## ANEXO 6

## *Modelo de Documento de seguridad*[[1]](#footnote-1)

|  |  |
| --- | --- |
| Fecha versión del Documento de seguridad | dd/mm/aaaa |
| Versió del Document de seguretat | XXX |

**Documento de seguridad de los ficheros de** ..............

*(indicar el órgano responsable de los ficheros)*[[2]](#footnote-2)

**Aviso de confidencialidad**

A este documento, así como al resto de documentación y de informaciones relacionadas con las medidas de seguridad de los ficheros de .................... *(indicar el órgano responsable de los ficheros),* sólo tienen acceso las personas designadas en este mismo documento, sin perjuicio que el cumplimiento de las obligaciones derivadas de la regulación del derecho a la protección de datos de carácter personal o de otras normativas aplicables implique el acceso a este documento por parte de terceros.

***Estructura del documento de seguridad***

Este documento y sus anexos recogen las medidas de carácter técnico y organizativo necesarias para garantizar la seguridad de los datos y de los tratamientos relacionados con los ficheros responsabilidad de .................... *(indicar el órgano responsable de los ficheros).* Estas medidas sirven para evitar la alteración, la pérdida, el tratamiento o el acceso no autorizado a los datos que contienen y garantizar su disponibilidad.

* **Parte general**
* *(Incluir en esta parte los aspectos más generales de las medidas de seguridad y menos susceptibles de ser modificados en periodos cortos de tiempo)*

1. Ámbito de aplicación del documento

2. Normativa aplicada y medidas de seguridad aplicables

3. Funciones y obligaciones del personal

4. Estructura de los ficheros y descripción de los sistemas de tratamiento

5. Gestión de incidencias

6. Copias de seguridad

7. Gestión de soportes y documentos

8. Destrucción de información y reutilización de soportes

9. Auditoría

10. Revisión del documento de seguridad

* **Anexos**
* (*Incluir en los anexos las descripciones técnicas, informaciones, normas, procedimientos, registros, etc., que pueden ir variando fácilmente en el tiempo. Se pueden identificar con un código descriptivo del tipo de información que contiene, como por ejemplo INF (Información relevante para la seguridad de la información o REG (registros y/o inventarios). Cuando se establezca en el documento de seguridad, estos anexos pueden estar en formato electrónico.)*

|  |  |
| --- | --- |
| **Código documento**  *(indicar la codificación/clasificación utilizada)* | **Descripción**  *(indicar la denominacinó del documento anexo)* |
| *INF001* | *Descripción del sistema informático. Características*  *técnicas del hardware y el software* |
| *INF002* | *Usuarios y autorizaciones de acceso a los datos* |
| *INF003* | *Estructura de los ficheros* |
| *INF004* | *Delegación de autorizaciones* |
| *INF005* | *Encargados del tratamiento* |
| *INF006* | *Prestadores de servicios sin acceso a datos* |
| *REG001* | *Entrega del documento de seguridad* |
| *REG002* | *Registro de incidencias* |
| *REG003* | *Registro de copias de seguridad* |
| *REG004* | *Inventario de soportes* |

**1.Ámbito de aplicación del documento**

Este documento de seguridad ha sido elaborado por *............... (indicar el órgano responsable de los ficheros),* que es responsable de los ficheros que se detallan a continuación:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Denominación del fichero** | **Código de inscripción** | **Fecha de la resolución de inscripción** | **Nivel de seguridad** | **Sistema de tratamiento** |
| *......................*  *(indicar la denominación del fichero, p. ej. "alumnos", "personal", "proveedores", etc.)* | *.................*  *(indicar el código de inscripción asignado al fichero)* | *dd/mm/aaaa*  *(indicar la fecha de la resolución de inscripción del fichero)* | *..................*  *(indicar  el nivel básico/medio/alto de seguridad del fichero)* | *.................................*  *(indicar el sistema automatizado/no automatizado/parcial-mente automatizado en qué se organiza el sistema de información)* |

Este documento se tiene que mantener permanentemente actualizado y cualquier modificación relevante tiene que comportar su revisión y, si procede, la modificación parcial o total.

**2.Normativa aplicada y medidas de seguridad aplicables**

En la elaboración de este documento de seguridad se ha tenido en cuenta la normativa siguiente:

* Art. 9 de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
* Art. 79 a 114 del reglamento de desarrollo de la LOPD (RLOPD), aprobado por el Real decreto 1720/2007, de 21 de diciembre
* Apartado tercero de la disposición adicional vigésimotercera de la Ley orgánica 2/2006, de 3 de mayo, de educación
* Disposición adicional decimocuarta de la Ley 12/2009, del 10 de julio, de educación ........

.................... (*indicar, si procede, otra normativa aplicable)*

Son de aplicación a los diferentes ficheros a que se refiere este documento de seguridad las medidas de seguridad previstas en el RLOPD y las que se concretan en este documento, de acuerdo con el nivel de seguridad que se describe para cada uno de ellos en el apartado 1 de este documento.

Las medidas que se describen en este documento para cada nivel de seguridad son de carácter acumulativo, es decir que en cada nivel se tienen que aplicar no sólo las medidas indicadas específicamente para este nivel, sino también las que corresponden a los niveles inferiores.

El incumplimiento de este documento de seguridad puede ser objeto de sanción, de acuerdo con.............. *(indicar el régimen sancionador aplicable).*

**3.Funciones y obligaciones de las persones autorizadas a tratar los datos**

Las personas que tengan acceso o que traten los datos contenidos en los ficheros del .................... *(indicar el responsable de los ficheros)* tienen que conocer y observar las medidas de seguridad y obligaciones relacionadas establecidas en este documento de seguridad*.*

Con este objetivo, se les tiene que entregar una copia del documento de seguridad vigente[[3]](#footnote-3), con la advertencia que se trata de un documento confidencial y que tienen que mantener reserva sobre su contenido. Para acceder a los datos, hace falta que hayan firmado la recepción del documento.

Obligaciones de carácter general para las personas con acceso a los datos de los ficheros:

1. Conocer y cumplir, en aquello que les sea de aplicación, lo que prevé este documento de seguridad.
2. Notificar a ................... *(indicar la persona o el servicio a quién hay que informar)* cualquier incidencia que pueda afectar a la seguridad de los datos.
3. Guardar secreto y confidencialidad sobre los datos personales de los ficheros.

El documento anexo .................. *(indicar el código utilizado para designar el documento anexo relativo a la "entrega del documento de seguridad". Siguiendo el ejemplo de los anexos de este modelo, sería el documento REG001)* recoge la lista de las personas a quienes se ha entregado el documento de seguridad, con la fecha y la firma de recepción.

El personal ajeno a ......... *(indicar el centro o la organización de que se trata)* con acceso a los datos, está sometido a las mismas condiciones y obligaciones de seguridad que el personal propio así como a las previsiones específicas incluidas en este documento de seguridad y las que se incluyan en el acuerdo o contrato de encargo del tratamiento.

En el caso de incumplimiento de lo que se prevé en este documento, el ................... *(indicar el responsable de los ficheros)* se reserva el derecho de iniciar las acciones legales que considere más adecuadas para proteger sus intereses o los de terceros.

3.1. Control d’accés a les dades

El personal sólo puede acceder a los datos y a los recursos necesarios para ejercer sus funciones. Las personas autorizadas a acceder a los datos de los ficheros y las operaciones que pueden realizar cada uno de ellos figuran en el documento anexo .................. (*indicar el código utilizado para designar el documento anexo relativo a los "usuarios y autorizaciones de acceso a los datos". Siguiendo el ejemplo de los anexos de este modelo, sería el documento INF002*). Las personas con acceso a los datos sólo pueden hacer uso de ellos en relación con las funciones que tienen atribuidas.

Para que otras personas que no figuran en este documento de seguridad puedan acceder a la información, hay que contar con la autorización del responsable del fichero (*o personas en quienes delegue*) o del responsable de seguridad.

|  |
| --- |
| NIVEL ALTO. **REGISTRO DE ACCESOS**  FICHEROS AUTOMATIZADOS  Para cada acceso a los datos de los ficheros de nivel alto, se tiene que registrar la identificación del usuario, la fecha y la hora en la que ha accedido, a qué fichero ha accedido, el tipo de acceso y si el acceso ha sido autorizado o denegado. Si se autorizó el acceso, también se tiene que almacenar la información que permite identificar el registro al que se ha accedido.  *(indicar, si procede, otra información relativa al sistema de registro de accesos)*  Los datos del registro de accesos se tienen que conservar durante .................... *(concretar el periodo, que como mínimo tiene que ser de dos años).*  Este registro está bajo el control directo del responsable de seguridad. No se permite desactivarlo en ningún caso.  El responsable de seguridad tiene querevisar una vez al mes, como mínimo, la información de control registrada y tiene que elaborar un informe.  *(indicar los procedimientos para hacer el informe mensual sobre el registro de acceso a datos de nivel alto, regulado por el artículo 103 del RLOPD).*  FICHEROS NO AUTOMATIZADOS  El acceso a la documentación se limita exclusivamente al personal autorizado que consta en el documento anexo .................. *(indicar el código utilizado para designar el documento anexo, relativo a los "usuarios y autorizaciones de acceso a los datos". Siguiendo el ejemplo de los anexos de este modelo, sería el documento INF002).*  El mecanismo para identificar los accesos a los documentos relacionados es el que sigue ..................... *(indicar los tipos de documentos que pueden utilizar múltiples usuarios, así como el mecanismo establecido para controlar los accesos).* |

3.2. Identificación y autenticación

Cada usuario autorizado a acceder a los datos de los ficheros tiene asignado un código de usuario personal y una palabra de paso o contraseña, que lo identifica de forma inequívoca y le permite autenticarse en los equipos necesarios para acceder a la información.

Corresponde al .................... *(indicar el responsable de los ficheros o, si es el caso, el responsable de seguridad)* dar de alta y de baja a los usuarios al sistema y proporcionarles el código de usuario y la palabra de paso asignada .................. *(indicar la manera en qué se proporcionará esta información para garantizar la confidencialidad).* La palabra de paso otorgada y sus modificaciones se tienen que almacenar de manera cifrada.

Las palabras de paso o contraseñas asignadas tienen que reunir las características siguientes: ..................... *(indicar las características de las contraseñas. Se recomienda una longitud mínima de ocho caracteres y la combinación de letras, números, mayúsculas, minúsculas y, si el sistema lo permite, símbolos*).

Las palabras de paso o contraseñas se tienen que modificar la primera vez que el usuario accede al ordenador y antes de acceder o tratar los datos incluidos en los ficheros. Asimismo, cada usuario tiene que modificar su palabra de paso o contraseña cada ................... *(indicar la periodicidad, que como mínimo tiene que ser una vez al año*).

|  |
| --- |
| NIVEL MEDIO O ALTO  En los ficheros de nivel medio y alto, se limita la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información de la manera siguiente ................... *(indicar los mecanismos, como por ejemplo bloquear el código de usuario después de tres intentos frustrados de acceso).* |

3.3. Responsable de seguridad

Se designa como responsable de seguridad ..................... *(indicar la persona o las personas designadas)*, que se encarga de coordinar y controlar las medidas establecidas en este documento de seguridad en relación con ...................... *(indicar si la designación es única para todos los ficheros o no. En este último caso, hay que especificarlo),* calificados de nivel medio o alto.

En ningún caso la designación supone la exoneración de la responsabilidad que corresponde a ................... *(indicar el responsable de los ficheros)* como responsable del fichero, de acuerdo con el RLOPD.

La designación se hace por un periodo de ................. *(indicar el periodo durante el cual se ejercerá el cargo).* Transcurrido este plazo, se puede nombrar la misma persona como responsable de seguridad u otra diferente.

El anexo .................... *(indicar el anexo que, si procede, contiene los nombramientos (original o copia) que afectan a los diferentes perfiles incluidos en este documento de seguridad)* incluye ....... (*el original/la copia)* del nombramiento del responsable de seguridad.

El responsable de seguridad tiene que hacer controles periódicos, como mínimo cada ............ meses, para verificar el cumplimiento de lo que dispone este documento de seguridad.

3.4. Prestación de servicios por terceros con acceso a datos

La prestación de servicios por terceras personas o entidades que comporta el acceso a datos personales de los ficheros o de los sistemas de que es responsable ................. *(indicar el responsable de los ficheros)* requiere la suscripción del contrato o el acuerdo de encargo a que se refiere el artículo 12 de la LOPD, y se considera un encargo del tratamiento.

En el documento anexo .................. *(indicar el código utilizado para designar el documento anexo relativo a "Encargados del tratamiento". Siguiendo el ejemplo de los anexos de este modelo, sería el documento INF005),* se relacionan los terceros que actúan como encargados del tratamiento por cuenta de ..................... *(indicar el responsable del fichero),* con indicación de si los datos necesarios para prestar los servicios se tratan en los locales del ..................... *(indicar el responsable del fichero)* o bien en los del encargado de los ficheros o tratamientos afectados por el encargo, y del contrato o acuerdo de encargo suscrito y su vigencia.

El encargado del tratamiento tiene que guardar secreto y confidencialidad sobre los datos personales de los ficheros a los cuales tiene acceso para prestar el servicio encargado.

*3.4.1. Tratamiento de los datos en los locales de*..................*(indicar la organización a la cual pertenece el responsable de los ficheros):*

Si, de conformidad con el contrato o el acuerdo de encargo suscrito, el servicio se presta en los locales de ................... *(indicar* *la organización a la cual pertenece el responsable de los ficheros)*, el acceso del encargado del tratamiento a los datos de los ficheros y los sistemas se debe hacer con los recursos y los sistemas de información que facilite el .................... *(indicar el responsable de los ficheros).*

El personal del encargado del tratamiento tiene que cumplir las medidas de seguridad previstas en el RLOPD y en este documento de seguridad, de conformidad con el nivel de seguridad que se describe para cada uno de los ficheros en el apartado 1 de este documento. A este efecto, se les tiene que entregar una copia íntegra del documento de seguridad vigente y dejar constancia en el documento anexo .................. *(indicar el código utilizado para designar el documento anexo relativo a la "entrega del documento de seguridad". Siguiendo el ejemplo de los anexos de este modelo, sería el documento REG001).*

Los datos de los ficheros a que se accede para prestar el servicio no pueden salir fuera de los locales del .................... *(indicar la organización a la cual pertenece el responsable de los ficheros).*

Para que los datos se puedan tratar fuera de los locales de .................... *(indicar los locales habituales de trabajo)*, así como para incorporarlos en dispositivos portátiles, hace falta que la autorización conste en el Anexo ...................... *(indicar el código utilizado para designar el documento anexo relativo a los "usuarios y autorizaciones de acceso a los datos". Siguiendo el ejemplo de los anexos de este modelo, sería el documento INF002)* de este documento de seguridad*.* En estos casos, hay que garantizar el nivel de seguridad correspondiente.

Una vez cumplida la prestación del servicio, el encargado del tratamiento tiene que destruir o devolver las copias de los datos y, si procede, los soportes donde constan*,* según lo que se establece en el Anexo ............. *(indicar el código utilizado para designar el documento anexo relativo a "Encargados del tratamiento". Siguiendo el ejemplo de los anexos de este modelo, sería el documento INF005)* de este documento de seguridad.

Si se ha establecido que el encargado tiene que devolver, al responsable de los ficheros o a otro encargado que haya designado, los datos personales y, si procede, los soportes donde constan, el encargado del tratamiento garantiza que el retorno comporta el borrado total de los datos de sus equipos informáticos utilizados para prestar el servicio, para impedir su reutilización.

Si se ha establecido que los datos personales y, si procede, los soportes donde constan, se tienen que destruir, la destrucción se tiene que hacer de acuerdo con el procedimiento establecido en el apartado 8 de este documento de seguridad y, en cualquier caso, se tiene que certificar por escrito. Este certificado se tiene que transmitir al .................. *(indicar el responsable de los ficheros)* lo antes posible.

El acceso remoto del encargado del tratamiento a datos, cuando así consta en el contrato o acuerdo de encargo suscrito, se hace mediante el sistema de autenticación de usuarios registrados establecido en el apartado 3.2 de este documento de seguridad.

El encargado del tratamiento tiene que poner en conocimiento de ................... *(indicar la persona o servicio a quien hay que informar de una incidencia)* cualquier incidencia que pueda afectar a la seguridad de los datos, de conformidad con el procedimiento establecido en el apartado 5 de este documento de seguridad.

3.4.2. *Tratamiento de los datos en los locales del encaregado del tratamiento:*

*(Se tienen que anotar en el documento de seguridad los casos en que los datos necesarios para prestar el servicio encargado se incorporan y se tratan de manera exclusiva en los sistemas del encargado del tratamiento, de conformidad con el contrato o el acuerdo de encargo suscrito.)*

Cuando, de conformidad con el contrato o acuerdo de encargo suscrito, los datos de los ficheros de los cuales es responsable ....................... *(indicar el responsable de los ficheros),* necesarios para prestar el servicio, se tratan en los locales del encargado del tratamiento, y exclusivamente con sus sistemas, éste se compromete a elaborar un documento de seguridad o bien a completar su propio documento de seguridad, si procede, con la indicación de:

* Ficheros afectados por la prestación del servicio
* Responsable de los ficheros
* Condiciones del encargo, en especial las medidas de seguridad establecidas en el contrato o el acuerdo de encargo
* Periodo de vigencia del encargo

Los datos de los ficheros a que se accede para prestar el servicio no pueden salir fuera de los locales del encargado del tratamiento. En caso de que sea necesario cambiar los locales donde se tratan, el encargado lo tiene que comunicar previamente al ...................... *(indicar el responsable de los ficheros*).

Para tratar los datos fuera de los locales del encargado del tratamiento, así como para incorporarlos a dispositivos portátiles, hace falta que conste la autorización en el Anexo ......... *(indicar el código utilizado para designar el documento anexo relativo a los "usuarios y autorizaciones de acceso a los datos". Siguiendo el ejemplo de los anexos de este modelo, sería el documento INF002)* de este documento de seguridad*.* En estos casos, hay que garantizar el nivel de seguridad correspondiente.

El encargado del tratamiento tiene que anotar las incidencias de seguridad en su registro de incidencias y tiene que poner en conocimiento de ................... *(indicar la persona o servicio a quien hay que informar de una incidencia),* de forma inmediata, cualquier incidencia que se produzca durante la ejecución del contrato que pueda afectar a la seguridad de los datos, de conformidad con el procedimiento establecido en el apartado 5 de este documento de seguridad.

Si la prestación del servicio encargado comporta el tratamiento de datos de ficheros de nivel medio o alto el encargado del tratamiento tiene que comunicar lo antes posible al ...................... *(indicar el responsable de los ficheros)* la identidad y el perfil profesional de la persona (o personas) designada como responsable de seguridad.

El encargado del tratamiento se tiene que someter a las auditorías de cumplimiento de la normativa de protección de datos decididas por ...................... *(indicar el responsable de los ficheros)* al inicio de la prestación, como mínimo cada .................... *(indicar el periodo que, en ficheros calificados de nivel medio y alto, tiene que ser mínimo de dos años)* y, en cualquier caso, siempre que se produzcan modificaciones sustanciales en los sistemas de información.

Una vez cumplida la prestación del servicio, el encargado del tratamiento tiene que destruir, entregar a un tercero o devolver las copias de los datos y, si procede, los soportes donde constan, de acuerdo con lo que se establece en el Anexo ............. *(indicar el código utilizado para designar el documento anexo relativo a "Encargados del tratamiento". Siguiendo el ejemplo de los anexos de este modelo, sería el documento INF005)* de este documento de seguridad. Todo esto, sin perjuicio que pueda guardar una copia, bloqueada, para hacer frente a las posibles responsabilidades derivadas del encargo.

Si se ha establecido que el encargado tiene que devolver los datos personales y, si procede, los soportes donde constan, al responsable de los ficheros o a otro encargado que haya designado,el encargado del tratamiento garantiza que el retorno comporta el borrado total de los datos de sus equipos informáticos utilizados para prestar el servicio.

Si se ha establecidoque los datos personales y, si procede, los soportes donde constan se tienen que destruir, la destrucción se tiene que certificar por escrito. Este certificado se tiene que transmitir al .................. *(indicar el responsable de los ficheros),* lo antes posible.

3.5. Prestación de servicios por terceros sin acceso a datos

El prestador del servicio se tiene que comprometer a poner en conocimiento de su personal las medidas que se detallan a continuación y a conservar la acreditación del cumplimiento de este deber.

El personal de las empresas contratadas para prestar servicios que no comportan el tratamiento de datos personales no puede acceder a los datos que figuran en archivos, documentos, ficheros y sistemas de información del .................... *(indicar el responsable de los ficheros).*

El personal de la empresa prestadora del servicio que tiene que acceder a los locales del .................... *(indicar el responsable de los ficheros)* ha de ...................... *(indicar el régimen/control de acceso físico a los locales).*

En el anexo ....................... *(indicar el código utilizado para designar el documento anexo relativo a los "prestadores de servicios sin acceso a datos". Siguiendo el ejemplo de los anexos de este modelo, sería el documento INF006)* se relacionan los prestadores de servicios del .................... *(indicar el responsable de los ficheros)* sin acceso a datos personales.

El acceso a los lugares en que están ubicados los servidores del .................... *(indicar el responsable de los ficheros)* se tiene que hacer ....................... *(indicar el régimen/control de acceso físico a los servidores o archivos donde se ubican los datos).*

El acceso a la documentación se limita exclusivamente al personal autorizado que consta en el documento anexo .................. *(indicar el código utilizado para designar el documento anexo relativo a los "usuarios y autorizaciones de acceso a los datos". Siguiendo el ejemplo de los anexos de este modelo, sería el documento INF002).*

El prestador del servicio tiene que poner en conocimiento del ...................... *(indicar la persona o servicio a quien se tiene que comunicar)*, de manera inmediata, cualquier incidencia que se produzca durante la ejecución del servicio que pueda afectar a la integridad o la confidencialidad de los datos personales tratados por el ...................... *(indicar el responsable de los ficheros),* de conformidad con el procedimiento establecido en el apartado 5 de este documento de seguridad.

Esta circunstancia se tiene que anotar en el registro de incidencias.

En caso de acceso accidental a datos personales, el personal del prestador del servicio está obligado a guardar secreto, incluso una vez finalizada la relación contractual. En ningún caso puede utilizar los datos ni revelarlos a terceros.

3.6. Delegación de autorizaciones y funciones de control

En el anexo .......... *(indicar el código utilizado para designar el documento anexo relativo a la "delegación de autorizaciones". Siguiendo el ejemplo de los anexos de este modelo, sería el documento INF004*) se recoge una relación de las personas a las cuales el responsable del fichero delega las autorizaciones que se mencionan.

**4. Estructura de los ficheros y descripción de los sistemas de tratamiento**

La estructura de los ficheros se detalla en el anexo .............. *(indicar el código utilizado para designar el documento anexo relativo a "Estructura de los ficheros y descripción de los sistemas de tratamiento". Siguiendo el ejemplo de los anexos de este modelo, sería el documento INF003).*

El sistema de tratamiento de los datos de los ficheros es parcialmente automatizado, ya que hay datos en ficheros informáticos, según las características descritas en los documentos ................. y................... *(indicar el código utilizado para designar los documentos anexos relativos a la "Descripción del sistema informático. Características técnicas del hardware y software" y en "Estructura de los ficheros y descripción de los sistemas de tratamiento". Siguiendo el ejemplo de los anexos de este modelo serían los documentos INF001 y INF003, respectivamente),* y también se dispone de información en formato papel, ya sea como soporte a la recogida de datos o para las salidas impresas del sistema informático.

Las medidas de seguridad implantadas son las del nivel que se indica en el apartado 1 de este documento para cada fichero, previstas en la normativa de protección de datos para los tratamientos automatizados y no automatizados.

Los datos de los ficheros pueden ser objeto de cualquier operación relacionada con su finalidad. Por lo tanto, de acuerdo con lo que se establece en el anexo .................. *(indicar el código utilizado para designar el documento anexo relativo a los "Usuarios y autorizaciones de acceso a los datos". Siguiendo el ejemplo de los anexos de este modelo, sería el documento INF002),* los usuarios autorizados pueden hacer operaciones de recogida, grabación, conservación, elaboración, modificación, consulta, utilización, cancelación, bloqueo o supresión, y también, si procede, la cesión a terceros como resultado de comunicaciones, consultas, interconexiones o transferencias de datos.

Estas operaciones se realizan tanto en relación a soportes automatizados como no automatizados, en cada caso adaptadas al sistema concreto de tratamiento.

4.1. Sistema de información

El sistema de información de los ficheros se basa en ........................ *(indicar, para todos los ficheros o para cada uno de ellos, el número de ordenadores/servidores en que se almacenan las bases de datos y/o los soportes en que se encuentran, con una breve descripción de los datos que contienen).*

El sistema de información de los ficheros se complementa con un archivo físico de papel, donde de manera estructurada se archivan los documentos relacionados con ....................... *(indicar, en relación con cada fichero, qué información hay en soporte papel).*

4.2. Copias de trabajo de documentos o fitcheros temporales

Una copia de trabajo parcial o total de los ficheros o de documentos en papel, para una tarea concreta o auxiliar relacionada con las finalidades de los ficheros, se considera un "fichero temporal". Le es de aplicación el nivel de seguridad que corresponda de acuerdo con los criterios establecidos en el RLOPD y lo que establece este documento de seguridad.

Una vez finalizada la tarea temporal, la copia de trabajo del fichero o de la documentación se tiene que destruir, según el procedimiento que prevé el apartado 8 de este documento.

4.3. Régimen de trabajo fuera de los locales de............*(indicar los locales habituales de trabajo)*

Se pueden hacer los tratamientos de datos personales de los ficheros .................... *(indicar los ficheros que afectan estos tratamientos)* fuera de los locales del ....................... *(indicar el responsable de los ficheros)*, en los supuestos siguientes: ..................... *(indicar los casos en que se pueden utilizar los datos fuera de los locales del responsable).* Se pueden utilizar dispositivos portátiles en los supuestos siguientes: ................... *(indicar los casos en que se pueden utilizar dispositivos móviles).*

Las personas autorizadas a este efecto son las que figuran en el anexo ...................... *(indicar el código utilizado para designar el documento anexo relativo a los "usuarios y autorizaciones de acceso a los datos". Siguiendo el ejemplo de los anexos de este modelo, sería el documento INF002).*

4.4. Acceso a datos a través de redes de comunicaciones

Se puede acceder a través de redes de comunicaciones a los ficheros siguientes ................... *(relacionar los accesos previstos y los ficheros a que se puede acceder).*

El acceso a los ficheros a través de redes de comunicaciones se tiene que hacer con medidas que garanticen un nivel de seguridad equivalente al exigido para los accesos en modo local.

|  |
| --- |
| NIVEL ALTO  La comunicación de los datos personales de ficheros de nivel alto que se transmitan a través de redes públicas o redes sin hilo de comunicaciones electrónicas se tiene que hacer............................ *(indicar si los datos se transmiten cifrados, o bien con otros mecanismos diferentes al cifrado de la información que garantizan que la información no será inteligible ni manipulada por terceros)* |

**5. Gestión de incidencias**

Se considera "incidencia de seguridad" cualquier incumplimiento de la normativa aplicable o de este documento de seguridad, así como cualquier otra anomalía que afecta o pueda afectar a la seguridad de los datos personales de ...................... *(indicar el responsable de los ficheros).*

......................... *(indicar las personas obligadas a notificar la incidencia, como por ejemplo, las personas autorizadas a acceder a los ficheros)* tienen que comunicar lo antes posible la incidencia a ............................. *(indicar la persona o el servicio a quien se tienen que comunicar los hechos o las circunstancias que se sospecha o se tiene la certeza de que pueden afectar a la seguridad de los datos).*

Esta comunicación se tiene que hacer ........................ *(indicar la manera en que se tiene que comunicar la incidencia: comunicación oral, por escrito o por cualquier otro medio que se considere oportuno).*

....................... *(indicar la persona o el servicio que gestiona las incidencias)* gestiona las comunicaciones recibidas, las valora y adopta, si procede, las medidas oportunas para corregir la situación detectada.

....................... *(indicar la persona o el servicio que gestiona las incidencias)* tiene que anotar en el registro de incidencias (ver documento anexo ....................) *(indicar el código utilizado para designar el documento anexo relativo a "Registro de incidencias". Siguiendo el ejemplo de los anexos de este modelo, sería el documento REG002*)) los datos siguientes relacionados con la incidencia detectada:

1. Tipo de incidencia
2. Momento en que se ha producido y detectado
3. Quién la ha notificado
4. A quién la ha comunicado
5. Consecuencias
6. Medidas correctoras adoptadas o que se proponen

|  |
| --- |
| NIVEL MEDIO y ALTO  En el registro de incidencias se tienen que consignar también las recuperaciones de datos que afectan a los ficheros de nivel medio o alto ................... *(detallar el procedimiento seguido para recuperar los datos, con indicación de la persona que lo ha ejecutado, los datos restaurados y, si procede, los datos que se han tenido que grabar manualmente en el proceso de recuperación. En caso de gestión automatizada,* *en la información relativa al tipo de incidencia preveer un código específico para recuperaciones de datos).*  Para los procedimientos de recuperación de datos en estos ficheros, hace falta la autorización por escrito de ................... *(indicar el responsable del fichero).* |

**6. Copias de seguridad y recuperación**

6.1. Copia de seguridad

Se tiene que hacer una copia de seguridad .................. *(indicar la periodicidad que, como mínimo, tiene que ser semanal)* de los ficheros, a menos que los datos no se hayan modificado en todo el periodo mencionado.

Este proceso consiste en copiar los ficheros en un dispositivo externo, de acuerdo con el procedimiento siguiente:

El proceso de copia de seguridad tiene que permitir garantizar la reconstrucción de los ficheros al estado que tenían en el momento de producirse una eventual pérdida o destrucción de los datos.

La copia de seguridad la tiene que hacer .................... *(indicar la persona o el servicio encargado de hacer las copias de seguridad).*

Cada seis meses ...................... *(indicar la persona o el servicio encargado de verificar este proceso)* tiene queverificar que las copias se hacen correctamente y que se pueden restaurar. Para hacerlo, tiene que aplicar los procedimientos de copia y restauración sin afectar a los datos reales. Los ficheros resultantes se tienen que suprimir una vez hechas las verificaciones.

Si, entre la fecha en que se hizo la última copia de seguridad y la fecha en que es necesario hacer la restauración, la información se ha modificado y se puede recuperar manualmente a partir de documentación en papel, esta circunstancia se tiene que hacer constar en el registro de incidencias con el máximo detalle posible.

Si hace falta modificar el hardware o bien sustituir los ordenadores, o trasladar los datos a otro tipo de fichero, antes se tiene que hacer una copia de seguridad.

Se tiene que evitar hacer pruebas con datos reales, antes de implantar o modificar los sistemas de información. Si no es posible, se tiene que hacer previamente una copia de seguridad, se tiene que asegurar el nivel de seguridad correspondiente al tratamiento realizado y anotar las pruebas en este documento de seguridad.

En el documento ................. *(indicar el código utilizado para designar el documento anexo relativo al "Registro de copias de seguridad". Siguiendo el ejemplo de los anexos de este modelo, sería el documento REG003) se* tiene que anotar la fecha y la hora de ejecución de cada copia de seguridad, la persona que lo ha hecho y las observaciones relativas al proceso.

6.2. Recuperación

Si hay que utilizar la copia de seguridad para recuperar la información, se tiene que seguir el procedimiento de copia a la inversa, copiando la información del dispositivo externo de almacenamiento a la carpeta del ordenador donde tiene que quedar ubicado el fichero.

Si la información de recuperación se introduce manualmente, hay que dejar constancia en el registro de incidencias.

|  |
| --- |
| NIVEL MEDIO Y ALTO  Para la ejecución del procedimiento de recuperación de datos hace falta la autorización del responsable del fichero.  En los ficheros que contienen datos de nivel medio y alto, la recuperación se tiene que anotar en el documento ... *(indicar el código utilizado para designar el documento anexo relativo al "Registro de incidencias". Siguiendo el ejemplo de los anexos de este modelo, sería el documento REG002)* indicandola persona que ha ejecutado el proceso, los datos restaurados y, si procede, qué datos ha sido necesario grabar manualmente en el proceso de recuperación. |

|  |
| --- |
| NIVEL ALTO  En los ficheros de nivel alto, se tiene que conservar una copia de seguridad de los datos y de los procedimientos de recuperación de datos en ...................... *(indicar el lugar, que tiene que ser diferente de donde se ubican los sistemas informáticos que tratan los datos y tiene que cumplir con las medidas de seguridad o bien utilizar elementos que garanticen la integridad y la recuperación de la información).* |

**7. Gestión de soportes y documentos**

Los soportes con datos de carácter personal se deben identificar con los tipos de información que contienen, se deben inventariar y se deben almacenar en el lugar de acceso restringido que consta en el anexo .................. *(indicar el código utilizado para designar el documento anexo relativo a "Inventario de Soportes". Siguiendo el ejemplo de los anexos de este modelo, sería el documento REG004*), al cual sólo tienen acceso las personas que se relacionan en el anexo mencionado.

En el inventario de soportes constan las personas autorizadas para acceder a cada uno de los soportes.

En caso de que, por razón de urgencia o fuerza mayor, tenga que acceder personal no autorizado, es necesario .................... *(describir el procedimiento para acceder a los locales en estos casos).*

Estas obligaciones no se aplican a los soportes siguientes .................... *(indicarlos)*, dado que sus características físicas imposibilitan su cumplimiento.

Los soportes se tienen que almacenar de acuerdo con las normas siguientes: ...................... *(indicar las normas de etiquetado y almacenaje de los soportes).*

Si hay que traspasar los datos a un soporte externo (p. ej. disco duro externo, memoria USB, CD o DVD, etc.) fuera del equipo donde se tratan habitualmente, este soporte se tiene que etiquetar con el nombre ......................... *(indicar el nombre del fichero y la fecha en que se traspasan los datos, por ejemplo, fichero X\_dd/mm/aaaa),* de manera que se pueda reconocer con facilidad el contenido y la fecha de copiado de los datos.

7.1. Dispositivos de almacenamiento de los documentos en papel

Para guardar los documentos en soporte papel con datos personales se pueden utilizar los elementos de almacenaje siguientes: ......................... (*armarios y archivadores u otros, así como las características de que disponen para obstaculizar la apertura o, en su defecto, las medidas adoptadas por el responsable del fichero para evitar que personas no autorizadas accedan a la información).*

|  |
| --- |
| NIVEL ALTO  Los documentos en papel que contienen datos de carácter personal se tienen que almacenar en ......................... *(armarios y archivadores u otros elementos utilizados),* que hay que cerrar con ......................... *(indicar el mecanismo para obstaculizar la apertura, tales como clavos u otros dispositivos)* que se tienen que ubicar en las zonas siguientes:........................... *(indicar el lugar donde están ubicados los elementos de almacenaje)*. Estos espacios tienen que permanecer cerrados cuando no sea necesario acceder a los documentos.  *(Si no es posible cumplir con lo que se expone, el responsable tiene que adoptar medidas alternativas que impidan que personas no autorizadas accedan a la información y describirlas en este apartado del documento de seguridad).* |

7.2. Criterios de archivo de la documentación en papel

El archivo de los soportes o de la documentación se tiene que hacer de acuerdo con los criterios ...................... *(indicar los criterios de archivo previstos en la legislación que los afecte o, en su defecto, los establecidos por el responsable del fichero. En cualquier caso, tienen que garantizar la conservación y la localización de la documentación y la consulta de la información, así como la posibilidad de atender los derechos de acceso, rectificación, oposición y cancelación).*

7.3. Custodia de los documentos en papel

Cuando la documentación en soporte papel no está depositada en los dispositivos de almacenamiento habituales, circunstancia que sólo se puede dar cuando se está trabajando, la persona que la utiliza la tiene que custodiar e impedir que puedan acceder personas no autorizadas. Hay que tener especial cuidado de no descuidar papeles en la mesa de trabajo o en otros espacios comunes o de libre acceso.

7.4. Salida de soportes y documentos

En el inventario de soportes constan las autorizaciones de salida de los soportes y documentos, incluidos los contenidos en correos electrónicos o en cualquier dispositivo móvil, fuera de .................... *(indicar el lugar habitual de tratamiento de la información)* y la persona que la ha autorizado*.* Tienen que constar, de manera diferenciada, tanto las autorizaciones de salida de soportes y documentos genéricos de procesos periódicos que se prevén en el documento de seguridad, como las autorizaciones de salidas puntuales de soportes y documentos hechas específicamente por el responsable de los ficheros.

La autorización de la salida de los soportes se tiene que hacer de la forma siguiente .................... *(indicar el procedimiento a seguir para autorizarla).*

Durante el traslado físico de los soportes que contienen datos personales se tienen que aplicar las medidas siguientes para evitar la sustracción, el acceso indebido o la pérdida de la información: ..................... *(indicar las medidas y procedimientos previstos).*

La persona que transporta el soporte es la responsable de custodiarlo. Por lo tanto, tiene que actuar con la diligencia necesaria para aplicar estas medidas y evitar incidentes con los datos. En todo caso, el .................. *(indicar el responsable de los ficheros)* puede dar instrucciones concretas de protección cuando lo considere conveniente. Esta circunstancia tiene que quedar recogida en el inventario de soportes.

|  |
| --- |
| NIVEL MEDIO Y ALTO. **REGISTRO DE ENTRADA Y SALIDA DE SOPORTES**  Las entradas y salidas de soportes relativos a ficheros de nivel medio y alto se tienen que registrar de acuerdo con el procedimiento siguiente ................... *(detallar el procedimiento de registro de las entradas y salidas de soportes).*  El registro de entrada y salida de soportes se gestiona mediante .................... *(indicar si el registro se tiene que almacenar manualmente o* de forma informática) y tiene que constar ................... *(indicar los campos del registro que, como mínimo tienen que ser: el tipo de documento o soporte, la fecha y la 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 autorizada responsable de la recepción (para las entradas); el tipo de documento o soporte, la fecha y la 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 autorizada responsable de la entrega (para las salidas)).*  *(Si el registro se gestiona de manera automatizada, indicar en este apartado el sistema informático utilizado).* |
| NIVEL ALTO. **GESTIÓN Y DISTRIBUCIÓN DE SOPORTES**  Los soportes se tienen que identificar mediante una etiqueta .................... *(indicar los criterios de etiquetado que tienen que ser comprensibles para los usuarios autorizados a acceder y permitirles identificar el contenido y, al mismo tiempo, dificultar la identificación para el resto de personas).*  La distribución y salida de soportes que contienen datos personales de ficheros de nivel alto se tiene que hacer .................. *(indicar el procedimiento para cifrar los datos o, si procede, para utilizar el mecanismo que garantiza que esta información no es inteligible ni manipulada mientras se transporta. También hay que cifrar los datos contenidos en dispositivos portátiles, cuando se encuentran fuera de las instalaciones que están bajo el control del responsable).*  Los dispositivos portátiles siguientes ................. *(indicar los que no permiten el cifraje de los datos),* por motivo de .................. *(motivar la necesidad*), en lugar de utilizar mecanismos de cifraje tienen que aplicar las medidas que se detallan a continuación ................... *(indicar las medidas alternativas al cifraje, que tienen que tener en cuenta los riesgos de hacer tratamientos en entornos no seguros).* |

7.5. Copia o reproducción de los documentos en papel

Las copias o la reproducción de documentos con datos personales de ficheros de nivel alto sólo se pueden hacer bajo el control del personal autorizado que figura en el anexo ........... *(indicar el código utilizado para designar el documento anexo relativo a los "usuarios y autorizaciones de acceso a los datos". Siguiendo el ejemplo de los anexos de este modelo, sería el documento INF002).*

Las copias rechazadas se tienen que destruir, de manera que se imposibilite el acceso posterior a la información que contienen, de acuerdo con lo que se describe en el apartado 8 de este documento.

**8. Destrucción y reutilización de soportes**

* 1. . Información en soportes digitales

Los soportes digitales -tipo disco duro externo o interno, o memoria flash con interfaz USB- que se tengan que rechazar o reutilizar para otras finalidades se tienen que formatear de nuevo.

Esto se puede hacer mediante ............ *(indicar el programa de borrado "seguro" escogido. El borrado "seguro" de información en soporte digital utilizando un software específico se basa en reescribir diversas veces el dispositivo, de manera que la recuperación o reconstrucción de la información resulta prácticamente imposible).*

La función simple de borrar o suprimir un fichero no es suficiente, considerando que no es un procedimiento seguro y que la información podría ser recuperada por terceros.

Los dispositivos tipo CD o DVD, ante la imposibilidad de hacer uno borrado "seguro", se tienen que destruir físicamente mediante la destructora ..............(*indicar la ubicación de la destructora*), de manera que quede inutilizable.

Para los casos en que no se tiene que rechazar el soporte o reutilizarlo con otra finalidad, sino sólo borrar los ficheros o informaciones que contienen los ordenadores, hay que utilizar la opción "eliminar" o "suprimir" y, a continuación, vaciar la carpeta de los mensajes eliminados o la papelera de reciclaje del ordenador.

* 1. . Información en soporte papel

Se pueden rechazar documentos en soporte papel que incluyan datos personales, de acuerdo con alguno de los sistemas siguientes:

1. Utilizar la destructora de papel ubicada en ................... *(indicar la ubicación de la destructora, tipo y modelo, etc.)*.
2. Depositar los papeles en los contenedores cerrados identificados como ................ *(indicar la identificación que se utilizará para estos contenedores*) y ubicados en ................... *(indicar la ubicación de los contenedores*), a los cuales sólo puede acceder el personal autorizado de la empresa contratada para su destrucción segura.

Se prohíbe tirar documentos que contengan información personal en las papeleras o similares así como reutilizarlos.

**9. Auditoría**

|  |
| --- |
| NIVEL MEDIO Y ALTO**. AUDITORÍA**  *(indicar los procedimientos para realizar, como mínimo cada dos años, la auditoría interna o externa para verificar el cumplimiento del título VIII del RLOPD, relativo a las medidas de seguridad, de acuerdo con los artículos 96 y 110 en relación con los ficheros automatizados y no automatizados, respectivamente.*  *También se tiene que ejecutar cuando hay modificaciones sustanciales en el sistema de información que pueden repercutir en el cumplimiento de las medidas de seguridad implantadas, con el objeto de verificar la adaptación, la adecuación y la eficacia. Esta auditoría inicia el cómputo de los dos años señalado.*  *El informe tiene que analizar la adecuación de las medidas y controles a la LOPD y al RLOPD, identificar las deficiencias y proponer las medidas correctoras o complementarias necesarias.*  *El responsable de seguridad tiene que analizar los informes de auditoría y elevar las conclusiones al responsable del fichero, para que adopte las medidas correctoras. El informe tiene que quedar a disposición de la Autoridad Catalana de Protección de Datos).* |

**10. Revisión del documento de seguridad**

Este documento de seguridad se tiene que adecuar a las disposiciones vigentes en materia de seguridad de los datos de carácter personal y se tiene que mantener permanentemente actualizado mediante una revisión periódica bienal.

También se tiene que revisar y actualizar cuando se produzcan cambios relevantes en los sistemas de tratamiento o en la información tratada. Se consideran cambios relevantes los que pueden repercutir en el cumplimiento de las medidas de seguridad implantadas.

La versión original y actualizada de este documento de seguridad está en poder y bajo el control de ....................... *(indicar la persona física, el área o el departamento que tiene el original).*

La tabla siguiente recoge las modificaciones y actualizaciones de que ha sido objeto este documento de seguridad, así como las revisiones periódicas realizadas a fecha de hoy.

|  |  |  |  |
| --- | --- | --- | --- |
| **Control de versiones del documento de seguridad** | | | |
| **Versión** | **Fecha** | **Contenido  actualizado/revisión** | **Revisado por** |
| XXX | dd/mm/aaaa | ...............................  *(indicar el contenido actualizado o revisado)* | ............................................  *(indicar la persona física, área o departamento que lo ha revisado o actualizado)* |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Control de versiones de los anexos** | | | | |
| **Anexo** | **Versión** | **Fecha** | **Contenido  actualizado/revisión** | **Revisado por** |
| XXX | XXX | dd/mm/aaaa | *..............................*  *(indicar el contenido actualizado o revisado)* | .............................  *(indicar la persona física, área o departamento que lo ha revisado o actualizado)* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Anexo** ............

|  |  |
| --- | --- |
| Fecha versión del Anexo INF001 | dd/mm/aaaa |
| Versión | XXX |

|  |  |
| --- | --- |
| ***INF001*** | *Descripción del sistema informático*  *Características técnicas de hardware y software* |

Características técnicas de los equipos y programas con los cuales se tratan los datos del fichero .................... *(indicar la denominación del fichero).*

|  |
| --- |
| **HARDWARE** |

Marca y modelo del ordenador:

Número de serie:

Memoria RAM:

**Dispositivos de Almacenamiento**

Disco duro interno [etiqueta] *(indicar la capacidad)*

CD grabador *(sí/no)*

DVD grabador *(sí/no)*

Puertos USB *(indicar el número de puertos)*

Disquetera *(sí/no)*

Otros puertos / interfaces externas *(describirlos)*

**Conectividad**

Conectado a una red de área local *(sí/no)*

Interfaz red *(cable/sin cables)*

Conectado a Internet *(sí/no)*

Servicio acceso a Internet *(red o ADSL dedicado o compartido*

*[con / sin cable])*

**Otross dispositivos**

Impresora *(sí/no)*

Escáner *(sí/no)*

|  |
| --- |
| **SOFTWARE** |

Sistema operativo *(indicar nombre y versión)*

Antivirus *(sí (indicar nombre y versión) /no)*

Cortafuegos *(sí/no)*

Navegador Internet *(nombre y versión)*

Cliente de correo electrónico *(nombre y versión)*

**Aplicaciones ofimáticas**

Tratamiento de textos *(indicar nombre y versión)*

Hojas de cálculo *(indicar nombre y versión)*

Presentaciones *(indicar nombre y versión)*

**Otras aplicaciones**

*(indicar la funcionalidad) (indicar nombre y versión)*

**Anexo** ............

|  |  |
| --- | --- |
| Fecha versión del Anexo INF002 | dd/mm/aaaa |
| Versión | XXX |

|  |  |
| --- | --- |
| ***INF002*** | *Usuarios y autorizaciones de acceso a los datos* |

Relación de usuarios autorizados a acceder a los ficheros con indicación de las operaciones que tienen autorizadas, tanto con respecto a tratamientos automatizados como no automatizados.

**Fichero** ................. *(indicar la denominación del fichero)*

Usuario *(indicar nombre y apellidos usuario)*

Cargo / función *(indicar cargo o función)*

Otros puertos / interfaces externas *(indicar sólo el código de usuario,*

*no la palabra de paso)*

**Autorizaciones**

Consultar *(sí/no)*

Añadir *(sí/no)*

Modificar *(sí/no)*

Cancelar *(sí/no)*

Suprimir definitivamente *(sí/no)*

Imprimir *(sí/no)*

Copiar *(sí/no)*

Comunicar *(sí/no)*

Desbloquear *(sí/no)*

Supervisar realización copias en papel *(sí/no)*

**Operaciones técnicas**

Administrar sistema *(sí/no)*

Hacer copias de seguridad *(sí/no)*

Restaurar copias de seguridad *(sí/no)*

Destruir / borrar dispositivos *(sí/no)*

Reutilizar dispositivos *(sí/no)*

***Trabajo fuera de los locales de*** *............ (sí/no)*

***Acceso físico a los equipos*** *............ (sí/no)*

*(Añadir tantas fichas como sea necesario, una para cada usuario de los ficheros).*

**Anexo** ............

|  |  |
| --- | --- |
| Fecha versión del Anexo INF003 | dd/mm/aaaa |
| Versión | XXX |

|  |  |
| --- | --- |
| ***INF003*** | *Estructura de los ficheros y descripción de los sistemas de tratamiento* |

|  |
| --- |
| **Identificación del fichero:** .............*(indicar la denominación del fichero)*  **Sistema de tratamiento:** ...............*(indicar automatizado, no automatizado o*  *parcialmente automatizado)* |

**Datos de** ............ *(indicar los titulares de los datos, por ejemplo alumnos)*

Nombre y apellidos

DNI

Nacionalidad

Dirección postal

Teléfono

Correo electrónico

Etc.

**Datos de** .............*(indicar los titulares de los datos, por ejemplo profesorado)*

Nombre y apellidos

DNI

Nacionalidad

Sexo

Teléfono particular

Etc.

**Anexo** ............

|  |  |
| --- | --- |
| Fecha versión del Anexo INF004 | dd/mm/aaaa |
| Versión | XXX |

|  |  |
| --- | --- |
| ***INF004*** | *Usuarios y autorizaciones de acceso a los datos* |

El ..................... *(indicar al responsable de los ficheros)* delega las funciones que se relacionan a continuación en las personas siguientes:

Persona Función delegada

....................................... ................................................

*(indicar las delegaciones que se hagan, como por ejemplo autorizar la salida de dispositivos portátiles; autorizar la destrucción de soportes, revisar las copias de seguridad cada 6 meses; etc.).*

**Anexo** ............

|  |  |
| --- | --- |
| Fecha versión del Anexo INF005 | dd/mm/aaaa |
| Versión | XXX |

|  |  |
| --- | --- |
| ***INF005*** | *Encargados del tratamiento* |

Relación de las personas físicas o jurídicas, públicas o privadas, u órganos administrativos a los cuales ................... *(indicar el responsable de los ficheros)* ha encargado la prestación de servicios que comportan el acceso a datos personales de ficheros o sistemas de los cuales es responsable.

..................... ***(indicar el nombre del encargado del tratamiento)*: prestación del servicio de** .................. ***(indicar el servicio encargado)***

Para prestar el servicio consistente en .................... *(indicar el servicio encargado)* y exclusivamente con esta finalidad, se proporciona a ..................... *(indicar el encargado del tratamiento)* el acceso a los datos personales de los ficheros ........................ *(indicar la denominación de los ficheros afectados),* con el fin de hacer posible la prestación del servicio encargado, de conformidad con lo que establece el ................... *(indicar el contrato o acuerdo que regula las condiciones del encargo suscrito con el tercero. Opcionalmente, se puede anexar una copia del contrato o acuerdo a este documento de seguridad).*

Los datos de estos ficheros se tienen que tratar en ....................... *(indicar en los locales del responsable de los ficheros o en los locales del encargado)*.

*(Opcional para los casos en que se ha autorizado acceso remoto)* se prohíbe al encargado del tratamiento incorporar estos datos a sistemas o soportes diferentes de los del ................... *(indicar la organización a la cual pertenece el responsable de los ficheros).*

........................... *(indicar el encargado del tratamiento)* se compromete a aplicar en el tratamiento de estos datos personales las medidas de seguridad de nivel ........................ *(indicar el nivel básico/medio/alto de seguridad que corresponde a los ficheros afectados)* previstas en este documento de seguridad, de conformidad con lo que se establece en el apartado 3.4.

*(Opcional)* se delega al encargado del tratamiento la elaboración y la administración del documento de seguridad del .................... *(indicar el responsable de los ficheros).* Esta delegación no afecta a los datos incluidos en los sistemas de información propios del .................... *(indicar el responsable de los ficheros).* En este caso, el encargado tiene que entregar una copia del documento de seguridad a ................. *(indicar el responsable de los ficheros).*

El encargo del tratamiento tiene una vigencia de ...................... *(indicar el periodo previsto).*

Una vez cumplida la prestación del servicio, el encargado del tratamiento ha de .................... *(indicar el destino: devolver al responsable/entregar al encargado designado por el responsable/destruir)* los datos y, si procede, los soportes donde constan.

*(Añadir al anexo tantos apartados como sea necesario)*

**Anexo** ............

|  |  |
| --- | --- |
| Fecha versión del Anexo INF006 | dd/mm/aaaa |
| Versión | XXX |

|  |  |
| --- | --- |
| ***INF006*** | *Prestadores de servicios sin acceso a datos* |

Relación de las personas físicas o jurídicas, públicas o privadas, contratadas por ................... *(indicar el responsable de los ficheros)* para la prestación de servicios que no comportan el acceso a datos personales de ficheros o sistemas de los cuales es responsable.

|  |  |
| --- | --- |
| **Prestador** | **Servicio** |
|  |  |

*(indicar la denominación del tercero) (indicar el servicio contratado)*

**Anexo** ............

|  |  |
| --- | --- |
| Fecha versión del Anexo REG001 | dd/mm/aaaa |
| Versión | XXX |

|  |  |
| --- | --- |
| ***REG001*** | *Entrega del documento de seguridad* |

**Usuario Fecha entrega Firma del receptor**

(nombre y apellidos usuario) (dd/mm/aaaa)

....................................... ........................ ...................................

*(Añadir tantas filas como sea necesario)*

**Anexo** ............

|  |  |
| --- | --- |
| Fecha versión del Anexo REG002 | dd/mm/aaaa |
| Versión | XXX |

|  |  |
| --- | --- |
| ***REG002*** | *Registro de incidencias* |

*(La información registrada de cada incidencia se incluye en una ficha separada y numerada)*

**Código incidencia**

**Número** ............ *(indicar el número de la incidencia, por ejemplo 1-2011)*

|  |  |
| --- | --- |
| Tipo o descripción del incidente | *(describir las circunstancias en que se ha producido la incidencia)* |
| Momento en que se ha producido | *(indicar el día, la hora y el minuto, si es posible)* |
| Momento en que se ha detectado | *(indicar el día, la hora y el minuto, si es posible)* |
| Persona que ha notificado la incidencia | *(indicar nombre y apellidos)* |
| Persona a quien se ha notificado la incidencia | *(indicar nombre y apellidos)* |
| Consecuencias de la incidencia | *(describir cómo afecta la incidencia a los datos)* |
| Medidas adoptadas | *(describir qué medidas correctoras se han adoptado a raíz de la incidencia)* |
| Restauración de datos | *(sí/no, indicar si ha sido necesario restaurar datos)* |
| Otras informaciones en relación con la incidencia | *(añadir otras informaciones que puedan completar el registro de la incidencia)* |

**Operaciones de recuperación**

*(Hay que incluir en este documento el registro de las recuperaciones de información de ficheros de nivel medio o alto. Para los de nivel básico, sólo cuando se graben los datos manualmente)*

Usuario que ha hecho la restauración Fecha Tipo y observaciones

(nombre y apellidos) dd/mm/aaaa *(datos restaurados;*

*si se ha hecho*

*manualmente;*

*otras observaciones,*

*como la justificación*

*de la grabación manual).*

(nombre y apellidos) dd/mm/aaaa

.............................. ..........................

*(Añadir tantas filas como sea necesario)*

**Anexo** ............

|  |  |
| --- | --- |
| Fecha versión del Anexo REG003 | dd/mm/aaaa |
| Versión | XXX |

|  |  |
| --- | --- |
| ***REG003*** | *Registro de copias de seguridad* |

**Usuario que ha realizado la copia Fichero Fecha**

(nombre y apellidos) dd/mm/aaaa

........................................................... .................... .....................

**Tipo y observaciones** .....................

*(Afegiu tantes files com sigui necessari)*

**Anexo** ............

|  |  |
| --- | --- |
| Fecha versión del Anexo REG004 | dd/mm/aaaa |
| Versión | XXX |

|  |  |
| --- | --- |
| ***REG004*** | *Inventario de soportes* |

Inventario de los soportes tanto electrónicos como en papel, que contienen datos de carácter personal del fichero .................... *(indicar la denominación del fichero).*

**A) Soportes electrónicos**

|  |  |
| --- | --- |
| Etiqueta del soporte: .............. | *(indicar la información que tiene que constar en la etiqueta)* |
| Ubicación del soporte: .............. | *(indicar el lugar donde se encuentra el soporte)* |
| Tipo y observaciones: ............. | *(indicar el tipo de copia y las observaciones apropiadas, por ejemplo Memoria USB - Soporte destinado a copias de seguridad)* |
| Personas autorizadas a acceder: ......... | *(indicar nombre y apellidos)* |
| Autorización de salida: ............ | *(G= General / P = Puntual*) |
| Instrucciones de seguridad: .......... | *(describir las instrucciones especiales para el transporte del soporte)* |

**B) Soportes en papel**

**Tipo de expediente o información:** ....................

|  |  |
| --- | --- |
| Etiqueta del soporte: .............. | *(indicar la información que tiene que constar en la etiqueta)* |
| Ubicación del soporte: ............... | *(indicar el lugar donde se encuentra el soporte)* |
| Tipo y observaciones: ............... | *(indicar el tipo de documentación y / o las observaciones apropiadas)* |
| Personas autorizadas a acceder: ........ | *(indicar nombre y apellidos)* |
| Autorización de salida: .............. | *(G= General / P = Puntual)* |
| Instrucciones de seguridad: ............ | *(describir las instrucciones especiales para la conservación y el transporte del soporte)* |

*(Añadir tantas fichas como sea necesario, una por cada soporte que se deba inventariar)*

1. *Este modelo de documento de seguridad se redacta con el objetivo de recopilar las exigencias mínimas establecidas por el RLOPD. Es posible y recomendable incorporar cualquier otra medida que se considere oportuna para aumentar la seguridad de los tratamientos que lleva a cabo el centro educativo, de acuerdo con sus circunstancias particulares.* [↑](#footnote-ref-1)
2. *En el caso de los centros educativos públicos, indicar el órgano que el departamento de la Administración de la Generalitat del cual depende ha establecido como responsable de los ficheros. En el caso de los centros educativos concertados, indicar el órgano que el centro educativo ha establecido como responsable de los ficheros.*  [↑](#footnote-ref-2)
3. *Según cuál sea el perfil del usuario la entrega se puede limitar a las partes del documento de seguridad y, si procede, de los anexos, que le afecten.* [↑](#footnote-ref-3)