Documento de Seguridad

CES Alberta Giménez

Revisado: Nombre y Firma:	Aprobado: Nombre y Firma:
Fecha:	Fecha:

ÍNDICE DEL DOCUMENTO

1. Objeto del Documento 3
2. Política General de Seguridad 3
3. Ámbito de aplicación 4
3.1. Ámbito jurídico 4
3.2. Ámbito organizativo 5
3.3. Ámbito físico 5
3.4. Ámbito de ficheros 5
4. Funciones y Obligaciones del Personal 6
4.1. Todo el personal 6
4.1.1. Uso de la información 6
4.1.2. Confidencialidad de la información 6
4.1.3. Seguridad de acceso físico 7
4.1.4. Seguridad de acceso lógico 7
4.1.5. Incidencias de Seguridad 7
4.1.6. Formación 8
4.1.7. Uso de Ficheros Ofimáticos 8
4.1.8. Uso de Soportes con Datos de Carácter Personal 8
4.1.9. Uso de información en Soporte Papel 8
4.2. Funciones del Responsable del Fichero 10
4.3. Funciones del Responsable de Seguridad 11
5. Normas y Procedimientos de Medidas de Seguridad 14
6. Tratamiento de datos por cuenta de terceros 15
Anexo 1 - Detalle de los recursos protegidos 16
Software de Aplicación 17
Software de Aplicación - Ficheros 18
Relación de Locales 19
Redes 20
Sistemas Informáticos y de Comunicaciones 21
Anexo 2 – Relación de Ficheros de Datos Personales y su Estructura 22
Anexo 3 – Detalle de Asignación de Funciones 24
Anexo 4 – Tratamiento de datos por cuenta de terceros 26
Tratamientos realizados por la empresa 27
Encargados del tratamiento Externos ¡Error! Marcador no definido.
Anexo 5 – Personal Autorizado para Acceder al Fichero 28
Anexo 6 - Modelo de Contrato para Tratamiento de Datos Personales por Cuenta de Terceros 30
Anexo 7 – Listado de controles periódicos para el cumplimiento de la LOPD 36

1. Objeto del Documento

La Dirección de la empresa, considera a sus sistemas de información una herramienta fundamental en el desarrollo de sus operaciones. Estos sistemas dan tratamiento a la información requerida para la gestión de la entidad, que además comprende datos de carácter personal. Tanto la Dirección de la empresa, como la legislación actual, consideran fundamental el respeto a la privacidad e intimidad en el tratamiento de esta información.

Con el propósito de establecer un entorno seguro que permita garantizar razonablemente la protección, confidencialidad, integridad y disponibilidad de los datos así como el cumplimiento de la legislación correspondiente, se ha elaborado este Documento de Seguridad.

Este Documento se fundamenta en el cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal 15/1999, de 13 de Diciembre, en adelante LOPD, y del Real Decreto 1720/2007, que aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, en los que se desarrollan las directrices para proporcionar un nivel de seguridad adecuado para el tratamiento de la información, no obstante, también se incluyen otras directrices relativas a la protección de los datos y recursos asociados que complementan el enfoque basado en la protección de datos de carácter personal.

2. Política General de Seguridad

Objeto

Los activos de información y los sistemas informáticos son recursos importantes y vitales de la empresa para cumplir con su misión. Para proteger estos recursos es necesario crear un entorno de seguridad adecuado que permita garantizar su confidencialidad, integridad y disponibilidad de los mismos.

La responsabilidad sobre la seguridad de la información corresponde a la Dirección de la empresa, encargada de poner los medios adecuados para el cumplimiento de la presente Política de Seguridad. No obstante, todo el personal de la misma y colaboradores deberán asumir su parte de responsabilidad respecto a los medios que utilizan. Para ello, se definen una serie de políticas y procedimientos con el propósito de establecer las medidas organizativas y técnicas apropiadas para garantizar la integridad, disponibilidad y confidencialidad de los datos, y en particular los considerados de carácter personal conforme exige el Real Decreto 1720/2007, del 21 de diciembre.

Ámbito

Esta política es de obligado cumplimiento para TODO EL PERSONAL de la empresa, en particular para aquellas personas que tengan acceso a los ficheros que contienen datos de carácter personal y que se encuentran obligadas por ley a cumplir lo establecido en este Documento, incluido el personal de cualquier Encargado de Tratamiento del fichero o ficheros del Responsable de Fichero.

Política

El compromiso de la empresa, con respecto a la seguridad de la información y al tratamiento de datos de carácter personal y aquellos especialmente sensibles, se resume en los siguientes puntos:

- Responsabilidad de la Seguridad de la Información. La responsabilidad sobre la Seguridad de la Información corresponde a la Dirección y representantes de la entidad, no obstante, todos los trabajadores de la misma y colaboradores deberán asumir su parte de responsabilidad respecto a los medios que utilizan. Para lo cual, y en cumplimiento con el artículo 89.1 del Reglamento, se establecen de un modo detallado, las funciones y obligaciones de las personas con acceso a datos de carácter personal y a los sistemas de información.

- Políticas y procedimientos. La empresa, como responsable de los ficheros, se compromete a implantar, distribuir y actualizar este Documento, así como sus normas y procedimientos anexos atendiendo a la obligatoriedad marcada por la ley y a todos aquellos requerimientos de seguridad necesarios para la empresa.

  El conjunto de políticas se especificará a través de normas, guías, estándares, y procedimientos, realizando las correspondientes actualizaciones de las mismas según sea necesario.

- Difusión de información y conocimiento. La empresa fomentará la difusión de información y el conocimiento en seguridad a su personal y colaboradores, previniendo que se produzcan errores, omisiones, fraudes o delitos tratando de detectar su posible existencia lo antes posible.

- Control de riesgos. Se deberán establecer controles adecuados y razonables con objeto de garantizar razonablemente la seguridad de los datos y que eventos no deseables serán prevenidos, detectados y corregidos ante cualquier causa que pueda influir en que la información no cumpla los objetivos de ser eficaz, eficiente, confidencial, integra, disponible y confiable.

  Estos controles tendrán relación con la criticidad de los activos a proteger y su clasificación.

- Designación de responsables. Se designará internamente al personal Responsable de cada fichero, cuya función será la de promover el establecimiento de controles y medidas orientadas a proteger los recursos críticos y en especial, los datos de carácter personal.

  El Responsable del Fichero designará uno o varios Responsables de Seguridad encargados de coordinar y controlar las medidas definidas en este Documento. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al Responsable del Fichero de acuerdo con esta Política

- Realización de Auditorías de Seguridad. Se realizarán Auditorías de Seguridad para verificar y garantizar el cumplimiento de este Documento.

Finalmente, el personal que no cumpla lo determinado en esta Política, podrá ser sancionado de acuerdo con la legislación laboral y sin perjuicio de otras sanciones a que hubiere lugar, o bien penalizado si está vinculado a la empresa bajo contratos no laborales, de acuerdo con las cláusulas que figuren en dichos contratos.

3. Ámbito de aplicación

De acuerdo al artículo 88.3.a) del Reglamento aprobado por Real Decreto 1720/2007, de 21 de Diciembre, de desarrollo de la LOPD, es necesario establecer el ámbito de aplicación de las Medidas de Seguridad referidas en este Documento. Para definir el alcance de la aplicación de estas Medidas, se ha realizado la siguiente clasificación que representa las distintas áreas de protección según las Medidas de Seguridad:

1. Ámbito jurídico
2. Ámbito organizativo
3. Ámbito físico
4. Ámbito de ficheros

3.1. Ámbito jurídico

CES Alberta Giménez

R0700117E

Costa de Saragossa, 16

07013 - Palma de Mallorca

Illes Balears

3.2. Ámbito organizativo

El Documento de Seguridad es de obligado cumplimiento para todo el personal de la empresa con acceso a datos de carácter personal o a los sistemas de información que los tratan, así como para las empresas y para el personal externo de éstas que preste sus servicios a aquella, cuando tengan acceso a los mismos.

Las funciones y obligaciones del personal se incluyen en el apartado correspondiente, estableciendo las diferencias de acuerdo al grado de responsabilidad en la aplicación de las Normas de Seguridad previstas.

3.3. Ámbito físico

Las Medidas de Seguridad dispuestas en el presente Documento de Seguridad son de aplicación a todos los ficheros, centros de tratamiento, locales, equipos, sistemas, programas y personas que intervengan en el tratamiento de datos de carácter personal.

Los recursos que deben ser controlados por la presente normativa por servir de medio directo o indirecto para acceder a los ficheros son:

- Los centros de proceso de datos y locales donde se ubican los ficheros o se almacenen los soportes que los contengan.
- Los entornos de tratamiento de los ficheros con datos de carácter personal: servidores, ordenadores personales, locales o en conexión remota, utilizados para acceder a los ficheros.
- El entorno de comunicaciones entre ubicaciones en el cual se transfieren datos de carácter personal.
- Los sistemas de información mediante los que se accede a los ficheros.

La especificación detallada de los mismos se incluye en el *Anexo 1 – Detalle de recursos protegidos.*

3.4. Ámbito de ficheros

En este apartado se recogen los ficheros con datos de carácter personal declarados ante la Agencia Española de Protección de Datos (AEPD) ver *Anexo 2 - Relación de Ficheros de Datos Personales y su Estructura.*

4. Funciones y Obligaciones del Personal

El personal de la empresa, en el cumplimiento de sus funciones, debe aplicar la normativa relativa a la Seguridad de Datos que se especifica en este Documento el cual es difundido a todo el personal, de acuerdo con lo establecido en el artículo 89 del RLOPD.

El personal de la entidad se clasifica de acuerdo con los siguientes tipos de usuarios:

1. Todo el personal
2. Responsable del Fichero
3. Responsable de Seguridad

4.1. Todo el personal

Para lograr una mejor comprensión de las funciones y obligaciones, a las que el personal de la empresa y sus colaboradores deben dar cumplimiento, se han agrupado según la siguiente clasificación:

4. Uso de la información
5. Confidencialidad de la información
6. Seguridad de acceso físico
7. Seguridad de acceso lógico Seguridad de la información
8. Incidencias de Seguridad
9. Formación
10. Uso de Ficheros Ofimáticos
11. Uso de Soportes con Datos de Carácter Personal
12. Uso de información en Soporte Papel

4.1.1. Uso de la información

Todo el personal que en el desarrollo de su trabajo tenga acceso a datos de carácter personal; de sus alumnos, proveedores, otros trabajadores de la empresa o terceros en general; o a los datos de la entidad definidos como sensibles debe conocer las finalidades de uso de los mismos y los tratamientos definidos por el Responsable del Fichero.

En caso de que la finalidad del tratamiento de los datos no haya sido definida, o surjan nuevos requerimientos de información, se deberá reportar al Responsable del Fichero para que se evalúen los nuevos requerimientos y se apliquen los procedimientos correspondientes a la creación, declaración y/o mantenimiento de los Ficheros.

El uso de la información en cualquier formato o soporte de forma distinta a la establecida por el Responsable del Fichero y sin conocimiento de la entidad constituye una falta grave.

4.1.2. Confidencialidad de la información

El usuario que tenga acceso a datos debe guardar un estricto secreto profesional sobre cualquier información que conozca en el desempeño de su trabajo, por tiempo indefinido. Esta obligación continuará vigente incluso tras la extinción de su relación con la entidad.

En cuanto a lo dispuesto en el artículo 10 de la Ley Orgánica 15/1999 de Protección de Datos, el usuario se compromete a no tratar, ni ceder, ni comunicar, ni utilizar en beneficio propio, así como no revelar a terceros los datos de carácter personal o a cualquier información a la que tenga acceso, respetando en todo momento la privacidad y confidencialidad de la misma.

4.1.3. Seguridad de acceso físico

Es necesario evitar el acceso a los datos de carácter personal, tanto para los ficheros automatizados, como para los no automatizados.

Para ello, en el caso de despachos y puestos de trabajo, especialmente cuando los datos son de nivel medio o alto, se ha de tener especial cuidado para, en la medida de lo posible:

- Mantener cerrados los despachos
- Cerrar armarios y/o cajones
- Guardar soportes informáticos o listados
- En el caso de ficheros automatizados se deben establecer mecanismos para evitar el acceso a los ordenadores personales ya sea apagando los ordenadores personales o estableciendo mecanismos que impidan el acceso a los datos durante la ausencia del puesto de trabajo, como puede ser la activación de salvapantallas con contraseña para evitar accesos no autorizados al ausentarse del puesto de trabajo o establecer el bloqueo de la sesión tras un periodo de inactividad razonable.

4.1.4. Seguridad de acceso lógico

El sistema de seguridad, de acceso lógico a los sistemas de información, está basado en el uso de identificadores de usuario y contraseñas ligadas a perfiles de acceso establecidos de acuerdo a las funciones que desempeña cada usuario.

El identificador de usuario, tanto como la correspondiente contraseña, que se asigna al personal que lo requiera, es confidencial, personal e intransferible. Es responsabilidad del titular el uso que se haga del mismo.

El usuario es responsable de la confidencialidad de su contraseña, y en ningún caso, debe mantenerla de forma legible en archivos digitales, papel o cualquier otro tipo de soporte donde pueda ser accesible. Queda prohibido comunicar a otra persona el identificador de usuario y su contraseña.

En caso de que el usuario sospeche que su contraseña ha sido conocida fortuita o fraudulentamente por personas no autorizadas, deberá proceder a su modificación y notificar la incidencia al Responsable de Seguridad.

La contraseña debe modificarse periódicamente de acuerdo a las normas establecidas en el Documento de Seguridad.

4.1.5. Incidencias de Seguridad

Una Incidencia de Seguridad consiste en cualquier circunstancia que afecte o pueda afectar a la seguridad de los datos.

Es deber del usuario notificar inmediatamente al Responsable de Seguridad de cualquier Incidencia de Seguridad de la que tenga conocimiento.

El conocimiento y la no notificación de una incidencia por parte de un usuario será considerado como una falta grave contra la seguridad de los datos.

4.1.6. Formación

Con referencia a la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) el personal deberá conocer:

- Los principios básicos de LOPD así como de las obligaciones particulares, relativas al tratamiento de datos de carácter personal, requeridas para el desempeño de sus funciones.
- Conocer el procedimiento de tramitación de derechos LOPD de los interesados.
- Conocer y aplicar el Documento de Seguridad.

4.1.7. Uso de Ficheros Ofimáticos

Los usuarios sólo podrán crear ficheros ofimáticos, y en especial aquellos que contengan datos de carácter personal, cuando sea necesario para el desempeño de su trabajo. Todos los ficheros ofimáticos creados por los usuarios son responsabilidad del mismo (identificar en Anexo3 "Detalle de Asignación de Funciones"), en cuanto a sus requerimientos de adaptación a la LOPD y a las Medidas de Seguridad aplicadas a los mismos.

Adicionalmente, se ha de garantizar que:

- Están ubicados en los directorios asignados a los usuarios por el personal de informática para garantizar que existen los controles técnicos preestablecidos, nunca en unidades locales de disco de los ordenadores personales del usuario.
- El cumplimiento de todas las Medidas de Seguridad previstas de acuerdo al Nivel de Seguridad definido para el fichero.
- Serán eliminados cuando hayan dejado de ser útiles para la finalidad para la cual se crearon.

En caso de cualquier duda se ha de consultar con el Responsable de Seguridad.

En las agendas de contactos de las herramientas ofimáticas (por ejemplo en Outlook) los usuarios únicamente introducirán datos identificativos y direcciones o teléfonos de personas. En ningún caso introducirán datos o valoraciones de personas físicas relativos a ideología, religión, creencias, origen racial, salud o vida sexual. En caso de incumplimiento de esta norma, las posibles responsabilidades recaerán en el usuario que introdujo los datos.

4.1.8. Uso de Soportes con Datos de Carácter Personal

Los usuarios autorizados a manejar soportes que contienen información de la empresa y en particular datos de carácter personal, deben guardarlos en un lugar seguro cuando no estén en uso, especialmente fuera de la jornada laboral.

Adicionalmente, el usuario que gestione soportes debe inventariar los soportes bajo su custodia y mantener el inventario actualizado.

4.1.9. Uso de información en Soporte Papel

Debido a que en soporte papel se registran datos de carácter personal, es necesario establecer criterios de uso, control y destrucción de los mismos.

Se deben establecer Medidas de Seguridad para los datos impresos, es imprescindible hacer un uso racional de los informes que se imprimen y cuidar la confidencialidad de los mismos. Las directrices a seguir son las siguientes:

- Utilizar el menor número de informes en formato papel que contengan datos de carácter personal y mantener los mismos en lugar seguro y fuera del alcance de terceros.
- Se recogerán de las impresoras los documentos que contienen datos clasificados con objeto de evitar que sean accedidos por personas no autorizadas, se debe asegurar especialmente que no queden documentos impresos en la bandeja de salida que contengan datos clasificados de nivel alto.
- Se deberán conservar en cajones o armarios con llave.
- Cada persona revisará periódicamente los informes que estén bajo su custodia, procediendo a destruir los documentos obsoletos.
- La documentación que contenga datos clasificados, sean o no personales, se procederá a su destrucción cuando ésta ya no sea necesaria.
- Se destruirán utilizando, siempre que sea posible, una destructora de papel o manualmente de forma que no puedan ser utilizados posteriormente.
- Nunca se reciclará dichos documentos evitando, cuando sea posible, proceder a su destrucción en instalaciones externas.

4.2. Funciones del Responsable del Fichero

La LOPD define como Responsable del Fichero o Responsable del Tratamiento a la Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que solo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento aunque no lo realizase materialmente.

Sus funciones se detallan a continuación:

- Dar cumplimiento de todos los requisitos establecidos en la legislación vigente sobre protección de datos de carácter personal.
- Adoptar las medidas, de índole técnica y organizativa, necesarias para garantizar la seguridad de los datos de carácter personal en los términos establecidos en la legislación vigente con independencia de cual sea su sistema de tratamiento. Esta responsabilidad es aplicable tanto para los ficheros en los cuales se actúa como Responsable del Fichero, como para aquellos en los que se actúa únicamente como encargado del tratamiento.
- Elaborar y mantener actualizado el Documento de Seguridad, que será de obligado cumplimiento para todo el personal de la empresa, en el que se recogen las Medidas de Seguridad identificadas para la protección de los datos de carácter personal.
- Realizar la designación de funciones relativas al cumplimiento de LOPD (Anexo "Detalle de Asignación de Funciones") garantizando la formación correspondiente del personal designado. Estas designaciones no suponen la exención de la responsabilidad correspondiente siempre, en última instancia, al Responsable del Fichero. Las funciones previstas son:
  - Designar uno o varios Responsables de Seguridad para coordinar y controlar el seguimiento de lo establecido en el Documento de Seguridad.
  - Designar a los Usuarios Responsables de los Ficheros para colaborar en el seguimiento del tratamiento de los ficheros con datos de carácter personal.
- Adoptar las Medidas necesarias para que el personal conozca las Normas de Seguridad que afecten al desarrollo de sus funciones, así como las consecuencias a que daría lugar su incumplimiento.
- Identificar y mantener actualizados los ficheros con datos de carácter personal tanto en el Registro de la Agencia Española de Protección de Datos como en el Documento de Seguridad.
- Cumplir con el deber de información al interesado.
- Obtener el consentimiento del interesado para el tratamiento de sus datos personales en los casos y términos aplicables.
- Cumplir los requisitos legales en caso de que se produzcan cesiones de datos o accesos por cuenta de terceros.
- Implantar procedimientos para la atención de derechos LOPD de los interesados y resolver las peticiones de ejercicio de los mismos en los plazos previstos.
- Adoptar las Medidas adecuadas para limitar el acceso a datos personales, soportes o recursos que los contengan, al personal, tanto interno como externo, que no requiera acceso a los mismos para la realización de los trabajos encomendados.
- Implantar mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados. Debe velar por el cumplimiento del principio de mínimo privilegio que

consiste en proporcionar a un usuario solo aquellos permisos o privilegios que son necesarios para realizar las tareas que le han sido encomendadas.

- Elaborar procedimientos de identificación y autenticación para el acceso a los datos personales en colaboración con el Responsable de Seguridad. Mantener la relación actualizada de usuarios autorizados para acceder a los datos.
- Establecer mecanismos de seguridad que impidan el acceso no autorizado a datos de carácter personal.
- Verificar, al menos semestralmente, la correcta definición, funcionamiento y aplicación de los procedimientos de copias de respaldo.
- Para los ficheros no automatizados:
  - Establecer los criterios y procedimientos de actuación para el archivo de ficheros no automatizados, en caso de que no exista norma aplicable para ello.
  - Adoptar medidas que impidan el acceso físico a datos de carácter personal en ficheros no automatizados.
- En la Auditoria, será el responsable de implantar las medidas correctoras necesarias en función de los informes realizados.
- Delegar las autorizaciones que le correspondan, a las personas designadas al efecto. No obstante, ésta designación en ningún caso supone una delegación de la responsabilidad que le corresponde. A continuación se detallan éstas autorizaciones:
  - Autorizar las altas, modificaciones y bajas de acceso de usuarios a las aplicaciones que realizan tratamientos de los ficheros.
  - Autorizar por escrito la ejecución de los procedimientos de recuperación de datos.
  - Autorizar el almacenamiento de datos en dispositivos portátiles o el tratamiento de aquéllos fuera de los locales del responsable del fichero o del encargado del tratamiento. En todo caso, debe garantizar el nivel de seguridad correspondiente al tipo de fichero tratado.
  - Autorizar expresamente la ejecución del tratamiento de datos de carácter personal fuera del lugar de la ubicación del fichero vigilando que se cumplan los niveles de seguridad correspondientes al nivel de los ficheros tratados.
  - Autorizar o documentar la autorización en el Documento de Seguridad, la salida de soportes y/o documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera del ámbito de locales protegidos por las Medidas de Seguridad establecidas en este Documento.

4.3. Funciones del Responsable de Seguridad

Se define como Responsable de Seguridad a la persona o personas a las que el Responsable del Fichero ha asignado formalmente la función de coordinar y controlar las Medidas de Seguridad aplicables.

Deberá realizar las siguientes funciones:

- Colaborar con el Responsable del Fichero en la correcta notificación de ficheros a la Agencia de Protección de Datos.

- Colaborar con el Responsable del Fichero en la elaboración del Documento de Seguridad y el desarrollo de los procedimientos correspondientes. Difundirlos al personal afectado.
- Implantar las Medidas de Seguridad, técnicas y organizativas, definidas en el presente Documento y dar el seguimiento correspondiente para garantizar su cumplimiento.
- Identificar los cambios realizados en el entorno para determinar si éstos implican una actualización de los ficheros o de las Medidas de Seguridad establecidas en el Documento de Seguridad y colaborar con el Responsable del Fichero para proceder a su adecuación. Difundir las modificaciones al personal correspondiente.
- Participar en el diseño e implantación de aplicaciones informáticas en la definición de requisitos sobre las Medidas de Seguridad necesarias y la correcta implantación de las mismas.
- Implantar los procedimientos de identificación y autenticación para el acceso a datos de carácter personal.
- Implantar la especificación de perfiles de acceso de los aplicativos que tratan el Fichero realizado en colaboración con el Responsable de Seguridad de Aplicativos.
- Controlar los requerimientos de administración de usuarios, desde la solicitud hasta su concesión, manteniendo actualizado al registro de usuarios autorizados para el acceso a los ficheros en el Documento de Seguridad.
- Implantar mecanismos de registro de control de accesos a datos de nivel alto y mantenerlos activos. Deberá revisarlos periódicamente y elaborar un informe mensual detallando el análisis realizado y los problemas detectados.
- Supervisar el acceso físico a la sala de servidores y establecer los requerimientos de acceso a la misma.
- Supervisar la seguridad física de los equipos del Responsable del Fichero.
- Establecer e implantar los procedimientos de respaldo y recuperación de datos.
- Colaborar con el Responsable del Fichero para verificar, al menos semestralmente, la correcta definición, funcionamiento y aplicación de los procedimientos de copia.
- Custodiar los soportes del Responsable del Fichero y controlar el mantenimiento del inventario, y registros de entrada y salida de soportes.
- Autorizar las salidas de equipos para operaciones de mantenimiento y reparación.
- Habilitar un Registro de Incidencias, con el fin de incluir en él cualquier incidencia que pueda suponer un peligro para la seguridad.
- Analizar los informes de auditoria realizados y elevar sus conclusiones al Responsable del Fichero.
- Efectuar los controles periódicos de seguimiento de seguridad previstos, incluidos en el '*Anexo 7 - Listado de controles periódicos para el cumplimiento de la LOPD* ', para evaluar el cumplimiento de lo establecido en este Documento.
- Controlar los soportes generados por las áreas usuarias:
  - Identificar, inventariar y controlar los soportes que contengan datos de carácter personal propiedad del Responsable del Fichero.

- Actualizar el inventario con la creación, modificación o destrucción de cualquier soporte que contenga información de carácter personal.
- Etiquetar los soportes inventariados.
- Garantizar el almacenamiento adecuado de dichos soportes.
- Supervisar el cumplimiento de las normas de etiquetado y reutilización/destrucción de los soportes.

Responsable de Seguridad de Ficheros no Automatizados

Debido a la cantidad de ficheros no automatizados gestionados, se ha considerado conveniente la designación de un Responsable de Archivo cuyas funciones se detallan a continuación:

- Realizar la clasificación de los ficheros no automatizados de acuerdo con los ficheros declarados.
- Implantar las Medidas de Seguridad necesarias de acuerdo al nivel establecido para cada uno de los ficheros que garanticen la confidencialidad de los datos contenidos en los mismos y evitar accesos no autorizados.
- Establecer los niveles de acceso dentro de la documentación, relativa a cada uno de los ficheros declarados, estableciendo perfiles que definan la información a la que se permite el acceso.
- Llevar a cabo una relación del personal autorizado para acceder a los ficheros no automatizados según los perfiles definidos para este tipo de ficheros.
- Controlar el acceso a los locales donde se encuentran ubicados los ficheros no automatizados y establecer los controles ambientales necesarios para la conservación del archivo, con el fin de evitar su deterioro prematuro.
- Establecer el tiempo de conservación de acuerdo a los requerimientos legales y realizar planes de depuración de la documentación, con una periodicidad mínima de un año, y se deberá crear y mantener un registro de entrada y salida de documentos, que permita su localización en cualquier momento evitando pérdidas.
- Crear y mantener un registro de entrada y salida de documentos, que permita su localización en cualquier momento evitando pérdidas.

5. Normas y Procedimientos de Medidas de Seguridad

Con el fin de agilizar el mantenimiento, actualización y, sobre todo, su utilización, se han desarrollado las normas y procedimientos de Medidas de Seguridad de forma independiente. Éstos contienen las actuaciones necesarias para alcanzar los requerimientos del Reglamento aplicables a Ficheros, cualquiera que sean los datos que contienen, clasificados de acuerdo a los distintos niveles definidos como: básico, medio y alto.

Cada documento independiente mantiene una estructura común para facilitar su comprensión, donde se describe brevemente el procedimiento, luego se detalla y desarrolla, para finalmente aportar los anexos correspondientes.

Todas estas normas y procedimientos forman parte del Documento de Seguridad, de forma homogénea, y deberá existir la posibilidad de aunar todos los documentos en uno sólo en cualquier momento.

La responsabilidad sobre su aplicación recae en el Responsable de Seguridad. No obstante, si la función informática recae sobre proveedores externos, el Responsable de Seguridad debe trabajar en coordinación con ellos y solicitar que dichos requisitos se cumplan.

Las normas y procedimientos que se adjuntan se resumen de la siguiente manera:

Código	Nombre
PR-001	Procedimiento de Creación, Modificación y Supresión de ficheros de titularidad privada
PR-002	Procedimiento para el Ejercicio de Derechos
PR-003	Procedimiento de Ficheros no Automatizados
PR-004	Normas de Control de Acceso Lógico
PR-005	Procedimiento de Administración de Usuarios
PR-006	Procedimiento de Gestión de Soportes
PR-007	Procedimiento de Copias de Respaldo y Recuperación
PR-008	Procedimiento de Gestión de Incidencias
PR-009	Normas de Identificación y Autenticación
PR-010	Normas de Acceso Físico
PR-011	Procedimiento videovigilancia
OP-001	Operativa de Gestión de la entidad
OP-003	Operativa de Recursos Humanos
OP-005	Operativa de acceso remoto

6. Tratamiento de datos por cuenta de terceros

Comprende aquellos supuestos en los que un tercero, Encargado del tratamiento, tiene acceso a los datos personales del Responsable con motivo de la prestación de un servicio solicitado por este último. Es decir, la correcta prestación del servicio contratado por el Responsable de los datos, implica la necesidad de que el tercero tenga acceso a los datos personales, ya que si no se produjera este acceso no tendría lugar la prestación del servicio.

Esta circunstancia es calificada por la LOPD como un Acceso a los datos por cuenta de terceros, estableciéndose la obligatoriedad de realizar un contrato entre el Encargado del tratamiento y el Responsable de los datos, en el que queden reguladas las instrucciones del tratamiento a seguir por el encargado, con motivo de la prestación del servicio. Además, se recogerán en el mismo las medidas de seguridad que se deberán aplicar, así como la obligación de destruir o bien de devolver los datos una vez finalizado el servicio. En el *Anexo 6* se incluye el modelo de *'Contrato para Tratamiento de Datos Personales por Cuenta de Terceros'*.

A diferencia de la figura de la cesión, en el acceso no rige la obligación de recabar el consentimiento del interesado, así como tampoco la obligación de informar sobre el encargado del tratamiento.

En caso de que seamos nosotros los encargados del tratamiento por cuenta del responsable del fichero, deberemos validar que la información que trataremos ha sido obtenida atendiendo a la legislación vigente y procurar que exista un contrato de por medio.

En el *Anexo 4* de este documento se detallan todos los accesos de datos que realiza la empresa (encargada del tratamiento), en el marco de la ejecución de la prestación de servicios antes mencionados a un Responsable. Asimismo se detallan los accesos que realizan otras empresas (encargadas del tratamiento) sobre los datos de la empresa (Responsable).

Anexo 1 - Detalle de los recursos protegidos

Este Anexo contiene las tablas tipo, las tablas cumplimentadas se almacena en:

Documento: DS001A001- Detalle de los recursos protegidos

Referencia: DS001A001

Carpeta:

Ubicación:

Anexo 1 – Detalle de los Recursos Protegidos — Software de Aplicación

Nombre	[Identificativo de la aplicación]
Descripción	[Breve explicación de la aplicación y sus funciones]
Fabricante	[Nombre y forma de contacto con el fabricante de la aplicación]
Versión	[Número o denominación de la última versión instalada]
Control de Acceso	[Rellenar en el caso en que el acceso a la aplicación este controlado por un sistema de control propio de la misma, p.ej. Usuario/Password. Especificar si el acceso a los componentes de la aplicación (menús) es configurable por usuario]

Anexo 1 – Detalle de los Recursos Protegidos		Software de Aplicación - Ficheros
	Fichero	Aplicación
1		
2		
3		
4		
5		

Anexo 1 – Detalle de los Recursos — Relación de Locales

Tipo	[Tipo: Edificio, Oficina, Despacho, Archivo ,…]
Nombre	[Identificativo del local]
Ubicación física	[Dirección o localización]
Responsable	[Encargado o responsable del local o edificio]
Ficheros	[Ficheros almacenados en el Local]
Controles de acceso	[Medios para controlar los accesos, como sistemas de apertura automática, video vigilancia, puertas con cerradura, candados, custodia de llaves …]
Sistemas de Continuidad	[En caso de interrupción de la corriente eléctrica, qué sistemas existen para mantener la energía]
Controles ambientales	[Sistemas de detección de humos y fuego, CO2, extintores y tipo (dióxido de carbono y polvo polivalente), …]

Anexo 1 – Detalle de los Recursos Protegidos — Redes

Nombre	[Identificativo de la Red]
Tipo	[Sistema de comunicaciones al exterior, Red física de comunicaciones, Red inalámbrica de comunicaciones,…]
Tipología	[Estructura de la Red y características]

Nombre	[nombre que se le da al equipo o servidor]
Tipo	[Especificar Marca, modelo y características]
Función	[Funciones asignadas al sistema, Dominio, servidor de aplicaciones, servidor de ficheros, estación de trabajo, equipo de comunicaciones, …)
Sistema Operativo	[nombre y versión del sistema operativo]
Sistema de comunicaciones	[redes o subredes a las que se conecta el equipo, así como los medios utilizados para ello]
Unidades de almacenamiento	[sistemas de almacenamiento , como discos duros, DAT, Grabadoras CD/DVD, sistema redundante de archivo (raid), zip, …]
Ficheros	[Ficheros o bases de datos se almacenan en el equipo]
Herramientas de Seguridad	[Herramientas utilizadas contra el software maligno y accesos malintencionados]
Control de Acceso	[Especificar los sistemas de control de acceso, si existe dominio, definición de usuarios y contraseñas …]
Aplicaciones	[Relación de las aplicaciones instaladas en el equipo]
Local	[Ubicación, local en que se ubica el sistema]

Anexo 2 – Relación de Ficheros de Datos Personales y su Estructura

Este Anexo contiene las tablas tipo, las tablas cumplimentadas se almacena en:

Documento: DS001A002- Relación de Ficheros de Datos Personales y su Estructura

Referencia: DS001A002

Carpeta:

Ubicación:

Anexo 2 - Relación de Ficheros de Datos Personales y su Estructura

A continuación se señalan los ficheros identificados con información de carácter personal, relacionándolos con las aplicaciones y entornos que los tratan:

No	Nombre Fichero	Finalidad/Usos	Estructura Básica	Nivel[1]	No. de registro
1					
2					
3					
4					
5					
6					

[1] Nivel de seguridad a implantar. **B**= Basico / **M**= Medio / **A**= Alto

Anexo 3 – Detalle de Asignación de Funciones

Este Anexo contiene las tablas tipo, las tablas cumplimentadas se almacena en:

Documento: DS001A003- Detalle de Asignación de Funciones

Referencia: DS001A003

Carpeta:

Ubicación:

Anexo 3 – Detalle de Asignación de Funciones

Nombre del Fichero	Nombre persona	Fecha		Perfil				
		Alta	Baja	Responsable del Fichero	Responsable de Seguridad	Resp. Seguridad Ficheros no automatizados	Usuario responsable de fichero	Director de Sistemas

Anexo 4 – Tratamiento de datos por cuenta de terceros

Este Anexo contiene las tablas tipo, las tablas cumplimentadas se almacena en:

Documento: DS001A004- Tratamiento de datos por cuenta de terceros

Referencia: DS001A004

Carpeta:

Ubicación:

Anexo 4 - Tratamiento de datos por cuenta de terceros	Tratamientos realizados por la empresa

Identificación del Responsable del Fichero	Ficheros o tratamientos	Nivel[1]	Contrato de tratamiento	Vigencia del tratamiento	
				Fecha inicio	Fecha fin

[1] Nivel de seguridad a implantar. **B**= Basico / **M**= Medio / **A**= Alto

Anexo 5 – Personal Autorizado para Acceder al Fichero

Este Anexo contiene las tablas tipo.

La definición de Perfiles de acceso se almacena en:

Documento: 'DS001A005_1- Personal Autorizado para Acceder al Fichero - Perfiles'

Referencia: DS001A005_1

Carpeta:

Ubicación:

Las tablas cumplimentadas se almacena en:

Documento: 'DS001A005_2- Personal Autorizado para Acceder al Fichero'

Referencia: DS001A005_2

Carpeta:

Ubicación:

[Definir perfiles de Acceso]

Anexo 5 – Personal Autorizado para Acceder al Fichero

Fichero: [Anexo 2 - Relación de Ficheros de Datos Personales y su Estructura y Anexo 4- Tratamientos realizados por la empresa]

Nombre	Perfil	Lógico	Físico	Autorizado por	Fecha	
					Alta	Baja
				[Anexo 1 - Personal Autorizado para conceder Acceso o Responsable fichero]		

Anexo 6 - Modelo de Contrato para Tratamiento de Datos Personales por Cuenta de Terceros

REUNIDOS

De una Parte,

[Nombre fiscal de la empresa], entidad de nacionalidad española con domicilio social en [localidad], [calle/avenida] [número] y provista de Código de Identificación Fiscal [código de Identificación Fiscal] constituida mediante escritura pública autorizada por el Notario de [ciudad] Don [nombre del Notario] el [día] de [mes] de [año], bajo el número [número] de su protocolo, e inscrita el [día] de [mes] de [año] en el Registro Mercantil de [ciudad], en el tomo [número], folio [número], hoja [número], inscripción [número] (en adelante, “el Responsable del Fichero”).

Se halla representada en este acto por [nombre del representante], quien actúa en su condición de [cargo] en virtud de la escritura de apoderamiento otorgada el [día] de [mes] de [año] ante el Notario de [ciudad] Don [nombre], bajo el número [número] de su protocolo.

Y de otra Parte,

[nombre de la entidad/sociedad/persona jurídica], entidad de nacionalidad [española] con domicilio social en [ciudad], [calle/avenida/plaza], número [número] y provista de Código de Identificación Fiscal [código de Identificación Fiscal]. Constituida mediante escritura pública autorizada por el Notario de [ciudad] Don [nombre del Notario] el [día] de [mes] de [año], bajo el número [número] de su protocolo, e inscrita el [día] de [mes] de [año] en el Registro Mercantil de [ciudad], en el tomo [número], folio [número], hoja [número], inscripción [número] (en adelante, “el Encargado del Tratamiento”).

Se halla representada en este acto por [nombre del representante], quien actúa en su condición de [cargo] en virtud de la escritura de apoderamiento otorgada el [día] de [mes] de [año] ante el Notario de [ciudad] Don [nombre], bajo el número [número] de su protocolo.

Las Partes, de sus libres y espontáneas voluntades, manifiestan tener y reconocerse, mutua y recíprocamente, la capacidad legal necesaria para otorgar el presente contrato a cuyos efectos, podrán ser denominadas conjuntamente como “las Partes”

MANIFIESTAN

I. Que el Responsable del Fichero es [relación y servicios]

II. Que el Encargado del Tratamiento presta servicios de [servicios realizados por el encargado].

III. Que, en virtud de las consideraciones precedentes, las Partes, de sus libres y espontáneas voluntades, han acordado otorgar el siguiente contrato para tratamiento por cuenta de terceros (en adelante, “el Contrato”) con sujeción a las siguientes

ESTIPULACIONES

Primera El Responsable del Fichero manifiesta que es titular de los ficheros de [nombre de los ficheros sobre el cual se ha de realizar el tratamiento] con datos de carácter personal debidamente inscritos en el Registro General de la Agencia de Protección de Datos en adelante, "el Fichero", con números de registro: [número de registro] y que, en virtud de lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, "LOPD") y en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 (en adelante "RLOPD") manifiesta que ha obtenido dichos datos de forma legal.

Segunda.- En virtud de lo establecido en la LOPD y en el RLOPD el Responsable del Fichero entregará los datos de carácter personal, que figuren en el Fichero, al Encargado del Tratamiento, para que este realice su tratamiento.

Tercera.- El Encargado del Tratamiento única y exclusivamente aplicará dichos datos para realizar por cuenta del Responsable del Fichero la [tratamientos contratados], u otros servicios análogos que le sean solicitadas.

En ningún caso el Encargado del Tratamiento utilizará o aplicará los datos contenidos en el Fichero a finalidades distintas de las establecidas en el presente Contrato.

Cuarta.- El Encargado del tratamiento deberá aplicar a los datos de carácter personal entregados por el Responsable del Fichero las medidas de seguridad de nivel [nivel establecido para el fichero objeto del tratamiento – básico, medio o alto] según lo establecido en el Título VIII del RLOPD.

Quinta.- El Encargado del Tratamiento se compromete a cumplir con lo establecido en el presente Contrato y en lo establecido en la normativa aplicable en materia de protección de datos. En el supuesto de incumplir cualquiera de sus obligaciones, el Encargado del Tratamiento será considerado como responsable del tratamiento y además se obliga a indemnizar al Responsable del Fichero de todos los daños y perjuicios que sufra o de cualquier sanción administrativa que se le obligara a afrontar.

Sexta.- El presente acuerdo entrará en vigor desde la fecha de su firma y estará vigente hasta la fecha de la finalización de la prestación encomendada por el Responsable del Fichero. Una vez finalizado el tratamiento el Encargado del Tratamiento deberá destruir y/o devolver cualquier dato personal que haya sido entregado o generado a partir de los datos del Fichero pertenecientes al Responsable del Fichero. No procederá tal destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los datos por parte del Encargado del Tratamiento, garantizando el Responsable del Fichero dicha conservación. El Encargado del Tratamiento se encontrará obligado a conservar los datos, debidamente bloqueados, en caso de existir posibilidad de derivarse responsabilidades de su relación con el Responsable del Tratamiento.

Séptima.- Medidas de seguridad [adaptable de acuerdo al nivel del fichero tratado]

En todo caso y de forma no excluyente y a meros efectos indicativos, para dar cumplimiento a lo establecido en la normativa relativa a datos personales, el Encargado del Tratamiento deberá cumplir las siguientes medidas:

Medidas de seguridad de nivel básico

7.1. Las medidas de seguridad para los accesos a los datos de carácter personal en el supuesto que se realicen a través de la red deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

7.2. La ejecución de tratamiento de datos fuera de los locales de la ubicación del Fichero deberá ser autorizada expresamente por el Responsable del Fichero, constando así en el documento de seguridad determinando un usuario o perfil de usuarios y un periodo de validez para la autorización. Además se garantizará el nivel de seguridad correspondiente al tipo de Fichero tratado.

7.3. Todo Fichero temporal o copia de documentos que se hubiesen creado exclusivamente par la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda. Además, serán borrados o destruidos una vez que haya dejado de ser necesario para los fines que motivaron su creación.

7.4. Debe existir una normativa de seguridad formalizada en el Documento de Seguridad de acuerdo a lo establecido por la LOPD y RLOPD que debe ser de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información.

7.5. Las funciones y obligaciones del personal con respecto al tratamiento de los datos personales deben estar claramente definidas y documentadas y deben ser conocidas por el personal correspondiente.

7.6. Se habilitará un procedimiento de notificación y gestión de incidencias conteniendo un registro en el que se hará constar el tipo de incidencia, el momento en que se produce, la persona que realiza la notificación, a quién se le comunica, los efectos que se derivaron de la misma y las medidas correctoras aplicadas.

7.7. Si el mecanismo de autenticación de los usuarios que accedan a los datos se basa en la existencia de contraseñas, existirá un listado de usuarios autorizados por el responsable del fichero, un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad y se han de modificar periódicamente, en ningún caso la periodicidad será superior a un año, y mientras estén vigentes serán almacenadas de forma ininteligible.

7.8. Los accesos concedidos a los datos deben corresponder únicamente a los requeridos para realizar las funciones propias del trabajo a realizar. El acceso sólo puede ser autorizado por el personal designado expresamente en el Documento de seguridad.

7.9. Los soportes y documentos con datos de carácter personal deben estar inventariados, sólo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad y deberán almacenarse en un lugar de acceso restringido.

7.10. La salida fuera de los locales donde se ubica el fichero, únicamente podrá ser autorizada, por el Responsable del Fichero o debidamente autorizada en el documento de seguridad. 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.

7.11. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal, deberá procederse a su destrucción o borrado para evitar el acceso a la información contenida en el mismo o su recuperación posterior.

7.12. La identificación de los soportes que contengan datos considerados especialmente sensibles por la organización, se podrá realizar mediante etiquetado comprensible y con significado entendible para el personal con acceso autorizado y que dificulten la identificación para el resto de personas.

7.13. Deberán establecerse procedimientos para la realización, como mínimo semanal (a no ser que no se haya producido actualización alguna), de copias de respaldo. Los procedimientos establecidos para la realización de copias de seguridad y para la recuperación de los datos deberán garantizar su reconstrucción en el estado en que se encontraban en el momento de producirse una pérdida o destrucción de datos, sólo se procederá a grabar manualmente cuando, en caso de pérdida o destrucción, afectase a ficheros o tratamientos parcialmente automatizados, y además, se deberá dar constancia en el documento de seguridad.

7.14. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias.

7.15. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote como tal en el documento de seguridad. Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

Medidas de seguridad de nivel medio (*según corresponda)*

7.16. El Documento de Seguridad debe contener designar, adicionalmente a los requisitos mínimos establecidos por la LOPD y el RLOPD, a un responsable o responsables de seguridad, y los controles periódicos de verificación de seguimiento de las medidas de seguridad previstas.

7.17. Además de lo establecido anteriormente con respecto al registro de incidencias se deberá incluir información sobre los procedimientos realizados para la recuperación de los datos indicando el responsable de la ejecución del proceso, los datos restaurados y los datos grabados manualmente, adjuntando la autorización expresa del Responsable del fichero.

7.18. Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los locales donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

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

soportes incluidos en el envío, el tipo de información que contienen, la forma de envío, y la persona responsable de la entrega que deberá estar debidamente autorizada

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

7.21. Los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una Auditoría interna o externa, que verifique el cumplimiento de la normativa vigente en Protección de Datos de Carácter Personal. Con carácter extraordinario se realizará siempre que se produzcan modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas.

Medidas de seguridad de nivel alto (*según corresponda)*

7.22. Cuando se trate de datos de nivel alto se ha de mantener un registro de accesos incluyendo la identificación de usuarios, la fecha y hora, el fichero accedido, el tipo de acceso y si ha sido autorizado o negado. Para los accesos autorizados se ha de identificar los registros accedidos.

7.23. La responsabilidad del registro de accesos es del responsable de seguridad quien debe garantizar que no se desactive en ningún momento y se conserve por un periodo no menor a dos años. Adicionalmente debe realizar un seguimiento mensual periódico del registro elaborando un informe y los problemas detectados. No será necesario el registro de accesos definido en caso de que concurran las siguientes circunstancias: que el responsable del fichero o del tratamiento sea una persona física; y que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales. La concurrencia de las dos circunstancias deberá hacerse constar expresamente en el documento de seguridad.

7.24. La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

7.25. La distribución de soportes que contengan datos de carácter personal se realizará cifrando dichos datos o utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte. Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

7.26. Debe conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso, las medidas de seguridad exigidas por la legislación LOPD y RLOPD; o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

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

(opcional) Octava.- El Encargado del Tratamiento podrá subcontratar el almacenamiento de dichos datos a terceras empresas. En este supuesto, será necesario que contractualmente regule el tratamiento realizado por esta tercera empresa de los datos contenidos en el Fichero.

En todo caso, deberá comunicar por escrito al Responsable del Fichero que ha subcontratado dichos servicios.

En ningún caso y bajo ningún concepto el Encargado del Tratamiento podrá subcontratar dichos servicios a una empresa que se encuentre fuera del territorio español.

(opcional) Novena.- Comunicación de datos a terceros.

El Responsable del Fichero autoriza de forma expresa al Encargado del Tratamiento a comunicar los datos personales contenidos en el Fichero a una tercera parte, si fuera necesario para dar cumplimiento al objeto de los servicios contratados entre ambas Partes.

Décima – Controles y Auditorías. El Responsable del fichero se reserva el derecho de efectuar en cualquier momento los controles y auditorias que se estimen oportunas para verificar el correcto cumplimiento de las medidas del presente contrato. El encargado del tratamiento deberá facilitar cuantos datos o documentos le sean solicitados por el auditor nombrado por el responsable del fichero.

Y, en prueba de conformidad, las Partes firman el presente Acuerdo, por duplicado ejemplar y a un solo efecto,

En [localidad], a [día] de [mes] de [año]

Don/Doña [nombre]
Por el Responsable del Fichero

Don/Doña [nombre]
Por el Encargado del Tratamiento

Anexo 7 – Listado de controles periódicos para el cumplimiento de la LOPD

Listado de controles periódicos para el cumplimiento de la LOPD

Control	Procedimiento	Periodicidad	Nivel de seguridad	Fecha control
1. Aplicación del Documento de Seguridad				
1.1. Revisar cambios en el ámbito de aplicación del Documento de Seguridad	DS001	Semestral	Bajo	
1.2. Verificar si existen cambios en la estructura de los ficheros declarados y la posibilidad de declarar nuevos ficheros	DS001	Semestral	Bajo	
1.3. Comprobar cambios en la asignación de funciones	DS001	Semestral	Bajo	
1.4. Verificar el inventario de Locales	DS001	Semestral	Bajo	
1.5. Comprobar cambios en el inventario de sistemas informáticos y redes	DS001	Semestral	Bajo	
1.6. Verificar cambios en el software de aplicación de los ficheros	DS001	Semestral	Bajo	
1.7. Actualizar el registro de tratamientos de datos por cuenta de terceros	DS001	Semestral	Bajo	
2. Ficheros no automatizados				
2.1. Comprobar cambios en la estructura de ficheros no automatizados	PR003	Semestral	Bajo	
2.2. Verificar el listado de usuarios que tienen acceso a los ficheros	PR003	Semestral	Bajo	
2.3. Revisar las medidas de seguridad aplicadas para los accesos a los ficheros con datos de nivel alto	PR003	Mensual	Alto	
2.4. Comprobar el registro de accesos a documentación de nivel alto	PR003	Mensual	Alto	

Listado de controles periódicos para el cumplimiento de la LOPD

Control	Procedimiento	Periodicidad	Nivel de seguridad	Fecha control
3. Seguridad lógica				
3.1. Comprobar el acceso de los usuarios a las aplicaciones e información según su perfil asignado	PR004	Semestral	Bajo	
3.2. Comprobar el sistema de definición y actualización de los antivirus	PR004	Mensual	Bajo	
3.3. Verificar si los usuarios autorizados conceden los permisos de acceso lógico	PR004	Mensual	Bajo	
3.4. Analizar y aplicar, en su caso, cambios en el proceso de alta de usuarios	PR005	Semestral	Bajo	
3.5. Actualizar el registro de usuarios con acceso lógico según los cambios funcionales, contratación y bajas del personal	PR004	Mensual	Bajo	
3.6. Comprobar la existencia de usuarios inactivos	PR009	Semestral	Bajo	
3.7. Comprobar los registros de accesos por usuarios remotos	OP005	Mensual	Bajo	
3.8. Comprobar el bloqueo de los usuarios tras los intentos de acceso fallidos al sistema, realizando una prueba sustantiva. Analizar los bloqueos sucedidos durante el periodo	PR004	Semestral	Medio	
3.9. Registro de accesos a ficheros de nivel alto	PR004	Mensual	Alto	
4. Inventario y gestión de soportes				
4.1. Comprobar el inventario de soportes	PR006	Mensual	Bajo	
4.2. Evaluar el Registro de entrada y salida de soportes	PR006	Mensual	Medio	

Listado de controles periódicos para el cumplimiento de la LOPD

Control	Procedimiento	Periodicidad	Nivel de seguridad	Fecha control
4.3. Verificar que las autorizaciones de salida de soportes se han realizado de forma correcta	PR006	Mensual	Medio	
4.4. Comprobar el etiquetado y cifrado de soportes	PR006	Mensual	Alto	
5. Copias de respaldo y recuperación				
5.1. Llevar a cabo una prueba de recuperación selectiva de los datos	PR007	Mensual	Bajo	
5.2. Verificar físicamente los soportes para evaluar si corresponden con el registro	PR007	Mensual	Bajo	
5.3. Comprobar el registro de copias de respaldo	PR007	Mensual	Bajo	
6. Gestión de incidencias				
6.1. Llevar a cabo una comprobación de los registros y resoluciones de las incidencias detectadas	PR008	Mensual	Bajo	
7. Control de acceso físico				
7.1. Comprobar el listado de personal con acceso físico a las ubicaciones del Responsable del Fichero	PR010	Semestral	Bajo	
8. Otras cuestiones				
8.1. Analizar el contenido de las cláusulas de información y consentimiento para aplicar cambios, en su caso		Semestral		
8.2. Firmar los contratos con los nuevos encargados del tratamiento		Semestral		

OPERATIVA de GESTIÓN de la ENTIDAD

ÍNDICE DEL PROCEDIMIENTO

1. Objeto. 2
2. Ámbito 2
3. Desarrollo 2
3.1. Proceso de matriculación 2
3.1.1. Acceso mediante matriculación presencial: 2
3.1.2. Procesos Web de recogida de datos personales sin entrega de formulario firmado 2
3.1.3. Formulario Web de recogida de datos personales para su entrega en mano en CESAG 2
3.2. Gestión de Clientes 2
3.3. Cancelación de datos 3
3.4. Gestión de currículum 3
3.5. Solicitud de datos por las Fuerzas y Cuerpos de Seguridad del Estado (se incluye la figura del Policía-Tutor) 3
3.6. Solicitud de datos por las Administraciones Públicas 4
Anexo 1 – Cláusulas información y consentimiento 5
Cláusula de Información en la Recogida de Datos de los alumnos 6
CLÁUSULA TIPO PARA EL APARTADO "POLÍTICA DE PRIVACIDAD" DE LA PÁGINA WEB 8 8
Cláusula tipo para formularios obtenidos en la WEB a entregar firmados en CESAG 9
Anexo 2 - Cesión de Datos a las Fuerzas y Cuerpos de Seguridad del Estado 10
Anexo 3 - Cesión de Datos a las Administraciones Públicas 11

Revisado: Nombre y Firma:	Aprobado: Nombre y Firma:
Fecha:	Fecha:

1. Objeto.

Establecer los principales criterios a aplicar, dentro de la operativa propia a la gestión de la empresa, en relación a protección de datos de carácter personal.

2. Ámbito

El Responsable del Fichero y el Responsable de Seguridad deben velar por la correcta aplicación de las tareas relativas a protección de datos y llevar a cabo el seguimiento de su consecución y mantenimiento.

3. Desarrollo

3.1. Proceso de matriculación

Al recabar los datos de carácter personal de los alumnos que inician sus estudios en el Centro, debemos hacerles entrega de una cláusula de información y consentimiento sobre la recogida y tratamiento de sus datos constatando su entrega y recepción.

Según el medio de acceso a los estudios se utilizará uno de los sistemas descritos a continuación.

3.1.1. Acceso mediante matriculación presencial:

Se entregará y requerirá firmada la cláusula "*Información y consentimiento para el tratamiento de datos personales de los alumnos*" del Anexos 1 del presente documento.

3.1.2. Procesos Web de recogida de datos personales sin entrega de formulario firmado

En los procesos realizados a través de la página web de CESAG en que se recojan datos de carácter personal deberá de asegurarse que se ha leído y se acepta la política de privacidad, para ello se incorporará una casilla que el usuario marcará indicando que acepta dichas políticas del tipo:.

☐ He leído y acepto la Política de Privacidad

La casilla no puede estar premarcada y no se permitirá el envío de información si el usuario no la ha marcado, también debe existir un hipervínculo asociado a la palabra 'Política de Privacidad' que mostrará una página con el texto correspondiente a la política de privacidad el CESAG.

La cláusula correspondiente a dichos procesos se detalla en "*CLÁUSULA TIPO PARA EL APARTADO "POLÍTICA DE PRIVACIDAD" DE LA PÁGINA WEB"* del Anexo 1 del presente documento.

3.1.3. Formulario Web de recogida de datos personales para su entrega en mano en CESAG

Se entregará y requerirá la firma del formulario que contendrá la cláusula "*Cláusula tipo para formularios obtenidos en la WEB a entregar firmado en CESAG*" del Anexos 1 del presente documento.

3.2. Gestión de Clientes

Cuando un cliente solicite un servicio, que no este regulado en contrato, le haremos entrega de la cláusula '*Cláusula de Información y consentimiento en la Recogida de Datos*' del *Anexo 1*, que deberá firmarnos a fin de tener constancia, de que ha sido informado de todo aquello que obliga la normativa

y de que hemos recabado los consentimientos necesarios, si ha lugar, para el uso, tratamiento y cesión de los datos proporcionados por el cliente.

En la prestación de servicios, que impliquen el tratamiento de datos de terceros, suscribiremos con el cliente un contrato por cuenta de terceros, según el modelo *Contrato para Tratamiento de Datos Personales por Cuenta de Terceros* incluido en el *Anexo 5* del documento DS0001

Si suscribimos un contrato con clientes a fin de prestarles servicios, que no impliquen el tratamiento de datos personales de terceros, en dicho contrato incluiremos las cláusulas especificadas en el *Anexo 2- Cláusula de información y consentimiento para clientes (incluir en contratos)*.

3.3. Cancelación de datos

Los datos personales recabados en el transcurso de las actividades realizadas deberán ser cancelados cuando dicha información quede obsoleta o deje de ser necesaria para las finalidades previstas.

Se procederá a su adecuada destrucción de acuerdo con las normativas de destrucción de soportes especificadas en los procedimientos *PR-006 Procedimiento Gestión de Soportes* y *PR-003 Procedimiento de ficheros no automatizados*.

Únicamente para cumplir con los periodos de retención previstos por la ley se guardarán los datos que han alcanzado el final de su vida útil.

3.4. Gestión de currículum

A la recepción de un currículum, ya sea a través de la publicación de ofertas de trabajo en prensa, recepción de currículum en mano o bien directamente a través del correo electrónico de la empresa, se ha de informar al interesado.

La información al interesado se realizará a través de las cláusulas indicadas en el procedimiento *OP003_Procedimiento Recursos Humanos*. Se incluyen los siguientes supuestos:

1. Solicitud presencial.

   En el caso de que alguien entregue su currículum de forma presencial, se le entregará la cláusula para currículum (presencial); deberá firmarla y se adjuntará con su currículum como evidencia de que se ha recabado su consentimiento.

2. Solicitud no presencial.

   A la recepción de currículum a través de correo electrónico de la empresa, de correo ordinario o por cualquier otro medio no presencial se contestará con la cláusula de información y consentimiento por email, a través de carta certificada o burofax.

Y deberá procederse según lo especificado en dicho procedimiento.

3.5. Solicitud de datos por las Fuerzas y Cuerpos de Seguridad del Estado (se incluye la figura del Policía-Tutor)

La persona de la empresa que reciba la petición de información personal deberá:

- ❑ Comprobar la identidad del agente solicitando su documento acreditativo (p.e. carné profesional identificativo).

- Solicitará la documentación acreditativa, el requerimiento judicial u orden donde se indique la información requerida y se justifiquen los motivos de la solicitud de los datos de carácter personal.

  El agente podrá negarse a dar la explicación del asunto (p.e. secreto de sumario…). En caso de que no exista documento justificativo se le solicitará a quien represente a las Fuerzas y Cuerpos de Seguridad tanto la exposición de motivos para la cesión de los datos solicitados, así como los motivos por los cuales no se adjunta documentación acreditativa para la cesión correspondiente. Esta información se recogerá en el documento de cesión incluido en el *Anexo 2- Cesión de Datos a las Fuerzas y Cuerpos de Seguridad del Estado,* que deberá firmar el solicitante de los datos y quien los proporciona.

  Se debe valorar si la información solicitada responde a una petición concreta y específica de datos. La solicitud de datos en ningún caso podrá ser una solicitud masiva de datos. En caso de duda, contactar con el Responsable del Fichero.

- Por último, se deberá comunicar la cesión de datos al Responsable del Fichero/Responsable de Seguridad para que proceda a su registro en el Registro de Incidencias de Seguridad de acuerdo al procedimiento establecido en el Documento de Seguridad.

3.6. Solicitud de datos por las Administraciones Públicas

- Las Administraciones Públicas podrán recabar información para el ejercicio de sus funciones Públicas en el ámbito de las competencias que les atribuya una norma con rango de Ley.
- La persona de la empresa que reciba la petición de información demandará la documentación que acredite la solicitud de la misma. Ésta documentación deberá exponer los motivos que justifiquen el requerimiento de los datos solicitados.
- La información demandada debe responder a una petición concreta y específica de datos, explicando explícitamente sobre que personas se solicita la información, qué datos concretos se solicitan y la finalidad para la cual se recaban, en ningún caso podrá ser una solicitud masiva. En caso de duda, se consultará al Responsable del Fichero.
- Esta información se recogerá en el documento de cesión incluido en el *Anexo 3- Cesión de Datos a las Administraciones Públicas.*
- Aconsejamos en estos casos, que se pongan en contacto con el Responsable del Fichero/Responsable de Seguridad.

Anexo 1 – Cláusulas información y consentimiento

Cláusula de Información en la Recogida de Datos de los alumnos

En cumplimiento con lo dispuesto en la Ley Orgánica 15/1999 de protección de datos de carácter personal, de 13 de diciembre, le informamos que todos los datos de carácter personal contenidos en su matrícula, además de toda la información personal que fuera suministrada verbalmente, por escrito o por cualquier otra vía serán incluidos en uno o varios ficheros cuya responsabilidad corresponde al Centre d'Ensenyamen Superior Alberta Giménez (en adelante, CESAG), con el fin de poder ofrecerle unas mejores prestaciones en el ámbito de los servicios educativos ofrecidos por nuestro centro, tales como la gestión académica, gestión psicopedagógica, actividades extraacadémicas, contratación de servicios complementarios, u otros fines compatibles con los anteriores.

A continuación, se detallan los supuestos en los que, a través de la marcación de la casilla correspondiente, situada al final del presente documento, usted podrá manifestar su negativa al CESAG para la recogida, almacenamiento, tratamiento, uso y publicaciones de los datos e imágenes a los que se refieran, todo ello bajo las instrucciones previstas en esta cláusula. El consentimiento prestado podrá ser revocado en cualquier momento, sin efectos retroactivos y por causa justa.

Los tratamientos de datos efectuados son los siguientes:

- El CESAG dispone de medios propios; en Internet a través de su página Web, y de publicaciones en formato papel (revistas, agendas, trípticos...); donde informa de las actividades académicas lectivas, extraacadémicas y complementarias. En éstos pueden publicarse datos e imágenes en las que aparezcan, individualmente o en grupo, los alumnos realizando las actividades mencionadas.
- La distribución de datos e imágenes al resto de alumnos y profesores.
- Los datos personales de los alumnos podrán ser publicados en zonas de acceso público, dentro de nuestras instalaciones. Le indicamos que el fin de dicha publicación es claramente informativo.
- El tratamiento de datos de salud que usted nos suministre, o bien le sean solicitados por nuestro personal, con el fin de adecuar nuestros servicios a sus posibles necesidades.

Le recordamos que para poder llevar a cabo la correcta gestión del tratamiento de sus datos personales es preciso que facilite los datos correctos y veraces y que se comprometa a comunicar a esta entidad cualquier modificación de los mismos.

Le informamos que Usted goza de la posibilidad de ejercitar gratuitamente los derechos de acceso, cancelación, rectificación y oposición con relación a sus datos personales y de los ficheros que los contienen, para lo que podrá dirigirse a Secretaría del CESAG sito en Costa de Saragossa 16, 07013 Palma de Mallorca, aportando copia de documento oficial válido que lo identifique.

☐	NO Autorizo el tratamiento y publicación de los datos e imágenes en los medios propios.
☐	NO Autorizo la distribución de datos e imágenes al resto de alumnos y profesores.
☐	NO Autorizo la distribución de datos e imágenes a difusión pública no comercial ni a las publicaciones de ámbito académico.
☐	NO Autorizo la publicación de los datos en zonas de acceso público dentro del centro.
☐	NO Autorizo el tratamiento de datos de salud

Firma del alumno/a
Nombre: DNI:

Fecha: _____ de _____ de 20_____

CLÁUSULA TIPO PARA EL APARTADO "POLÍTICA DE PRIVACIDAD" DE LA PÁGINA WEB

Cláusula POLITICA de PRIVACIDAD

En cumplimiento con lo dispuesto en la Ley Orgánica 15/1999 de protección de datos de carácter personal (en adelante LOPD), de 13 de diciembre, le informamos que todos los datos de carácter personal contenidos en su matrícula, además de toda la información personal que fuera suministrada verbalmente, por escrito o por cualquier otra vía serán incluidos en uno o varios ficheros cuya responsabilidad corresponde al Centro Enseñanza Superior Alberta Giménez (en adelante CESAG), con el fin de poder ofrecerle unas mejores prestaciones en el ámbito de los servicios ofrecidos por nuestro centro, tales como la gestión académica, gestión psicopedagógica, u otros fines compatibles con los anteriores.

A continuación, se detallan los tratamientos de datos efectuados por el CESAG; tratamientos que que usted autoriza salvo que recibamos su negativa por escrito en el plazo de 30 días. Su consentimiento podrá ser revocado en cualquier momento, sin efectos retroactivos y por causa justa.

Los tratamientos de datos efectuados son los siguientes:

- CESAG dispone de medios propios; en Internet a través de su página Web, y de publicaciones en formato papel (revistas, agendas, trípticos...); donde informa de las actividades académicas lectivas, extraacadémicas y complementarias. En éstos pueden publicarse datos e imágenes en las que aparezcan, individualmente o en grupo, los alumnos realizando las actividades mencionadas.
- La distribución de datos e imágenes al resto de alumnos y profesores.
- Las imágenes y el nombre del alumno podrán ser publicadas en medios de difusión pública no comercial y en las revistas y publicaciones de ámbito educativo.
- Los datos personales de los alumnos podrán ser publicados en zonas de acceso público, dentro de nuestras instalaciones. Le indicamos que el fin de dicha publicación es claramente informativo.
- El tratamiento de datos de salud que usted nos suministre, o bien le sean solicitados por nuestro personal, con el fin de adecuar nuestros servicios a sus posibles necesidades.

Le recordamos que para poder llevar a cabo la correcta gestión del tratamiento de sus datos personales es preciso que facilite los datos correctos y veraces y que se comprometa a comunicar a esta entidad cualquier modificación de los mismos.

Le informamos que Usted goza de la posibilidad de ejercitar gratuitamente los derechos de acceso, cancelación, rectificación y oposición con relación a sus datos personales y de los ficheros que los contienen, para lo que podrá dirigirse a Secretaría del CESAG sito en Costa de Saragossa 16, 07013 Palma de Mallorca, aportando copia de documento oficial válido que lo identifique.

Cláusula tipo para formularios obtenidos en la WEB a entregar firmados en CESAG

En cumplimiento con lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, los datos suministrados por el usuario quedarán incorporados a un fichero cuya responsabilidad corresponde al Centro Enseñanza Superior Alberta Giménez (en adelante CESAG), con la finalidad de gestionar la prestación de los servicios académicos solicitados.

Le recordamos que para poder llevar a cabo la correcta gestión del tratamiento de sus datos personales es preciso que facilite los datos correctos y veraces y que se comprometa a comunicar a esta entidad cualquier modificación de los mismos.

Si Vd. no marca la casilla correspondiente, con la firma del presente documento autoriza el tratamiento y publicación de los datos e imágenes en los medios propios (página Web y publicaciones en papel), la distribución de datos e imágenes al resto de alumnos y profesores, a la difusión pública no comercial y a las publicaciones de ámbito académico así como la publicación de los datos en zonas de acceso público dentro del centro.

Si Vd. nos suministra datos de salud, o bien le son solicitados por nuestro personal, con el fin de adecuar nuestros servicios a sus posibles necesidades, otorgará consentimiento para ello si no realiza la marcación de la casilla correspondiente y firma el presente documento.

Le informamos que Usted goza de la posibilidad de ejercitar gratuitamente los derechos de acceso, cancelación, rectificación y oposición con relación a sus datos personales y de los ficheros que los contienen, para lo que podrá dirigirse a Secretaría del CESAG sito en Costa de Saragossa 16, 07013 Palma de Mallorca, aportando copia de documento oficial válido que lo identifique.

- ☐ NO Autorizo el tratamiento y publicación de los datos e imágenes.
- ☐ NO Autorizo el tratamiento de datos de salud

Anexo 2 - Cesión de Datos a las Fuerzas y Cuerpos de Seguridad del Estado

D./Dña. _____ Nº Identificación _____

En su condición de representante de las Fuerzas y Cuerpos de Seguridad reclama la comunicación de los datos de carácter personal referidos a:

(Señalar concreta y específicamente qué datos de carácter personal se reclaman)

Con la finalidad y motivación siguiente:

(Detallar qué objetivo/s tiene la solicitud de datos de carácter personal)

Señale con una (X). Se adjunta documentación justificativa:

- ☐ Mandamiento judicial
- ☐ Requerimiento del Ministerio Fiscal
- ☐ Otros (indicar) _____

En caso contrario indicar motivo para no aportar documentación justificativa

Se informa que, a tenor de lo dispuesto en el artículo 22.4 de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos, los datos personales ahora cedidos o comunicados deberán ser cancelados cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

_____

Firma del receptor de la información

Nombre y firma del trabajador responsable de la entrega:	Fecha y hora:

Anexo 3 - Cesión de Datos a las Administraciones Públicas

Administración Pública competente:
(*Indicar exactamente que Administración Pública solicita la información)*

Los siguientes datos personales:
(Señalar concreta y específicamente qué datos de carácter personal se reclaman)

Con la finalidad y motivación siguiente:
(Detallar qué objetivo/s tiene la solicitud de datos de carácter personal)

Indicar si se adjunta documentación justificativa:

_____

En caso contrario indicar motivo para no aportar documentación justificativa

---

Se informa que, a tenor de lo dispuesto en el artículo 22.4 de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos, los datos personales ahora cedidos o comunicados deberán ser cancelados cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

_____

Firma del receptor de la información
D./Dña.

DNI

Nombre y firma del trabajador responsable de la entrega:	Fecha y hora:

OPERATIVA DE RECURSOS HUMANOS

ÍNDICE DEL PROCEDIMIENTO

1. Objeto. 2
2. Ámbito. 2
3. Desarrollo. 2
3.1. Recepción de Currículums 3
3.2. Selección de personal 3
3.3. Contratación de Personal 4
3.4. Administración de Personal 5
3.5. Gestión de Partes de Accidentes Laborales 5
3.6. Finalización de Contratos 6
3.7. Externalización de servicios de Recursos Humanos 6
Anexo 1 - Cláusulas de información y consentimiento 7
Cláusula a incluir en el contrato laboral 8
Modelo de Carta a remitir para la actualización de datos 9
Contestación currículum (presencial) 10
Contestación currículum (no presencial) 11

Revisado:	Aprobado:
Nombre y Firma:	Nombre y Firma:
Fecha:	Fecha:

1. Objeto.

Los procesos de recursos humanos y personal requieren especial atención. En el desarrollo de estas funciones se maneja una gran cantidad de información de carácter personal que además suele incluir información confidencial. Por consiguiente, es fundamental conservar el máximo cuidado en el tratamiento de los datos en todas y cada una de las actividades que se realizan.

En este procedimiento se exponen los puntos que deben considerarse para el tratamiento de datos de carácter personal.

2. Ámbito.

El Responsable de Seguridad debe velar por la correcta aplicación del siguiente procedimiento y llevar a cabo el seguimiento de su consecución.

Asimismo el responsable del departamento de Recursos Humanos velará por el cumplimiento y mantenimiento del presente procedimiento, en conjunción con el Responsable de Seguridad.

3. Desarrollo.

Para una mejor comprensión de los puntos a aplicar, hemos dividido los criterios de buenas prácticas en los siguientes apartados:

- Recepción de currículums
- Selección de personal
- Contratación de personal
- Administración de personal
- Gestión de partes de accidentes laborales
- Finalización de contratos
- Externalización de servicios de nómina

Por otra parte, y debido a la sensibilidad de la información, es especialmente importante almacenar la documentación bajo llave y limitar el acceso de personal no autorizado al área de trabajo. Para más información sobre cómo almacenar la información en formato papel, consultar el procedimiento PR-004.

La eliminación de información del área de Recursos Humanos debe realizarse con el máximo de garantías. Por ello, si la documentación está en papel, se utilizarán destructoras de papel o se troceará de tal forma que no sea factible su reconstrucción. No se reciclarán los documentos ni se enviarán a destruir a instalaciones externas.

En cuanto a la información automatizada se solicitará al Responsable de Seguridad que aplique las medidas oportunas para que ésta no pueda volver a ser recuperada por ningún medio.

Toda información relativa a datos personales del área, que sea enviada fuera de las instalaciones en soportes magnéticos, debe ser registrada en el Registro de Entradas y Salidas de Soportes (procedimiento PR-007) y debe cifrarse en caso de contener datos de nivel alto.

3.1. Recepción de Currículums

En todos los casos de recepción de currículums, se ha de informar al interesado, a través de las cláusulas de información, de de todo aquello que establece la LOPD. Esto incluye publicación de ofertas de trabajo en prensa o bien directamente a través del correo electrónico de la empresa.

Al final de este documento se adjuntan las cláusulas de información y consentimiento correspondientes a los siguientes supuestos:

1. Solicitud presencial.

   En el caso de que alguien entregue su currículum de forma presencial, se le entregará la cláusula para currículums (presencial); deberá firmarla y se adjuntará con su currículum para así tener la certeza que nos ha prestado su consentimiento.

2. Solicitud no presencial.

   Si se recibe un currículum a través del correo electrónico, ya sea en una dirección de correo dedicado a la recepción de currículum, así como en cualquier otro, se contestará con la cláusula de información y consentimiento por email.

   En caso de que se reciban por correo ordinario se contestará con las mismas cláusulas mediante correo certificado a la dirección del remitente o por e-mail si dicho currículum lo especificara.

   Las contestaciones a la recepción de currículum que se envíen por mail se realizarán con confirmación de lectura.

Una vez que se ha informado al interesado, en cualquiera de las modalidades, habrá que contemplar los siguientes aspectos:

- Si las cláusulas de información y consentimiento incluyen la cesión a otras entidades, en el caso de recepción de currículum a través del correo electrónico, debemos esperar al plazo de 30 días que se le otorga al afectado para manifestar su negativa a la cesión sus datos. Una vez transcurrido el plazo se remitirá el currículum al resto de entidades para las que se ha solicitado consentimiento.
- Resulta importante mantener la observancia respecto a la inclusión de datos de nivel alto (salud, afiliación sindical,…), ya que puede alterar el nivel de seguridad del fichero declarado.
- En caso de que interese el currículum, y este contenga datos de nivel alto, se ponderará si resulta necesario mantenerlos.
- Los currículum que interesen podrán mantenerse durante el proceso de selección para el que fueron presentados o como máximo durante un periodo de 12 meses.
- El resto de currículums que no interesen, deberán ser destruidos.

3.2. Selección de personal

El curriculum vitae (CV) es la materia prima para este proceso, por lo cual se hacen las siguientes consideraciones sobre el mismo.

En los procesos de selección se comprobará que los curriculum vitae cuentan con las autorizaciones correspondientes para su uso en el proceso de selección que se ha de realizar (comprobar si no existe una negativa para ceder el currículum). Las comprobaciones a realizar se detallan a continuación:

1. La información que se mantenga en un registro informático debe ser únicamente la necesaria para la evaluación de si los candidatos reúnen o no las aptitudes y capacidad profesional necesarias para el puesto, evitando que la misma pueda abarcar aspectos de la vida del solicitante de empleo no influyentes en la determinación de su capacidad profesional.
2. Toda información, referida a los datos de los candidatos, solicitada al departamento de Recursos Humanos deberá ser tratada con el máximo nivel de confidencialidad y se extremarán las precauciones en la selección del medio o método de envío de dicha información, de acuerdo al nivel de seguridad del fichero, considerando los requisitos de la LOPD.
3. Una vez iniciado el proceso de selección con los candidatos previstos, la información complementaria que se solicite a los candidatos debe ser únicamente la que guarde relación directa con el puesto de trabajo que vaya a desempeñar. Durante el proceso de selección en ningún caso se harán anotaciones que atenten contra la dignidad de la persona, ni por escrito ni en formato electrónico. Este aspecto se aplica tanto para el personal del departamento de recursos humanos como para el personal ajeno al área responsable de entrevistar a los candidatos en la evaluación de su adecuación al puesto.
4. Por otra parte, el personal que no forme parte del departamento de recursos humanos también debe adherirse a los requerimientos de confidencialidad y tratamiento de la información de candidatos de acuerdo a lo descrito en los puntos anteriores, y en ningún caso debe conservar la información utilizada durante el proceso de selección en el que haya participado.
5. Una vez que el proceso de selección previsto ha finalizado o ha transcurrido el periodo de retención establecidos (12 meses), el currículum vitae pierde todo el sentido y debe ser destruido ya que no se puede garantizar la exactitud de la información que contiene.

3.3. Contratación de Personal

- ❑ El contrato de trabajo debe incluir entre sus cláusulas los derechos que le otorga la LOPD al nuevo empleado ante la empresa.
- ❑ Durante el proceso de contratación, se le informará de cómo acceder a una copia del Documento de Seguridad, en lo relativo al cumplimiento sobre protección de datos que le corresponda según sus funciones. Se hará especial hincapié en la importancia de salvaguardar la seguridad de los datos de carácter personal de clientes, proveedores, empleados, etc. El empleado debe firmar la aceptación de las políticas de seguridad de la empresa.
- ❑ Toda la documentación generada para la contratación (como por ejemplo los documentos TC1 y TC2) serán tratados con los máximos niveles de seguridad y no deberán dejarse en armarios que no puedan ser cerrados con llave, ni se dejarán las llaves al alcance de cualquiera, ni los armarios abiertos. En cualquier caso se podrá consultar el procedimiento PR003 donde se hallan las normas de almacenamiento para ficheros no automatizados.

Finalmente, al contratar a un nuevo empleado, el personal de recursos humanos debe notificarlo al Responsable de Seguridad para que se proceda a:

- Dar de alta el acceso del usuario a los sistemas de información y de los recursos informáticos tales como cuentas de correo, accesos a través de redes u otros.
- Comunicar el acceso a las instalaciones de la empresa.

- Actualizar los registros de personal autorizado de acceso al fichero en el Documento de Seguridad.
- Dar a conocer sus responsabilidades con respecto a la Política de Seguridad y las políticas de uso de recursos informáticos

3.4. Administración de Personal

En el proceso de Administración de Personal deberemos tener en cuenta los siguientes aspectos:

- ❑ La gestión que se realiza de los datos personales en el departamento de Recursos Humanos conlleva el tratamiento de datos de distintos niveles, en algunos casos, altamente sensibles, como los datos de minusvalías o afiliación sindical, por lo que se deben establecer las medidas organizativas y técnicas que garanticen los niveles de seguridad correspondientes. Los datos de salud que aparecen en currículums, los utilizados para liquidar impuestos o solicitar ayudas para la discapacidad, etc. se consideran de nivel básico siempre y cuando no se utilicen para otras cuestiones.
- ❑ Toda información que se solicite al área de Recursos Humanos referida a los datos personales de los empleados o de sus datos de nómina deberá ser debidamente justificada y con la autorización correspondiente. Deberá ser tratada con el nivel de seguridad adecuado en cuanto a su envío y tratamiento fuera del departamento de Recursos Humanos. Por ello se consultará con el Responsable de Seguridad, antes de realizar el envío, si los niveles de seguridad previstos se ajustan a los requerimientos de la LOPD y si la solicitud está debidamente aprobada por el Responsable del Fichero.
- ❑ El envío de información a los empleados de sus recibos de nómina, debe cumplir con los requisitos de seguridad correspondientes tanto si se entrega de forma impresa como si se realiza por vía electrónica, en cuyo caso los datos deberán transmitirse cifrados o ilegibles, de modo que se impida que la información pueda ser interpretada por terceros. La entrega de nóminas de forma presencial se hará personalizada al trabajador o bien al responsable que gestione las mismas.
- ❑ Toda la información solicitada u obtenida de las Administraciones Públicas, ya sea para la ejecución de retenciones, seguridad social u otros fines, debe estar necesariamente amparada en la legislación vigente para su validez y debe gestionarse con el máximo nivel de seguridad en cuanto al tratamiento y envío, el cual debe ser verificado y aprobado por el Responsable de Seguridad.

3.5. Gestión de Partes de Accidentes Laborales

- ❑ Los partes de accidentes laborales deben ser tratados como estrictamente confidenciales y se les dará un tratamiento de nivel de seguridad alto.
- ❑ Los partes de accidente en formato papel deben gestionarse en sobre totalmente cerrado y únicamente por el personal autorizado.
- ❑ De igual forma, la comunicación de esta información al Ministerio de Trabajo y a la Mutua correspondiente se hará bajo el máximo nivel de seguridad, validando con el Responsable de Seguridad los mecanismos de envío de datos.

3.6. Finalización de Contratos

Al finalizar o rescindir el contrato de trabajo, el personal de recursos humanos debe notificarlo al Responsable de Seguridad para que se proceda a:

- Dar de baja el acceso del usuario a los sistemas de información y de los recursos informáticos tales como cuentas de correo, accesos a través de redes u otros.
- Comunicar/restringir el acceso a las instalaciones de la empresa.
- Actualizar los registros de personal autorizado de acceso al fichero en el Documento de Seguridad.

3.7. Externalización de servicios de Recursos Humanos

Si se subcontratan servicios externos, p.e. selección de candidatos, confección de nóminas, prevención de riesgos, etc., se ha de contar con el contrato de servicios correspondiente que garantice los niveles de seguridad y confidencialidad correspondientes.

Anexo 1 - Cláusulas de información y consentimiento

Cláusula a incluir en el contrato laboral

Los datos personales contenidos en su contrato laboral así como el resto de información personal surgida a raíz del mismo, incluyendo la información que pueda existir en un futuro, serán convenientemente incluidos en uno o varios ficheros cuya responsabilidad corresponde a la entidad CES Alberta Giménez. El responsable de los ficheros y quienes intervengan en cualquier fase del tratamiento de datos están obligados a guardar el debido secreto profesional sobre los mismos.

De conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos, se le informa que la finalidad del tratamiento de sus datos personales es el adecuado desarrollo de la relación laboral que nos une, con el objeto de poder prestar los servicios relacionados con su labor profesional.

Cabe recordar al trabajador, que para poder llevar a cabo la correcta gestión de la presente contratación es preciso que facilite los datos correctos y veraces y que se comprometa a comunicar a esta entidad cualquier modificación de los mismos.

En cuanto a lo dispuesto en el artículo 10 LOPD, el empleado se compromete a no tratar, ni ceder, ni comunicar, ni utilizar en beneficio propio, ni revelar a terceros, los datos de carácter personal a los que tenga acceso, y a guardar estricto secreto profesional sobre cualquier información que conozca en el desempeño de su trabajo, tanto en el tiempo que dure su contrato laboral, como posteriormente al finalizar dicha relación.

Además de lo anterior le comunicamos que se dispone [en internet de una página web, y de publicaciones en formato papel] *(indicar el medio en cada caso: web, revistas, agendas, trípticos…)* donde se informa de las actividades académicas lectivas, extraacadémicas y complementarias respectivamente. En éstas pueden publicarse imágenes en las que Usted aparezca. Con la firma de este documento, Vd. nos autoriza a que sus datos, incluida la imagen, correspondientes a las actividades antes mencionadas, puedan ser publicados en el soporte correspondiente, puedan ser distribuidas al resto de personal y alumnos del centro, así como a filmaciones destinadas a difusión pública no comercial o a las revistas o publicaciones de ámbito académico.

Por último debe Vd. saber que goza de la posibilidad de ejercitar gratuitamente los derechos de acceso, rectificación, cancelación y oposición con relación a sus datos personales y los ficheros que los contienen, siempre y cuando ello no afecte al normal desarrollo de su relación laboral vigente, para lo que podrá dirigirse a CES Alberta Giménez, sito en Costa de Saragossa, 16 de Palma de Mallorca, aportando copia del documento oficial que le identifique.

Modelo de Carta a remitir para la actualización de datos

Palma de Mallorca a _____ de _____ de _____

Apreciado [Nombre del trabajador]:

En la empresa CES Alberta Giménez estamos realizando una actualización de nuestros procedimientos de protección de datos personales de acuerdo con lo establecido en la Ley Orgánica 15/1999 (LOPD), de 13 de diciembre.

Por ello le recordamos, como usted ya sabe, que los datos personales obtenidos a lo largo de la relación laboral, están incluidos en uno o varios ficheros cuya responsabilidad corresponde a la entidad CES Alberta Giménez

De conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos, se le informa que la finalidad del tratamiento de sus datos personales es el adecuado desarrollo de la relación laboral que nos une, con el objeto de poder prestar los servicios relacionados con su labor profesional.

Tenga presente que para poder llevar a cabo correctamente los tratamientos descritos, es preciso que nos comunique cualquier modificación de sus datos personales.

En cuanto a lo dispuesto en el artículo 10 LOPD, el empleado se compromete a no tratar, ni ceder, ni comunicar, ni utilizar en beneficio propio, ni revelar a terceros, los datos de carácter personal a los que tenga acceso y a guardar estricto secreto profesional sobre cualquier información que conozca en el desempeño de su trabajo, tanto en el tiempo que dure su contrato laboral, como posteriormente al finalizar dicha relación.

Además de lo anterior le comunicamos que se dispone [en internet de una página web, y de publicaciones en formato papel] *(indicar el medio en cada caso: web, revistas, agendas, trípticos…)* donde se informa de las actividades académicas lectivas, extraacadémicas y complementarias respectivamente. En éstas pueden publicarse imágenes en las que Usted aparezca. Con la firma de este documento, Vd. nos autoriza a que sus datos, incluida la imagen, correspondientes a las actividades antes mencionadas, puedan ser publicados en el soporte correspondiente, puedan ser distribuidas al resto de personal y alumnos del centro, así como a filmaciones destinadas a difusión pública no comercial o a las revistas o publicaciones de ámbito académico.

Por último debe Vd. saber que goza de la posibilidad de ejercitar gratuitamente los derechos de acceso, rectificación, cancelación y oposición con relación a sus datos personales y los ficheros que los contienen, siempre y cuando ello no afecte al normal desarrollo de su relación laboral vigente, para lo que podrá dirigirse a CES Alberta Giménez, sito Costa de Saragossa, 16 de Palma de Mallorca, aportando copia del documento oficial que le identifique

Firma del trabajador
Nombre:
DNI

Contestación currículum (presencial)

Le informamos que los datos personales contenidos en su currículum serán convenientemente archivados por CES Alberta Giménez.

En cumplimiento de lo dispuesto en la Ley Orgánica 15/1999 de protección de datos personales, de 13 de diciembre, le comunicamos que con la entrega de la mencionada información, se entenderá que Vd. nos autoriza a la recogida, almacenamiento, tratamiento y uso de sus datos de carácter personal, así como de otros datos que sean suministrados a esta empresa a lo largo del proceso selectivo de personal, y que resulten adecuados para la prestación de los servicios de gestión de la presente oferta laboral u otras que pudieran surgir en un futuro.

Asimismo le informamos que si Vd. no marca la casilla siguiente, consiente, con la firma del presente documento a que su currículum sea remitido a las entidades detalladas a pie de página, para los mismos fines antes mencionados.

☐ NO consiento que cedan mis datos a las entidades mencionadas, para la finalidad de selección de personal.

Por medio de la firma del presente documento usted autoriza a CES Alberta Giménez la recogida, almacenamiento, tratamiento y uso de los datos aportados, consentimiento que podrá ser revocado por usted en cualquier momento sin efectos retroactivos y por causa justa.

Por último debe Vd. saber que goza de la posibilidad de ejercitar gratuitamente los derechos de acceso, rectificación, cancelación y oposición con relación a sus datos personales y los ficheros que los contienen, siempre y cuando ello no afecte al normal desarrollo de su relación laboral vigente, para lo que podrá dirigirse a CES Alberta Giménez, sito en Costa de Saragossa, 16 de Palma de Mallorca, aportando copia del documento oficial que le identifique.

En Palma de Mallorca, a _____ de _____ de _____

Fdo: [Nombre y apellidos del interesado]

DNI: [DNI del interesado]

Entidades: [Relacionar entidades a las que se cederá el currículum]

Contestación currículum (no presencial)

Le informamos que los datos personales contenidos en el currículum que usted nos ha remitido serán convenientemente archivados por CES Alberta Giménez

En cumplimiento de lo dispuesto en la Ley Orgánica 15/1999 de protección de datos personales, de 13 de diciembre, le comunicamos que con la entrega de la mencionada información se entiende que Vd. nos autoriza a la recogida, almacenamiento, tratamiento y uso de sus datos de carácter personal, así como de otros datos que sean suministrados a esta empresa a lo largo del proceso selectivo de personal, y que resulten adecuados para la prestación de los servicios de gestión de la presente oferta laboral u otras que pudieran surgir en un futuro.

Asimismo le informamos que su currículum será remitido a las entidades detalladas al pie de este documento [o bien hacer referencia al enlace de la web donde aparezcan todas las sociedades], para los mismos fines antes mencionados de la entidad a la que se ceden los datos.

- Por medio de la lectura del presente documento usted esta autorizando, salvo que recibamos instrucciones suyas en sentido contrario en el plazo de treinta días, a la cesión de dichos datos para los fines y a las empresas antes mencionados, consentimiento que podrá ser revocado por Vd. en cualquier momento.

Por último debe Vd. saber que goza de la posibilidad de ejercitar gratuitamente los derechos de acceso, rectificación, cancelación y oposición con relación a sus datos personales y los ficheros que los contienen, siempre y cuando ello no afecte al normal desarrollo de su relación laboral vigente, para lo que podrá dirigirse a CES Alberta Giménez, sito en Costa de Saragossa, 16 de Palma de Mallorca, aportando copia del documento oficial que le identifique.

[Responsable Recursos Humanos]

Firma del Responsable

Entidades: [Relacionar entidades a las que se cederá el currículum]

OPERATIVA PARA LOS ACCESOS REMOTOS

ÍNDICE DEL PROCEDIMIENTO

1. Objeto. 2
2. Ámbito. 2
3. Desarrollo. 2
   3.1. Identificación del requerimiento conexión remota 2
   3.2. Aprobar solicitud de acceso remoto 2
   3.3. Definición/validación de los requisitos de conexión 3
   3.4. Alta de la conexión remota 3
   3.5. Distribución de credenciales 3
Anexo 1 - Petición de Acceso Remoto a SSI 5

Revisado:	Aprobado:
Nombre y Firma:	Nombre y Firma:
Fecha:	Fecha:

1. Objeto.

Este procedimiento establecerá los mecanismos de autorización y control sobre los accesos que realice personal, tanto ajeno como propio, a los sistemas de información de la empresa.

2. Ámbito.

El Responsable de Seguridad ha de velar por la correcta aplicación del siguiente procedimiento y llevar a cabo el seguimiento de su consecución.

Asimismo, si se ha establecido la figura del Administrador de sistemas, este velará por el cumplimiento y mantenimiento del presente procedimiento, en conjunción con el Responsable de Seguridad.

3. Desarrollo.

3.1. Identificación del requerimiento conexión remota

Usuario/Proveedor informático

Para habilitar una conexión de acceso remoto, se ha de realizar una petición de acceso indicando:

- Datos del solicitante de la conexión
- Motivos que generan la conexión
- Información sobre el ámbito de acceso requerido

Esta petición se debe hacer al Responsable de Seguridad a través del formulario *Petición de Acceso Remoto a SSI* incluido en el *Anexo 1* del presente procedimiento.

3.2. Aprobar solicitud de acceso remoto

El Responsable de Seguridad, en conjunto con el Administrador de sistemas, debe evaluar la solicitud, y en caso de que la petición de acceso implique el acceso de Ficheros con datos de carácter personal, se debe anotar la autorización correspondiente de acuerdo al personal designado en el *Anexo 5 (Personal Autorizado para Acceder al Fichero)* del documento *DS001*.

El acceso otorgado a los usuarios (internos o externos) que se conectan de forma remota debe estar restringido únicamente al ámbito requerido de acuerdo a las finalidades que han generado el requerimiento de conexión.

En caso de que la solicitud de acceso sea denegada, se informará al solicitante sobre los motivos de la denegación y se finaliza el procedimiento archivando la solicitud.

3.3. Definición/validación de los requisitos de conexión

Una vez aprobada la necesidad de conexión remota y, considerando los requerimientos de seguridad y funcionalidad, se determinarán las características necesarias para establecer la conexión:

- Tipo de conexión a utilizar
- Requerimientos de compatibilidad para realizar la conexión
- Niveles de seguridad requeridos:
  - Método de identificación y autenticación necesario
  - Nivel de cifrado de datos requerido

Una vez que se han definido las características se realizarán tantas pruebas como sean necesarias a fin de garantizar el correcto funcionamiento de la conexión y el adecuado registro de la misma en un log de accesos.

3.4. Alta de la conexión remota

Finalmente, antes de habilitar la conexión, se debe informar sobre las obligaciones derivadas del uso de esta funcionalidad.

En el caso de usuarios, su deber de confidencialidad y el detalle de normas de seguridad a seguir sobre los equipos remotos.

En el caso de proveedores informáticos se ha de garantizar:

- Existencia de un contrato por cuenta de terceros que regule el tratamiento de los datos personales.
- La obligación de registro, en caso de incidencias, indicando el acceso del proveedor incluyendo la siguiente información: fecha y hora de la conexión, persona que la ha autorizado, objeto, fecha y hora de la desconexión así como copia de la sesión, y la descripción del trabajo realizado (*Anexo 1* del Procedimiento de gestión de incidencias *PR-008*).
- En la medida de lo posible, se mantendrá un registro en detalle de las conexiones realizadas y la actividad realizada por el proveedor correspondiente.

3.5. Distribución de credenciales

En el momento en el que se habilite la conexión se procederá a proporcionar al usuario o proveedor externo las credenciales de acceso de la siguiente forma:

- En el caso de usuarios con conexión remota al centro de trabajo desde ordenadores portátiles propiedad de la propia empresa, se les configurará la conexión por parte del personal informático sin proporcionarles estas credenciales. La contraseña de acceso se generará de forma aleatoria con una longitud mínima de 8 caracteres; esta contraseña no será custodiada por el personal informático de ninguna forma.
- En el caso de usuarios o empresas externas se proporcionarán las credenciales vía correo electrónico, a la dirección que se haya acordado en el contrato de prestación de servicios. Al igual que el caso anterior la contraseña no será custodiada por el personal informático de ninguna forma.

En caso de incidencia referente a las credenciales de usuario de estos accesos remotos, se notificará de inmediato al Responsable de Seguridad, quien procederá a registrar la incidencia y se procederá a generar una nueva contraseña para dicha conexión.

Anexo 1 - Petición de Acceso Remoto a SSI

Este Anexo contiene el modelo de petición de acceso, los registros cumplimentados se almacena en:

Documento: 'OP005A001- Petición de Acceso Remoto a SSI'

Referencia: OP005A001

Carpeta:

Ubicación:

Anexo 1 - Petición de Acceso Remoto a SSI

Datos de la petición de Acceso Remoto	
Fecha petición:	
Petición:	[Descripción de la conexión]
Motivos que generan la conexión:	
Peticionario: (nombre, NIF /CIF)	[Obligatorio poner CIF o NIF de la empresa o solicitante.]
Datos de contacto del peticionario:	[Incluir datos de contacto, correo electrónico, teléfono, etc...]
Tipo de solicitud:	[Temporal / Definitiva]
Horario de acceso:	
Identificador único de Terminal Server:	
Datos de contacto técnico:	
Aprobado por:	

Estado:	[Aprobada / Denegada]
Fecha realización:	
Fecha de anulación:	
Motivo de la anulación:	

PROCEDIMIENTO DE CREACIÓN, MODIFICACIÓN Y SUPRESIÓN DE FICHEROS DE TITULARIDAD PRIVADA

ÍNDICE DEL PROCEDIMIENTO

1. Objeto ____ 2
2. Ámbito de Aplicación ____ 2
3. Desarrollo ____ 2
   3.1. Creación del Fichero. ____ 2
   3.2. Modificación del Fichero. ____ 3
   3.3. Supresión del Fichero. ____ 3
   3.4. Especial mención al Sistema de Notificaciones de la Agencia Española de Protección de Datos (Sistema NOTA). ____ 4
   3.5. Cuestiones básicas del Procedimiento de Inscripción de la Creación, Modificación o Supresión de Ficheros. ____ 4
Anexo 1. Solicitud de Creación/Modificación/Supresión de Fichero ____ 5

Revisado:	Aprobado:
Nombre y Firma:	Nombre y Firma:
Fecha:	Fecha:

1. Objeto

La Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal, en adelante LOPD, y el Real Decreto 1720/2007, de 21 de Diciembre, de desarrollo de la LOPD determinan los pasos a seguir para la Creación, Modificación y Supresión de Ficheros de Titularidad Privada.

Es necesario acotar la definición de Fichero como todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Concretamente, el Fichero de Titularidad Privada es aquél del que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.

2. Ámbito de Aplicación

El Responsable del Fichero autorizará cada una de las notificaciones de creación, modificación o supresión de un Fichero de Titularidad Privada.

El Responsable de Seguridad ha de velar por la correcta aplicación del siguiente procedimiento y llevar a cabo el seguimiento de su consecución.

3. Desarrollo

3.1. Creación del Fichero.

El artículo 25 de la LOPD establece que: “Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas”.

Por tanto, para crear un fichero es requisito que éste resulte necesario para el logro de la actividad u objeto legítimos de la entidad y que, además, se respeten las garantías establecidas por la normativa de protección de datos.

Los pasos a seguir son:

- Definir detalladamente los datos que se precisan y el uso que se le dará al fichero con objeto de identificar los datos requeridos para el tratamiento, que deberán ser, necesariamente, adecuados, pertinentes y no excesivos para cumplir así con el Principio de Calidad.
- Clasificar el Fichero, con objeto de establecer el Nivel de Seguridad requerido para su tratamiento.
- El Responsable del fichero, de manera previa, procederá a su inscripción ante la Agencia Española de Protección de Datos (el procedimiento se encuentra explicado en el último apartado del documento).

La notificación que remita la persona o entidad privada a la Agencia Española de Protección de datos, deberá contener lo siguiente:

- Identificación del Responsable del Fichero
- Identificación del Fichero
- Especificar sus finalidades y usos previstos
- Indicar que sistema de tratamiento se ha empleado en su organización
- El colectivo de personas sobre el que se obtienen los datos
- Procedimiento y procedencia de los datos
- Las categorías de datos, el servicio o unidad de acceso, la indicación del nivel de Medidas de Seguridad básico, medio o alto exigible.
- Identificación del Encargado del Tratamiento donde se encuentre ubicado el fichero
- Los destinatarios de cesiones y transferencias internacionales de datos

En este mismo Documento, el Responsable del Fichero deberá declarar un domicilio a efectos de notificaciones en el procedimiento.

Se requerirá una única notificación del Fichero aunque los datos de carácter personal, objeto de tratamiento, estén almacenados en diferentes soportes (automatizados y no automatizados) o exista una copia en soporte no automatizado de un fichero automatizado.

Deberán notificar al Registro General de Protección de Datos, cada una de las personas o entidades que simultáneamente sean Responsables del Fichero, para que se proceda a la inscripción de éste.

El Responsable del Fichero autorizará al personal, interno o externo que deba tener acceso al fichero. Además, en colaboración con el Responsable de Seguridad, establecerá las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

3.2. Modificación del Fichero.

La actualización del fichero es imprescindible. Por tanto, toda modificación que afecte al contenido, detallado en el apartado anterior, de la inscripción de un fichero, deberá ser previamente notificada a la Agencia Española de Protección de Datos, con el objeto de proceder a su inscripción en el Registro correspondiente.

Para poder efectuar la notificación de la modificación, se debe indicar en la misma, el código de inscripción del fichero en el Registro General de Protección de Datos.

3.3. Supresión del Fichero.

Cuando el Responsable del Fichero decida su supresión, deberá notificarla para proceder a la cancelación de la inscripción en el Registro correspondiente.

Para poder efectuar la notificación de la supresión, se debe indicar en la misma, el código de inscripción del fichero en el Registro General de Protección de Datos.

3.4. Especial mención al Sistema de Notificaciones de la Agencia Española de Protección de Datos (Sistema NOTA).

Esta herramienta fue aprobada mediante Resolución de la Agencia Española de Protección de Datos de 12 de julio de 2006 (BOE núm. 181 de 31 de julio de 2006), y su objetivo es permitir a los Responsables de Ficheros con datos de carácter personal de titularidad privada:

- Cumplir con la obligación que la LOPD establece de notificar sus ficheros a la Agencia Española de Protección de Datos a través de una herramienta que le informa y asesora acerca de los requerimientos de la notificación.
- Presentar sus notificaciones a través de Internet con y sin firma electrónica.
- Presentar sus notificaciones en otros soportes: soporte informático o papel.
- Realizar notificaciones precumplimentadas de forma simplificada.
- Conocer el estado de tramitación de las notificaciones remitidas a través de Internet, mediante certificado de firma electrónica o mediante el código de envío generado por el formulario electrónico.
- Consultar el contenido completo de la inscripción de sus ficheros en la web de la Agencia.

El formulario interactivo NOTA, en formato PDF permite la presentación de notificaciones a través de Internet con y sin certificado de firma electrónica. Además, para los responsables que utilicen sus propios programas informáticos o los desarrolladores de aplicativos de protección de datos, se encuentran disponibles los formatos y especificaciones que deben cumplir sus aplicaciones para enviar notificaciones a la AEPD.

Desde la página web de la Agencia Española de Protección de Datos (www.agpd.es) se proporcionan, de manera gratuita, los modelos o formularios electrónicos de notificación de creación, modificación o supresión de ficheros, que permiten su presentación a través de medios telemáticos o en soporte papel.

3.5. Cuestiones básicas del Procedimiento de Inscripción de la Creación, Modificación o Supresión de Ficheros.

El procedimiento, que lleva a cabo la Agencia Española de Protección de Datos, se iniciará como consecuencia de la notificación de la creación, modificación o supresión del fichero por el interesado.

El Director de la Agencia Española de Protección de Datos puede realizar tres tipos de actuaciones, a partir de la recepción de la notificación:

1. Acordar la inscripción del Fichero resultante de la notificación que contenga la información preceptiva y resto de exigencias legales. A esta inscripción se le asignará un código de inscripción.

   La inscripción de un fichero en el Registro General de Protección de Datos, no exime al responsable del cumplimiento del resto de las obligaciones previstas en la normativa de protección de datos.

2. Solicitar la subsanación o petición de completar los datos que falten en la notificación.

En este caso, nada más reciba, desde la Agencia Española de Protección de Datos, el aviso de requerimiento de subsanación se ha de poner en contacto con Llabrés-Viñas S.L para así guiarle en los siguientes pasos a ejecutar.

3. Denegar la inscripción del Fichero, de forma motivada, indicando expresamente las causas que impiden dicha inscripción, si de los documentos aportados se desprende que la notificación no resulta conforme a la normativa de protección de datos.

Cuando el Responsable del Tratamiento comunique la notificación de supresión del Fichero a la Agencia Española de Protección de Datos, el Director procederá a dictar resolución de supresión. También podrá darse tal cancelación de oficio, cuando concurran circunstancias que acrediten la imposibilidad de su existencia.

El plazo máximo para dictar y notificar resolución, desde la Agencia Española de Protección de Datos, acerca de la inscripción, modificación o supresión será de 1 mes. Si en dicho plazo no se hubiese dictado o notificado nada, el fichero se entenderá inscrito, modificado o cancelado a todos los efectos.

Anexo 1. Solicitud de Creación/Modificación/Supresión de Fichero

Este Anexo contiene el formulario tipo, las peticiones cumplimentadas se almacena en:

Carpeta: PR001A001- Solicitud de Crea/Modi/Supr de Fichero

Ubicación:

Anexo 1. Solicitud de Creación/Modificación/Supresión de Fichero

□ Creación □ Modificación □ Baja	
1. Solicitado por	
2. Fichero (Nombre)	
3. Responsable del Fichero:	
4. Descripción del fichero	
5. Ubicación	
6. Encargado del tratamiento	
7. Nivel de seguridad	□ Básico□ Medio □ Alto

8. Tipo de datos de carácter personal (marcar lo que proceda)

Datos especialmente protegidos
- □ Ideología
- □ Afiliación sindical
- □ Religión
- □ Creencias

Otros Datos especialmente protegidos
- □ Origen racial o étnico
- □ Salud
- □ Vida Sexual

Datos de carácter identificativo
- □ D.N.I./C.I.F.
- □ Nº S.S./Mutualidad
- □ Nombre y apellidos
- □ Dirección (postal, electrónica)
- □ Teléfono
- □ Firma/Huella digitalizada
- □ Imagen/Voz
- □ Marcas físicas
- □ Firma electrónica

Datos académicos y profesionales
- □ Formación, titulaciones
- □ Historial de estudiante
- □ Experiencia profesional
- □ Pertenencia a colegios o asociaciones profesionales
- □ Otros (indicar)

Datos de detalles de empleo
- □ Profesión
- □ Puestos de trabajo
- □ Datos no económicos de nómina
- □ Historial del trabajador
- □ Otros (indicar)

Datos de información comercial
- □ Actividades y negocio
- □ Licencias comerciales
- □ Suscripciones a publicaciones/medios de comunicación
- □ Creaciones artísticas, literarias, científicas o técnicas
- □ Otros (indicar)

Anexo 1. Solicitud de Creación/Modificación/Supresión de Fichero

Datos de características personales ▫ Datos de Estado Civil ▫ Datos de familia ▫ Fecha de nacimiento ▫ Lugar de nacimiento ▫ Edad ▫ Sexo ▫ Nacionalidad ▫ Lengua materna ▫ Características físicas o antropométricas ▫ Otros (indicar)	Datos económico-financieros y de seguros ▫ Ingresos, rentas ▫ Inversiones, bienes patrimoniales ▫ Créditos, préstamos, avales ▫ Datos bancarios ▫ Planes de pensiones, jubilación ▫ Datos económicos de nómina ▫ Datos deducciones impositivas/impuestos ▫ Seguros ▫ Hipotecas ▫ Subsidios, beneficios ▫ Historial créditos ▫ Tarjetas de crédito ▫ Otros (indicar)
Datos de circunstancias sociales ▫ Características de alojamiento, vivienda ▫ Situación militar ▫ Propiedades, posesiones ▫ Aficiones y estilos de vida ▫ Pertenencia a clubes, asociaciones ▫ Licencias, permisos, autorizaciones ▫ Otros (indicar)	Datos de transacciones ▫ Bienes y servicios suministrados por el afectado ▫ Bienes y servicios recibidos por el afectado ▫ Transacciones financieras ▫ Compensaciones / Indemnizaciones ▫ Otros (indicar)

Anexo 1. Solicitud de Creación/Modificación/Supresión de Fichero

9. Descripción detallada de la finalidad y usos previstos (marcar lo que proceda)

Gestión contable, fiscal y administrativa
- ▫ Gestión económica y contable
- ▫ Gestión fiscal
- ▫ Gestión administrativa
- ▫ Gestión de facturación
- ▫ Gestión de clientes
- ▫ Gestión de proveedores
- ▫ Gestión de cobros y pagos
- ▫ Administración de fincas
- ▫ Consultorías, auditorías, asesorías y serv. relacionados
- ▫ Históricos de relaciones comerciales

Recursos humanos
- ▫ Gestión de personal
- ▫ Gestión de Nóminas
- ▫ Formación de personal
- ▫ Prestaciones sociales
- ▫ Selección de personal
- ▫ Gestión de trabajo temporal
- ▫ Promoción y gestión de empleo
- ▫ Prevención riesgos laborales
- ▫ Control horario

Servicios económico - financieros y seguros
- ▫ Cuenta de crédito
- ▫ Cuenta de Depósito
- ▫ Gestión de patrimonios
- ▫ Gestión de fondos de pensiones y similares
- ▫ Gestión de tarjetas de crédito y similares
- ▫ Registro de acciones y obligaciones
- ▫ Otros servicios financieros
- ▫ Cumplimiento / incumplimiento obligaciones dinerarias
- ▫ Prestación de servicios de solvencia patrimonial y crédito
- ▫ Seguros de vida y salud
- ▫ Otro tipo de seguros

Publicidad y prospección comercial
- ▫ Publicidad
- ▫ Venta a distancia
- ▫ Encuestas de opinión
- ▫ Análisis de perfiles
- ▫ Prospección comercial

Servicios de telecomunicaciones
- ▫ Prestación de servicios de telecomunicaciones
- ▫ Guías, repertorios de servicios de telecomunicaciones
- ▫ Comercio electrónico
- ▫ Prestación de servicios de certificación

Actividades asociativas, culturales, recreativas, deportivas y sociales
- ▫ Gestión actividades culturales
- ▫ Gestión de clubes o asociaciones deportivas, culturales, profesionales o similares
- ▫ Gestión de asociados o miembros de partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro
- ▫ Actividades asociativas diversas
- ▫ Asistencia social
- ▫ Gestión de medios de comunicación

Educación
- ▫ Enseñanza infantil primaria
- ▫ Enseñanza secundaria
- ▫ Enseñanza universitaria
- ▫ Educación especial
- ▫ Otras enseñanzas

Sanidad
- ▫ Gestión y control sanitario
- ▫ Historial clínico
- ▫ Investigación epidemiológica y actividades análogas

Seguridad
- ▫ Investigaciones privadas a personas
- ▫ Seguridad y control acceso a edificios
- ▫ Otras actividades de seguridad

Finalidades varias
- ▫ Fidelización de clientes
- ▫ Reservas y emisión de billetes
- ▫ Fines históricos, científicos o estadísticos
- ▫ Otras finalidades

Anexo 1. Solicitud de Creación/Modificación/Supresión de Fichero

▫ Segmentación de mercados ▫ Sistemas de ayuda a la toma de decisiones ▫ Recopilación de direcciones	

10. Procedencia y procedimiento de recogida

Procedencia de datos	Procedimiento de recogida	Soporte utilizado para la obtención
▯ El interesado o su representante legal ▯ Otras personas físicas distintas afectado ▯ Entidad privada ▯ Administración pública ▯ Fuentes accesibles al público	▯ Encuestas o entrevistas ▯ Formularios o cupones ▯ Transmisión electrónica de datos/Internet ▯ Otros (Indicar)	▯ Soporte papel ▯ Soporte informático /magnético ▯ Vía telemática ▯ Otros (indicar)

11. Cesiones de datos	
12. Transferencias a terceros países	

Autorizado por:

Fecha:

PROCEDIMIENTO PARA EL EJERCICIO DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN, OPOSICIÓN Y REVOCACIÓN DEL CONSENTIMIENTO.

Revisado: Nombre y Firma:	Aprobado: Nombre y Firma:
Fecha:	Fecha:

ÍNDICE DEL PROCEDIMIENTO

1. Objeto ____ 3
2. Ámbito de Aplicación ____ 3
3. Desarrollo del Procedimiento ____ 3
3.1. Cuestiones generales. ____ 3
3.2. Trámite de una Solicitud de Derechos. ____ 4
3.2.1. Introducción. ____ *4*
3.2.2. Solicitud. ____ *4*
3.2.3. Recepción y Tramitación. ____ *4*
3.2.4. Respuesta y Cierre. ____ *5*
4. Derechos de los Afectados. ____ 6
4.1. Derecho de Acceso. ____ 6
4.1.1. Introducción. ____ *6*
4.1.2. Plazos. ____ *6*
4.1.3. Tramitación. ____ *6*
4.2. Derecho de Rectificación. ____ 7
4.2.1. Introducción. ____ *7*
4.2.2. Plazos. ____ *7*
4.2.3. Tramitación. ____ *8*
4.3. Derecho de Cancelación. ____ 8
4.3.1. Introducción. ____ *8*
4.3.2. Plazos. ____ *8*
4.3.3. Tramitación. ____ *8*
4.4. Derecho de Oposición. ____ 9
4.4.1. Introducción. ____ *9*
4.4.2. Plazos. ____ *9*
4.4.3. Tramitación. ____ *10*
4.5. Revocación del Consentimiento. ____ 10
4.5.1. Introducción. ____ *10*
4.5.2. Plazos. ____ *10*
4.5.3. Tramitación. ____ *10*
Anexo 1.- Formulario para el Ejercicio del Derecho de Acceso ____ 13
Anexo 2.- Formulario para el Ejercicio del Derecho de Rectificación ____ 15
Anexo 3.- Formulario para el Ejercicio del Derecho de Cancelación ____ 17
Anexo 4.- Formulario para el Ejercicio del Derecho de Oposición ____ 19
Anexo 5.- Formulario para la Revocación del Consentimiento prestado para el Tratamiento de Datos Personales ____ 22

Objeto

De acuerdo a la normativa vigente, la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007, de 21 de Diciembre, que aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal, los derechos que puede ejercer la persona física son:

- Derecho de Acceso
- Derecho de Rectificación
- Derecho de Cancelación
- Derecho de Oposición
- Revocación del Consentimiento

Este procedimiento hace referencia al ejercicio de estos derechos para los ficheros inscritos ante la Agencia General de Protección de Datos por parte de la empresa. Los ficheros se encuentran detallados en el *Anexo 2* del Documento de Seguridad, *DS001*, de la empresa

1. Ámbito de Aplicación

Este procedimiento y las normas dispuestas en él, serán de obligado cumplimiento para todo el personal de la empresa que esté autorizado al acceso a datos de carácter personal que deba informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

El Responsable del Tratamiento deberá velar por el cumplimiento de las normas detalladas en este procedimiento. Le corresponderá, en todo caso, contestar la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado en sus ficheros; la prueba del cumplimiento del deber de respuesta, debiendo conservar la acreditación del cumplimiento del mencionado deber; y adoptar las medidas oportunas para garantizar que las personas autorizadas al acceso a datos de carácter personal, mencionadas en el anterior párrafo, puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

2. Desarrollo del Procedimiento

2.1. Cuestiones generales.

Se deben cumplir los siguientes requisitos:

- Designar dentro de la empresa la persona o departamento responsable de atender el ejercicio de los derechos de los afectados y dotarlo con los medios necesarios. En este sentido, señalar que la empresa deberá establecer un Departamento o responsable encargado de la atención al ejercicio de los derechos, cuya responsabilidad será recibir, coordinar y solventar cualquier solicitud al respecto.
- Proporcionar la formación necesaria en Protección de Datos a las personas involucradas en puestos de atención al público para informar y dirigir a los afectados hacia el responsable asignado de atender sus derechos.
- Establecer los modelos necesarios para atender la tipología de peticiones que se reciban. En este documento se adjuntan los modelos.

- Implantar un procedimiento para la acreditación de la personalidad del afectado, así como del resto de requisitos establecidos para la solicitud expuestos en la normativa vigente de protección de datos.

2.2. Trámite de una Solicitud de Derechos.

2.2.1. Introducción.

La atención a estos derechos debe limitarse a los datos recogidos en los ficheros de la empresa (*Anexo 2* del Documento de Seguridad, *DS001*,, donde se detallan los ficheros que pertenecen a la empresa y, por tanto, que están sujetos al presente procedimiento de atención de derechos en su totalidad).

Por último, el ejercicio de derechos es independiente y no se debe entender que ejercitar ninguno de ellos sea requisito previo para el ejercicio de otro. Por ejemplo, no es necesario ejercitar el derecho de acceso con anterioridad a solicitar la rectificación/cancelación de los datos.

2.2.2. Solicitud.

- De acuerdo al tipo de solicitud que realiza el interesado se ha de identificar cuál de sus derechos quiere ejercer, y por ello la recepción la realizará el Encargado de la Tutela y Ejercicio de Derechos.
- Se le entregará una impresión del formulario de solicitud correspondiente en papel de la empresa y se le explicará cómo cumplimentar el formulario.
- La solicitud contendrá el método de entrega de la documentación al solicitante, bien sea remitida por correo certificado, o bien recogiéndola en las propias oficinas de la empresa.

2.2.3. Recepción y Tramitación.

Se le da entrada la solicitud en el Registro, indicando la fecha de recepción y se procede a entregarlo de inmediato al Responsable del Tratamiento.

El Responsable procederá a resolver los siguientes pasos:

1. Comprobación de la documentación recibida

La solicitud debe ir dirigida a la empresa (dónde se pretende ejercitar el derecho) y deberá contener:

- ✓ Nombre y apellidos del interesado.
- ✓ Petición en que se concreta la solicitud.
- ✓ Domicilio a efectos de notificaciones, fecha y firma del solicitante.
- ✓ Fotocopia del documento que acredite la identidad del interesado (Documento Nacional de Identidad o pasaporte)

2. Comprobación de la identidad del interesado:

La persona interesada en ejercitar cualquiera de los derechos de los afectados aportará la documentación que permita comprobar su identidad (DNI, Pasaporte, etc.).

El representante legal del interesado podrá actuar en nombre de éste (p.e. abogado). Designado por el propio titular, y deberá cumplir con los siguientes requisitos:

- ✓ Se ejercitará el derecho a través del representante pero en nombre y por cuenta del

afectado.

- ✓ El apoderamiento debe ser expreso y suficiente para el ejercicio del derecho que se pretende ejercitar.

Casos específicos:

- ✓ Menores de edad:

Salvo en casos de incapacidad, los mayores de *catorce años* se encuentran habilitados para ejercitar cualquiera de los derechos LOPD.

Para los menores de catorce años, el solicitante ha de acreditar que ejerce la patria potestad o que es tutor, mediante copia del DNI y del libro de familia o, mediante una resolución judicial.

- ✓ Incapacitados:

Se aplicarán las mismas normas que para la representación legal.

- ✓ Fallecidos!

El Nuevo Reglamento no será de aplicación a los datos referidos a las personas fallecidas. No obstante, las personas vinculadas al fallecido por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos.

3. Comprobación del objeto de la solicitud:

Una tarea necesaria ante la recepción de una solicitud es la interpretación de la voluntad del afectado. Por ello, resulta importante que se identifique exactamente qué tipo de información necesita el solicitante, ya que puede solventarse mediante la entrega de un solo documento.

Se comprobará la existencia de solicitudes anteriores, en las que, por ejemplo, se solicitara la subsanación de algún requisito o el interesado realizara diferente o idéntica petición.

Con independencia del derecho ejercitado, o de la denegación del mismo por motivos formales, si de la gestión de una solicitud recibida se pone de manifiesto una posible inexactitud o incorrección en los datos recogidos, ésta será subsanada, puesto que el mantenimiento de la exactitud o actualización de los datos es una obligación que pesa sobre la empresa, como Responsable del Tratamiento, debiendo realizar de oficio las gestiones pertinentes para su efectividad, con independencia del ejercicio de los derechos de rectificación, cancelación u oposición.

2.2.4. Respuesta y Cierre.

Una vez comprobada y registrada la solicitud, se deberá extraer la información existente relativa al interesado en los distintos ficheros sobre los que ejercita su derecho.

La documentación se entregará al solicitante por el medio apuntado en la solicitud. Si se ha optado por la recogida en las oficinas de la empresa, se le facilitará la documentación al propio interesado o a su representante, en sobre cerrado para conservar su confidencialidad. En caso de haber seleccionado su envío por correo certificado, se procederá a su tramitación antes de finalizar los plazos de comunicación explicados posteriormente según el derecho ejercido.

Una vez la solicitud ha sido contestada, deberán proceder al archivo de la misma y de los acuses de recibo, en su caso, de manera que se pueda ejercer un control sobre el solicitante y sobre la fecha que ha ejercido alguno de sus derechos.

3. Derechos de los Afectados.

3.1. Derecho de Acceso.

3.1.1. Introducción.

Este derecho faculta al interesado a conocer si sus datos personales están siendo objeto de tratamiento, qué la finalidad de dicho tratamiento, la información que esté disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.

El afectado puede ejercitar el derecho de acceso siempre y cuando la configuración o implantación material del fichero lo permita, por los siguientes medios:

- ✔ Visualización en pantalla.
- ✔ Escrito, copia o fotocopia remitida por correo.
- ✔ Telecopia.
- ✔ Correo electrónico u otros sistemas de comunicaciones electrónicas.
- ✔ Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el Responsable.

3.1.2. Plazos.

La ley señala dos plazos diferenciados en el transcurso de la tramitación de una solicitud de acceso:

- ✔ *Plazo de un mes a* contar desde la recepción de la solicitud, en el que el Responsable del Fichero resolverá sobre la solicitud de acceso. Si transcurrido dicho plazo no se responde a la petición de acceso de forma expresa, el interesado podrá interponer reclamación ante la Agencia Española de Protección de Datos para la consecuente apertura de Procedimiento de Tutela de Derechos.
- ✔ Cuando la solicitud de acceso fuese estimada y el Responsable no acompañase a su comunicación la información, el acceso se hará efectivo en el *PLAZO DE LOS 10 DÍAS* siguientes a dicha comunicación.

3.1.3. Tramitación.

Se le facilitará el formulario incluido al final de este procedimiento.

Existen dos tipos de contestación posibles:

- ❑ Aceptación del derecho de acceso: los datos existentes que se comuniquen, con independencia del soporte utilizado, se deberán trasladar de forma inteligible para que el afectado pueda reconocer todos los datos incluidos en el fichero.
- ❑ Denegación de acceso: El Responsable del Fichero podrá denegar el acceso a los datos de carácter personal cuando ya se haya ejercitado ese derecho en los 12 meses anteriores a la solicitud, a no ser que pudiera acreditarse un interés legítimo. También podrá denegarse el acceso en aquellos supuestos en los que así lo prevea una Ley, o bien cuando ésta impida al responsable revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.

Detectada la información relativa al titular en el fichero al cual se solicita acceso, se deberá elaborar la contestación a remitir al solicitante, con el siguiente contenido mínimo:

- La inexistencia de datos, en su caso, mediante el modelo de contestación,

  o bien,

- Los datos existentes, en concreto:
  - Los datos de base del afectado.
  - Los datos resultantes de cualquier elaboración o proceso informático.
  - El origen de los datos.
  - Los cesionarios de los datos.
  - Los usos y finalidades para los que se almacenan los datos.
  - La fuente de la que proviene cada dato.
  - Una mención a la posibilidad de ejercitar los derechos de rectificación, cancelación y, en su caso, oposición.

En cualquier caso, la solicitud de acceso deberá ser contestada, figuren o no datos del titular en los ficheros de la empresa.

Hay que tener en cuenta que si transcurrido el plazo de un mes no se contesta expresamente la solicitud, ésta se entenderá desestimada, y por tanto el titular podrá interponer la correspondiente reclamación ante la Agencia de Protección de Datos para la consecuente apertura de Procedimiento de Tutela de Derechos.

3.2. Derecho de Rectificación.

3.2.1. Introducción.

El derecho de rectificación faculta al interesado a rectificar sus datos cuando éstos resulten inexactos o incompletos.

En este caso, la solicitud además deberá indicar el dato que es erróneo y la corrección que debe realizarse y deberá ir acompañada de la documentación justificativa de la rectificación solicitada,

3.2.2. Plazos.

En el plazo máximo de diez días hábiles a contar desde la fecha de recepción de la solicitud, se comunicará al afectado, tanto la desestimación de la solicitud en su caso (tal hecho ocurrirá en el caso que se deniegue por una Ley o norma de aplicación directa, o cuando éstas impidan al Responsable del Tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso), como la ejecución de la rectificación solicitada.

Si los datos rectificados hubieran sido cedidos por la empresa a un tercero, se notificará la rectificación efectuada al cesionario en idéntico plazo -diez días- para que éste a su vez proceda a rectificarlo en sus ficheros.

3.2.3. Tramitación.

Como regla general la admisión o denegación del derecho de rectificación deberá tener como base la prueba documental presentada por el afectado que justifique la modificación de los datos.

El ejercicio de este derecho requiere la comprobación de la adecuación de los datos existentes y, por tanto, de la pertinencia o no de la rectificación que se solicita, salvo que ésta dependa exclusivamente del consentimiento del afectado.

En el caso de no ser pertinente la rectificación, deberán comunicar al afectado la denegación del derecho de rectificación, debidamente justificada (no se aporta prueba de su pertinencia, ya figuran rectificados los datos, etc.). En los casos en los que la rectificación no dependa del consentimiento del interesado, y éste no haya aportado documentación que justifique la procedencia de la misma, deberá solicitarse su envío, o bien, en caso de resultar pertinente, se comunicará la rectificación realizada directamente sobre las bases de datos correspondientes.

Hay que tener en cuenta que si transcurrido el plazo de diez días hábiles no se contesta expresamente la solicitud, ésta se entenderá desestimada, y por tanto el titular podrá interponer una reclamación ante la Agencia de Protección de Datos para la consecuente apertura de Procedimiento de Tutela de Derechos.

3.3. Derecho de Cancelación.

3.3.1. Introducción.

El derecho de cancelación faculta al interesado para solicitar la cancelación de sus datos existentes en los ficheros de la empresa. En este supuesto, la solicitud deberá indicar si se trata de la supresión de un dato inadecuado o excesivo, en cuyo caso deberá acompañar la documentación justificativa.

3.3.2. Plazos.

La comunicación (denegación y mantenimiento o aceptación y cancelación de datos) al solicitante deberá hacerse efectiva como máximo dentro de los diez días hábiles siguientes a la recepción de su solicitud.

Si los datos cancelados hubieran sido cedidos previamente se deberá notificar la rectificación efectuada al cesionario en idéntico plazo -diez días- para que éste a su vez lo realice en sus ficheros.

3.3.3. Tramitación.

El ejercicio de este derecho requiere la comprobación de la adecuación de los tratamientos actualmente efectuados sobre los datos del solicitante y, por tanto, de la pertinencia o no de la cancelación (por ejemplo, un trabajador no podrá solicitar la cancelación de sus datos mientras continúe trabajando en la empresa) que se solicita, salvo que ésta dependa exclusivamente del consentimiento del afectado.

La cancelación automática de los datos una vez cumplida la finalidad para la que fueron recabados, dará lugar al bloqueo automático de los mismos, conservándose, únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas.

En caso de que se constatara que los datos se hubieran recogido o registrado por medios fraudulentos, desleales o ilícitos, deberán ser suprimidos y, deberán realizarse las acciones necesarias, para destruir el soporte (papel, cd-rom, etc.) en el que aquellos figuren (ejemplo del jubilado que no se hubiera requerido su autorización para convocarle a los actos sociales y hubiera ejercitado su derecho de cancelación).

Como regla general, al igual que en el caso de la rectificación, la admisión o denegación de derecho de cancelación deberá tener como base soporte documental respecto de la procedencia de la misma y que haga prueba de ésta. En ocasiones, este soporte estará a disposición de la propia empresa, (por ejemplo, cuando el titular solicite el borrado de datos por extinción de la relación laboral que mantenía con lal empresa), en otras, será necesario que aporte el documento.

Igual que ocurría en el derecho de acceso y rectificación, si transcurrido el plazo de diez días hábiles no se contesta expresamente la solicitud, ésta se entenderá desestimada, y por tanto el titular podrá interponer una reclamación ante la Agencia de Protección de Datos para la consecuente apertura de Procedimiento de Tutela de Derechos.

Como en el supuesto de rectificación de datos, el envío de la comunicación al afectado informando de la cancelación efectuada o de la desestimación de la solicitud, debe ir precedida, en cualquier caso, de la realización efectiva de la misma en todas las bases de datos en las que existan los datos objeto de cancelación.

3.4. Derecho de Oposición.

3.4.1. Introducción.

Este derecho es el relativo a la voluntad del interesado a oponerse a un tratamiento de datos o a su cese en el mismo cuando:

- ✔ No sea necesario su consentimiento para el tratamiento: el interesado podrá oponerse a un tratamiento de datos cuando, sin ser preceptivo el consentimiento previo, existan motivos fundados y legítimos relativos a su concreta situación personal que lo justifique.
- ✔ Se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial: se podrá llevar a cabo a través de la llamada a un número telefónico gratuito o mediante la remisión de un correo electrónico; y en el caso de que el Responsable del Fichero o Tratamiento disponga de servicios de cualquier índole para la atención a sus clientes o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, deberá concederse la posibilidad al afectado de ejercer su oposición a través de dichos servicios.

- ✔ El tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos, es decir, los interesados tienen derecho a no verse sometidos a una decisión jurídica sobre ellos o a una decisión que les afecte significativamente y que se base exclusivamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad (rendimiento laboral, crédito, fiabilidad o conducta).

3.4.2. Plazos.

El Responsable del Fichero deberá resolver sobre la solicitud del ejercicio de este derecho, en el plazo máximo de 10 días a contar desde la recepción de la solicitud.

Si la oposición se ejercitara sobre datos que hubieran sido cedidos previamente, se deberá notificar la oposición efectuada al cesionario en idéntico plazo -diez días- para que éste a su vez lo realice en sus ficheros.

3.4.3. Tramitación.

El derecho de oposición se ejercitará mediante solicitud dirigida al Responsable del Tratamiento. El modelo de la misma se encuentra al final del Documento.

Cuando la oposición se realice respecto a un supuesto en que no ha sido necesario su consentimiento, deberán hacerse constar los motivos fundados y legítimos, relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho.

Se denegará la solicitud del derecho de oposición cuando se refiera al supuesto en que el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos si la decisión que le afecta:

- Se hubiese adoptado en el marco de la celebración o ejecución de un contrato a petición del interesado, siempre que se le dé la posibilidad de alegar lo que encuentre oportuno, para defender su derecho o interés. Aunque el Responsable del Tratamiento deberá informar previamente al afectado, de forma clara y precisa, que se adoptará esta medida y que cancelará los datos en caso de que no llegue a celebrarse, finalmente, el contrato.
- Esté autorizada por una norma con rango de Ley que establezca medidas que garanticen el interés legítimo del interesado.

El Responsable del Fichero o Tratamiento deberá excluir del tratamiento los datos relativos al afectado que ejercite su derecho de oposición o a denegar motivadamente la solicitud del interesado en el plazo de 10 días.

Hay que tener en cuenta que igual que en el resto de derechos, si transcurrido el plazo de diez días hábiles no se contesta expresamente la solicitud, ésta se entenderá desestimada, y por tanto el titular podrá interponer una reclamación ante la Agencia de Protección de Datos para la consecuente apertura de Procedimiento de Tutela de Derechos.

3.5. Revocación del Consentimiento.

3.5.1. Introducción.

El consentimiento que presta el interesado o afectado para autorizar el tratamiento de sus datos de carácter personal, puede ser revocado por el mismo cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

3.5.2. Plazos.

El Responsable cesará en el tratamiento de los datos en el plazo máximo de 10 días a contar desde el de la recepción de la revocación del consentimiento, sin perjuicio de su obligación de bloquear los datos.

Si la revocación se ejercitara sobre datos que hubieran sido cedidos previamente, se deberá notificar la revocación efectuada al cesionario en idéntico plazo -diez días- para que éste a su vez lo realice en sus ficheros.

3.5.3. Tramitación.

El afectado podrá revocar su consentimiento a través de un medio sencillo, gratuito y que no implique ingreso alguno para el Responsable del Fichero o Tratamiento.

Como medios válidos se consideran: el envío prefranqueado al Responsable del Tratamiento, el correo ordinario, la llamada a un número de teléfono preferentemente gratuito o a los servicios de atención al

público que hubiera establecido el Responsable, y la utilización de servicios de telecomunicaciones, siempre que no implique una tarificación adicional al afectado (es decir que el ejercicio de estos derechos no suponga un enriquecimiento de cualquier tipo para el responsable del tratamiento)

No se consideran medios válidos:

- El envío de cartas certificadas o envíos semejantes; o cualesquiera otros medios que impliquen un coste adicional al interesado, entendiendo por adicional un coste añadido al estrictamente mínimo y necesario.
- Cuando el interesado exija la confirmación del cese en el tratamiento de sus datos por parte del Responsable del Tratamiento, éste deberá responder expresamente a la solicitud.
- Cuando el interesado exija la confirmación del cese en el tratamiento de sus datos por parte del Responsable del Tratamiento, éste deberá responder expresamente a la solicitud.

Anexos - Formularios para el Ejercicio de los Derechos

Este Anexo contiene los formularios tipo, los formularios cumplimentados se almacena en:

Carpeta: PR002A001- Formularios para el Ejercicio de los Derechos

Ubicación:

Anexo 1.- Formulario para el Ejercicio del Derecho de Acceso

DATOS DEL RESPONSABLE DEL FICHERO:

Nombre/razón social: CES Alberta Giménez

CIF: R0700117E

Dirección Costa de Saragossa, 16

Localidad Palma de Mallorca C.P. 07013

Provincia Illes Balears

DATOS DEL AFECTADO:

Adjuntar copia del documento nacional de identidad o documento equivalente, a la presente solicitud

Nombre _____ DNI _____

Apellidos _____

C/Plaza _____ Nº _____ Piso _____

Localidad _____ C.P. _____

Provincia

DATOS DEL REPRESENTANTE DEL AFECTADO:

Adjuntar copia del documento nacional de identidad o documento equivalente, además de la representación otorgada por el afectado, a la presente solicitud.

Nombre _____ DNI _____

Apellidos _____

C/Plaza _____ Nº _____ Piso _____

Localidad _____ C.P. _____

Provincia _____

Anexo 1.- Formulario para el Ejercicio del Derecho de Acceso

PETICIÓN DEL DERECHO DE ACCESO A LOS DATOS DE CARÁCTER PERSONAL:

Por medio del presente escrito, D. /Dª _____, en calidad de afectado; o D./Dª _____, actuando en representación de D./Dª _____, afectado del tratamiento de los datos personales llevado a cabo por la entidad Responsable que figura indicada más arriba, efectúa el ejercicio del derecho de acceso, de conformidad con lo previsto en el artículo 15 de la Ley Orgánica de Protección de datos personales 15/1999 (LOPD), de 13 de diciembre, y en los artículos 23 a 30 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y en consecuencia,

SOLICITA,:

Que se le facilite el derecho de acceso a los ficheros de _____ _____ (Nombre o razón social) en el plazo máximo de 1 mes a contar desde la recepción de esta solicitud, entendiendo que si transcurre este plazo sin que de forma expresa se conteste a la mencionada petición de acceso se considerará denegada, y a consecuencia de ello, informo que se justificaría la interposición de reclamación ante la Agencia Española de Protección de Datos con amparo del artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos.

.Que si la solicitud del derecho de acceso fuese estimada, se remita por correo la información a la dirección arriba indicada, o bien se acuerde cita para la visualización de los datos.

En _____, a _____ de _____ de 20__.

Firmado.

Anexo 2.- Formulario para el Ejercicio del Derecho de Rectificación

DATOS DEL RESPONSABLE DEL FICHERO:

Nombre/razón social: CES Alberta Giménez

CIF: R0700117E

Dirección Costa de Saragossa, 16

Localidad Palma de Mallorca C.P. 07013

Provincia Illes Balears

DATOS DEL AFECTADO:

Adjuntar copia del documento nacional de identidad o documento equivalente, a la presente solicitud

Nombre _____ DNI _____

Apellidos _____

C/Plaza _____ Nº _____ Piso _____

Localidad _____ C.P. _____

Provincia

DATOS DEL REPRESENTANTE DEL AFECTADO:

Adjuntar copia del documento nacional de identidad o documento equivalente, además de la representación otorgada por el afectado, a la presente solicitud.

Nombre _____ DNI _____

Apellidos _____

C/Plaza _____ Nº _____ Piso _____

Localidad _____ C.P. _____

Provincia _____

Anexo 2.- Formulario para el Ejercicio del Derecho de Rectificación

DATOS OBJETO DE SOLICITUD DE RECTIFICACIÓN:

Escriba brevemente los datos concretos que desea rectificar indicando la correspondiente modificación

PETICIÓN DEL DERECHO DE RECTIFICACIÓN DE DATOS DE CARÁCTER PERSONAL

Por medio del presente escrito, D. /Dª _____, en calidad de afectado; o D./Dª _____, actuando en representación de D./Dª _____, afectado del tratamiento de los datos personales llevado a cabo por la entidad Responsable que figura indicada más arriba, efectúa el ejercicio del derecho de rectificación, de conformidad con lo previsto en el artículo 16 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y en los artículos 23 a 26 y 31 a 33 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y en consecuencia,

EXPONE, *(Marque con una X los motivos que procedan. No olvide adjuntar la documentación justificativa que acredite la rectificación.)*

☐ Que los datos objeto de rectificación resultan ser inexactos, en parte o en todo.

☐ Que los datos objeto de rectificación resultan ser incompletos.

SOLICITA,:

Que se proceda a acordar la rectificación de los datos personales indicados, que se realice en el plazo de diez días hábiles a contar desde la recepción de esta solicitud, y que se me notifique de forma escrita el resultado de la rectificación practicada.

Que en caso de que se acuerde que no procede acceder a practicar total o parcialmente las rectificaciones requeridas, se me comunique motivadamente a fin de, en su caso, solicitar la tutela de la Agencia Española de Protección de Datos, al amparo del artículo 18 de la mencionada ley Orgánica 15/1999, opción que también cabrá si no obtuviese respuesta expresa, a la presente solicitud, en el plazo mencionado en el párrafo anterior.

En _____, a _____ de _____ de 20__.

Firmado.

Anexo 3.- Formulario para el Ejercicio del Derecho de Cancelación

DATOS DEL RESPONSABLE DEL FICHERO:

Nombre/razón social: CES Alberta Giménez

CIF: R0700117E

Dirección Costa de Saragossa, 16

Localidad Palma de Mallorca C.P. 07013

Provincia Illes Balears

DATOS DEL AFECTADO:

Adjuntar copia del documento nacional de identidad o documento equivalente, a la presente solicitud

Nombre _____ DNI _____

Apellidos _____

C/Plaza _____ Nº _____ Piso _____

Localidad _____ C.P. _____

Provincia

DATOS DEL REPRESENTANTE DEL AFECTADO:

Adjuntar copia del documento nacional de identidad o documento equivalente, además de la representación otorgada por el afectado, a la presente solicitud.

Nombre _____ DNI _____

Apellidos _____

C/Plaza _____ Nº _____ Piso _____

Localidad _____ C.P. _____

Provincia _____

Anexo 3.- Formulario para el Ejercicio del Derecho de Cancelación

DATOS OBJETO DE SOLICITUD DE CANCELACIÓN:

Escriba brevemente los datos concretos que desea cancelar del tratamiento efectuado por el Responsable del Fichero

PETICIÓN DEL DERECHO DE CANCELACIÓN DE DATOS DE CARÁCTER PERSONAL

Por medio del presente escrito, D. /Dª _____, en calidad de afectado; o D./Dª _____, actuando en representación de D./Dª _____, afectado del tratamiento de los datos personales llevado a cabo por la entidad Responsable que figura indicada más arriba, efectúa el ejercicio del derecho de cancelación, de conformidad con lo previsto en el artículo 16 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y en los artículos 23 a 26 y 31 a 33 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y en consecuencia,

EXPONE, *(Marque con una X los motivos que procedan. No olvide adjuntar la documentación justificativa que acredite la cancelación.)*

☐ Que los datos objeto de cancelación son innecesarios o impertinentes para la finalidad para la cual se recabaron.

☐ Que el tratamiento efectuado por el Responsable de los datos no se ajusta a lo dispuesto en la LOPD 15/1999.

SOLICITA,:

Que se proceda a acordar la cancelación de los datos personales indicados, que se realice en el plazo de diez días hábiles a contar desde la recepción de esta solicitud, y que se me notifique de forma escrita el resultado de la cancelación practicada.

Que en caso de que se acuerde que no procede acceder a practicar total o parcialmente las cancelaciones requeridas, se me comunique motivadamente a fin de, en su caso, solicitar la tutela de la Agencia Española de Protección de Datos, al amparo del artículo 18 de la mencionada ley Orgánica 15/1999, opción que también cabrá si no obtuviese respuesta expresa, a la presente solicitud, en el plazo mencionado en el párrafo anterior.

En _____, a _____ de _____ de 20__.

Firmado.

Anexo 4.- Formulario para el Ejercicio del Derecho de Oposición

DATOS DEL RESPONSABLE DEL FICHERO:

Nombre/razón social: CES Alberta Giménez

CIF: R0700117E

Dirección Costa de Saragossa, 16

Localidad Palma de Mallorca C.P. 07013

Provincia Illes Balears

DATOS DEL AFECTADO:

Adjuntar copia del documento nacional de identidad o documento equivalente, a la presente solicitud

Nombre DNI

Apellidos

C/Plaza Nº Piso

Localidad C.P.

Provincia

DATOS DEL DEL REPRESENTANTE DEL AFECTADO:

Adjuntar copia del documento nacional de identidad o documento equivalente, además de la representación otorgada por el afectado, a la presente solicitud.

Nombre DNI

Apellidos

C/Plaza Nº Piso

Localidad C.P.

Provincia

DATOS OBJETO DE SOLICITUD DE OPOSICIÓN:

Escriba brevemente los datos concretos a los que desea oponer del tratamiento efectuado por el responsable del fichero

Anexo 4.- Formulario para el Ejercicio del Derecho de Oposición

PETICIÓN DEL DERECHO DE OPOSICIÓN DE DATOS DE CARÁCTER PERSONAL

Por medio del presente escrito, D. /Dª _____, en calidad de afectado; o D./Dª _____, actuando en representación de D./Dª _____, afectado del tratamiento de los datos personales llevado a cabo por la entidad Responsable que figura indicada más arriba, efectúa el ejercicio del derecho de oposición, de conformidad con lo previsto en los artículos [6.4 y 17] de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y en los artículos 23 a 26 y 34 a 36 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y en consecuencia,

EXPONE, *(Marque con una X los motivos que procedan. No olvide adjuntar la documentación justificativa que acredite la cancelación.)*

☐ Que se trata de un supuesto en el que no se precisa mi consentimiento y no existe Ley que disponga lo contrario, teniendo, por ello, un motivo legítimo y fundado, referido a mi concreta situación personal que lo justifique. A continuación detallo el motivo legítimo y fundado:

☐ Que se trata de ficheros que tienen por finalidad la realización de actividades de publicidad y prospección comercial.

Tiene opción de remitir la presente solicitud al correo electrónico siguiente _____ _____.

☐ Que el tratamiento tiene por finalidad la adopción de una decisión que me afecta, basada, únicamente, en un tratamiento automatizado de mis datos de carácter personal, dándose la evaluación de determinados aspectos de mi personalidad (rendimiento laboral, crédito, fiabilidad o conducta).

En su virtud, SOLICITA

Que se proceda a ejecutar la oposición de los datos personales indicados, que se realice en el plazo de diez días hábiles a contar desde la recepción de esta solicitud, y que se me notifique de forma escrita el resultado de la cancelación practicada.

Que en caso de que se acuerde que no procede acceder a practicar total o parcialmente las oposiciones requeridas, se me comunique motivadamente a fin de, en su caso, solicitar la tutela de la Agencia Española de Protección de Datos, al amparo del artículo 18 de la mencionada ley Orgánica 15/1999, opción que también cabrá si no obtuviese respuesta expresa, a la presente solicitud, en el plazo mencionado en el párrafo anterior.

En _____, a _____ de _____ de 20__.

Firmado.

Anexo 5.- Formulario para la Revocación del Consentimiento prestado para el Tratamiento de Datos Personales

DATOS DEL RESPONSABLE DEL FICHERO:

Nombre/razón social: CES Alberta Giménez

CIF: R0700117E

Dirección Costa de Saragossa, 16

Localidad Palma de Mallorca C.P. 07013

Provincia Illes Balears

DATOS DEL AFECTADO:

Adjuntar copia del documento nacional de identidad o documento equivalente, a la presente solicitud

Nombre _____ DNI _____

Apellidos _____

C/Plaza _____ Nº _____ Piso _____

Localidad _____ C.P. _____

Provincia

DATOS DEL DEL REPRESENTANTE DEL AFECTADO:

Adjuntar copia del documento nacional de identidad o documento equivalente, además de la representación otorgada por el afectado, a la presente solicitud.

Nombre _____ DNI _____

Apellidos _____

C/Plaza _____ Nº _____ Piso _____

Localidad _____ C.P. _____

Provincia _____

Anexo 5.- Formulario para la Revocación del Consentimiento prestado para el Tratamiento de Datos Personales

DATOS y TRATAMIENTOS OBJETO DE REVOCACIÓN DE CONSENTIMIENTO:

Escriba brevemente los datos concretos para los que desea revocar el consentimiento prestado al Responsable del Fichero

Por medio del presente escrito, D. /Dª _____, en calidad de afectado; o D./Dª _____, actuando en representación de D./Dª _____, titular de los datos objeto de tratamiento, de conformidad con lo previsto en el artículo 6.3 de la Ley Orgánica 15/1999, de Protección de Datos Personales, de 13 de diciembre, solicita la revocación del consentimiento para el tratamiento de los datos indicados más arriba, aceptando la no atribución de efectos retroactivos a este acto, y en consecuencia,

EXPONE, *(Indicar las causas de la revocación. No olvide adjuntar la documentación que la acredite.)*

En su virtud, SOLICITA

Que se proceda a la revocación del consentimiento prestado en su momento para el tratamiento de los datos indicados en este documento, habiéndose expuesto los motivos que justifican este acto, y reconociendo la no atribución de efectos retroactivos.

En _____, a _____ de _____ de 20__.

Firmado.

PROCEDIMIENTO PARA FICHEROS NO AUTOMATIZADOS

Revisado: Nombre y Firma:	Aprobado: Nombre y Firma:
Fecha:	Fecha:

ÍNDICE DEL PROCEDIMIENTO

1. Objeto ____ 3
2. Ámbito ____ 3
2.1. Todo el personal de la empresa ____ 3
2.2. Responsable de Seguridad de ficheros no automatizados . ____ 3
3. Desarrollo ____ 4
3.1. Cuestiones generales ( ) ____ 4
3.2. Medidas de Seguridad de nivel básico ____ 4
3.2.1. Criterios de archivo ( ) *4*
3.2.2. Dispositivos de almacenamiento ( ) *4*
3.2.3. Custodia de soportes ( ) *5*
3.2.4. Destrucción de documentación ( ) *5*
3.3. Medidas de Seguridad de nivel medio ____ 5
3.3.1. Responsable de seguridad ( ) *5*
3.3.2. Auditoría ( ) *5*
3.3.3. Registro de entrada y salida de documentos ( ) *5*
3.4. Medidas de Seguridad de nivel alto ____ 5
3.4.1. Almacenamiento de la información ( ) *5*
3.4.2. Copia o reproducción ( ) *6*
3.4.3. Acceso a la documentación ( ) *7*
3.4.4. Traslado de documentación ( ) *7*
Anexo 1 - Formulario de creación de Archivos No Automatizados ____ 8
Anexo 2 - Registro de accesos autorizados a Ficheros No Automatizados de Nivel Alto __ 10
Anexo 3 - Formulario para la ENTRADA de Ficheros No Automatizados ____ 12
Anexo 4 - Formulario para la SALIDA de Ficheros No Automatizados ____ 14

1. Objeto

Los ficheros no automatizados hacen referencia al tipo de soporte que permita la consulta directa de la información contenida en él sin que medie ningún proceso automatizado. Debido a que en soporte papel se registran datos de carácter personal, se aplicarán las Medidas de Seguridad establecidas en el Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de protección de datos de carácter personal.

Por otro lado, en este documento se describen las medidas y controles antes mencionados, así como las responsabilidades sobre su tratamiento. Al final del documento se adjuntan los anexos necesarios para el cumplimiento de los controles.

Los documentos en formato papel se pueden dividir, en función de la temporalidad de su uso, en los siguientes tipos:

(🔓) Activos: Esta etapa es en la que los documentos se encuentran en periodo de uso frecuente, están en trámite y tienen que mantenerse disponibles en los puestos de trabajo.

(🔒) Permanentes: Estos documentos no se utilizan diariamente y su tramitación ha finalizado, no obstante, se tienen que mantener disponibles en un almacenamiento permanente o archivo para consultas o por requerimientos legales.

(⃠) Bloqueados: Consisten en la documentación cuya vida activa ha finalizado y se archiva para un posible uso posterior, ya sea por motivos judiciales o por el cumplimiento de normas obligatorias (legislación fiscal, laboral, sanitaria, etc.).

Por último, existen los documentos Obsoletos, que son aquellos que no tienen ya uso, han cubierto los periodos de retención previstos por la ley y pueden ser destruidos. Para ello se llevará a cabo el procedimiento de destrucción de documentación, en el punto 3.2.4 de Medidas de Seguridad de nivel básico.

El ámbito de aplicación comprenderá las acciones, controles y normas que afectan a todos los tipos de documentos. Por ello se indicará a qué tipo de documentos aplica cada punto en concreto, adjuntando el símbolo junto al título.

2. Ámbito

2.1. Todo el personal de la empresa

Este procedimiento y las normas dispuestas en él, serán de obligado cumplimiento para todo el personal de la organización al que se haya autorizado al acceso, manejo y custodia de los ficheros no automatizados. En el *Anexo 5 del documento DS001* se detalla la relación de personal autorizado al acceso a los archivos de documentación.

2.2. Responsable de Seguridad de ficheros no automatizados .

El Responsable de Seguridad será el encargado de velar por el cumplimiento de las normas detalladas en este procedimiento. Asimismo, también queda determinada la misma responsabilidad para la persona delegada por el propio Responsable de Seguridad, en las funciones de control y supervisión de este procedimiento.

3. Desarrollo

3.1. Cuestiones generales (🔓🔒⃠)

En términos generales se deben observar como mínimo las siguientes medidas:

- En la medida de lo posible se evitará generar ficheros en papel de los datos que se tienen automatizados siempre y cuando no sea estrictamente necesario.
- Se recogerán de las impresoras los documentos que contienen datos de carácter personal con objeto de evitar que sean accedidos por personas no autorizadas, se debe asegurar especialmente que no queden documentos impresos en la bandeja de salida ni en los faxes.
- Los listados que contengan datos con información personal no se reciclarán.
- Cada persona revisará periódicamente los documentos que estén bajo su custodia, procediendo a destruir los que se encuentren obsoletos. La documentación que contenga datos de carácter personal que se vaya a desechar deberá ser eliminada mediante destructoras de papel de tal forma que no pueda ser reconstruido para acceder a los datos.
- Cuando el volumen de listados e informes obsoletos impida su destrucción se almacenarán bajo llave en los puntos designados a tal efecto, con el fin de proceder a su posterior destrucción o entrega a empresas designadas a tal efecto.

La información que haya que mantener pasará a formar parte del archivo para lo que se procederá a su clasificación.

Por último, en caso de existir un Encargado del Tratamiento para ficheros no automatizados, le serán de aplicación las normas del presente procedimiento. En cualquier caso, se deberá firmar un contrato de tratamiento de datos por cuenta de terceros donde se incluya una referencia a dichas normas.

3.2. Medidas de Seguridad de nivel básico

3.2.1. Criterios de archivo (🔒⃠)

Se procederá a clasificar la documentación existente en la organización, basándose en criterios de confidencialidad, contenido, ubicación, etc. En el *Anexo 1* existe un formulario para la creación y clasificación de los archivos. Dicha clasificación permitirá la localización de la información contenida con la mayor exactitud posible, de tal manera que posibilite el ejercicio de los derechos de acceso, modificación, cancelación y oposición, dentro de los plazos y eficacia exigidos por la ley.

A partir de dicha clasificación se procederá al etiquetado de los soportes que contengan la documentación, de forma que se permita su identificación inequívoca.

Por último, se aplicará la legislación específica sobre documentación, archivo y periodos de retención (Registro Civil, Historia Clínica, etc.), siempre y cuando permita cumplir con los requisitos mínimos de la normativa en protección de datos.

3.2.2. Dispositivos de almacenamiento (🔒⃠)

Se utilizarán armarios, cajones, archivadores o similares para impedir el acceso a la documentación siempre que se encuentre archivada o no vigilada.

Resulta importante utilizar medios de almacenaje de forma que se consiga la máxima conservación de la documentación, en relación con el periodo de retención, así como dotar de medios de control ambiental (extintores, sistemas de detección de humos, etc.) con el fin de prevenir cualquier contingencia posible.

3.2.3. Custodia de soportes (💣🔒🚫)

Todo el personal con acceso a la documentación de la organización se responsabilizará de su custodia, siempre que la tenga fuera de sus lugares de almacenamiento. Siempre que no se trate de ficheros catalogados de nivel alto, no será necesario el control de acceso a los ficheros, aunque ello no exima de responsabilidad al personal que mantenga la custodia del fichero.

3.2.4. Destrucción de documentación (💣🔒🚫)

Cuando la documentación tanto activa, como permanente o bloqueada, se convierta en obsoleta, deberá procederse a su destrucción de forma definitiva. La destrucción se hará de forma que se impida su recuperación o reutilización, ya sea de forma accidental o intencionada. Por ello se evitará la reutilización de documentación con datos de carácter personal o catalogada como confidencial.
Se llevarán a cabo procedimientos de destrucción mediante destructoras de papel de nivel 2, como mínimo (trazas de 6mm. como máximo), o bien se contratarán empresas de destrucción y reciclaje de documentación, en cuyo caso se regulará por contrato dicha actividad.

3.3. Medidas de Seguridad de nivel medio

3.3.1. Responsable de seguridad (💣🔒🚫)

El Responsable del Fichero debe designar a un Responsable de Seguridad que podrá ser específico para los ficheros no automatizados, por motivos de volumen u organización de los archivos. Dicho nombramiento quedará reflejado en el Documento de Seguridad.

3.3.2. Auditoría (💣🔒🚫)

Se realizará una auditoría interna o externa sobre los ficheros de carácter personal en soporte no automatizado, esta podrá realizarse de forma conjunta o separada de los ficheros automatizados.

En cualquier caso se elaborará un plan de auditoría que recoja el alcance de los ficheros a auditar.

3.3.3. Registro de entrada y salida de documentos (💣🔒🚫)

En los *Anexos 3 y 4* se encuentran los registros que deberán utilizarse para controlar la entrada y salida de documentos en la organización, siempre que contengan datos de nivel medio o alto.

3.4. Medidas de Seguridad de nivel alto

3.4.1. Almacenamiento de la información (💣🔒🚫)

Para los ficheros de nivel alto, se dispondrá de una sala o zona restringida, protegida con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Estas zonas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos.

En caso de no poder disponer de zona restringida se adoptarán mediadas alternativas, debidamente motivadas en el Documento de Seguridad.

3.4.2. Copia o reproducción ( )

La fotocopia o reproducción de documentos únicamente puede realizarla el personal autorizado, quien será el responsable del control, archivo y/o destrucción de la información copiada. Asimismo, deberá responsabilizarse de que no se produzcan accesos no autorizados a la información que mantiene bajo su custodia y se le aplicarán las normas en función de su nivel de seguridad.

La destrucción de las fotocopias o reproducciones de documentación deberá realizarse mediante destructoras de papel de nivel 4 (partículas con un tamaño máximo de 30 mm^2).

Se podrá contratar a empresas de destrucción de documentación. En el contrato de prestación de servicios se incluirá una cláusula de auditoría por parte del Responsable del Fichero.

3.4.3. Acceso a la documentación (🔓🔒⃠)

La autorización de acceso a cualquier documento de un fichero no automatizado de nivel alto se realizará por las personas designadas a tal efecto en el Documento de Seguridad.

La documentación accedida por la persona autorizada debe ser devuelta al archivo tan pronto como haya cesado el motivo que justificó el acceso y se controlará su devolución.

Se habilitará un registro de accesos autorizados (*Anexo 2 del procedimiento)*, a conservar durante un periodo no inferior a dos años.

El Responsable de Seguridad revisará este registro al menos mensualmente y emitirá un informe con los problemas o riesgos detectados en cada revisión. Este informe se ha de incluir como parte de los controles periódicos realizados en el Documento de Seguridad donde debe quedar constancia.

3.4.4. Traslado de documentación (🔓🔒)

La distribución de documentos con datos de nivel alto se realizará en sobre cerrado y lacrado o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte (cajas, precintos, vigilancia, entrega en mano, etc.).

Anexo 1 - Formulario de creación de Archivos No Automatizados

Este Anexo contiene el modelo, los registros cumplimentados se almacena en:

Documento: 'PR003A001- Formulario de creación de Archivos No Automatizados

Referencia: PR003A001

Carpeta:

Ubicación:

Anexo 1 – Formulario de creación de Archivos No Automatizados	
Nombre del Archivo:	Confidencial ⓘ
Fichero LOPD asociado:	
Fecha creación:	Fecha baja:
Controles de acceso:	Controles ambientales:
Contenido:	

Ubicación del archivo	Responsable del archivo
Firma del Responsable:	

Anexo 2 - Registro de accesos autorizados a Ficheros No Automatizados de Nivel Alto

Este Anexo contiene el modelo, los registros cumplimentados se almacena en:

Documento: 'PR003A002- Registro de accesos autorizados a Ficheros No Automatizados de Nivel Alto

Referencia: PR003A002

Carpeta:

Ubicación:

Anexo 2 – Registro de accesos autorizados a Ficheros No Automatizados de Nivel Alto

Nombre del Archivo:	Ubicación:

Nombre de Usuario	Documento accedido	Fecha / hora de acceso	Fecha / hora de devolución	Firma

Anexo 3 - Formulario para la ENTRADA de Ficheros No Automatizados

Este Anexo contiene el modelo, los registros cumplimentados se almacena en:

Documento: 'PR003A003- Formulario para la ENTRADA de Ficheros No Automatizados

Referencia: PR003A003

Carpeta:

Ubicación:

Anexo 3 – Formulario para la ENTRADA de Ficheros No Automatizados			
Nombre del Archivo:		Ubicación:	
FICHERO NO AUTOMATIZADO			
Tipo de documento			
Número de documentos enviados			
Tipo de información que contienen			
ORIGEN			
Remitente			
Forma de envío			
Fecha y hora de entrada			
AUTORIZACIÓN			
Persona responsable de la recepción		Cargo / Puesto	
Comentarios		Firma	

Anexo 4 - Formulario para la SALIDA de Ficheros No Automatizados

Este Anexo contiene el modelo, los registros cumplimentados se almacena en:

Documento: 'PR003A004- Formulario para la SALIDA de Ficheros No Automatizados

Referencia: PR003A004

Carpeta:

Ubicación:

Anexo 4 – Formulario para la SALIDA de Ficheros No Automatizados		
Nombre del Archivo:	Ubicación:	
FICHERO NO AUTOMATIZADO		
Tipo de documento		
Número de documentos incluidos en el envío		
Tipo de información que contienen		
DESTINO		
Destinatario		
Forma de envío		
Fecha y hora de salida		
AUTORIZACIÓN		
Persona responsable de la entrega		Cargo / Puesto
Comentarios		Firma

NORMAS DE CONTROL DE ACCESO LÓGICO

ÍNDICE DEL PROCEDIMIENTO

1. Objeto ____ 2
2. Ámbito de aplicación ____ 2
3. Desarrollo ____ 2
3.1. Normas generales ____ 2
3.1.1. Seguridad lógica del entorno informático ... 2
3.1.2. Protección contra virus y software maligno ... 2
3.1.3. Seguridad Lógica de los Sistemas de Aplicación ... 3
3.1.4. Custodia del fichero de contraseñas ... 3
3.2. Medidas de nivel básico ____ 3
3.2.1. Autorización de accesos ... 3
3.2.2. Normas de Asignación y Distribución de Claves de Acceso ... 3
3.2.3. Inventario de usuarios actualizado ... 4
3.3. Medidas de nivel medio ____ 4
3.3.1. Bloqueo de usuario ... 4
3.4. Medidas de nivel alto ____ 4
3.4.1. Registro de accesos ... 4

Revisado:	Aprobado:
Nombre y Firma:	Nombre y Firma:
Fecha:	Fecha:

1. Objeto

Establecer las normas necesarias para garantizar que los mecanismos de control de acceso están implantados y permiten el seguimiento de la actividad de los usuarios dentro del sistema.

2. Ámbito de aplicación

El cumplimiento de esta normativa corresponde al Responsable del Fichero, Responsable de Seguridad y del Administrador de Sistemas.

Asimismo, este procedimiento se aplicará a todo el personal, ya sea interno o externo, que tenga acceso a los sistemas y aplicaciones informáticas de la empresa.

3. Desarrollo

3.1. Normas generales

3.1.1. Seguridad lógica del entorno informático

La seguridad lógica del entorno comprende el control de acceso al sistema operativo, a las herramientas o programas utilitarios y al entorno de comunicaciones. Esta seguridad debe impedir que personal no autorizado tenga acceso a los ficheros.

A continuación se detallan los puntos mínimos a seguir para la administración de los sistemas de información:

- Las contraseñas para administrar el sistema operativo, redes, herramientas, etc. propios del entorno de sistemas, deben modificarse en el momento de la instalación, de manera que no se correspondan con las contraseñas estándar por defecto del producto instalado. Por otra parte, la frecuencia de modificación debe ser al menos anual.
- Se ha de restringir el uso y acceso a cualquier software o herramienta de sistemas a usuarios no autorizados. Asimismo, se debe asegurar que los usuarios tengan acceso únicamente a los sistemas de aplicación y software de ofimática al que hayan sido autorizados y que se requiera para realizar sus labores diarias.
- Se debe contar con herramientas de control de acceso que impidan que los usuarios y personal no autorizado puedan acceder a los ficheros restringidos.
- Cada usuario del sistema tendrá una carpeta personal con acceso restringido y para la cual se establecerán procedimientos de copia que garanticen la seguridad en la recuperación de la misma. En el caso de que sea necesario compartir documentos, se habilitarán carpetas de acceso público para estos fines.

3.1.2. Protección contra virus y software maligno

El servidor, así como todos los equipos personales deberán disponer de un programa antivirus. Para su efectividad se han de considerar los siguientes puntos:

- Actualizar de forma periódica los archivos de definiciones y firmas de virus, preferiblemente de forma automática. Se validará semestralmente la corrección del procedimiento.

- Todo el software adquirido deberá revisarse contra los virus antes de su instalación y uso. Ello también incluye archivos (descargas) de Internet, software y aplicaciones gratuitas y de prueba.

3.1.3. Seguridad Lógica de los Sistemas de Aplicación

Los sistemas de aplicación son todos aquellos sistemas informáticos, programas o aplicaciones con las que se puede acceder a los datos del Fichero, y que son utilizados por los usuarios en el desarrollo de su función diaria.

El Responsable del Fichero establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

El Responsable del Fichero, en colaboración con el Responsable de Seguridad y el Administrador de Sistemas, establecerá los criterios de acceso a cada uno de los sistemas de información mediante la definición de perfiles, en los que se especificarán los accesos permitidos y el tipo de acción que se puede realizar (lectura, modificación , altas o bajas).).

Los accesos de los usuarios a los sistemas que contengan información de la entidad, y especialmente de datos de carácter personal, estarán basados en el uso de identificadores y contraseñas ligadas a los perfiles de acceso que se concederán de acuerdo a las funciones que desempeña cada usuario.

El identificador de usuario, junto con la contraseña, debe introducirse siempre para iniciar una sesión de acceso a los sistemas de información.

3.1.4. Custodia del fichero de contraseñas

El Responsable de Seguridad garantizará el correcto almacenamiento del fichero de contraseñas mediante algoritmos de cifrado, asegurando que las mismas no sean legibles y así mantener su confidencialidad e integridad.

3.2. Medidas de nivel básico

3.2.1. Autorización de accesos

El Responsable del Fichero, o el personal en quién se delega esta función, incluido en el '*Anexo 2 - Personal Autorizado para conceder Accesos'* del documento *'PR005_Procedimiento de administración de usuarios* ', es el único con competencia para conceder, alterar o anular los accesos autorizados a los sistemas. Para realizar la autorización correspondiente se debe considerar lo siguiente:

- Los permisos de acceso de la solicitud deben estar acordes con las necesidades de acceso para el desempeño de sus funciones diarias, de manera que sean los mínimos necesarios para realizar la función correspondiente.
- La compatibilidad de la solicitud de acceso con otras solicitudes previas y con otras funciones que pueda desempeñar (principio de segregación de funciones).

3.2.2. Normas de Asignación y Distribución de Claves de Acceso

Será responsabilidad del Responsable de Seguridad la asignación y distribución de contraseñas, a través del Procedimiento de Administración de Usuarios (Procedimiento PR-005).

No obstante, se ha de tener en consideración los siguientes puntos:

- Los accesos autorizados a los sistemas de información deben corresponder a un usuario único.
- La distribución del identificador de usuario y la contraseña inicial asignada se realizará de forma confidencial y directamente al interesado, asegurando la recepción de la misma por parte de éste. Al momento de la entrega del identificador de usuario y su contraseña, se le entregarán las normas de identificación y autenticación para su información.
- El Responsable de Seguridad debe archivar las solicitudes y autorizaciones de acceso.
- El Responsable del Fichero debe mantener actualizada la relación de usuarios del '*Anexo 5 - Personal Autorizado para Acceder al Fichero'* del documento *DS001*, para ello, mensualmente el encargado del mantenimiento del sistema de información, Administrador de sistemas, o/y los usuarios autorizados a conceder accesos, entregarán al Responsable del Seguridad el detalle de las modificaciones realizadas en el periodo que no le hubieran entregado previamente.
- En el caso de que la asignación y distribución de claves para accesos remotos, se llevará a cabo lo establecido en el procedimiento de acceso remoto (*OP005*).

3.2.3. Inventario de usuarios actualizado

La relación de usuarios que tienen acceso autorizado al sistema de información elaborada por el Responsable del Fichero se incluye en el '*Anexo 5 - Personal Autorizado para Acceder al Fichero' del documento DS001*.

La custodia y actualización de la relación de todos los usuarios que tienen acceso autorizado al sistema de información, ya sea personal propio o ajeno, la realiza el Responsable del Fichero, a la que tendrá acceso el Responsable de Seguridad para sus labores de verificación y control.

3.3. Medidas de nivel medio

3.3.1. Bloqueo de usuario

En el supuesto que se trate de datos de nivel medio y alto, el Responsable del Fichero establecerá un límite de intentos reiterados que, mediante el bloqueo del usuario, permita evitar accesos no autorizados al sistema de información.

El bloqueo del identificador del usuario se ha de producir después de 5 intentos y permanecerá bloqueado durante 10 minutos.

Para reactivar la contraseña se reportará la incidencia al Responsable de Seguridad para su registro y tramitación a través del procedimiento correspondiente.

3.4. Medidas de nivel alto

3.4.1. Registro de accesos

Para todos aquellos ficheros que estén declarados de nivel alto, debe mantenerse un registro de acceso a los datos que indique:

- Usuario
- Fecha y hora
- Fichero accedido

- Si el acceso ha sido autorizado o denegado
- En el caso de acceso autorizado, identificación del registro accedido
- Tipo de acceso: lectura, escritura o borrado

Dicha información debe registrarse automáticamente en un log o bitácora a través del sistema informático.

El Responsable de Seguridad debe estructurar este mecanismo de acuerdo a las posibilidades de los sistemas individuales, minimizando el riesgo de que dichos mecanismos puedan ser desactivados.

La información de este registro debe mantenerse por un periodo mínimo de dos años y debe revisarse por el Responsable de Seguridad, por lo menos una vez al mes elaborando los informes correspondientes.

PROCEDIMIENTO DE ADMINISTRACIÓN DE USUARIOS

ÍNDICE DEL PROCEDIMIENTO

1. Objeto ____ 2
2. Ámbito de aplicación ____ 2
3. Desarrollo ____ 2
3.1. Descripción del Procedimiento ____ 2
3.1.1. Crear solicitud ... 2
3.1.2. Tramitar solicitud ... 2
3.1.3. Administrar derechos de acceso en el aplicativo ... 3
3.1.4. Entrega del identificador al usuario ... 3
Anexo 1 - Solicitud de alta/modificación de usuario ____ 4
Anexo 2 - Personal Autorizado para conceder Accesos ____ 6
Diagrama Procedimiento de administración de usuarios ____ 8

Revisado:	Aprobado:
Nombre y Firma:	Nombre y Firma:
Fecha:	Fecha:

1. Objeto

El objeto de este procedimiento es describir cómo se realiza la administración de los usuarios con acceso a los sistemas de información.

En cualquier caso dichas figuras podrán delegar en otros Responsables sin que esto suponga una exoneración de sus responsabilidades.

2. Ámbito de aplicación

Esta normativa será de aplicación a todo el personal, ya sea interno o externo, usuario del sistema.

La definición, implantación y control de la ejecución de lo establecido en este procedimiento es competencia del Responsable de Seguridad.

La responsabilidad sobre la autorización de acceso a los sistemas de aplicación corresponde al Responsable del Fichero o personal en el que se haya delegado dicha función.

La responsabilidad sobre la ejecución reside sobre el administrador del aplicativo.

3. Desarrollo

3.1. Descripción del Procedimiento

A continuación se recoge la descripción del procedimiento y su representación gráfica, diferenciando entre los procedimientos de administración de usuarios y de gestión de bajas del personal.

3.1.1. Crear solicitud

Cuando surge un requerimiento de acceso al sistema o a los ficheros para un usuario, ya sea un alta o una modificación en los accesos que tiene concedidos, se genera una solicitud utilizando el formulario Solicitud de Alta/modificación de Usuario que se adjunta al final del procedimiento.

La solicitud será revisada por el Responsable de Seguridad y la comunicará al Responsable del Fichero.

El perfil de acceso solicitado ha de corresponder a la categoría profesional o a las funciones que ha de desempeñar.

Asimismo el Responsable de Seguridad deberá tener en cuenta las siguientes consideraciones:

- La necesidad del usuario de acceder a la información solicitada para desempeñar las funciones que ha de realizar.
- La compatibilidad de la autorización requerida con otras autorizaciones que pueda poseer previamente el usuario y/o con otras funciones que pueda desempeñar.
- El nivel de clasificación de la información.

3.1.2. Tramitar solicitud

- Se procederá a enviar la solicitud, con los requerimientos de accesos necesarios, al responsable de la administración del sistema o a las personas a las que se les ha autorizado a conceder accesos según relación existente en el Anexo 2- Personal Autorizado para conceder Acceso.
- Finalmente, se archivará una copia de las solicitudes tramitadas con el objeto de facilitar las revisiones periódicas de la correcta aplicación de los procedimientos correspondientes.

3.1.3. Administrar derechos de acceso en el aplicativo

Al recibir la petición de alta/modificación enviada por el Responsable de Seguridad, el responsable autorizado a conceder accesos procederá a:

- Validar la información, y si fuera necesario la completará o rectificará.
- Realizar el alta según las normas establecidas de identificación y autenticación para el aplicativo correspondiente.
- En caso de petición de modificación, habilitando, anulando o modificando los derechos de acceso de usuario que correspondan a la solicitud aprobada.

3.1.4. Entrega del identificador al usuario

Se generará un documento en el que se indicará:

- En caso de alta:
  - Normas de uso de recursos informáticos
  - Normas de identificación y autentificación
- En caso de modificación, la confirmación de los cambios realizados.

En ningún caso se dará de alta a ningún usuario que no sea solicitado a través del Responsable de Seguridad.

Una vez generada la documentación, en el caso de alta de usuario, se contactará con el usuario para, una vez validada su identidad mediante documento acreditativo:

- Entregarle compromiso de uso de recursos informáticos, con su identificador de usuario y contraseña inicial de entrada al sistema, para su firma y guardar/enviar una copia firmada para el expediente del usuario en RRHH.
- Entregarle las normas de identificación y autentificación.

El sistema de información, en la medida de lo posible, solicitará el cambio de contraseña durante el primer acceso, en caso contrario indicar al usuario que la modifique durante el primer acceso, según el procedimiento establecido para ello.

Anexo 1 - Solicitud de alta/modificación de usuario

Este Anexo contiene el modelo de 'Solicitud de alta/modificación de usuario', los registros cumplimentados se almacena en:

Documento: PR005A001- Solicitud de alta/modificación de usuario

Referencia: PR005A001

Carpeta:

Ubicación:

Anexo 1 Solicitud de alta/modificación de usuario

Datos del usuario		
Nombre	[Nombre solicitante]	
DNI	[Num. DNI]	Fecha: [fecha de solicitud]
Área	[Área o Departamento]	
Datos contacto	[teléfono./correo electrónico]	
Tipo:	☐ permanente ☐ temporal*	
*Periodo	Inicio: [fecha]	Fin: [fecha]

Accesos	
Generales: ☐ Dominio ☐ Correo electrónico	
Locales: ☐	☐
☐	☐
Ficheros: ☐	Perfil asignado por fichero
☐	
☐	
Aplicativos:	Perfil asignado por aplicativo
☐	
☐	

Solicitado por:	Autorizado por:	Comentarios:

Palma de Mallorca, a de de 20

Anexo 2 - Personal Autorizado para conceder Accesos

Este Anexo contiene las tablas tipo, las tablas cumplimentadas se almacena en:

Documento: PR005A001- Personal Autorizado para conceder Accesos

Referencia: PR005A001

Carpeta:

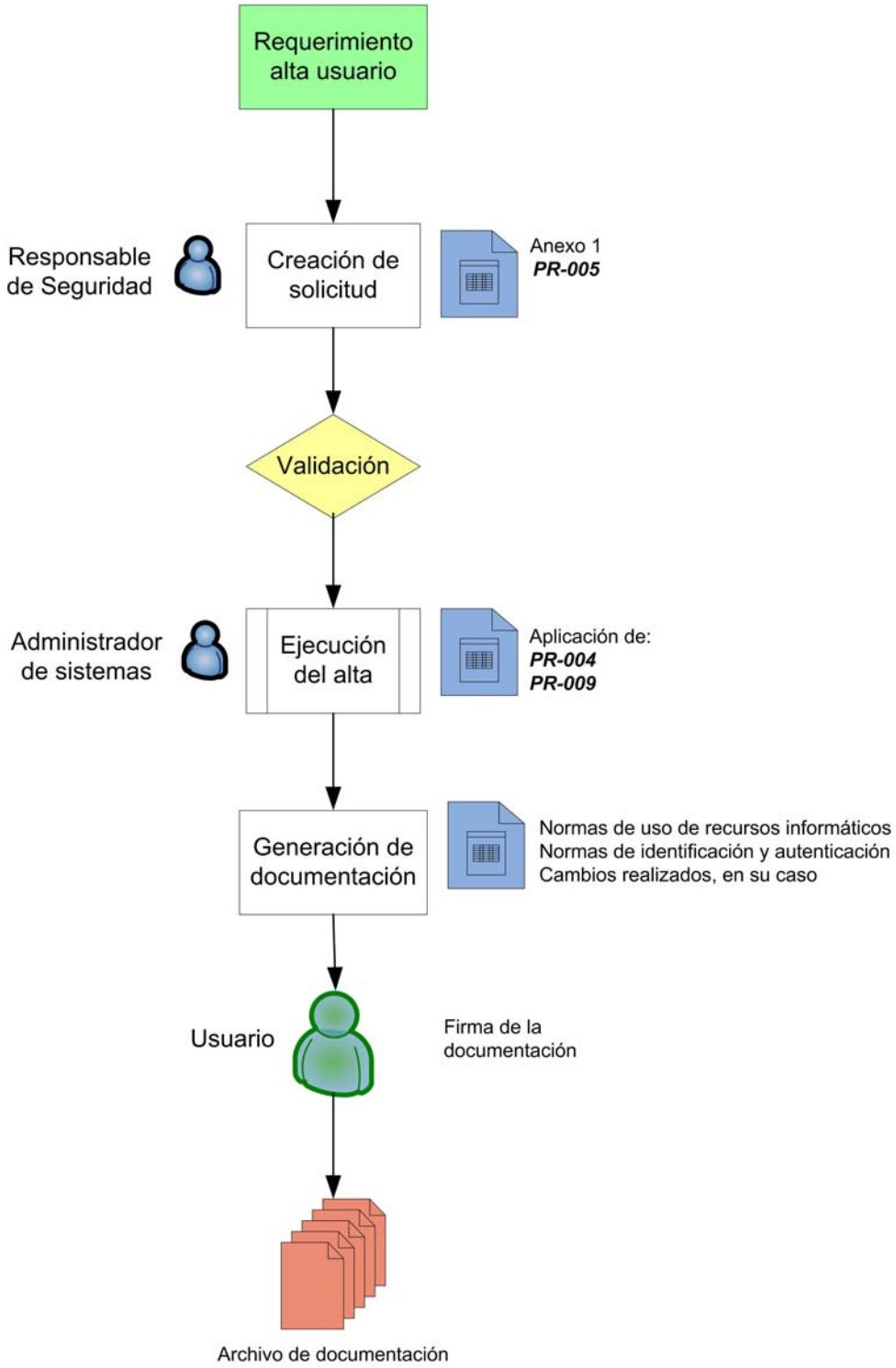
Ubicación:

Anexo 2 - Personal Autorizado para conceder Accesos

Personal designado por el Responsable del fichero en quien se delega la autorización de las altas, modificaciones y bajas de accesos, lógicos y físicos, de usuarios a las Aplicaciones, los Ficheros y los Locales

Aplicación / Fichero/Local	Nombre Área/Departamento	Datos de contacto	Fecha	
			Alta	Baja
		[teléfono y dirección correo electrónico]		

Diagrama Procedimiento de administración de usuarios



PROCEDIMIENTO DE GESTIÓN DE SOPORTES

ÍNDICE DEL PROCEDIMIENTO

1. Objeto. 2
2. Ámbito. 2
3. Desarrollo. 2
3.1. Medidas de Seguridad de nivel básico 2
3.1.1. Inventario de soportes 2
3.1.2. Medidas de transporte, reutilización y destrucción 2
3.2. Medidas de Seguridad de nivel medio 3
3.2.1. Registro de entrada y salida de soportes 3
3.3. Medidas de Seguridad de nivel alto 3
3.3.1. Medidas de identificación 3
3.3.2. Cifrado de soportes y dispositivos portátiles 3
Anexo 1 - Inventario de soportes informáticos 4
Anexo 2 - Registro de entrada de soportes informáticos 6
Anexo 3 - Registro de salida de soportes informáticos 8

Revisado:	Aprobado:
Nombre y Firma:	Nombre y Firma:
Fecha:	Fecha:

1. Objeto.

Este procedimiento se aplicará a todos los soportes que contengan datos de carácter personal; para ello, el RLOPD describe un soporte como "*Objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos*".

Se elaborará, en primer lugar, un inventario de los soportes antes descritos, y posteriormente se llevará un seguimiento acerca de su entrada y salida de la empresa.

Por último se establece un procedimiento de destrucción o reutilización de soportes que impida el acceso a la información contenida en ellos.

2. Ámbito.

Este procedimiento y las normas dispuestas en él, serán de obligado cumplimiento para todo el personal de la empresa que tenga acceso a soportes que contengan datos de carácter personal.

El Responsable de Seguridad será el encargado de velar por el cumplimiento de las normas detalladas en este procedimiento.

3. Desarrollo.

3.1. Medidas de Seguridad de nivel básico

3.1.1. Inventario de soportes

El Responsable de Seguridad debe de elaborar y mantener actualizado el inventario de dichos soportes, incluido en el *Anexo 1* del presente Documento.

Cada soporte debe estar etiquetado indicando el número de soporte y el nivel de seguridad aplicado al contenido.

En el inventario de soportes se debe de registrar para cada soporte la fecha de inicio de utilización y la fecha de la última verificación de su contenido. Asimismo, se constatará si el Responsable del Fichero autoriza su salida fuera de los locales.

Dicho inventario debe mantenerse actualizado con la creación, modificación o destrucción de cualquier soporte que contenga información que incluya datos, y en especial los de carácter personal, así como con la información de las entradas o salidas de soportes desde o hacia la empresa.

3.1.2. Medidas de transporte, reutilización y destrucción

Reutilización y Destrucción

Aquellos soportes que sean reutilizables, deben ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables. Para ello se utilizarán técnicas de borrado como *Zero Write, Ramdom and Zero Write* o bien, en caso de borrado de máxima seguridad, el Método Gutman (DoD 5220.22-M).

En el caso de destrucción de los soportes se destruirán físicamente. La destrucción física consistirá en la fragmentación del soporte (CD's o DVD's) o bien magnetización (discos duros).

Transporte

Los soportes en tránsito deben ser protegidos contra su pérdida, deterioro o uso indebido, desde que la empresa de origen los cede hasta que son recibidos por la empresa de destino.

Durante su traslado, deben asegurarse los siguientes aspectos del soporte y la información contenida:

- Protección física, para que no sean robados, sustituidos o dañados.
- Protección lógica, para que no sean leídos, copiados o modificados.

Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

3.2. Medidas de Seguridad de nivel medio

3.2.1. Registro de entrada y salida de soportes

Cuando un determinado soporte se encuentre autorizado para su salida, se debe registrar la correspondiente salida en el 'Registro de Salidas de Soportes Informáticos' del *Anexo 2* de este procedimiento en el que se detalla, además de la información relativa al soporte, la información de fecha y hora de salida, destinatario, número de soportes incluidos en el envío, forma de envío y persona responsable de la entrega, que deberá estar previamente autorizada.

En el caso de que se realicen entradas de soportes informáticos con datos de carácter personal, se debe registrar la entrada del soporte en el *Anexo 3* del presente procedimiento. El anexo contendrá el tipo de soporte que entra en la organización, la fecha y hora de entrada, emisor, número de soportes incluidos, tipo de información contenida, forma de envío y persona autorizada para la recepción.

3.3. Medidas de Seguridad de nivel alto

3.3.1. Medidas de identificación

La identificación de los soportes que contengan datos de carácter personal de nivel alto o confidenciales, se deberá llevar a cabo utilizando sistemas de etiquetado comprensibles y con significado que permita a los usuarios con acceso autorizado a los citados soportes, identificar su contenido, y que dificulten la identificación para el resto de las personas.

3.3.2. Cifrado de soportes y dispositivos portátiles

La salida o distribución de soportes con datos de nivel alto y dispositivos portátiles, tales como memorias USB, se realizará utilizando un sistema de cifrado que impida el acceso a la información en ellos contenida.

Anexo 1 - Inventario de soportes informáticos

Este Anexo contiene el modelo, los registros cumplimentados se almacena en:

Documento: 'PR006A001- Inventario de soportes informáticos'

Referencia: PR006A001

Carpeta:

Ubicación:

Anexo 1 – Inventario de soportes informáticos

Núm. Soporte	Estado	Fecha	Datos que contiene	Comentarios
	Inicio uso		[Breve descripción del contenido del soporte y si existen datos confidenciales o de nivel alto]	[Introducir si está autorizado para su salida fuera de los locales del Responsable de Fichero, así como si está preparado para ser reutilizable]
	Baja			
	Destrucción			
	Alta			
	Baja			
	Destrucción			
	Alta			
	Baja			
	Destrucción			
	Alta			
	Baja			
	Destrucción			
	Alta			
	Baja			
	Destrucción			

Anexo 2 - Registro de entrada de soportes informáticos

Este Anexo contiene el modelo, los registros cumplimentados se almacena en:

Documento: 'PR006A002- Registro de entrada de soportes informáticos

Referencia: PR006A002

Carpeta:

Ubicación:

Anexo 2 – Registro de entrada de soportes informáticos

Fecha y hora de entrada de soporte			
SOPORTE			
Tipo de soporte y número			
Contenido			
ORIGEN Y FINALIDAD			
Finalidad			
Origen			
FORMA DE ENVÍO			
Medio de envío			
Remitente			
AUTORIZACIÓN			
Persona responsable de la recepción		Cargo / Puesto	
Comentarios		Firma	

Anexo 3 - Registro de salida de soportes informáticos

Este Anexo contiene el modelo, los registros cumplimentados se almacena en:

Documento: 'PR006A003- Registro de salida de soportes informáticos

Referencia: PR006A003

Carpeta:

Ubicación:

Anexo 3 – Registro de salida de soportes informáticos

Fecha y hora de salida de soporte	

SOPORTE			
Tipo de soporte y número		Fecha de creación	
Contenido			
Ficheros de donde proceden los datos			
FINALIDAD Y DESTINO			
Destino		Destinatario	
Finalidad			
FORMA DE ENVÍO			
Medio de envío		Remitente	
Precauciones para el transporte		Persona responsable de la entrega	
AUTORIZACIÓN			
Persona que autoriza		Cargo/puesto	

Anexo 3 – Registro de salida de soportes informáticos

Fecha y hora de salida de soporte			
Comentarios		Firma	

PROCEDIMIENTO DE COPIAS DE RESPALDO Y RECUPERACIÓN

ÍNDICE DEL PROCEDIMIENTO

1. Objeto. 2
2. Ámbito de aplicación. 2
3. Desarrollo. 2
   3.1. Medidas de Seguridad de nivel básico 2
   3.2. Medidas de Seguridad de nivel medio 3
   3.3. Medidas de Seguridad de nivel alto 3
Anexo 1 - Registro de copias de respaldo 4

Revisado: Nombre y Firma:	Aprobado: Nombre y Firma:
Fecha:	Fecha:

1. Objeto.

Establecer los procedimientos y normas necesarios para realizar las copias de respaldo y recuperación de los datos de carácter personal, que se encuentran en los sistemas de información de la empresa.

2. Ámbito de aplicación.

El Responsable de Seguridad será el encargado de velar por el cumplimiento de las normas detalladas en este procedimiento. En su caso, podrá delegar esta función en una o varias personas autorizadas de la organización, en cuyo caso quedará reflejado en el Documento de Seguridad.

3. Desarrollo.

3.1. Medidas de Seguridad de nivel básico

El proceso de copias de seguridad se regirá por las siguientes normas:

Se dispondrá cuando menos de los siguientes juegos de soportes:

- 4 correspondientes a Lunes, Martes, Miércoles y Jueves
- 4 correspondientes a Viernes-1, Viernes-2, Viernes-3 y Viernes-4
- 11 correspondientes a Mes-1 hasta Mes-11
- 5 copias Anuales

La copia de seguridad se realizará rotando dichos soportes, de tal forma que siempre se disponga al menos de una copia de los últimos 4 días, de las últimas cuatro semanas, de los últimos once meses y de los últimos cinco años.

Los soportes deben cumplir con la norma de etiquetado que se establece en el Procedimiento de Gestión de Soportes.

Los soportes utilizados deberán aparecer en el inventario de soportes que se detalla en el Procedimiento de Soportes.

Todas las copias de seguridad que se realizan deben estar debidamente documentadas mediante e modelo del *Anexo 1 - Registro de Copias de Seguridad*.

Una vez cada seis meses, se realizará una prueba de recuperación de datos selectiva, con el fin de comprobar la integridad de los datos en los soportes de copias de seguridad, así como verificar que efectivamente se respaldan los datos previstos.

En caso de que se vayan a realizar pruebas con datos reales, es decir, por cuestiones de migración de datos, cambio de software, mejoras en los sistemas existentes, etc. se llevará a cabo el procedimiento de copias de seguridad.

El procedimiento de recuperación de datos podrá ser automático o manual; en ambos casos deberá controlarse la sobreescritura de información actual o bien la restauración en directorios o medios distintos. En caso de error, se comprobará la integridad del soporte y se procederá a restaurar la copia inmediatamente anterior. Por último, el soporte defectuoso pasará a ser destruido mediante las normas detalladas en el Procedimiento de Gestión de Soportes.

3.2. Medidas de Seguridad de nivel medio

En el caso de que se deba restaurar todo o parte de una copia de respaldo, se deberá contar con la autorización expresa del Responsable del Fichero.

Para ello se presentará una Hoja de Incidencia, según el modelo incluido en el procedimiento *PR008- Gestión de incidencias* en su *Anexo1- Registro de incidencias,* con la solicitud de restauración de datos y el Responsable del Fichero deberá autorizar dicha restauración.

3.3. Medidas de Seguridad de nivel alto

Deberá almacenarse una copia, tanto de los datos como de los procedimientos de recuperación, fuera de las instalaciones en que se encuentran ubicados los ficheros de nivel alto. Asimismo se estima conveniente mantener un sistema de recuperación idéntico al dispuesto en los locales del Responsable del Fichero para evitar obsolescencias.

Anexo 1 - Registro de copias de respaldo

Este Anexo contiene el modelo, los registros cumplimentados se almacena en:

Documento: 'PR007A001-Registro de copias de respaldo'

Referencia: PR007A001

Carpeta:

Ubicación:

Anexo 1 – Registro de copias de respaldo

Número Soporte	Fecha y hora	Nombre y firma responsable	Comentarios

PROCEDIMIENTO DE GESTIÓN DE INCIDENCIAS

ÍNDICE DEL PROCEDIMIENTO

1. Objeto. _____ 2
2. Ámbito. _____ 2
3. Desarrollo. _____ 2
Anexo 1 - Registro de Incidencias _____ 4

Revisado: Nombre y Firma:	Aprobado: Nombre y Firma:
Fecha:	Fecha:

1. Objeto.

Registrar y realizar el seguimiento de las incidencias que se produzcan en materia de protección de datos de carácter personal.

2. Ámbito.

El Responsable de Seguridad será el encargado de velar por el cumplimiento de las normas detalladas en este procedimiento. En su caso, podrá delegar esta función en una o varias personas autorizadas de la organización, en cuyo caso quedará reflejado en el Documento de Seguridad.

Este procedimiento y las normas dispuestas en él, serán de obligado cumplimiento para todo el personal de la organización que tenga acceso a soportes que contengan datos de carácter personal.

3. Desarrollo.

Una incidencia de seguridad es cualquier evento que se produzca y que pueda suponer un peligro para la seguridad del Fichero, entendida bajo sus tres vertientes de confidencialidad, integridad y disponibilidad de los datos.

Ejemplos de incidencias de seguridad:

- Sospecha de conocimiento de la clave de acceso personal por parte de terceros.
- Intento no autorizado de salida de soportes.
- Cambios en la estructura de los datos, ubicación o calidad de los mismos, sin conocimiento de los responsables.
- Caída del sistema que derive en corrupción de datos o pérdida.
- Recuperación de datos de una copia de seguridad
- Pérdida física o lógica de información.
- Destrucción o deterioro irreversible de soportes con datos de carácter personal.
- Intentos de acceso no autorizados a los ficheros.

Todo el personal deberá notificar inmediatamente al Responsable de Seguridad cualquier anomalía que detecte y que afecte o pueda afectar a la seguridad de los datos.

El retraso en la notificación de incidencias constituirá una falta que puede ser sancionable según la normativa laboral aplicable.

Para el registro y seguimiento de incidencias el Responsable de Seguridad habilitará un Libro de Incidencias con el modelo del Anexo único de este procedimiento. Si la resolución de incidencias la realiza un proveedor externo, es conveniente que al proceder a la resolución de la misma, redacte un informe que dé cobertura a los puntos previstos en el Libro de incidencias y se adjunte este informe al mismo.

El Responsable de Seguridad se asegurará que se da respuesta a la incidencia detectada en un periodo de tiempo adecuado de acuerdo a su criticidad y supervisará la solución de la misma elaborando un informe detallado de los pasos que se han realizado y el impacto producido.

Finalmente, el Responsable de Seguridad debe prever e implantar, junto con el Responsable del Fichero, los mecanismos necesarios para minimizar el riesgo de reincidencia.

Datos de nivel medio o alto

En caso de que la solución de la incidencia haya dañado datos de carácter personal de nivel medio o alto o datos clasificados como especialmente sensibles, y sea necesario restaurar dichos datos, se ha de obtener una autorización expresa del Responsable del Seguridad y éste llevará a cabo, en su caso, las medidas del Procedimiento de Copias de Respaldo y Recuperación.

Anexo 1 - Registro de Incidencias

Este Anexo contiene el modelo, los registros cumplimentados se almacena en:

Documento: 'PR008A001- Registro de Incidencias

Referencia: PR008A001

Carpeta:

Ubicación:

Anexo 1 – Registro de Incidencias				
Número:	Fecha y hora de incidencia		Fecha y hora de notificación	
Nombre de la persona que realiza la notificación:			Persona(s) a quien(es) se comunica:	
Tipo de incidencia:				
Descripción detallada de la incidencia: Documentos asociados:				
Efectos de la incidencia Documentos asociados				
Seguimiento de la incidencia Documentos asociados				
Recuperación de Datos :(A rellenar sólo si la incidencia es de este tipo)				
*Procedimiento realizado: *Datos restaurados:			*Datos grabados manualmente: *Persona que ejecutó el proceso:	
Firma Notifica	Evaluación y Solución Responsable de Seguridad		Autorización Responsable fichero	

(*) Sólo para ficheros de nivel medio y alto

NORMAS DE IDENTIFICACIÓN Y AUTENTICACIÓN

ÍNDICE DEL PROCEDIMIENTO

1. Objeto 2
2. Ámbito de aplicación 2
3. Desarrollo 2
   3.1. Uso del identificador y contraseña 2
   3.2. Política de contraseñas 2

Revisado: Nombre y Firma:	Aprobado: Nombre y Firma:
Fecha:	Fecha:

1. Objeto

Identificar a cada una de las personas que hacen uso de los recursos informáticos de la empresa y garantizar que el usuario que accede mediante su identificador de usuario es el propietario de dicho identificador.

2. Ámbito de aplicación

Esta normativa se aplica a todo el personal, ya sea interno o externo, usuario del sistema.

3. Desarrollo

3.1. Uso del identificador y contraseña

Todos los usuarios autorizados a acceder a los sistemas de información utilizarán un identificador de usuario y una contraseña; para ello, se deberá consultar el Procedimiento de Administración de Usuarios (PR-005).

El identificador de usuario es una combinación alfanumérica de al menos 8 caracteres, única e irrepetible, que permitirá reconocer a la persona que accede al sistema, quedando expresamente prohibido utilizar identificadores de usuarios genéricos o ajenos.

La contraseña será una clave secreta, conocida únicamente por el propietario del identificador de usuario, que permitirá verificar la identidad del mismo

El identificador de usuario, tanto como su correspondiente contraseña, que se asigna al personal que lo requiera, es confidencial, personal e intransferible.

Cualquier acción realizada con un identificador de usuario es responsabilidad del titular del mismo por lo que es necesario que cada uno de los accesos autorizados al aplicativo este identificado unívocamente con el usuario correspondiente.

3.2. Política de contraseñas

Las contraseñas deben cumplir al menos con los siguientes criterios para reforzar su confidencialidad y, en la medida de lo posible, deben automatizarse dentro de los sistemas de información:

- La longitud deberá ser de, al menos, entre seis y ocho caracteres alfanuméricos (una combinación de letras y números) que no se corresponda con ninguna palabra fácilmente detectable a través de búsquedas en diccionarios.
- Bajo ninguna circunstancia deben usarse palabras fácilmente identificables con las características y el entorno del usuario.
- Al realizar el cambio de clave de acceso no deberán reutilizarse las 6 últimas instancias de la misma.
- Se permitirán como máximo 3 intentos de acceso al sistema antes de que se produzca el bloqueo del usuario.
- Si un usuario permanece sin acceder al sistema más de 90 días, se bloqueará la cuenta correspondiente.

El usuario cambiará la contraseña en las siguientes circunstancias:

- Se realizará el cambio de la contraseña inicial y mantendrá una frecuencia de cambio como máximo de 90 días.
- Siempre que se tenga la sospecha de que pueda haber sido transgredida su seguridad.
- Siempre que sea conocida por otro usuario o se sospeche que pueda serlo.

Está expresamente prohibido divulgar la propia contraseña. En este sentido, cada usuario será responsable de:

- Custodiar su contraseña, manteniéndola en secreto y no guardarla en una forma legible en archivos en disco, o cualquier otro tipo de soporte donde pueda ser accesible.
- Teclearla en el sistema en privado

NORMAS DE ACCESO FÍSICO

ÍNDICE DEL PROCEDIMIENTO

1. Objeto. 2
2. Ámbito de aplicación 2
3. Desarrollo 2
   3.1. Controles de seguridad física 2
   3.2. Control de acceso físico 2
   3.3. Autorización de acceso físico 2
   3.4. Equipos y ficheros ubicados en las áreas de usuario 3
Anexo 1 – Personal Autorizado para Acceso Físico 5

Revisado:	Aprobado:
Nombre y Firma:	Nombre y Firma:
Fecha:	Fecha:

1. Objeto.

Establecer las normas básicas de protección física de los recursos protegidos que dan tratamiento a los datos personales de la empresa.

2. Ámbito de aplicación

El ámbito de aplicación de esta normativa se circunscribe a las instalaciones definidas en el anexo de Recursos Protegidos detallado en el Anexo 1 del Documento de Seguridad *(DS001)*.

El cumplimiento de esta normativa es responsabilidad de cada uno de los Responsables de las ubicaciones protegidas y en general de todo el personal, interno o externo, que tenga bajo su custodia recursos informáticos proporcionados por la entidad.

3. Desarrollo

3.1. Controles de seguridad física

Las ubicaciones donde se encuentran los recursos protegidos (equipos, tanto servidores, como ordenadores personales y los soportes en los que se almacenan los ficheros con datos de carácter personal), deberán ser áreas protegidas, en la medida de lo posible, por un perímetro de seguridad en el que se puedan aplicar los controles ambientales necesarios y al que para acceder existan barreras de seguridad apropiadas.

Los servidores se deben ubicar en el interior del edificio lejos de ventanas, y en su caso, con las medidas de seguridad que minimicen el riesgo que esto supone.

Se ha de contar con los medios de seguridad física, tales como, detectores de humo y humedad, sistemas de alimentación eléctrica alternativos (por ejemplo. SAI, baterías o grupos electrógenos, etc.), que permitan identificar y evitar situaciones de riesgo que deriven en la indisponibilidad de los ficheros que pueda producirse como consecuencia de incidencias fortuitas o intencionadas.

3.2. Control de acceso físico

Los accesos a las dependencias donde están ubicados los servidores y equipos de comunicaciones deben estar limitados únicamente al personal autorizado.

Todas las puertas de acceso deberán estar permanentemente cerradas o, en caso de encontrarse en horario laboral, vigiladas de forma que cuando personal no autorizado acceda a las dependencias protegidas de la empresa lo haga acompañado por personal con acceso autorizado

Se debe contar con mecanismos de cierre, como tarjetas de identificación, llaves, identificación biométrica, etc. que impidan accesos físicos no autorizados.

3.3. Autorización de acceso físico

El acceso físico esta limitado únicamente al personal autorizado.

El responsable de conceder acceso a las dependencias en las que se encuentran los recursos protegidos es el Responsable del Fichero, designado en el '*Anexo3- Detalle de Asignación de Funciones*' del Documento '*DS001'*, o el personal en quién se delega esta función, incluido en el '*Anexo 2 - Personal Autorizado para conceder Accesos'* del documento *'PR005_Procedimiento de administración de usuarios* '.

El Responsable de cada una de las ubicaciones debe llevar un registro actualizado del Personal Autorizado para Acceso Físico a las mismas e incluirlo en el registro de '*Personal Autorizado para Acceso Físico'* que se incluye en el '*Anexo 1'* de esta normativa.

Para solicitar el acceso físico a las dependencias en las que se encuentran los recursos protegidos de la entidad se utilizará el formulario '*Anexo 1- Solicitud de alta/modificación de usuario'* incluido en el procedimiento *'PR005_Procedimiento de administración de usuarios'* de esta normativa.

La autorización de acceso sólo se concederá a las personas que por razón de trabajo requieran acceder a dicha ubicación, ya sea de forma permanente, o en un periodo limitado en cuyo caso se indicará la fecha de caducidad.

Debe ejercerse un estricto control para evitar el acceso del personal al que le sea revocada la autorización actualizando de inmediato el registro de personal autorizado y, en caso de que se utilicen elementos identificativos y/o de acceso (p. e . tarjetas), se ha de retirar al personal cuyo acceso haya sido cancelado.

Las visitas puntuales deben ser excepcionales y no requieren autorización por escrito, no obstante, se designará a una persona con acceso autorizado para acompañar al visitante durante su estancia.

Cualquier acceso no autorizado constituye una incidencia de seguridad que se ha de reportar de inmediato de acuerdo al procedimiento establecido.

3.4. Equipos y ficheros ubicados en las áreas de usuario

La seguridad física de los datos de carácter personal existentes en los ordenadores personales y en los soportes controlados por los usuarios debe estar protegida.

La protección de esta información es responsabilidad individual de los usuarios que la gestionan por lo que se ha de tener especial cuidado en evitar accesos a dicha información, incluyendo la simple visualización de los datos.

Los controles básicos para minimizar los accesos físicos pasan por seguir las siguientes pautas:

- Mantener cerrado el acceso a los despachos.
- Almacenar los soportes informáticos, ordenadores portátiles u otros dispositivos con datos de carácter personal en armarios o cajones cerrados cuando no estén en uso, especialmente fuera de las horas de trabajo.
- Para evitar el acceso a la información de los ordenadores personales se han de:
  - Bloquear automáticamente la sesión después de un tiempo establecido de inactividad del usuario para evitar el acceso durante ausencias cortas del puesto de trabajo.
  - Apagar ordenadores personales durante la ausencia prolongada del puesto de trabajo.
- Por otra parte, en cuanto al uso de los equipos y ficheros no está permitido:
  - Acceder o modificar la configuración de hardware de los equipos.
  - Almacenar ficheros con datos de carácter personal en las unidades locales de disco de los ordenadores si éstas no están protegidas de accesos no autorizados.

- Modificar la configuración de software de los equipos o instalar aplicaciones sin la autorización correspondiente.
- Ejecutar programas fuera de los previamente instalados.

Anexo 1 – Personal Autorizado para Acceso Físico

Este Anexo contiene las tablas tipo, las tablas cumplimentadas se almacenan en:

Documento: PR010A001- Personal Autorizado para Acceso Físico

Referencia: PR010A001

Carpeta:

Ubicación:

Anexo 1 - Personal Autorizado para Acceso Físico

Nombre	Ubicación/Local	Autorizado por	Fecha	
			Alta	Baja
	[Anexo 1 DS001, Relación de locales, NOMBRE]			

PROCEDIMIENTO DE VIDEOVIGILANCIA

ÍNDICE DEL PROCEDIMIENTO

1. Objeto. ____ **2**
2. Ámbito. ____ **2**
3. Ámbito de aplicación ____ **2**
3.1. Zonas Video vigiladas ____ 2
3.2. Equipos de Video Vigilancia ____ 2
3.3. Identificación de las personas ____ 2
4. Desarrollo ____ **2**
4.1. Legitimación del tratamiento ____ 2
4.2. Visionado de las imágenes ____ 3
4.3. Deber de informar ____ 3
4.4. Conservación de imágenes ____ 4
4.5. Atención de derechos de los interesados ____ 4
4.5.1. Derecho de acceso 5
4.5.2. Derechos de cancelación y rectificación 5
4.5.3. Derecho de oposición 6
5. Comunicación de datos de videovigilancia a las Fuerzas y Cuerpos de Seguridad del Estado. ____ **7**
Anexo 1 - Cláusula de información de videovigilancia ____ **9**
Anexo 2 – Cartel videovigilancia ____ **10**
Anexo 3 - Cesión de Datos a las Fuerzas y Cuerpos de Seguridad del Estado ____ **12**
Anexo 4 - Detalle de los recursos protegidos ____ **13**
Sistemas video vigilancia ____ 14
Cámaras ____ 14
Monitores ____ 14
Equipo de grabación ____ 14
Controles del documento ____ **15**

1. Objeto.

Establecer los procedimientos a aplicar en el tratamiento de imágenes obtenidas en el proceso de videovigilancia, por motivos de seguridad, ateniéndose a la legislación vigente en la materia.

2. Ámbito.

El Responsable de Seguridad será el encargado de velar por el cumplimiento de las normas detalladas en este procedimiento.

Este procedimiento y las normas dispuestas en él, serán de obligado cumplimiento para todo el personal de la organización o externo que tenga acceso al sistema de videovigilancia y los soportes que se generen con las imágenes obtenidas.

3. Ámbito de aplicación

3.1. Zonas Video vigiladas

La instalación de cámaras y videocámaras debe limitarse a los espacios privados, y no deberán obtenerse imágenes de espacios públicos, salvo cuando resultara imprescindible para la finalidad de vigilancia, o fuera imposible evitarlo por razón de la ubicación de las cámaras (p.ej: una cámara que se encuentre ubicada en la puerta de entrada de una entidad, destinada al control de acceso a las instalaciones, deberá orientarse de tal modo que la parte de vía pública que capte se limite al acceso vigilado, sin captar más que lo estrictamente imprescindible para cumplir con su finalidad. Por tanto, sería incorrecto que captara imágenes del resto de la acera o de la calle).

3.2. Equipos de Video Vigilancia

Los equipos que forman parte del sistema de video vigilancia son recursos protegidos ya que son los que posibilitan el tratamiento de las imágenes, datos de carácter personal.

Las características del sistema de video vigilancia se especifica en el '*Anexo 4 – Detalle de los recursos protegidos - Sistemas de video vigilancia*' del presente documento.

3.3. Identificación de las personas

Las imágenes sólo podrán ser consideradas datos de carácter personal en caso de que las mismas permitan la identificación de las personas que aparecen en dichas imágenes, no encontrándose amparadas por la LOPD en caso contrario.

4. Desarrollo

4.1. Legitimación del tratamiento

Puede prestar servicios de esta naturaleza cualquier particular o empresa aunque su actividad principal no sea la propia de una empresa de seguridad privada, siempre que

el sistema no esté conectado a una central de alarma, de acuerdo con lo que se desprende de la Disposición Adicional Sexta de la Ley de Seguridad Privada.

4.2. Visionado de las imágenes

El responsable del fichero designará a las personas que van a tener acceso a las imágenes. Dicha designación de los usuarios autorizados se reflejará en el '*Anexo 5- Personal Autorizado para Acceder al Fichero'* del '*Documento de Seguridad' (DS001)* y deberán ser informados de sus respectivas obligaciones.

Si las imágenes son visionadas por personal perteneciente a la empresa de seguridad, con independencia de que también lo pueda hacer el responsable, deberá realizarse un contrato de acceso a las imágenes por cuenta de terceros, según el modelo *Contrato para Tratamiento de Datos Personales por Cuenta de Terceros* incluido en el *Anexo 6* del documento '*Documento de Seguridad' (DS001)* adquiriendo esta empresa de seguridad la condición de encargado del tratamiento de aquéllas.

Si el personal de la propia empresa en la que se instala el sistema es el que procede a visionar las imágenes y gestionar los soportes de videovigilancia sin intervención de una empresa de seguridad, no resultará necesario firmar dicho contrato. No obstante, en este último supuesto se recogerá expresamente en el contrato de prestación de servicios realizado con la empresa de seguridad (encargada de la instalación de los sistemas de videovigilancia con fines de seguridad privada) la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

4.3. Deber de informar

Debe tenerse en cuenta que tanto si se declara la existencia de un fichero como si las imágenes se emiten en tiempo real sin grabación, existe la obligación de informar.

En cuanto al modo en que haya de facilitarse dicha información, debe tenerse en cuenta el artículo 3 de la Instrucción 1/2006 que establece que "Los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de La LOPD. A tal fin deberán:

- Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados. El distintivo se ubicará como mínimo en los accesos a las zonas vigiladas, sean estos exteriores o interiores. Debe tenerse en cuenta que si el lugar vigilado dispone de varios accesos se debe colocar en todos ellos al objeto de que la información sea visible con independencia de por donde se acceda.

- El contenido y el diseño del distintivo informativo se ajustará a lo previsto en la Instrucción 1/2006. Se adjunta modelo en el Anexo 2 Cartel videovigilancia.
- Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la LOPD, según modelo contenido en el Anexo 1 del presente documento.

4.4. Conservación de imágenes

Respecto al plazo de conservación de las imágenes, la elección de dicho plazo no es arbitraria sino que encuentra su fundamento en la Instrucción 1/2006, que en su artículo sexto dispone que "*Los datos serán cancelados en el plazo máximo de un mes desde su captación"*. Adicionalmente se ha tenido en cuenta el criterio utilizado en la regulación de las Fuerzas y Cuerpos de Seguridad del Estado que confirma esta afirmación, aunque se refiera a un ámbito específico de actuación.

Asimismo, es conveniente tener en consideración las siguientes medidas de seguridad:

- En caso de que existan monitores en los que se proyecten las imágenes, o que sea necesario visionar las grabaciones, se ha de realizar en áreas de acceso restringido para evitar el visionado por parte de personal no autorizado.
- Las imágenes almacenadas se deben guardar en un lugar de acceso restringido.
- El personal designado para la gestión del sistema de videovigilancia debe conocer los procedimientos relativos al acceso a las imágenes y a los procedimientos de seguridad y políticas de privacidad correspondientes.

4.5. Atención de derechos de los interesados

Respecto al modo de ejercitar los derechos de acceso, rectificación, cancelación y oposición de los afectados, cualquier interesado podrá ejercitar sus derechos ante el responsable del fichero y éste deberá en todo caso atenderlos y responderlos, con independencia de que se disponga o no de imágenes del interesado, ya sea debido a que las imágenes se borran cada cierto tiempo o a que no son grabadas sino únicamente emitidas en tiempo real, o simplemente porque no se ha recogido la imagen del interesado en las grabaciones.

El procedimiento a seguir es el mismo que para el resto de ficheros y se desarrolla en el '*PR002_Procedimiento Ejercicio de Derechos'*

Para proporcionar adecuadamente la atención de los derechos solicitados se deberá indicar al interesado la información necesaria sobre las imágenes requeridas.

Por otra parte la localización de las imágenes debe llevarse a cabo por el Responsable de Seguridad, quien debe tomar las decisiones correspondientes en cuanto a cómo se ha de proceder en cada una de las solicitudes recibidas.

4.5.1. Derecho de acceso

El acceso que se efectúe **no** puede implicar una violación a los derechos de terceros. A continuación indicamos el sistema previsto en la Instrucción 1/2006 en su artículo 5, apartado 2º:

> *"2. - El responsable podrá facilitar el derecho de acceso mediante escrito certificado en el que, con la mayor precisión posible y sin afectar a derechos de terceros, se especifiquen los datos que han sido objeto de tratamiento."*

Este procedimiento asegura el equilibrio entre ambos derechos, esto es, atender el acceso y no comunicar datos de terceros. No obstante, se pueden adoptar otros medios iguales de efectivos (p.e., deberá utilizar mecanismos que permitan ocultar la identidad de terceras personas que aparezcan en la imagen), siempre que dicho equilibrio se mantenga. En el caso de que se ejercitase este derecho ante el responsable de un sistema de videovigilancia que únicamente reprodujese imágenes en tiempo real sin registrarlas, se deberá responder indicando la inexistencia de imágenes grabadas de la persona que ejerciera el derecho.

4.5.2. Derechos de cancelación y rectificación

La Ley orgánica 15/1999 en su artículo 16 dispone que "el responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de cancelación del interesado en el plazo de diez días", estableciendo su apartado 2 que "serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos".

Por tanto, para proceder a la rectificación de las imágenes, el afectado debería de acreditar que sus datos resultan inexactos o incompletos, cuestiones que resultan imposibles de acreditar debido a las características de los datos (imágenes captadas de la realidad que en principio reflejan un hecho objetivo). En definitiva, no resulta posible el ejercicio del derecho de rectificación en este ámbito.

No obstante, si un particular solicita la cancelación de sus imágenes, el responsable del fichero debería de cancelar las imágenes en el plazo de 10 días desde que se produce la solicitud.

Si las grabaciones ya han sido borradas o son borradas en un plazo inferior a los 10 días únicamente se debe de informar al afectado que sus datos ya han sido cancelados.

Al ser la imagen el dato personal sobre el que se solicita la rectificación, el afectado no podrá indicar que el dato es erróneo, dado que nuestra imagen es la que es. No obstante, el Responsable del Fichero debe atender la solicitud del afectado y contestarla en el plazo de diez días establecido en el apartado segundo del art.32 del RLOPD, que señala que: *"El responsable del fichero resolverá sobre la solicitud de rectificación o cancelación en el plazo máximo de diez días a contar desde la recepción de la solicitud".*

4.5.3. Derecho de oposición

En cuanto al derecho de oposición, el artículo 6.4 de la LOPD dispone que "*En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado*".

El ejercicio del derecho de oposición en los casos en los que no sea necesario el consentimiento requiere la concurrencia de los requisitos exigidos en el artículo 6.4 antes expuesto y en la práctica resulta muy compleja su aplicación. Si entendemos que el derecho de oposición implica la imposibilidad de captar imágenes de una persona determinada por medio de las instalaciones de videovigilancia, para la finalidad de seguridad privada, este derecho no podría ejercitarse, puesto que primaría la protección de la seguridad sobre el ejercicio del derecho por la persona interesada.

Al ser necesario que se alegue un motivo fundado y legítimo relativo a la situación personal de cada afectado, para poder valorar si procede o no la oposición deberá analizarse caso por caso.

5. Comunicación de datos de videovigilancia a las Fuerzas y Cuerpos de Seguridad del Estado.

En relación con la posibilidad de cesión a la Policía, el artículo 22.2 de la Ley 15/1999, habilita a las Fuerzas y Cuerpos de Seguridad del Estado a recabar y tratar datos de carácter personal sin consentimiento de los afectados únicamente cuando se cumplan las siguientes condiciones:

- Que quede debidamente acreditado que la obtención de los datos resulta necesaria para la prevención de un peligro real y grave para la seguridad pública o para la represión de infracciones penales y que, tratándose de datos especialmente protegidos, sean absolutamente necesarios para los fines de una investigación concreta.
- Que se trate de una petición concreta y específica, al no ser compatible con lo señalado anteriormente el ejercicio de solicitudes masivas de datos.
- Que la petición se efectúe con la debida motivación, que acredite su relación con los supuestos que se han expuesto.
- Que, en cumplimiento del artículo 22.4 de la Ley 15/1999, los datos sean cancelados "cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento".

En consecuencia, las Fuerzas y Cuerpos de Seguridad del Estado podrán tener acceso a las imágenes sin consentimiento de los interesados, en las condiciones y con las cautelas indicadas anteriormente. 7

La persona de la empresa que reciba la petición de información personal deberá:

- ❑ Comprobar la identidad del agente solicitando su documento acreditativo (p.e. carné profesional identificativo).

- ❑ Solicitará la documentación acreditativa, el requerimiento judicial u orden donde se indique la información requerida y se justifiquen los motivos de la solicitud de los datos de carácter personal.

  El agente podrá negarse a dar la explicación del asunto (p.e. secreto de sumario…). En caso de que no exista documento justificativo se le solicitará a quien represente a las Fuerzas y Cuerpos de Seguridad tanto la exposición de motivos para la cesión de los datos solicitados, así como los motivos por los cuales no se adjunta documentación acreditativa para la cesión correspondiente. Esta información se recogerá en el documento de cesión incluido en el *Anexo 3- Cesión de Datos a las Fuerzas y Cuerpos de Seguridad del Estado,* que deberá firmar el solicitante de los datos y quien los proporciona.

  Se debe valorar si la información solicitada responde a una petición concreta y específica de datos. La solicitud de datos en ningún caso podrá ser una solicitud masiva de datos. En caso de duda, contactar con el Responsable del Fichero.

- Por último, se deberá comunicar la cesión de datos al Responsable del Fichero/Responsable de Seguridad para que proceda a su registro en el Registro de Incidencias de Seguridad de acuerdo al procedimiento establecido en el Documento de Seguridad.

Anexo 1 - Cláusula de información de videovigilancia

Según lo dispuesto en la Instrucción 1/2006, de 8 de noviembre y en el artículo 5.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos (en adelante LOPD) se le informa que existe posibilidad de que se capte su imagen por medio de cámaras de videovigilancia situadas en las instalaciones. Su acceso voluntario a estas dependencias llevará implícito su consentimiento para el tratamiento de dichas imágenes.

Sus datos personales se incorporarán al fichero, cuyo responsable es el CES Alberta Giménez, denominado 'Videovigilancia' y serán tratados con la finalidad de reforzar la seguridad de personas e instalaciones de la entidad.

Sus datos podrán ser cedidos a las fuerzas y cuerpos de seguridad para investigar actos ilícitos que se puedan haber cometido en nuestras instalaciones.

Además se le informa que puede ejercitar sus derechos de acceso, rectificación, cancelación y oposición ante CES Alberta Giménez ubicado en Costa de Saragossa, 16 de Palma de Mallorca, aportando documento oficial que le identifique.

Anexo 2 – Cartel videovigilancia

ZONA VIDEOVIGILADA

LEY ORGANICA 15/1999, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

De acuerdo el articulo 5 de la Ley Orgánica 15/1999 y la instrucción 1/2006, de 8 de noviembre, le informamos que existe la posibilidad de que cámaras de vídeo vigilancia situadas en nuestras instalaciones capten su imagen.

El acceso voluntario a nuestras dependencias comporta implícitamente el consentimiento para tratar sus imágenes.

Sus datos personales se incorporaran a un fichero debidamente inscrito en el registro de la Agencia Española de Protección de Datos, con la finalidad de de reforzar la seguridad de personas e instalaciones.

Sus datos podrán ser cedidos a las fuerzas y cuerpos de seguridad para investigar actos ilícitos que se puedan haber cometido en nuestras instalaciones.

CES Alberta Giménez es la responsable del fichero, la persona interesada podrá ejercer sus derechos de acceso, rectificación, cancelación y oposición ante CES Alberta Giménez ubicado en Costa de Saragossa, 16 de Palma de Mallorca, aportando documento oficial que le identifique.

Anexo 3 - Cesión de Datos a las Fuerzas y Cuerpos de Seguridad del Estado

D./Dña. _____ Nº Identificación _____

En su condición de representante de las Fuerzas y Cuerpos de Seguridad reclama la comunicación de los datos de carácter personal referidos a:
(Señalar concreta y específicamente qué datos de carácter personal se reclaman)

Con la finalidad y motivación siguiente:
(Detallar qué objetivo/s tiene la solicitud de datos de carácter personal)

Señale con una (X). Se adjunta documentación justificativa:

- ☐ Mandamiento judicial
- ☐ Requerimiento del Ministerio Fiscal
- ☐ Otros (indicar) _____

En caso contrario indicar motivo para no aportar documentación justificativa

Se informa que, a tenor de lo dispuesto en el artículo 22.4 de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos, los datos personales ahora cedidos o comunicados deberán ser cancelados cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

_____

Firma del receptor de la información

Nombre y firma del trabajador responsable de la entrega:	Fecha y hora:

Anexo 4 - Detalle de los recursos protegidos

Sistemas de video vigilancia

Este Anexo contiene las tablas tipo, las tablas cumplimentadas se almacena en:

Documento: PR011A004- Detalle de los recursos protegidos-VideoVigilancia

Referencia: PR011A004

Carpeta:

Ubicación:

Anexo 4 – Detalle de los Recursos	**Sistemas video vigilancia**
Identificador sistema	
Descripción	
Grabación	

Anexo 4 – Detalle de los Recursos	**Cámaras**
Identificador cámara	
Tipo:	
Marca:	
Modelo:	
Objetivo	
LEDS	
Líneas de resolución	
Alimentación	
Medidas	
Protección	
Lux	
Sensor	
Documentación	
Local	

Anexo 4 – Detalle de los Recursos	**Monitores**
Modelo	
Tamaño	
Tipo	
Documentación	
Sistema	
Local	

Anexo 4 – Detalle de los Recursos	**Equipo de grabación**
Identificador grabador	
Modelo	
Formato vídeo	
Modos visionado	
Conexiones E/S	
Modos grabación	
Resolución	
Disco duro	
Tiempo	
Seguridad	
Documentación	
Sistema	
Local	

Controles del documento

REVISADO	**NOMBRE:**	**FIRMA:**
	FECHA:	
APROBADO	**NOMBRE:**	**FIRMA:**
	FECHA:	

Histórico de revisiones

Edición	Fecha	Cambios respecto edición anterior
01.00		Original
02.00		Instalación Cámaras con grabación
Referencia	**Apartado**	
3	3.2	Ámbito de aplicación. Añadido "Equipos de Video Vigilancia"
4	4.4	Desarrollo. Añadido apartado de "Conservación de imágenes"
5		Añadido apartado. Comunicación de datos de videovigilancia a las Fuerzas y Cuerpos de Seguridad del Estado
Anexo 1		Modificada cláusula de información de videovigilancia
Anexo 2		Modificado cartel de videovigilancia
Anexo 3		Añadido formulario a utilizar en caso de "Cesión de Datos a las Fuerzas y Cuerpos de Seguridad del Estado"
Anexo 4		Añadidos formularios para la definición y control de los recursos protegidos del sistema de Videovigilancia.
Referencia	**Apartado**	

Anexo 4 – Detalle de los Recursos — Sistemas video vigilancia

Identificador sistema	**S1**
Descripción	[Para que se utiliza, ej. Control de accesos a ... para garantizar la seguridad de instalaciones y personas]
Grabación	Si

Anexo 4 – Detalle de los Recursos — Cámaras

Identificador cámara	**C1**
Tipo:	[Describir características o hacer referencia a al manual en la que aparezcan las características]
Marca:	
Modelo:	
Objetivo	
LEDS	
Líneas de resolución	
Alimentación	
Medidas	
Protección	
Lux	
Sensor	
Documentación	
Local	

Anexo 4 – Detalle de los Recursos — Monitores

Identificador monitor	**M1**
Modelo	[Describir características o hacer referencia a al manual en la que aparezcan las características]
Tamaño	
Tipo	
Documentación	
Sistema	
Local	

Anexo 4 – Detalle de los Recursos — Equipo de grabación

Identificador grabador	**G1**
Modelo	[Describir características o hacer referencia a al manual en la que aparezcan las características]
Formato vídeo	
Modos visionado	
Conexiones E/S	
Modos grabación	
Resolución	
Disco duro	
Tiempo	
Seguridad	
Documentación	
Sistema	
Local	

Controles del documento

REVISADO	**NOMBRE:**	**FIRMA:**
	FECHA:	
APROBADO	**NOMBRE:**	**FIRMA:**
	FECHA:	

Histórico de revisiones

Edición	Fecha	Cambios respecto edición anterior
01.00		Original
02.00		Instalación Cámaras con grabación

Referencia	Apartado	
3	3.2	Ámbito de aplicación. Añadido "Equipos de Video Vigilancia"
4	4.4	Desarrollo. Añadido apartado de "Conservación de imágenes"
5		Añadido apartado. Comunicación de datos de videovigilancia a las Fuerzas y Cuerpos de Seguridad del Estado
Anexo 1		Modificada cláusula de información de videovigilancia
Anexo 2		Modificado cartel de videovigilancia
Anexo 3		Añadido formularios a utilizar en caso de "Cesión de Datos a las Fuerzas y Cuerpos de Seguridad del Estado"

Referencia	Apartado	