones, consultas interconexiones y transferencias".

(Las definiciones de fichero y tratamiento se encuentran en los artículos 51.k y 51.t respectivamente del RLOPD).

Proceso de Registro.

Para inscibir, suprimir o modificar la inscripción de un fichero en el Registro General de Protección de Datos, se deberá cumplimentar el modelo establecido de la Agencia Española de Protección de Datos, por la que se aprueban los formularios electrónicos a través de los que deberán efectuarse las solicitudes de inscripción de ficheros en el Registro General de Protección de Datos.

Son objeto de inscripción en el Registro General de Protección de Datos:

- Los ficheros de Administraciones Públicas.
- Los ficheros de titularidad privada.
- Las autorizaciones de transferencias internacionales de datos de carácter personal con destino a países con un nivel de protección semejante al de la LOPD.
- Los códigos tipo referenciados en el artículo 32 de la LOPD.
- Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

Ficheros sometidos a inscripción.

Los ficheros se encontrarán sometido a la Ley, siendo obligatoria su inscripción en el Registro General de Protección de Datos (RGPD).

Todo fichero de datos de carácter personal de titularidad pública o privada, con excepción de algunos ficheros excluidos en el artículo 2.2 de la LOPD, serán notificados a la Agencia Española de Protección de Datos para su inscripción en el Registro General de Protección de Datos. No solicitar la inscripción constituye una infracción leve, además, la inscripción de ficheros debe estar actualizada en todo momento.

Sistema NOTA.

El **sistema de Notificaciones Telemáticas a la AEPD (NOTA)** permite a los responsables de ficheros con datos de carácter personal de titularidad pública y de titularidad privada:

- Cumplir con la obligación de notificar sus ficheros a la AEPD a través de una herramienta que informa y asesora acerca de los requerimientos de la notificación.
- Presentar de forma gratuita de notificaciones a través de Internet con certificado de firma electrónica. En caso de no disponer de un certificado de firma electrónica también puede presentar la notificación a través de Internet.

- Notificar de forma simplificada una serie de ficheros relacionados con distintas materias de titularidad pública y privada.
- Conocer el estado de tramitación de las notificaciones remitidas a través de Internet, mediante certificado de firma electrónica o mediante el código de envío generado por el formulario electrónico.
- Consultar el contenido completo de la inscripción de sus ficheros en la web de la Agencia.

Formatos y especificaciones XML.

La AEPD ha puesto en disposición de los responsables de ficheros un sistema de notificación basado en un formato estándar que permita el intercambio de información entre diferentes plataformas (formato XML). De esta forma tanto los responsables que desarrollen sus propios programas como aquellos que desarrollen paquetes ofimáticos de protección de datos pueden comunicarse con la AEPD para notificar sus ficheros.

Estos mensajes en formato XML pueden ser presentados con y sin certificado electrónico de firma reconocido.

En caso de que se presenten firmados electrónicamente:

- Deberán usar el estándar de firma XML.
- Una vez enviadas las notificaciones al Registro Telemático de la AEPD, este devolverá un mensaje confirmando la recepción del envío e incluyendo los datos neceasarios para que el programa desarrollado por terceros configure el acuse de recibo de acuerdo con el formato establecido por la AEPD.

En caso de que las notificaciones se presenten mediante formato XML sin certificado de firma electrónica:

- El servidor web de la AEPD devolverá un mensaje confirmando la recepción del mensaje.
- El mensaje devuelto incluirá los datos necesarios para que el programa desarrollado por terceros configure la Hoja de solicitud de acuerdo con el formato establecido por la AEPD.

3.- El Documento de Seguridad.

El documento de seguridad es un documento en el que se incluyen las normas, medidas de seguridad, procedimiento de actuación y tratamiento de datos para garantizar la seguridad de los datos en una organización determinada, acordada entre el responsable del fichero y el responsable de tratamiento de estos datos.

Este documento se encuentra regulado en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), concretamente en el capítulo 9.

Contenido.

1. Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

Los ficheros que la empresa tiene (clientes, pacientes, trabajadores, cámaras de seguridad, etc.) y su estructura, es decir, nombre del fichero, origen de los datos, forma de tratamiento de los datos (soporte papel o informático), tipos de datos que se recogen (nombre, apellidos, dirección postal, teléfono, dirección electrónica…), nivel de seguridad del fichero (básico, medio o alto) y la empresa encargada de gestionar el fichero si la hubiere.

2. Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

Cuáles son las medidas de seguridad que las empresa tiene para proteger esos ficheros, señalar, entre otras: armarios cerrados con llave, despachos cerrados con llave, destructoras de papel en los despachos que contiene documentación en soporte papel, contraseñas personales en los ordenadores con acceso a datos personales, caducidad de las contraseñas, cómo, dónde y cuándo se hacen las copias de seguridad, dónde se guardan las referidas copias de seguridad, con qué periodicidad se hacen, cuál es el procedimiento a seguir en caso de que se produzca una incidencia en la empresa respecto a datos personales, etc

3. Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros. BOE núm. 17 Sábado 19 enero 2008 4127

Especifica las obligaciones del personal de mantener un total secretismo sobre los datos que se manejan y los métodos que se emplean para mantener informado de sus obligaciones (Método de acceso a datos y identificación del personal).

También se informa de las consecuencias de lo especificado en el documento de seguridad.

4. Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

Este punto se tratará en el anexo 1 del documento y en el se describirán todos los ficheros y la estructura de cada uno de ellos.

5. Procedimiento de notificación, gestión y respuesta ante las incidencias.

En esta parte se redactará el procedimiento a llevar a cabo al detectar alguna incidencia. Se incluirán a quien hay que avisar de la incidencia, quien se encargará de corregirla y que métodos usará para ello.

6. Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

El documento de seguridad se actualizará siempre que se produzca un cambio relevante en el sistema, el contenido del fichero o en consecuencia de los controles periódicos.

En este punto se indican los procedimientos que se tienen que llevar a cabo para mantener el documento de seguridad siempre actualizado.

7. 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.

En este apartado se deberá de explicar cuáles serán los procedimientos a realizar en caso de migrar datos, la destrucción o la reutilización de estos.

Anexos.

- ## Anexo 1: Descripción de ficheros.

En este apartado se deberán de describir todos los ficheros Nombre, unidades con acceso al fichero, identificador del fichero en el Registro general, nivel de seguridad, administrador, leyes o regulaciones aplicables al fichero, estructura del fichero y toda la información del fichero (Finalidad, personas o colectivos que deben aportar los datos, procedimiento de recogida, cesiones previstas, transferencias internacionales, sistema de tratamiento, etc. Etc).

- ## Anexo 2: Nombramientos.

En este apartado se describirán todos los perfiles que afecten al fichero, como el del responsable de seguridad, quien tendrá acceso al mismo etc…

- **Anexo 3: Autorizaciones de salida o recuperación de datos.**

  Se incluyen las autorizaciones que el responsable del fichero ha otorgado para la salida de soportes que contengan una copia del fichero, aunque esta sea solo temporal. También se incluyen las autorizaciones para la realización de procedimientos de recuperación de datos.

- **Anexo 4: Delegación de autorizaciones.**

  Presenta una lista de las personas a las que el responsable del fichero delega las autorizaciones en caso de no poder otorgarlas él mismo.

  En su caso, personas en las que el responsable del fichero ha delegado. Indicar las autorizaciones, tales como: salida de dispositivos portátiles, la copia o reproducción de documentos en soporte papel…

- **Anexo 5: Inventario de soportes.**

  Indica los soportes que contienen la información que se incluye en el fichero, se indica que tipo de información contiene y donde se almacena.

  Los soportes 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 este documento.

  Si el inventario de soportes está informatizado, indicar la aplicación o ruta de acceso del archivo que lo contiene.

- **Anexo 6: Registro de incidencias.**

  Se amplían la información respecto a las incidencias especificas en el apartado 3 del documento de seguridad.

  Si el registro de incidencias no está informatizado, recoger en este anexo la información al efecto, según lo indicado en el apartado de "Procedimientos de notificación, gestión y respuesta ante las incidencias" de este documento.

  Si el registro de incidencias está informatizado, indicar la aplicación o ruta de acceso del acceso del archivo de lo contiene.

- **Anexo 7: Encargados de tratamiento.**

  Copia del contrato que firmará el encargado del tratamiento del fichero, el cuál estipula que los datos se trataran de acuerdo a las especificaciones del responsable del fichero y nunca con un fin distinto al especificado en dicho contrato.

  Establecerá expresamente que el encargado de tratamiento 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, y que no los comunicarán, ni siquiera para su conservación a otras personas.

- **Anexo 8: Registro de entrada y salida de soportes.**

  En este apartado se incluye un registro de los diferentes soportes de almacenamiento en los que figuran los datos especificados en el documento.

  Recoger en este anexo la información al efecto, según lo indicado el artículo 97 del RLOPD.

  Si el registro de entrada y salida está informatizado, indicar la aplicación o ruta de acceso del acceso del archivo de lo contiene.

- **Anexo 9: Medidas alternativas.**

  Se indican medidas alternativas para llevar el control de los dispositivos de almacenamiento que contienen el/los fichero/s y que no pueden registrarse y llevar un control respecto a lo indicado en el RLOPD.

En el caso de que no sea posible adoptar las medidas exigidas por el RLOPD en relación con la identificación de los soportes, los dispositivos de almacenamiento de los documentos o los sistemas de almacenamiento de la información, indicar las causas que justifican que ello no sea posible y las medias alternativas que se han adoptado.

4.- Personal Involucrado.

Responsables del fichero

Es una persona, empresa o entidad responsable de los datos de carácter personal almacenados en un fichero, para que se garantice su uso acorde la LOPD.

Puede haber más de un responsable

Entre las obligaciones del responsable del fichero están: notificación o inscripción de ficheros, aplicación de los principios de protección de datos, ejercicio de los derechos de los ciudadanos, la transferencia de datos y la colaboración con la Agencia.

Personal encargado del tratamiento

Es la persona, empresa o entidad que trate con los ficheros que almacenan datos personales y se encarguen de que se respete la LOPD y no se viole ningún derecho.

Se incluye al personal de seguridad y cualquier otro que tenga acceso al fichero sin restricciones o

pueda conceder acceso al mismo.

Interesado o afectado

Persona física titular de los datos que se almacenan en el fichero.

Puede ejercer su derecho al acceso, rectificación, cancelación u oposición del tratamiento de los datos en todo momento.

5.- Control de accesos.

El control de acceso implica quien tiene acceso a sistemas informáticos específicos y recursos en un momento dado. El concepto de control de acceso consta de tres pasos. Estos pasos son la identificación, autentificación y autorización.

Con el uso de estos tres principios un administrador del sistema puede controlar que recursos están disponibles para los usuarios de un sistema.

Objetivos

- Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red del Organismo y otras redes publicas o privadas.
- Registrar y revisar eventos y actividades criticas llevadas a cabo por los usuarios en los sistemas.
- Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

Principios del Control de Acceso

Uno de los principios que deben incorporarse al establecer una política de control de acceso eficaz es la práctica de un acceso mínimo o menos privilegios. Lo que esto significa es que un usuario debe tener la menor cantidad de acceso requerido para hacer su trabajo.

El principio del menor privilegio incluye la limitación de los recursos y aplicaciones accesibles por el usuario, así como el acceso en tiempo permitido. Por, ejemplo, a veces, puede no ser aconsejable permitir el acceso a los registros financieros a las 3:00 am por la mañana, cuando las instalaciones deberían estar cerradas.

Pasos para un Control de Acceso

La identificación se refiere las cosas como nombres de usuario y tarjetas de identificación. Es el medio por el cual un usuario del sistema identifica quiénes son. Este paso se realiza generalmente al iniciar sesión.

La autenticación es el segundo paso del proceso de control de acceso. Contraseñas, reconocimiento de voz, y escáneres biométricos son métodos comunes de autenticación. El objetivo de la autenticación es para verificar la identidad del usuario del sistema.

La autorización se produce después de que un usuario del sistema se autentica y luego es autorizado a utilizar el sistema. El usuario esta generalmente sólo autorizado a usar una porción de los recursos del sistema en función de su papel en la organización. Por ejemplo, el personal de ingeniería tiene acceso a diferentes aplicaciones y archivos que el personal de finanzas, o recursos humanos no.

Tipos de Control de Accesos

- Gestión de accesos de usuario.
    - Registro de usuarios
    - Gestión de privilegios.
    - Gestión de contraseñas de usuario.
    - Revisión de los derechos de acceso de los usuarios.

- Control de accesos al sistema operativo.
    - Procedimientos de conexión de terminales.
    - Identificación y autenticación de los usuarios.
    - Sistema de gestión de contraseñas.
    - Utilización de utilidades del sistema.
    - Timeout de sesiones.
    - Limitación del tiempo de conexión.

- Control de acceso a la información y aplicaciones.
    - Restricción de acceso a la información.
    - Aislamiento de sistemas sensibles.
- Control de accesos en red.
    - Política de uso de los servicios de red.

- Autenticación para conexiones externas.
- Identificación de equipos en la red.
- Protección a puertos de diagnóstico remoto y configuración.
- Segregación en las redes.
- Control de conexión a las redes.
- Control de enrutamiento en red.

Métodos de Control de Accesos

- Contraseñas.
- Certificados.
- Limitación del tiempo de conexión.
- Control de acceso a las aplicaciones.
- Restricciones por IP.
- Dispositivos Biometricos.
- Etc.

Asignación de Privilegios

El objetivo es asegurar el acceso autorizado de usuario y prevenir accesos no autorizados a los sistemas de información.

Debería restringirse y controlarse el uso y asignación de privilegios:

- Identificar los privilegios.
- Asignar privilegios a los individuos según los principios de "necesidad de uso".
- Mantener un proceso de autorización y un registro de todos los privilegios asignados. No se otorgarán privilegios hasta que el proceso de autorización haya concluido; promover el desarrollo y uso de rutinas del sistema.
- Promover el desarrollo y uso de programas.
- Asignar los privilegios a un identificador de usuario distinto al asignado para un uso normal. Un uso inapropiado de los privilegios puede ser causa de fallas.

Requerimientos Legales

Ley Orgánica de Protección de Datos, Real Decreto 994/1999 que desarrolla el Reglamento de Medidas de Seguridad.

Es importante señalar que tanto la Ley Orgánica como el Real Decreto 994/1999 que desarrolla el Reglamento de Medidas de Seguridad ligan el concepto de seguridad de los datos a los conceptos de:

a) Confidencialidad: entendido como el acceso autorizado a los datos.

b) Exactitud: la información no debe sufrir alteraciones no deseadas, en cuanto a su contenido.

c) Disponibilidad: sólo las personas autorizadas pueden tener acceso a la información.

Las medidas que deberán ser adoptadas e implantadas por el Responsable del Fichero son:

- **Medidas Organizativas:** aquellas medidas destinadas a establecer procedimientos, normas, reglas y estándares de seguridad, cuyos destinatarios son los usuarios que tratan los datos de los ficheros.
- **Medidas Técnicas:** medidas destinadas principalmente a la conservar la integridad de la información (su no alteración, pérdida o robo) y en menor medida a la confidencialidad de los datos personales. Se encuentran delimitadas en función del nivel de seguridad de los datos tratados: básico, medio y alto.

Los niveles de seguridad en el Reglamento.

Nivel Básico: Para todos los ficheros de datos de carácter personal.

Nivel Medio: Serán adoptadas para:

- Ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales.
- Ficheros que contengan datos sobre Hacienda Pública. Ficheros que contengan datos sobre Servicios Financieros.
- Ficheros que contengan datos sobre solvencia patrimonial y crédito.
- Ficheros que contengan un conjunto de datos suficientes que permitan elaborar un perfil del afectado (se les aplican las medidas descritas en los art.17 a 20).

Nivel Alto: Aquellos que contengan datos de ideología, religión, creencias, origen racial, salud, vida sexual.

6.- Gestión de soportes y documentos.

Tal y como establece el artículo 92 del Real Decreto 1720/2007, en todos los ficheros automatizados la gestión de los soportes y documentos que contengan datos de carácter personal se debe llevar a cabo de la siguiente manera:

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 autorizado por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.

3.- EN el traslado de la documentación se adaptarán las medidas dirigidas a evitar la sustracción, perdida 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.

Cuando se trate de ficheros automatizados que requieran de un nivel de seguridad medio o alto, la gestión de los soportes y documentos prevista para el nivel básico debe ser complementada con lo previsto en el artículo 97 del Real Decreto 1720/2007, en los siguientes términos:

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

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

7.- Copias de Seguridad.

Tal y como establece el artículo 94 del Real Decreto 1720/2007, en todos los ficheros automatizados el responsable del fichero debe establecer un procedimiento que permita realizar semanalmente copias de seguridad (backup) de los datos de carácter personal en algún tipo de soporte que permita su recuperación posterior en caso de problemas, dicho procedimiento debe cumplir con los siguientes requisitos:

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.

Cuando se trate de ficheros automatizados que requieran de un nivel de seguridad alto, el procedimiento de copias de respaldo y recuperación previsto para el nivel básico debe ser complementado con lo previsto en el artículo 102 del Real Decreto 1720/2007, en los siguientes términos:

- 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.

8.- Seguimiento y Control (Auditoría LOPD).

La Normativa en Protección de datos de carácter personal, obliga a las empresas y autónomos que manejen datos personales y tengan dado de alta los ficheros en la Agencia Española de Protección de Datos, cuyo nivel de protección sea media o alta, y sin importar el tipo de datos, ya sea automatizado o no automatizado, a hacer una auditoria cada dos años o con carácter extraordinario si se realizan modificaciones sustanciales en el sistema de información, para garantizar el cumplimiento de las medidas de seguridad en relación a la protección de los datos personales que en el desarrollo de su actividad pueda tener.

Entendiendo por auditoria, una herramienta de control y supervisión que permitan conocer fallos en el manejo de datos personales, a través de la investigación, revisión, consulta, comprobación, y obtención de toda evidencia sobre un hecho o sistemas establecido, para el cumplimiento y la garantía del buen uso de los datos personales, llevada a cabo por personal cualificado.

Tal y como establece el artículo 9ó6 del Real Decreto 1720/2007, en los ficheros automatizados que requieran de un nivel de seguridad medio o alto, se deberá realizar cada dos años una auditoria que verifique que los sistemas de información e instalaciones donde se tratan y almacenan los datos de carácter personal cumplen con las medidas de seguridad previstas en el Reglamento Lopd. Dicha auditoria debe realizarse conforme a los siguientes requisitos:

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 artículo. 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.

Será la empresa quien decida cómo quiere efectuar estas auditorías , teniendo en cuenta que está debe realizarse con objetividad e imparcialidad, basada en evidencias objetivas, es decir, es importante para poder emitir un informe final, tener en cuenta la información que se recopile para poderla efectuar, basada en hechos conocidos y observados durante el tiempo que se realice y los medios que se utilicen para la comprobación del cumplimiento de las medidas de seguridad definidas en el documento de seguridad.

La labor del auditor debe ejecutarse manteniendo imparcialidad de criterios sin dejar que influyan factores internos o externos, de tal manera que siempre haya un criterio de independencia frente a la empresa que va a auditar.

La auditoría debe realizarse mediante un proceso sistemático que implicaría la aplicación de una metodología, por ello la entidad auditora deberá elaborar sus propios procedimientos y protocolos de actuación, que permita obtener los datos necesarios, para elaborar el informe final, procedimientos que llevará a cabo a través de un auditor quien determinará el grado de precisión que existe entre los hechos que se generan en realidad y los informes que se han generado en relación al documento de seguridad.

Otro aspecto muy importante en su realización es la parte documental, al constituir la prueba más objetiva de lo que se dice es cierto y permiten evidenciar los hechos, la auditoria se centrará en los propios documentos que suministra el propio auditado y basado en el documento de seguridad, y los registros que se tengan en los ficheros mixtos o no automatizados.

Tipos de Auditorias.

Auditoria Externa

La externa, será la realizada por un profesional en la materia sin vinculo laboral con la empresa que va a auditar, utilizando técnicas y procedimientos determinados destinados a la revisión de los métodos empleados por las empresa para garantizar el cumplimiento de lo establecido por la ley respecto a las medidas de seguridad, que permitan garantizar la legalidad de la obtención de los datos, la legalidad de su uso y el buen manejo de los mismo.

En esta auditoria la relación es de tipo civil, entre el auditor y la empresa auditada, mediante la realización de un contrato de prestación de servicios

Auditoría Interna

Será la realizada por un profesional que posea un vínculo laboral con la empresa, con conocimientos específicos sobre dicha materia, que además sea abogado en ejercicio o ingeniero informático, quien utilizará técnicas determinadas destinadas a la revisión de los métodos de control o de seguridad empleados, para emitir un informe final, que permita evaluar el grado de cumplimiento de la empresa en relación a los compromisos adquiridos en cuanto al manejo de los datos de carácter personal que tenga en su poder.

Metodología del trabajo de Auditoria.

Las etapas de ejecución de la auditoría son las siguientes:

1. Reunión inicial.
2. La recogida de evidencias, que se realiza mediante cuatro estrategias:
   - Análisis de documentación aportada por la auditada.
   - Comprobación de registros.
   - Inspección visual de los sistemas de la información y entorno físico.
   - Entrevistas con el personal, tanto Responsable/s de Seguridad como diversos usuarios.
3. Documentación de los resultados.
4. Reunión final para comentario de las evidencias con el Responsable de Seguridad de la auditada.
5. Elaboración del informe de auditoría.

El informe de Auditoria debe contener.

1. Objetivo de la auditoria.
2. Identificación de los auditores.
3. Personas contactadas.
4. Fecha de la auditoria.
5. Normas de referencia.
6. Descripción de las no conformidades encontradas, y la toma de las acciones correctivas.
7. Eficacia del sistema para el cumplimiento de los requisitos de la norma y documentos.
8. Lista de distribución del informe.
9. Adjuntar observaciones y recomendaciones para adecuar la empresa a la protección de datos.

Este informe deberá dictaminar sobre la adecuación de Las medidas y controles a la ley y su desarrollo reglamentario, debe ser analizado por el responsable de seguridad, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas.

La estructura del informe puede ser

1. Entidad auditada.
2. Auditor.

3. Objetivos de la auditoria.

4. Ficheros y tratamientos auditados.

5. Ejecución del trabajo.

6. Entrega del informe.

7. Análisis de los niveles de seguridad asignados.

8. Tabla de resumen de medidas correctoras o complementarias.

9. Tabla de resumen de recomendaciones del auditor.

10. Conclusiones.