AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS

GUíA de Seguridad de Datos

PREGUNTAS FRECUENTES

NIVELES DE SEGURIDAD

¿Cuándo se aplica el nivel básico de seguridad a datos de salud?

El artículo 81.6 del Reglamento de desarrollo de la LOPD señala que "podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos."

Por tanto dos son los factores que deben concurrir necesariamente para aplicar medidas de nivel básico en este caso: 1) la existencia de una ley que imponga un deber cuyo cumplimiento obligue a tratar ciertos datos de salud; y 2) que dichos datos respondan a unas características concretas.

En el primer caso, y a título de ejemplo, pueden citarse las obligaciones contempladas en la legislación sobre IRPF o Seguridad social, que en los ficheros de nóminas obligan a tratar datos como el porcentaje de discapacidad o la existencia de una incapacidad laboral.

En el segundo caso, se podrá aplicar el nivel básico, tratándose de datos de salud, únicamente, en los siguientes tipos de dato:

DISCAPACIDAD	porcentaje, indicador "SI/NO"
Incapacidad laboral, enfermedad común, accidente laboral, enfermedad profesional	"SI/NO" fecha
Aptitud para el desempeño (por razones de salud)	"Apto/no apto".
Maternidad	"SI/NO"

La regulación del artículo. 81.6 RDLOPD establece una excepción y por tanto debe ser interpretada restrictivamente. Por tanto, si no se trata de esta tipología de datos personales no podrá aplicarse. De ahí que en el caso de que se incluya referencia a un dato específico de salud, como por ejemplo, la enfermedad concreta relacionada con el motivo de la baja laboral o un código que la identifique, el nivel aplicable será el ALTO.

Además debe existir una ley que imponga la obligación de tratar el dato y por ello, si en un fichero se incluye voluntariamente un dato del tipo "porcentaje de discapacidad" sin que exista obligación legal el nivel aplicable al fichero será ALTO.

Por último, la presencia aislada de alguno de estos datos no prejuzga necesariamente el nivel de seguridad aplicable. Así por ejemplo, la presencia de un dato del tipo apto/no apto en un fichero dedicado a la prevención de riesgos que incluya el historial clínico-laboral del trabajador no permite aplicar el nivel básico ya que, habida cuenta del contenido de la citada historia clínica procederá aplicar el nivel de seguridad ALTO.

- **¿Cuándo podrá aplicarse el nivel básico de medidas de seguridad a un fichero que contenga datos especialmente protegidos como la afiliación sindical?**

El artículo 81.5.a) permite aplicar el nivel básico en caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual cuando los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.

Existen dos ejemplos en los que se aprecia con claridad el criterio para aplicar esta excepción. En primer lugar, en el caso de que se tenga previsto tratar el dato relativo a las cuotas sindicales se deberá tener en cuenta que la deducción de la cuota sindical es una obligación impuesta por Ley al empresario. Así, el artículo 11 de la Ley Orgánica 11/1985, de 2 de agosto, de Libertad Sindical, establece que:

- *En los convenios colectivos podrán establecerse cláusulas por las que los trabajadores incluidos en su ámbito de aplicación atiendan económicamente la gestión de los sindicatos representados de la comisión negociadora, fijando un canon económico y regulando las modalidades de su abono. En todo caso, se respetará la voluntad individual del trabajador, que deberá expresarse por escrito en la forma y plazos que se determinen en la negociación colectiva.*

- *El empresario procederá al descuento de la cuota sindical sobre los salarios y a la correspondiente transferencia a solicitud del sindicato del trabajador afiliado y previa conformidad, siempre, de éste*".

Si atendemos al precepto anterior resulta claro que se impone al empresario un deber que se traduce en practicar un descuento y transferirlo al sindicato, es evidente que los datos relativos a la afiliación sindical son datos especialmente protegidos conforme al artículo 7 LOPD. No obstante, la excepción del Reglamento permite adoptar las medidas de seguridad de nivel básico.

Del mismo modo, y en segundo lugar, idéntica situación se produce en el caso de domiciliaciones bancarias para el pago de cuotas a sindicatos, partidos, confesiones, asociaciones etc. en los que la que el banco o caja trata los datos con la única finalidad de realizar la gestión consistente en un pago.

¿Qué se entiende por ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan datos especialmente protegidos?

En relación con el nivel de medidas de seguridad aplicable, sería necesario atender al tenor literal del artículo 81.5 del RLOPD que establece que "En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

- Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.

- Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad."

A este respecto, se debería tener en cuenta que la excepción prevista en el último inciso del artículo 81.5 se refiere a cuando los datos especialmente protegidos sean incluidos por el propio afectado a la hora al presentar documentación en la que por propia iniciativa desee aportar este tipo de datos, sin que su tratamiento tenga relación con la finalidad establecida por el responsable del fichero.

Es fundamental tener en cuenta que esta excepción únicamente se aplicara a los ficheros no automatizados.

¿Qué nivel de seguridad debe adoptarse en los ficheros que contengan datos de menores?

En esta materia el RLOPDen su artículo 13, únicamente regula la forma de recabar el consentimiento de los menores, sin que ello afecte, en modo alguno, a las medidas de seguridad que deben de adaptarse a los ficheros o tratamientos de datos por parte del responsable.

La regulación de las medidas de seguridad, se encuentran en el Título VIII, Capítulo I artículos del 79 al 86. Así el artículo 80 señala que "Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto." Por otra parte el artículo 81 regula la aplicación estos niveles de seguridad.

Por lo tanto, la determinación del nivel de seguridad que debe de adoptar un responsable dependerá de los criterios fijados por el artículo 81 del Reglamento para el que la condición de la minoría de edad no es relevante.

ENCARGADOS Y PRESTACIONES DE SERVICIOS SIN ACCESO A DATOS

□ ¿Qué obligaciones en materia de medidas de seguridad tienen los encargados de tratamiento?

Tanto las prestaciones de servicios realizadas por los encargados de tratamiento en los locales del responsable del fichero, como las realizadas en los propios locales del encargado, se encuentran sujetas a la normativa de protección de datos.

Con carácter general, las obligaciones del encargado del tratamiento en materia de implantación de las medidas de seguridad se encuentran reguladas en los artículos 82 y 88 del Reglamento de desarrollo de la LOPD. Además el documento de seguridad de un encargado debe tener un contenido adicional específico que permita identificar sus encargos indicando:

- La identificación de los ficheros o tratamientos que se traten en concepto de encargado.
- Referencia expresa al contrato o documento que regule las condiciones del encargo.
- Identificación del responsable.
- Período de vigencia del encargo.

En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a los restantes requisitos establecidos en el Reglamento de la LOPD.

Por último, el encargado de tratamiento debe implantar las medidas de seguridad adecuadas para sus propios ficheros. Entre ellas, debe mantener actualizado su documento de seguridad, fijar las obligaciones de su personal etc.

¿Puede el encargado hacerse cargo del documento de seguridad del responsable que le ha contratado?

No es infrecuente la existencia de tratamientos, como por ejemplo la confección de nóminas, en los que los datos se alojan y tratan casi por completo en los locales, recursos y soportes del encargado. Para estos casos, el reglamento se refiere en su artículo 88 a la "delegación de la llevanza del documento de seguridad". Para ello deben cumplirse ciertos requisitos:

- Que los datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado.
- Que esta circunstancia afecte a parte o a la totalidad de los ficheros o tratamientos del responsable.
- Que la delegación se indique de modo expreso en el contrato celebrado al amparo del artículo 12 LOPD, con especificación de los ficheros o tratamientos afectados.

No podrá delegarse en el encargado la llevanza del documento de seguridad en lo relativo a aquellos datos contenidos en recursos propios del responsable.

En las prestaciones sin acceso a datos ¿qué obligaciones de seguridad existen?

Se deberá tener en cuenta que la mayoría de las actividades que supongan un contacto directo o indirecto con el sistema de información y/o con su entorno físico o lógico puede ser susceptible de poner en riesgo la seguridad de los datos.

Así por ejemplo, el servicio de seguridad que custodia las llaves de las instalaciones debe ser advertido de las políticas de control de acceso físico a las instalaciones y de las eventuales restricciones de acceso que se hayan fijado.

Del mismo modo, los servicios de limpieza deberían ser informados de aspectos relacionados con las prohibiciones relacionadas con el desechado de documentos, -por ejemplo, utilizar medios convencionales como el contenedor de basuras-, o de la necesidad de que en determinadas salas se mantengan condiciones de refrigeración que garanticen la estabilidad de las máquinas que soportan el sistema de información.

Un último ejemplo, lo proporcionan los servicios de mantenimiento que, eventualmente, deben tener obligaciones cuando sus acciones pueden poner en peligro un sistema, - por ejemplo, la de advertir cuando una reparación haga necesario desconectar la red eléctrica obligando a un copiado y/o apagado preventivo.

En estos casos, para la realización de trabajos que no impliquen el tratamiento de datos personales, y de conformidad con lo establecido en el artículo 83 del Reglamento de la LOPD, el responsable del fichero debe adoptar las medidas adecuadas para limitar el acceso del personal a los datos personales.

Cuando se trate de personal ajeno, el contrato de prestación de servicios deberá recoger expresamente la prohibición de acceder a los datos personales y la obligación de secreto que el personal debe observar.

DOCUMENTO DE SEGURIDAD

□ ¿Qué debo hacer para documentar y/o notificar las funciones y obligaciones del personal?

La descripción de las funciones del personal con acceso a datos de carácter personal tienen que estar incluidas en el documento de seguridad y formarán parte de las medidas organizativas que el responsable del fichero y, en su caso, el encargado del tratamiento debe implantar.

El procedimiento de documentación y transmisión de las políticas que incluyan las funciones y obligaciones del personal con acceso a datos de carácter personal, puede ser diverso dependiendo de las particularidades de cada organización, pudiendo utilizarse documentos escritos, comunicaciones electrónicas, ya sea mediante correo electrónico, intranet corporativa, páginas de inicio de las aplicaciones, etc.

En todo caso, será necesario que el responsable del fichero y, en su caso, el encargado del tratamiento se aseguren que el personal con acceso a datos de carácter personal conoce las funciones y obligaciones que tiene con respecto al acceso a los datos de carácter personal, en particular, en lo relativo al deber de secreto y confidencialidad.

¿Qué permite la delegación de autorizaciones?

La delegación de autorizaciones, a la que se refiere el artículo 84 del Reglamento, es una posibilidad que permite flexibilizar la gestión de la seguridad en materia de protección de datos de carácter personal.

Esta previsión habilita al responsable para delegar en otras personas las funciones que el Reglamento atribuye al responsable del fichero. Estas delegaciones deben estar recogidas en el documento de seguridad y no suponen, en ningún caso, trasladar a la persona en quien se delega la responsabilidad en la que pudiera incurrir la organización o persona responsable del fichero.

¿Debe contener el registro de incidencias detalle de los problemas asociados a aspectos puramente técnicos de los ficheros: averías, caídas de tensión, problemas de red o conectividad?

El objetivo fundamental de implantar las medidas de seguridad a las que se refiere la LOPD (art. 9) y su Reglamento de desarrollo es garantizar que los datos de carácter personal se tratan con las adecuadas garantías que permitan asegurar la confidencialidad, la integridad y la disponibilidad de los datos.

En éste ámbito las incidencias poseen una gran relevancia debido tanto a su propia capacidad para comprometer los objetivos de la seguridad como por el conocimiento que su resolución aporta a los responsables. Así, por ejemplo una avería eléctrica puede poner en peligro la disponibilidad de un sistema de información.

Teniendo en cuenta los objetivos de la seguridad, la inclusión de las incidencias de este tipo deberá realizarse siempre cuando con motivo del funcionamiento de estos servicios la seguridad pudiera verse comprometida.

□ ¿Cuál es el alcance y el objetivo del registro de incidencias?

La obligación de establecer un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal, así como establecer un registro en el que se hagan constar los detalles de dichas incidencias, se encuentra regulado en el artículo 90 y 100 del Reglamento, dependiendo que el nivel de medidas de seguridad requeridas sea básico o medio.

El objetivo final perseguido por el Reglamento a este respecto, tal y como lo señala en el artículo 90 citado, es que se adopten las medidas correctoras para que dicha incidencia sea controlada, por lo que debe mantenerse una acción permanente de control, revisión y actuación sobre las medidas implantadas y las incidencias detectadas.

□ ¿Cuál es el alcance de la obligación de anotar las salidas de soportes mediante correo electrónico?

El envío de ficheros con datos de carácter personal mediante correo electrónico o fax conlleva ciertos riesgos específicos que deberán ser analizados por el responsable del fichero y, en su caso, por el encargado del tratamiento para establecer las medidas técnicas y organizativas que deben implantarse para controlar los riesgos inherentes a la utilización del dichos medios, en función de los tipos de datos que vayan ser objeto de transmisión.

En cualquier caso, tal y como establece el artículo 92 del Reglamento la salida de soportes y documentos que contengan datos de carácter personal, como los incluidos 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 o ser debidamente autorizada en el documento de seguridad.

En el caso de los ficheros que deben implantar las medidas catalogadas como de nivel medio, el artículo 97 del Reglamento establece la obligación de disponer de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer la información relacionada con el envío. En el caso de las medidas de seguridad de nivel alto, la distribución de los soportes deberá realizarse cifrando los datos o utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte (art. 101 Reglamento).

Por lo que respecta concretamente al sistema de registro, en el caso de que se remitan datos de carácter personal incluidos en un anexo a un correo electrónico, el propio gestor del correo electrónico puede servir como registro.

Esta obligación de anotar las salidas afecta a cualquier otro procedimiento electrónico como el protocolo FTP, descargas desde Internet, carpetas compartidas, así como al envío de fax cuando incorporan datos de carácter personal de un fichero o tratamiento.

- **¿Debe registrarse la salida de soportes con destino a otra sede de la entidad? ¿Y a la del encargado?**

Deben anotarse tanto en uno como en el otro caso, ya que se trata de asegurar el control y la trazabilidad de los soportes con datos de carácter personal que salen materialmente del sistema de información del responsable del fichero.

¿Debe notificarse a la AEPD el documento de seguridad?

El documento de seguridad es un documento interno de la organización y no debe ser notificado a la Agencia Española de Protección de Datos, quedando a disposición de la Agencia o, en su caso, de las autoridades de protección de datos de las Comunidades Autónomas.

MEDIDAS CONCRETAS

¿Qué significa guardar las copias de respaldo en lugar físico diferente?

Para los ficheros con datos de carácter personal sujetos a la obligación de implantar las medidas de nivel alto, el reglamento de desarrollo de la LOPD prevé la obligación de conservar una copia de respaldo de los datos de estos ficheros y de los procedimientos de recuperación de los mismos en un lugar diferente del que se encuentran los equipos informáticos que los tratan (art. 102 Reglamento LOPD), con el fin de que no se encuentren sometidos a las mismas contingencias que pudiera sufrir el lugar habitual de almacenamiento en caso de un accidente o desastre, como por ejemplo, un incendio o una inundación.

En el caso de que no sea posible guardar una copia de los ficheros en un lugar distinto y no sujeto a los mismos riesgos, se deberán adoptar medidas complementarias para paliar el riesgo, tales como ubicar la copia en armarios ignífugos, implantación de sistemas antiincendio, etc). En estos casos, cuando la sede del responsable cuente con distintas estancias o niveles de edificación se entenderá por lugar distinto una estancia diferenciada del lugar principal en el que se ubiquen los sistemas de información, preferiblemente en planta distinta y más protegida y, se deberá hacer constar estas circunstancias en el documento de seguridad.

Debe hacerse notar que la obligación de realizar copias de respaldo no es aplicable a los ficheros no automatizados, con independencia del resto de medidas aplicables e este tipo de ficheros, entre las que deberán observarse las previsiones establecidas en el Reglamento

de la LOPD, entre otras, en lo relativo a la custodia de los soportes y dispositivos de almacenamiento, así como a la copia o reproducción de los documentos con datos de carácter personal.

- **¿Cuál es el ámbito de la auditoría establecida en el RLOPD? ¿Quién debe realizarla? ¿Debe notificarse?**

El ámbito de la auditoría, previsto en el artículo 96 para los ficheros automatizados y 110 para los no automatizados, se refiere a la verificación del cumplimiento de las medidas de seguridad que deben implantarse en los ficheros automatizados y no automatizados con datos de carácter personal establecidas en el Título VIII del Reglamento de desarrollo de la LOPD, sin perjuicio de que cuando alguna de las materias reguladas la LOPD se proyecten sobre las medidas de seguridad deban ser tenidas en cuenta.

Así por ejemplo, es evidente que una salida de datos podría tener relación con una comunicación de datos pudiendo analizarse su licitud. Del mismo modo, la existencia de un encargado del tratamiento puede comportar una evaluación conexa del contenido del contrato.

Sobre quién debe realizarla, el Reglamento establece que puede ser interna o externa y no define el perfil funcional o profesional de los auditores, aunque la propia función de auditoría ha de llevar implícita la independencia y la debida capacitación profesional para que resulte adecuada para la función de verificación que pretende llevar a cabo.

Por último, el informe de auditoría deberá ser analizado por el responsable de seguridad que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras y quedará a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de la comunidades autónomas, no siendo necesario su notificación a la AEPD.

¿Cuál debe ser el alcance del registro de accesos?

La obligación de implantar y guardar, durante un período mínimo de dos años, los datos relativos a los accesos realizados a los datos catalogados como de nivel alto, prevista en el artículo 103 del Reglamento de la LOPD, persigue que se pueda identificar el registro accedido. En este sentido, el objetivo es el de ser capaz de establecer las acciones realizadas por un determinado usuario respecto del registro accedido sin necesidad de que tal conocimiento alcance al contenido concreto de la información accedida.

El citado artículo establece la información mínima que deberá guardarse de cara acceso a los datos de carácter personal sujetos a la obligación de implantar las medidas de nivel alto.

Así mismo, se establecen las circunstancias concretas en las que el Reglamento excepciona de la obligación de implantar el registro de accesos: el responsable debe ser una persona física y debe ser el único usuario del sistema. Esta circunstancia deberá hacerse constar en el documento de seguridad.

¿Cómo aplico el control de acceso previsto para los ficheros no automatizados o manuales?

En el caso de los ficheros no automatizados con nivel alto de seguridad, el Reglamento de la LOPD establece, en su artículo 113 las medidas que han de adoptarse para controlar el acceso a la documentación a la que deba implantarse las medidas de nivel alto.

Para implantar este control de acceso a la documentación se podrán utilizar, por ejemplo:

- Plantillas básicas en soporte papel incorporadas al inicio del expediente.
- Registros automatizados en la gestión de entradas y salidas al archivo.
- Cualquier otro sistema o procedimiento que permita alcanzar la finalidad perseguida por el Reglamento.

OTROS ASPECTOS

En caso de una sanción por falta de medidas de seguridad ¿qué responsabilidad tiene el Responsable de Seguridad?

La responsabilidad de implantar las medidas de seguridad en los ficheros con datos de carácter personal recae en el responsable del fichero y, en su caso, en el encargado del tratamiento.

Así, entre las medidas organizativas se procederá a nombrar uno o varios responsables de seguridad. Esta designación es una previsión establecida en el Reglamento de la LOPD para los ficheros que tengan que implantar las medidas de seguridad catalogadas como de nivel medio y alto.

La medida que establece el artículo 95 del Reglamento, no puede suponer, en ningún caso, una exoneración de la responsabilidad que corresponda al responsable del fichero o al encargado del tratamiento.

□ ¿Qué tengo que pedir al proveedor cuando adquiera un producto software que trate datos de carácter personal?

La Disposición adicional única del Reglamento de desarrollo de la LOPD establece que los productos software destinados al tratamiento automatizado de datos de carácter personal deberán incluir en su descripción técnica el nivel de seguridad que tiene implantado, por lo que cuando se adquiera o se contrate la construcción de un aplicativo software que trate datos de carácter personal, se deberá pedir que el constructor especifique el nivel de medidas de seguridad que cumple el producto.

- **Para el cómputo de plazos para la implantación de las medidas de seguridad ¿cuándo se considera que son ficheros preexistentes?**

Se consideran ficheros preexistentes a los efectos de, en su caso, disponer del período transitorio para implantar las medidas de seguridad al que se refiere la Disposición transitoria segunda del Reglamento de desarrollo de la LOPD, los ficheros que hubieran sido notificados para su inscripción con anterioridad a la entrada en vigor del Reglamento de desarrollo de la LOPD, aprobado mediante el RD 1720/2007, de 21 de diciembre, publicado en el BOE del 19 de enero de 2008.

FICHEROS EXISTENTES		NIVEL	PLAZO
AUTOMATIZADOS	SEGURIDAD SOCIAL, MUTUAS, PERFILES	MEDIO	1 AÑO
	VIOLENCIA DE GÉNERO	MEDIO	1 AÑO
		ALTO	18 MESES
	TELECOMUNICACIONES (TRÁFICO, LOCALIZACIÓN) REGISTRO DE ACCESOS	MEDIO	1 AÑO 18 MESES
	ADAPTACIÓN RESTO DE FICHEROS		1 AÑO
NO AUTOMATIZADOS		BÁSICO	1 AÑO
		MEDIO	18 MESES
		ALTO	2 AÑOS

Dado que en la citada disposición se establecía la entrada en vigor del Reglamento a los tres meses de su publicación en el BOE, tendrán la consideración de ficheros preexistentes, a los efectos de la implantación de las medidas de seguridad, los ficheros que hayan sido notificados al Registro General de Protección de Datos hasta el día 19 de abril de 2008.

Cualquier fichero notificado con posterioridad deberá incorporar el conjunto de medidas previstas para el nivel de seguridad que le corresponda.

En la web de la Agencia Española de Protección de Datos, se encuentra disponible la versión actualizada de las preguntas frecuentes relacionadas con esta Guía de Seguridad.

www.agpd.es

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS

www.agpd.es