

Ley Orgánica de Protección de Datos

...

Control de acceso y gestión de soportes y documentos

Paradox Studios

Niveles de seguridad.

- Las medidas de seguridad están clasificadas en tres niveles (**básico, medio y alto**).
- Se aplicarán en función del tipo de datos que contenga el fichero y la finalidad del tratamiento de dichos datos.
- Cuánto más sensibles sean los datos tratados o más comprometido sea el tratamiento será necesario un mayor nivel de seguridad.
- Las medidas de seguridad previstas en la LOPD se aplican acumulativamente.

Ficheros automatizados

Ficheros automatizados:

“Todo conjunto organizado de datos de carácter personal que permita acceder a la información relativa de una persona física determinada usando procedimientos de búsqueda automáticos”.

Aquí están incluidos los ficheros que almacenan la información en soportes informáticos, como bases de datos.

Ficheros no automatizados

Ficheros no automatizados:

“Todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas”.

Un ejemplo serían los archivadores existentes en la mayoría de organizaciones donde se almacenan **expedientes de documentos**.

¿Qué es el control de acceso?

Un sistema de control de acceso hace referencia al mecanismo que permite acceder a datos o recursos, es un mecanismo a través del cual puedes acceder a ciertos lugares físicos o datos lógicos si te has identificado y autenticado previamente.

En resumen, el control de acceso consiste en la verificación de si una entidad solicitando acceso a un recurso tiene los derechos necesarios para acceder.

Usos del control de acceso

Los mecanismos de control de accesos pueden ser usados para proteger los diferentes tipos de recursos:

- Recursos físicos: acceso a una habitación de servidores.
- Recursos lógicos: una cuenta de banco, solo determinadas personas acceden al recurso.
- Recursos digitales: archivo informático encriptado.

¿De qué está compuesto?

El control de acceso está compuesto por tres componentes:

1. Un mecanismo de identificación.
2. Un mecanismo de autenticación
3. Un mecanismo de trazabilidad

Pasos del control de acceso

- La **identificación** se refiere al proceso de validar quién es el usuario del sistema. Es el medio por el cual un usuario se identifica.
- 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 **trazabilidad** se produce después de que un usuario del sistema se autentica y luego es autorizado a acceder. El usuario está generalmente sólo autorizado a acceder ciertas áreas o zonas de los recursos del sistema en función de su papel en la organización.

Real Decreto 1720/2007, desarrollo de la ley Orgánica 15/1999 de protección de datos de carácter personal.

Control de acceso para ficheros automatizados

Para un nivel de seguridad básico:

Artículo 89 - Funciones y obligaciones del personal:

1. Las funciones y obligaciones de cada uno de los usuarios con acceso a los datos estarán definidas en el documento de seguridad.
2. El responsable del fichero adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones.

Control de acceso para ficheros automatizados

Artículo 91 - Control de acceso

1. Los usuarios tendrán acceso sólo a aquellos recursos que precisen para el desarrollo de sus funciones.
2. El responsable del fichero se encargará de que haya una relación actualizada entre los usuarios y los accesos para cada uno de ellos.
3. El responsable del fichero se encargará de que un usuario no pueda acceder a recursos con derechos distintos a los autorizados.
4. Solo el personal autorizado podrá alterar el acceso autorizado sobre los recursos.
5. Si existe personal ajeno al responsable del fichero con acceso a los recursos estará sometido a las mismas condiciones y obligaciones que el personal propio.

Control de acceso para ficheros automatizados

Para un nivel de seguridad medio:

Artículo 99 - Control de acceso físico

Exclusivamente el personal autorizado en el documento podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas e información

Control de acceso para ficheros automatizados

Para un nivel de seguridad alto:

Artículo 103 - Registro de accesos

1. En cada intento de acceso se guardará identificación, fecha, hora, fichero accedido, tipo de acceso y si ha sido autorizado o denegado.
2. En caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.
3. Los mecanismos del registro están bajo control del responsable de seguridad.

Control de acceso para ficheros automatizados

Artículo 103 - Registro de accesos

4. El periodo mínimo de conservación de datos registrados es 2 años
5. El responsable de seguridad tendrá que revisar al menos 1 vez al mes la información de control y elaborar un informe de las revisiones y problemas detectados
6. No será necesario el registro de acceso en caso de que el responsable del fichero sea una persona física y que el responsable del fichero garantice que únicamente él tiene acceso y trata los datos personales.

Resumen - Controles de accesos para ficheros automatizados

Nivel Básico	Nivel Medio	Nivel Alto
<ul style="list-style-type: none">✓ Los usuarios accederán únicamente a los datos y recursos necesarios para sus funciones.✓ Habrá mecanismos para evitar el acceso con distintos derechos de los autorizados.✓ La concesión de derechos de acceso sólo la dará personal autorizado.	<ul style="list-style-type: none">✓ Existirán controles de acceso físico a los locales donde se encuentren ubicados los sistemas de información.	<ul style="list-style-type: none">✓ Existirá un Registro de Accesos donde figurará:<ul style="list-style-type: none">✓ usuario,✓ hora,✓ fichero,✓ tipo acceso✓ registro accedido.✓ Estará bajo el control del responsable de seguridad.✓ Se hará un informe mensual.✓ Se conservará al menos durante 2 años.
<i>Aplicable a ficheros automatizados y manuales</i>	<i>Aplicable solo a ficheros automatizados</i>	

Control de acceso para ficheros no automatizados

Para un nivel de seguridad alto:

Artículo 113 - Acceso a la documentación

1. Se limitará exclusivamente al personal autorizado.
2. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos con múltiples usuarios.

Resumen - Control de Acceso ficheros no automatizados

Nivel Básico	Nivel Medio	Nivel Alto
<ul style="list-style-type: none">✓ Los usuarios accederán únicamente a los datos y recursos necesarios para sus funciones.✓ Habrá mecanismos para evitar el acceso con distintos derechos de los autorizados.✓ La concesión de derechos de acceso sólo la dará personal autorizado.		<ul style="list-style-type: none">✓ El acceso se limitará al personal autorizado.✓ Habrá mecanismos para identificar los accesos a documentos disponibles para múltiples usuarios✓ Procedimiento en el Documento de Seguridad para registrar los accesos de otras personas
<i>Aplicable a ficheros automatizados y manuales</i>		<i>Aplicable solo a ficheros manuales</i>

Gestión de soporte y documentos

Los soportes y documentos deberán permitir identificar el tipo de información que contienen y poder ser inventariados, a continuación hablaremos del conjunto de medidas y artículos relacionados con la gestión de soportes.

Gestión de soportes para ficheros automatizados

Para un nivel de seguridad básico:

Artículo 92 - Gestión de soportes y documentos

1. Los soportes y documentos deberán permitir identificar el tipo de información que contienen, ser inventariados y solo ser accesibles por el personal autorizado.
2. La salida de soportes y documentos fuera de los locales bajo el control del responsable del fichero deberá ser autorizada por el responsable del fichero.
3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida, o acceso indebido a la información durante su transporte.

Gestión de soportes para ficheros automatizados

4. Siempre que vaya a desecharse algún documento o soporte con datos de carácter personal deberá procederse a destrucción o borrado.
5. La identificación de soportes con datos de carácter personal especialmente sensibles podrá ser realizada utilizando sistemas de etiquetado comprensibles para los usuarios con acceso autorizado pero que dificulten la identificación del resto de personas.

Gestión de soportes para ficheros automatizados

Para un nivel de seguridad medio:

Artículo 97 - Gestión de soportes y documentos

1. Deberá establecerse un sistema de registro de entrada de soportes que permita conocer el tipo de documento o soporte, el emisor, la fecha y hora, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción.
2. Se dispondrá también de un sistema de registro de salida de soportes que permita conocer los mismos datos expuestos en el punto anterior.

Gestión de soportes para ficheros automatizados

Para un nivel de seguridad alto:

Artículo 101 - Gestión y distribución de soportes

1. La identificación de soportes se realizará utilizando sistemas de etiquetado comprensibles para los usuarios con acceso autorizado y difíciles de interpretar para el resto de personas.
2. La distribución de los soportes se realizará cifrando dichos datos o usando mecanismos que garanticen que la información no sea accesible o manipulada en el transporte.
3. Deberá evitarse el tratamiento de datos en dispositivos portátiles que no permitan su cifrado, en caso de que sea necesario se hará constar en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos.

Resumen - Gestión de soportes para ficheros automatizados

Nivel Básico	Nivel Medio	Nivel Alto
<ul style="list-style-type: none">✓ Debe identificarse el tipo de datos que contienen.✓ Existirá un inventario de soportes✓ Se almacenarán en un lugar con acceso restringido.✓ Deberá autorizarse la salida de soportes.	<ul style="list-style-type: none">✓ Habrá un registro de entrada y salida de soportes.✓ Se adoptarán medidas para impedir la recuperación posterior de información de un soporte que vaya a ser desechado o reutilizado.	<ul style="list-style-type: none">✓ Cuando sea necesario distribuir soportes, se hará cifrando los datos o mediante cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.
<i>Aplicable a ficheros automatizados y manuales</i>	<i>Aplicable solo a ficheros automatizados</i>	

Gestión de soportes para ficheros no automatizados

Para un nivel de seguridad básico y medio:

Artículo 106 - Criterios de archivo

El archivo de soportes se realizará usando criterios que garanticen 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 los casos sin norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación del archivo.

Gestión de soportes para ficheros no automatizados

Artículo 107 - Dispositivos de almacenamiento

Los dispositivos de almacenamiento de los documentos deberán disponer de mecanismos que obstaculicen su apertura.

Cuando las características físicas no permitan adoptar esta medida será el responsable del fichero quien adoptará medidas que impidan el acceso a personas no autorizadas.

Gestión de soportes para ficheros no automatizados

Artículo 108 - Custodia de los soportes

La persona que se encuentre a cargo de la documentación deberá custodiarla e impedir en todo momento que pueda ser accedida por una persona no autorizada.

Gestión de soportes para ficheros no automatizados

Para un nivel de seguridad alto:

Artículo 111 - Almacenamiento de la información

1. Los elementos en los que se almacenen los ficheros, como archivadores o armarios, deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso con un sistema de apertura mediante llave u otro dispositivo..
2. Si no fuera posible cumplir lo establecido en el punto anterior, el responsable adoptará medidas alternativas que se incluirán en el documento de seguridad.

Gestión de soportes para ficheros no automatizados

Artículo 114 - Traslado de documentación

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

Resumen - Gestión de soportes para ficheros no automatizados

Nivel Básico	Nivel Medio	Nivel Alto
<ul style="list-style-type: none">✓ Se aplicarán criterios de archivo que permitan la conservación, localización y consulta✓ Los dispositivos de almacenamiento tendrán mecanismos que obstaculicen su apertura✓ Cuando la documentación no se encuentre archivada, su depositario deberá custodiarla e impedir accesos no autorizados		<ul style="list-style-type: none">✓ El acceso a armarios, archivadores, etc. estará protegido mediante puertas con cerradura. Cuando no se acceda, permanecerán cerradas.✓ Soluciones alternativas, motivadas en el Documento de Seguridad✓ Siempre que se proceda al traslado físico de documentación, deberán adoptarse medidas para impedir su acceso o manipulación
<i>Aplicable solo a ficheros manuales</i>		