DEPUTACIÓN
OURENSE

DOCUMENTO DE SEGURIDAD

PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

El Servicio de Administración Electrónica de la Diputación Provincial de Ourense procede a la redacción del presente Documento de Seguridad, que contempla, exclusivamente (a falta por determinar las medidas de seguridad que afectan a los ficheros no automatizados por parte del responsable de ficheros), las medidas que afectan al tratamiento de los ficheros automatizados de carácter personal, para su conocimiento y cumplimiento por el personal de la Institución con acceso a los mismos.

Servicio de Administración Electrónica

Deputación de Ourense

TABLA DE CONTENIDO

INTRODUCCIÓN

1.1. INTRODUCCIÓN

La protección de los datos personales y de la privacidad ha adquirido en los últimos años una creciente importancia en los países de nuestro entorno, conscientes de la necesidad de salvaguardar el derecho a la intimidad personal y familiar de sus ciudadanos.

Por este motivo, han surgido numerosas disposiciones legales y normativas que han venido a regular la utilización y tratamiento de los datos de carácter personal, así como a imponer una serie de obligaciones en materia de seguridad informática a las organizaciones que necesiten recopilar y procesar datos de carácter personal.

En la Unión Europea el marco normativo viene determinado por la directiva 95/46/CE del Parlamento Europeo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de los mismos entre empresas de la Unión Europea.

En España el artículo 18.4 de la Constitución ya contempla que el Estado debe limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos. La publicación de la Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal (LOPD), que ha venido a sustituir a la famosa LORTAD, obliga a la implantación de importantes medidas de seguridad informática a las empresas que hayan creado ficheros con datos personales.

De acuerdo con lo estipulado en el artículo 9 de la citada LOPD, las empresas e instituciones con ficheros de titularidad privada o pública deben implantar todas las medidas de índole técnica y organizativa que permitan garantizar la seguridad de los datos de carácter personal, y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

El Reglamento de Medidas de Seguridad de los Ficheros Automatizados (Real Decreto 994/1999, de 11 de junio), que entró en vigor el 26/06/99, determina cuáles han de ser las medidas de índole técnica y organizativa que garanticen la integridad y seguridad de ficheros automatizados, centros de tratamiento, locales, equipos, sistemas, programas, así como de las personas que intervengan en el tratamiento automatizado de los datos.

La reciente aprobación del Reglamento de desarrollo de la LOPD (Real Decreto 1720/2007, de 21 de diciembre), plantea una revisión de estas medidas de seguridad y requiere asimismo una protección específica de los ficheros en soporte papel.

En el citado Reglamento se establecen tres “Niveles de Seguridad” para los datos de carácter personal:

- ***Nivel Básico***: de aplicación a todos los ficheros de datos de carácter personal.
- ***Nivel Medio***: de aplicación a los ficheros que contengan datos relativos a la comisión e infracciones, Hacienda Pública, ficheros de clientes de servicios financieros, ficheros de Entidades Gestoras y Servicios Comunes de la Seguridad Social, ficheros de mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social. Asimismo, se consideran dentro de este nivel aquellos ficheros que contengan un conjunto de datos de carácter personal que permitan obtener una evaluación de la personalidad del individuo.

- ***Nivel Alto***: de aplicación a los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual, así como los recabados para fines policiales.

No obstante, se podrán implantar las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos (nóminas, declaraciones IRPF, etc.).

Es importante la toma de conciencia de todas las personas con acceso a los datos de carácter personal de la necesidad de protección de los mismos, poniendo especial énfasis en la asignación de responsabilidades. El responsable del fichero tiene la obligación de implementar y verificar la normativa de seguridad, así como adoptar las medidas necesarias para que tanto la normativa como las consecuencias en caso de incumplimiento, sean conocidas por el personal afectado.

Con este fin, el Servicio de Informática y Nuevas Tecnologías de la Diputación Provincial de Ourense procede a la redacción del presente Documento de Seguridad, que contemplará, exclusivamente (a falta por determinar las medidas de seguridad que afectan a los ficheros no automatizados por parte del responsable de ficheros), las medidas que afectan al tratamiento de los ficheros automatizados de carácter personal, para su conocimiento y cumplimiento por el personal de la Institución con acceso a los mismos.

El presente Documento de Seguridad se mantiene en todo momento actualizado y es revisado siempre que se producen cambios relevantes en los Sistemas de Información o en la organización del mismo.

1.2. Identificación del Responsable del Fichero

Identificación del Responsable del Fichero	
Organización: *Diputación Provincial de Ourense*	***01/02/2015***
Se establece como Responsable del Fichero o del tratamiento la Diputación Provincial de Ourense, puesto que es el órgano administrativo que decide sobre la finalidad, contenido y uso del tratamiento.	

1.3. Identificación del Responsable de Seguridad

A falta de una designación específica del responsable o responsables de seguridad por parte del responsable de ficheros, y tomando como referencia las descripciones y especificación de funciones de los puestos de trabajo de la RPT actualmente vigente en esta Diputación, se considera oportuno incluir como responsables de seguridad las siguientes figuras:

Identificación del Responsable de Seguridad
Jefe del Servicio de Administración Electrónica
Técnico en Administración de Sistemas
Encargado de Redes Informáticas

Esta asignación de funciones, en ningún caso, supone una delegación de responsabilidades por parte del responsable de ficheros o tratamiento, ni implicará una mayor asunción de responsabilidades, más allá de las propias derivadas del ejercicio y desempeño del puesto de trabajo, cuyas funciones están recogidas en la Relación de Puestos de Trabajo de la Diputación Provincial de Ourense.

1.4. IDENTIFICACIÓN DE LOS RESPONSABLES PROPIETARIOS DE LOS FICHEROS

La figura del responsable propietario de ficheros no aparece en ninguno de los artículos del Reglamento no siendo obligatoria, por tanto, su existencia en este documento.

No obstante, atendiendo al carácter distribuido de los sistemas informáticos existente en la Diputación, se considera que esta figura toma una importancia relevante a la hora de exigir y aplicar las medidas de seguridad implantadas. Hará o pedirá, al servicio de Informática, que se habiliten los mecanismos necesarios para el buen uso de su fichero.

Cada uno de los responsables propietarios de los ficheros responderá, exclusivamente, ante la propia organización, mientras que la figura del responsable del fichero responderá también ante la Agencia Española de Protección de Datos.

IDENTIFICACIÓN DE LOS RESPONSABLE PROPIETARIOS DE LOS FICHEROS	
ORGANIZACIÓN: *DIPUTACIÓN PROVINCIAL DE OURENSE*	***01/02/2015***
Se establecen los siguientes Responsables Propietarios de los Ficheros:	
Cargo	***Departamento***	***Fichero***

ÁMBITO DE APLICACIÓN

2.1. ÁMBITO DE APLICACIÓN Y RECURSOS PROTEGIDOS

Las medidas de seguridad recogidas en el presente Documento de Seguridad son de aplicación:

2.1.1 Ámbito Jurídico

2.1.2 Ámbito Espacial.

A todas las áreas, servicios, negociados, departamentos y dependencias de la Excma. Diputación Provincial de Ourense.

2.1.3 Ámbito Personal.

Todas las personas, tanto empleados como entidades y profesionales contratados bajo otras modalidades cuando se especifique en sus contratos, que tengan acceso a los datos de los ficheros de carácter personal de la ***Excma. Diputación Provincial de Ourense***, bien a través del Sistema Informático habilitado para acceder al mismo, o bien a través de cualquier otro medio automatizado de acceso, se encuentran obligadas por ley a cumplir lo establecido en este documento, y sujetas a las consecuencias que pudieran incurrir en caso de incumplimiento.

Las normas internas contenidas en este documento se han puesto en conocimiento de todo el personal de la Entidad, con el objeto de dar debido cumplimiento a la Ley Orgánica 15/99, de 13 de Diciembre y al Real Decreto 1720/2007, de 21 de diciembre.

Una copia de este documento con la parte que le afecte será entregada, para su conocimiento, a cada persona autorizada a acceder a los datos del/de los ficheros, siendo requisito obligatorio para poder acceder a esos datos el haber firmado la recepción del mismo.

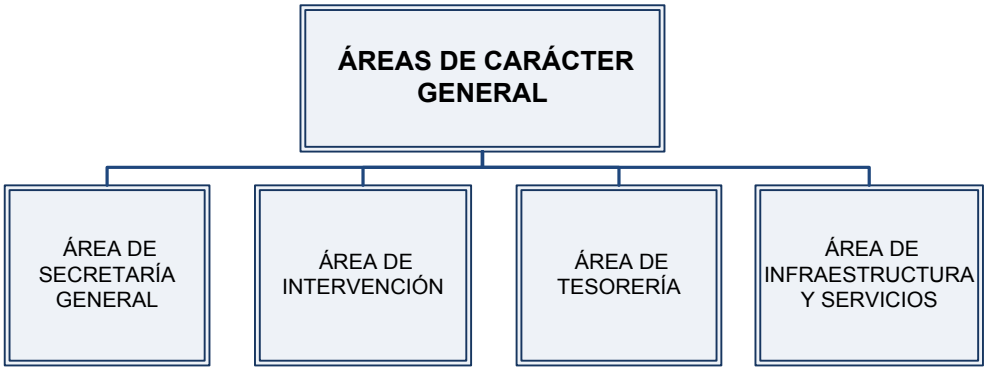
2.1.4 Ámbito de Contenidos.

Las bases de datos, ficheros automatizados, tratamientos, equipos, soportes, programas y sistemas, páginas Web, Intranet, red corporativa, servidores, terminales, ordenadores portátiles, etc.

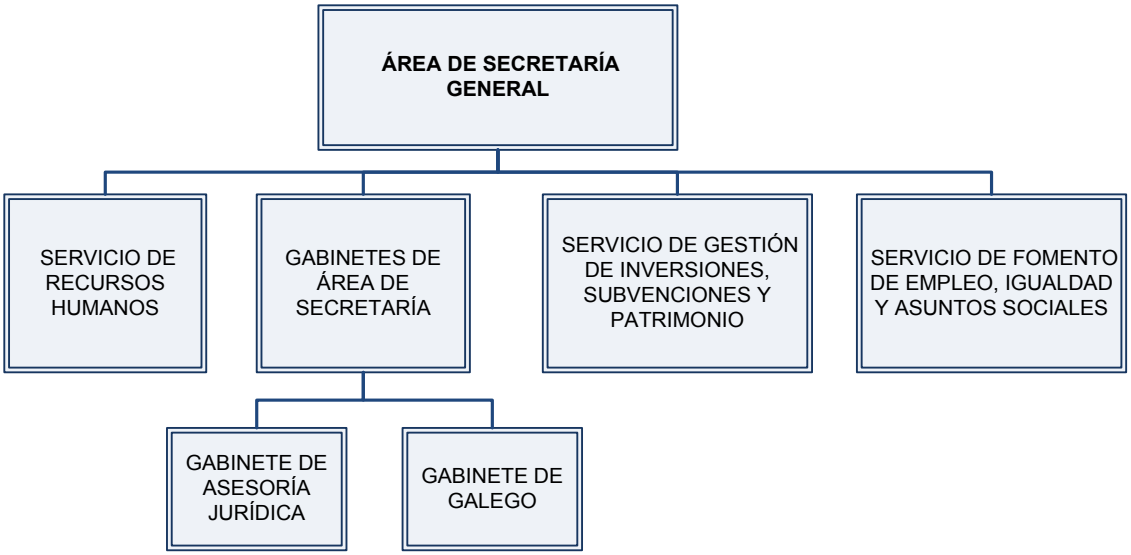
La protección de los datos de los ficheros frente a accesos no autorizados se deberá limitar mediante el control, a su vez, de todas las vías por las que se pueda tener acceso a dicha información. Las medidas de seguridad se aplicarán en función del nivel asignado al fichero correspondiente.

2.2. ORGANIGRAMA DE LA ORGANIZACIÓN

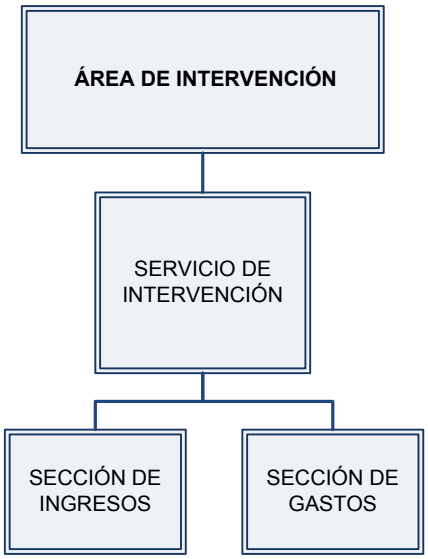
2.2.1. Organigrama General de la Diputación de Ourense



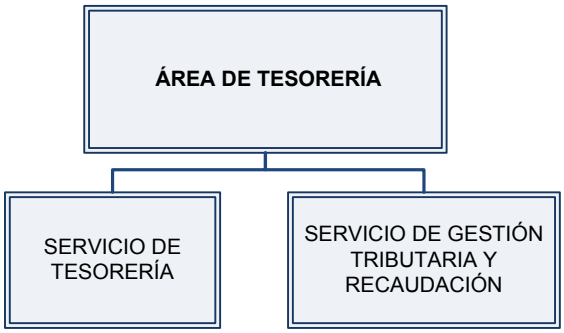
2.2.2. Área de Secretaría General



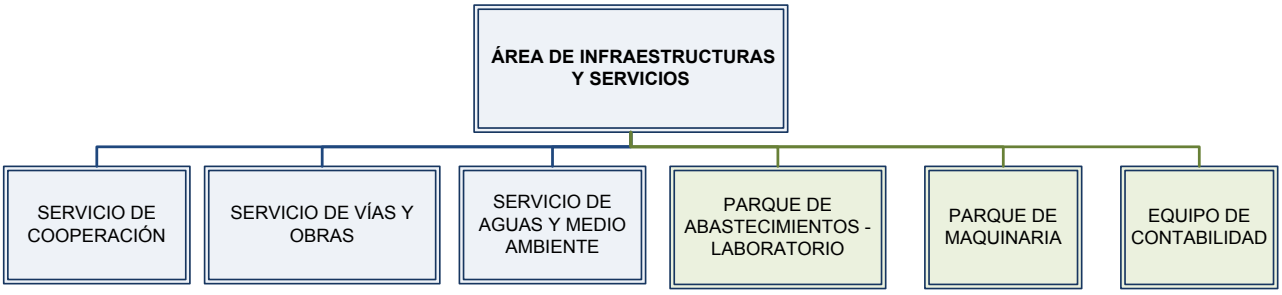
2.2.3. Área de Intervención



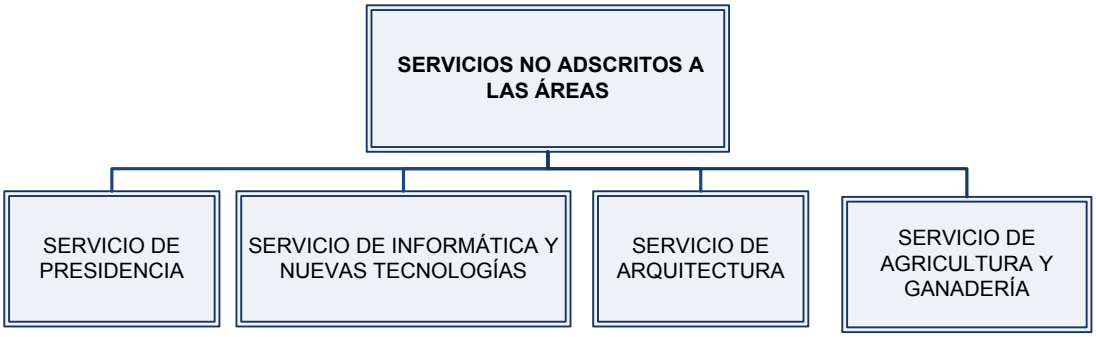
2.2.4. Área de tesorería



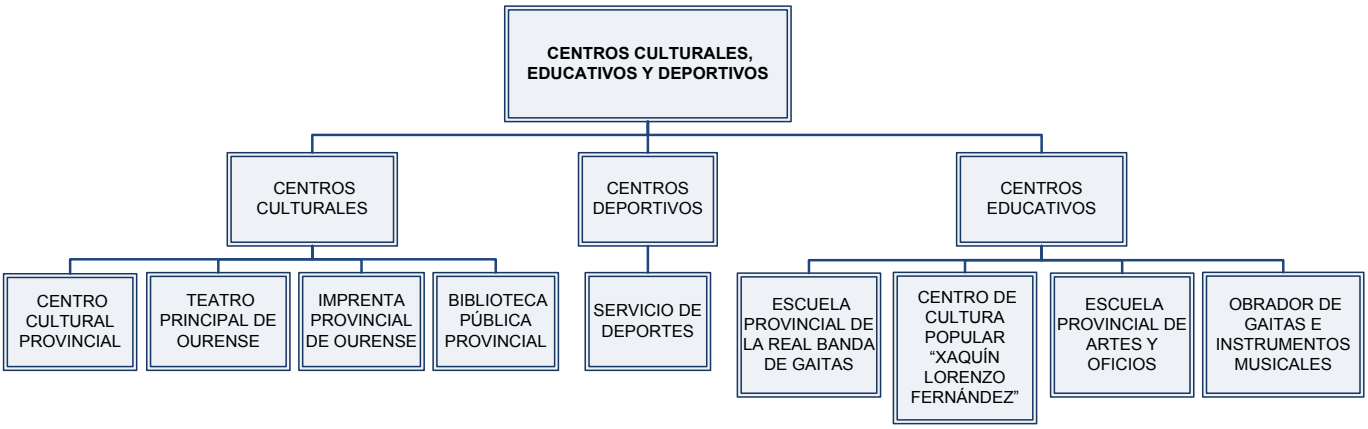
2.2.5. Área de Infraestructuras y Servicios



2.2.8. Servicios no Adscritos a las Áreas



2.2.9. Centros Culturales, Educativos y Deportivos



2.4. PRESTACIÓN DE SERVICIOS

La LOPD contempla la prestación de servicios de tratamiento automatizado de datos de carácter personal en su artículo 12:

«1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.»

Para la ***prestación de servicios***, la Excma. Diputación Provincial de Ourense dispone de la siguiente plantilla:

PRESTACIÓN DE SERVICIOS		
ORGANIZACIÓN: *DIPUTACIÓN PROVINCIAL DE OURENSE*		***01/02/2015***
Según el artículo 12.2 de la LOPD «la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. *En el contrato se estipularán, asimismo, las medidas de seguridad a aplicar, a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.* *3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.* *4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo a las infracciones en que hubiera incurrido personalmente. »*		
Encargado del tratamiento:		
Domicilio:	***Teléfono:***	***Fax:***
Ubicación de la instalación:	***Fecha:***	***Actividad:***
Ámbito de la prestación, estructura de los ficheros, descripción de los sistemas de información que los tratan, medidas de seguridad, procedimiento de copias de respaldo, etc. **(Nota: Se repetirán los datos anteriores tantas veces como encargados de tratamiento existan.)**		

2.5. ESTRUCTURA DE LOS FICHEROS DE DATOS DE CARÁCTER PERSONAL

En el ***Anexo I*** se describe la estructura de los ficheros automatizados con datos de carácter personal de la Diputación Provincial de Ourense.

Notas aclarativas sobre la interpretación de las fichas que describen los ficheros:

- En el campo ubicación del fichero se indica la localización física del fichero dentro de la red corporativa de la institución siguiendo este formato: Nombre de red del equipo\Directorio\Subdirectorio.
- En el campo departamentos que tienen acceso a las aplicaciones, se especifican los departamentos que tienen acceso habitual a las aplicaciones que trabajan con ficheros de datos de carácter personal. No obstante, también se puede producir la necesidad de un acceso esporádico por parte del departamento de Informática y Nuevas Tecnologías por razones de mantenimiento de las aplicaciones.

3.1. IDENTIFICACIÓN Y AUTENTICACIÓN PARA EL ACCESO A LA RED INFORMÁTICA

El Responsable de Seguridad custodia y actualiza la relación de todos los usuarios de la red que tienen acceso autorizado al sistema de información.

En el procedimiento de identificación y autenticación para el acceso a la red informática se llevan a cabo las siguientes tareas:

- Se dispone de un sistema de identificación por contraseñas contrastadas con un servidor central.
- Todos los usuarios del sistema tienen asignado un identificador y una contraseña. La contraseña tiene un número limitado mínimo de 6 caracteres alfanuméricos.
- El sistema de autenticación se basa en un entorno de clave de conexión de redes contrastada contra un servidor con Windows 2008 Server.
- El usuario introduce su identificador (que le identifica como usuario autorizado al acceso) y su contraseña (que le autentifica como el usuario identificado), que son verificados en el servidor, el cual le reconoce como usuario del sistema, permitiéndole acceder a los recursos de la red.

3.1.1. Procedimiento de asignación, distribución y almacenamiento de contraseñas para el acceso a la Red Informática

ASIGNACIÓN Y DISTRIBUCIÓN DE CONTRASEÑAS.

Es competencia del *Responsable de Seguridad*, que la atribución y asignación de contraseñas, así como la custodia de la relación de usuarios, se realice de forma que se garantice su confidencialidad e integridad.

La asignación de contraseñas se realiza por el propio usuario, quien determina su propia contraseña de acceso al sistema.

La distribución de las contraseñas se realizará de manera que ni siquiera el usuario pueda visualizar la clave asociada a su identificador. Esta visualización se produce por la entrada del símbolo asterisco en pantalla cada vez que se introduce un carácter en la misma.

ALMACENAMIENTO DE CONTRASEÑAS.

Durante el tiempo que estén vigentes, las contraseñas se almacenan de forma ininteligible mediante el propio sistema de encriptación que utiliza el Sistema Operativo.

CONTRASEÑAS SERVIDORES WEB.

Se dispone de dos servidores Web para alojar el portal web de la Diputación Provincial de Ourense, con todos sus servicios, los portales de los distintos centros adscritos (Centro Cultural, Pazo Deportes Paco Paz, Teatro Principal, etc.).

Las claves de administración de estos servidores se mantienen vigentes durante un mes y se almacenan en un sobre sellado, en la caja fuerte sita en las dependencias del *Servicio de Informática y Nuevas Tecnologías*. Al pasar este periodo, se procede al cambio de contraseña y al correspondiente cambio de sobre en la caja fuerte.

3.1.2. Identificadores y contraseñas son personales e intransferibles.

Los identificadores y contraseñas de acceso asignadas a cada usuario de la red corporativa de la Diputación, son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que se deriven del mal uso, divulgación o pérdida de los mismos.

3.1.3. Periodicidad de las contraseñas.

Las contraseñas de los usuarios autorizados se modifican en función de las necesidades del usuario. Se ha desarrollado un sistema de *Cambio de* Contraseñas, disponible en la Intranet de la entidad, para que los usuarios puedan proceder al cambio de contraseña. Por seguridad se recomienda cambiar la contraseña cómo mínimo de forma anual. Durante el tiempo que estén vigentes, las contraseñas se almacenarán de forma ininteligible.

3.1.4. Control de acceso a las aplicaciones

Una vez dentro de la red el usuario podrá acceder o no a recursos, dependiendo de las autorizaciones particulares y a los grupos a los que pertenezca. Los accesos que se habilitan son:

- ✓ Unidades compartidas a nivel de departamento.
- ✓ Aplicaciones que tratan información de carácter personal.

Además del control a través de privilegios de acceso a los recursos de la red, existen ciertas aplicaciones que tienen su propio sistema de autenticación por contraseña, o que se encuentran en un servidor cuyo sistema operativo también proporciona un sistema de autenticación particular.

El sistema de control de acceso a las aplicaciones empleado en cada caso particular, se especifica en el ***Anexo III***.

3.1.5. Control de acceso y confidencialidad de la información

1. Toda la información albergada en el sistema informático de la Diputación, de forma estática o en forma de mensajes de correo electrónico, es propiedad de la Entidad y tiene el carácter confidencial. Por ello, todo el personal con acceso a datos de carácter personal firma el "Compromiso de Confidencialidad", según ***Anexo I.***

2. Sólo el Responsable del fichero podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por la dirección de la entidad.

3.1.6. Gestión de Soportes

1. Únicamente el Responsable de Seguridad podrá autorizar la salida de soportes informáticos que contengan datos personales, fuera de los locales en los que esté ubicado el fichero.

2. Los soportes informáticos, que contengan datos de carácter personal, permitirán identificar el tipo de información que contienen, ser inventariados y almacenarse en armarios protegidos con cerraduras con llave y con acceso regulado por el Responsable de Seguridad.

3. Cuando un soporte que ha albergado datos de carácter personal vaya a ser reutilizado o desechado, se borra toda la información mediante su formateo o cualquier otro sistema que no permita su aprovechamiento. En el caso de que queden dudas sobre la información que pueda subsistir tras el proceso de borrado, se procederá a la inutilización física o a la destrucción del soporte.

4. Cuando los soportes salgan de las dependencias de la Entidad a causa de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

3.1.7. Origen de los Datos

Los datos con carácter personal provienen de: **Terceros y Personal de la institución**, que facilitan sus datos para la gestión de:

1. *Los servicios ofrecidos por la entidad.*
2. *El pago de sus servicios.*
3. *La contratación, nómina y sus derivados.*

Para garantizar la seguridad de estas fuentes y cumplir con los requisitos legales exigidos, los cuales salvaguardan los derechos de intimidad de los afectados, se establecen **cláusulas que recaban el consentimiento del afectado**, para todos los terceros y personal de la entidad.

Dentro de estas cláusulas, se contempla el informar a todos los afectados del tratamiento automatizado de sus datos, de los derechos que pueden ejercer por ser cedentes de datos, así como el nombre y dirección del Responsable del Fichero donde pueden ejercitar dichos derechos.

Así, la cláusula que se adjunta en los servicios ofrecidos por la entidad, establece:

PROTECCIÓN DE DATOS

El/Los firmantes queda/n informado/s de que los datos personales que se solicitan son necesarios para su formalización y gestión, y se incorporarán al correspondiente fichero de la DIPUTACIÓN para uso interno, y para la prestación de los servicios ofrecidos por esta Administración Pública, para lo cual da/n su autorización. El responsable de dicho fichero es la DIPUTACIÓN, cuyo domicilio figura en el presente documento, pudiendo el/los firmantes ejercitar los derechos de acceso, rectificación y cancelación de los datos obrantes en dicho fichero, en los términos establecidos en la Ley Orgánica 15/99, de 13 de diciembre, de Protección de Datos de Carácter Personal y demás normativa complementaria. El/Los firmante/s presta/n por tanto su conformidad a la recogida de datos, así como a la cesión, para las indicadas finalidades, que pueda ser realizada entre la DIPUTACIÓN y otras entidades relacionadas con la prestación de los servicios, en los términos previstos en la indicada Ley.

A continuación, se presenta la cláusula que informa a los trabajadores de la entidad del tratamiento de sus datos y adjunta en todos los contratos de personal:

"De acuerdo con lo establecido en la Ley Orgánica 15/1999, el Trabajador, queda informado de la incorporación de sus datos a los ficheros existentes en la institución. Asimismo, queda informado del tratamiento a que van a ser sometidos todos sus datos a los que la Institución tenga acceso como consecuencia de la relación laboral, para las finalidades de gestión de nóminas y gestión de personal, así como cualquier otra gestión que genere dicha relación laboral. El Trabajador tiene derecho a oponerse al tratamiento de cualquiera de sus datos que no sean imprescindibles para la gestión de nóminas y gestión de personal y a su utilización para cualquier finalidad distinta del mantenimiento de la misma.

El Trabajador queda, igualmente informado sobre la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición, en los términos establecidos en la legislación vigente. El responsable del fichero es: DIPUTACIÓN con domicilio en C/ Progreso, 32 de Ourense, donde el afecto también se podrá dirigir por escrito en el caso de que lo encontrara necesario.

El Trabajador presta por tanto su conformidad a la recogida de datos, así como a la cesión para las indicadas finalidades que pueda ser realizada entre la Entidad y otras sociedades relacionadas con la gestión del personal de la institución (tales como entidades financieras, mutuas o entidades de seguro, etc.) objeto de la relación laboral o auxiliares de éstas en los términos previstos en la indicada Ley."

3.1.8. Comunicación de Datos

La comunicación de datos debe estar autorizada. Siempre que se comuniquen datos de carácter personal es necesario comprobar que se al propio afectado, o a entidades previamente autorizadas por el Responsable de Seguridad a través de su firma. Es necesario:

- ✓ Identificar con una leyenda, el carácter de los datos.
- ✓ Especificar claramente el destinatario autorizado para recibir y acceder a los datos.

Todo ello se consigue mediante la siguiente Leyenda, adjunta a todo soporte que de salida a datos de carácter personal de los ficheros de la Entidad.

***AVISO SOBRE CONFIDENCIALIDAD**: Este Documento o Soporte se dirige Exclusivamente a su Destinatario por poder contener Información Confidencial o cuya divulgación debe estar autorizada en virtud de la Legislación Vigente. Se informa a quien lo recibiera sin ser el destinatario o persona Autorizada por éste, que la información contenida en el mismo es **reservada** y su utilización o divulgación con cualquier fin está **prohibida**. Si ha recibido este documento por error, le rogamos que nos lo comunique por teléfono y proceda a su destrucción.*

En el caso en el que se contraten servicios externos que impliquen el acceso o utilización temporal de cualquier fichero de datos personales que se encuentren bajo la responsabilidad de la Diputación se procede según lo estipulado en *IS-01-01 "Régimen de Contratación de Servicios Externos"*.

FUNCIONES Y OBLIGACIONES DEL PERSONAL

4.1. INTRODUCCIÓN

La Excma. Diputación Provincial de Ourense, con el fin de conseguir un eficaz cumplimiento de las funciones y obligaciones del personal mencionadas en el presente documento y relacionadas con la normativa vigente en materia de tratamiento de datos automatizados y seguridad de los sistemas informáticos, ha establecido un conjunto de ***normas internas*** que contemplan los deberes de los trabajadores en la utilización de los equipos y servicios informáticos de la institución.

Dicho conjunto de normas son de obligado conocimiento y aceptación por parte de los trabajadores que tienen acceso a los equipos y servicios informáticos. A continuación se presentan una serie de funciones y obligaciones generales y en apartados posteriores se concretarán las mismas para las figuras más relevantes.

4.2. REGLAMENTO GENERAL

El artículo 89 del Reglamento establece que:

1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.
   También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.
2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

En los modelos que vienen a continuación se desarrollan las funciones y obligaciones de las siguientes figuras:

- ✓ Responsable del fichero.
- ✓ Responsable de Seguridad.
- ✓ Usuario.
- ✓ Responsable propietario de los ficheros.
- ✓ Director de Sistemas de Información.
- ✓ Personal Informático:
- ✓ Personal de desarrollo.
- ✓ Administrador de Seguridad.
- ✓ Administrador del Sistema.

En organizaciones medias y pequeñas dentro de la figura de usuario se podrían incluir las de: responsable propietario de los ficheros, Director de Sistemas de Información y personal informático.

4.3. RESPONSABLE DEL FICHERO

A continuación se describen las principales funciones y obligaciones del responsable del fichero.

4.3.1. Funciones

Nivel básico

- ✓ Decidir sobre la finalidad, contenido y uso del tratamiento (artículo 3.d Ley).
- ✓ Autorizar la ejecución del tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero.
- ✓ Elaborar el Documento de Seguridad.
- ✓ 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.
- ✓ Se encargará de que exista una relación actualizada de usuarios que tengan acceso autorizado al Sistema de Información.
- ✓ Establecerá los procedimientos de identificación y autenticación para dicho acceso.
- ✓ Establecerá los mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.
- ✓ Establecerá los criterios con que el personal autorizado para ello conceda, altere o suprima el acceso a los ficheros que contengan datos de carácter personal y los recursos.
- ✓ Será quien únicamente pueda autorizar la salida fuera de los locales en que esté ubicado el fichero, de soportes informáticos que contengan datos de carácter personal.
- ✓ Verificará la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y recuperación de datos).
- ✓ Resolver sobre la petición de acceso en el plazo de un mes a contar desde la recepción de la solicitud.
- ✓ Resolver sobre la petición de rectificación o cancelación en el plazo de diez días a partir de la recepción de la solicitud.
- ✓ Proceder al bloqueo de los datos en los casos en que, siendo procedente su cancelación, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado.
- ✓ Formular las alegaciones que considere pertinentes cuando la Agencia Española de Protección de Datos le dé traslado de la reclamación de un afectado.

Nivel Medio

- ✓ Designar uno o varios responsables de seguridad.

4.3.2. Obligaciones

Nivel básico

- ✓ Excluirá el tratamiento de los datos relativos al afectado que ejercite su derecho de oposición.
- ✓ Adoptará las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural (artículo 9 Ley).
- ✓ Está obligado al secreto profesional y al deber de custodia, respecto de los datos de carácter personal de la instalación (artículo 10 Ley).

- ✓ Hará efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días (artículo 16.1 Ley).
- ✓ Si los datos rectificados o cancelados hubieran sido comunicados previamente, deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por esto último, que deberá proceder a la rectificación o cancelación, en su caso (artículo 16.4 Ley).
- ✓ En el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados (artículo 27.1 Ley).

Nivel Medio

- ✓ Adoptar las medidas correctoras adecuadas según las deficiencias detectadas en la auditoría.
- ✓ 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.
- ✓ Autorizar por escrito la ejecución de los procedimientos de recuperación de datos.

4.4. Funciones y Obligaciones del Responsable de Seguridad

A continuación se describen las principales funciones y obligaciones del responsable de seguridad, que pueden ser uno o varios y no tiene delegada la responsabilidad que le corresponde al responsable del fichero.

4.3.1. Funciones

Nivel Medio

- ✓ Coordinar y controlar las medidas definidas en el Documento de Seguridad.
- ✓ Analizar los informes de auditoría.

Nivel Alto

- ✓ Controlar los mecanismos que permiten el control de accesos.

4.4.2. Obligaciones

Nivel Medio

- ✓ Elevar al responsable del fichero las conclusiones del análisis del informe de auditoría.
- ✓ Guardar secreto de los datos de carácter personal que pueda conocer, así como sobre los controles y posibles debilidades, incluso después de haber causado baja en la entidad (artículo 10 Ley).

Nivel Alto

- ✓ Revisar periódicamente la información de control registrada.
- ✓ Mensualmente elaborará un informe de las revisiones efectuadas.

- ✓ Conocer la normativa interna en materia de seguridad, y especialmente la referente a protección de datos de carácter personal.
- ✓ Conocer las consecuencias que se pudieran derivar y las responsabilidades en que se pudiera incurrir en caso de incumplimiento de la normativa, que podrían derivar en sanciones.

4.5. Funciones y Obligaciones de los Responsables Propietarios de los Ficheros

A continuación se describen las principales funciones y obligaciones de los responsables propietarios de los ficheros.

4.5.1. Funciones

- ✓ Determinará quién puede acceder a los datos de carácter personal y que sean necesarios para la función que realice.
- ✓ Autorizará la realización de nuevos formularios de recogida de datos dentro de su Servicio de forma que lleven incorporada la leyenda informativa, la cual tendrá que ser elaborada por Asesoría Jurídica.
- ✓ Informará de la necesidad de creación de nuevos ficheros, con anterioridad a la misma, para poder desarrollar las funciones del departamento, de cara a que Asesoría Jurídica ponga en marcha, en su caso, el procedimiento para inscribirlo en la AEPD y solicitar el consentimiento si fuese necesario.
- ✓ Informará de la necesidad de realizar nuevas cesiones de datos de carácter personal para que Asesoría Jurídica pudiese evaluar si es necesario el consentimiento.
- ✓ Informará en el caso de actuar la Excma. Diputación Provincial de Ourense como cesionario de datos de carácter personal para que Asesoría Jurídica evaluase en función del origen de la información, su legalidad.
- ✓ Estará al tanto del tratamiento de datos especialmente protegidos, en su caso, o la necesidad de añadir nuevos para poner en marcha los procedimientos pertinentes.

4.5.2. Obligaciones

- ✓ Velará porque se concedan y revoquen oportunamente las autorizaciones para acceder a los datos de los cuales sea responsable.
- ✓ Guardará secreto de la información de carácter personal que conozca en el desempeño de su función aun después de haber abandonado la organización (artículo 10 Ley).

4.6. Funciones y Obligaciones del Director de Sistemas de Información

A continuación se describen las principales funciones y obligaciones del director de sistemas de información.

4.6.1. Funciones

- ✓ Definir la arquitectura de sistemas de información más adecuada para la organización, teniendo en cuenta la evolución tecnológica y la introducción de nuevos productos y servicios.

- ✓ Dirigir las actividades de desarrollo, mantenimiento y soporte técnico y explotación informáticos para garantizar el servicio a los cliente internos y externos
- ✓ Elaborar, ejecutar y controlar los planes de inversión en sistemas de información, coordinando con las diferentes áreas las prioridades y las disponibilidades.
- ✓ Participar en los planes de protección de datos e información no automatizados, en sus diferentes soportes, y tanto en transmisión como en proceso y almacenamiento.
- ✓ Acceder a los datos y documentos a que esté autorizado.

4.6.2. Obligaciones

- ✓ Contribuir a asegurar la confidencialidad, integridad y disponibilidad de la información en lo que a las Tecnologías de la Información y las Comunicaciones se refiere.
- ✓ Garantizar la implantación de las metodologías de desarrollo y mantenimiento de los sistemas informáticos.
- ✓ Guardar secreto de la información de carácter personal que conozca en el desempeño de su función, independientemente del soporte en que esté.
- ✓ Conocer la normativa interna en materia de seguridad, y especialmente la referente a la protección de datos de carácter personal.
- ✓ Cumplir lo dispuesto en la normativa interna vigente en cada momento.

4.7. FUNCIONES Y OBLIGACIONES DEL PERSONAL INFORMÁTICO

A continuación se describen las principales funciones y obligaciones del personal informático.

4.7.1. Funciones Personal de Desarrollo

- ✓ Se encarga del desarrollo y mantenimiento de las aplicaciones de la organización. Puede necesitar acceder a los ficheros para la resolución de problemas, pruebas de los desarrollos y excepcionalmente posibles modificaciones en el entorno de producción.
- ✓ Introducir en las aplicaciones los controles necesarios, tanto preventivos como de detección, según el tipo de datos a tratar y su nivel.
- ✓ Modificar sólo los programas para los que existe autorización previa, para introducir o adaptar exclusivamente la funcionalidad aprobada, todo ello de acuerdo con la normativa y estándares, y sin perjuicio de los controles que existan respecto al paso de los programas al entorno de aceptación o de explotación.

4.7.2. Obligaciones Personal de Desarrollo

- ✓ No realizar pruebas con datos reales que puedan identificar a personas físicas en los casos en que por su clasificación así lo determine la normativa interna, salvo que exista el nivel de seguridad exigido.
- ✓ Conocer la normativa interna en materia de seguridad, y especialmente la referente a la protección de datos de carácter personal.
- ✓ Cumplir lo dispuesto en la normativa interna vigente en cada momento.

- ✓ Conocer las consecuencias que se pudieran derivar y las responsabilidades en que se pudiera incurrir en caso de incumplimiento de la normativa, que podrían derivar en sanciones.
- ✓ Utilizar los controles y medidas que se hayan establecido para proteger tanto los datos de carácter personal como los propios sistemas de información y sus componentes: los ficheros automatizados, los programas, los soportes y los equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.
- ✓ No intentar saltar los mecanismos y dispositivos de seguridad, evitar cualquier intento de acceso no autorizado a los datos o recursos, informar de posibles debilidades en los controles, y no poner en peligro la disponibilidad de los datos ni la confidencialidad o integridad de los mismos.
- ✓ Guardar secreto sobre los datos que pueda conocer, así como sobre los controles y posibles debilidades, incluso después de haber causado baja en la entidad (artículo 10 Ley).

4.7.3. Funciones Administrador de Seguridad

- ✓ Como administrador de todos los accesos a los ficheros y recursos de la instalación pueden tener per se acceso a los mismos.
- ✓ Llevar a cabo las actividades de administración de la seguridad mediante la gestión de perfiles y controles de acceso.
- ✓ Verificar que las medidas de seguridad física y lógica implantadas protegen los datos de carácter personal, y mantener informado al responsable de seguridad.
- ✓ Colaborar en la identificación de los datos especialmente susceptibles de protección, según los modelos de clasificación que existan.
- ✓ Analizar posibles transgresiones e irregularidades en los accesos, e informar, en su caso, al responsable de seguridad.
- ✓ Evaluar la seguridad de paquetes, aplicaciones, productos y dispositivos, antes de su adquisición o implantación.
- ✓ Dar soporte técnico en materia de seguridad, a los desarrolladores, técnicos y usuarios en general.
- ✓ Coordinar aspectos de seguridad con Administradores/Técnicos de Sistemas, Técnicos de Comunicaciones, Administradores de Bases de Datos, Desarrolladores y Usuarios en general.

4.7.4. Obligaciones Administrador de Seguridad

- ✓ Conocer la normativa interna en materia de seguridad, y especialmente la referente a protección de datos de carácter personal. Dicha normativa puede consistir en: normas, procedimientos, reglas y estándares, así como posibles guías.
- ✓ Cumplir lo dispuesto en la normativa interna vigente en cada momento.
- ✓ Conocer las consecuencias que se pudieran derivar y las responsabilidades en que pudiera incurrir en caso de incumplimiento de la normativa, que podrían derivar en sanciones.
- ✓ Utilizar los controles y medidas que se hayan establecido para proteger tanto los datos de carácter personal como los propios sistemas de información y sus componentes: los ficheros automatizados, los programas, los soportes y los equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.
- ✓ No intentar saltar los mecanismos y dispositivos de seguridad, evitar cualquier intento de acceso no autorizado de datos o recursos, informar de posibles debilidades en los controles, y

no poner en peligro la posibilidad de los datos, ni la confidencialidad o integridad de los mismos.

- ✓ Guardar secreto sobre los datos que pueda conocer, así como sobre controles y posibles debilidades, incluso después de haber causado baja en la entidad.
- ✓ Usar de forma adecuada según la normativa los mecanismos de identificación y autenticación ante los sistemas de información, tanto sean contraseñas como sistemas más avanzados: biométricos u otros, y en ambos casos: mediante acceso local o mediante redes de comunicaciones, cuando está así previsto. En el caso de contraseñas cumplir lo recogido en la normativa, especialmente en cuanto a asignación, sintaxis, distribución, custodia y almacenamiento de las mismas, así como el cambio con la periodicidad que se termine.

4.7.5. Obligaciones

- ✓ Conocer la normativa interna en materia de seguridad, y especialmente la referente a protección de datos de carácter personal. Dicha normativa puede consistir en: políticas, normas, procedimientos, reglas y estándares, así como posibles guías.
- ✓ Cumplir lo dispuesto en la normativa vigente en cada momento.
- ✓ Conocer las consecuencias que se pudieran derivar y las responsabilidades en que pudiera incurrir en caso de incumplimiento de la normativa, que podrían derivar en sanciones.
- ✓ Utilizar los controles y medios que se hayan establecido para proteger tanto los datos de carácter personal como los propios sistemas de información y sus componentes: los ficheros automatizados, los programas, los soportes u los equipos empleados para almacenamiento y tratamiento de datos de carácter personal.
- ✓ No intentar saltar los mecanismos y dispositivos de seguridad, evitar cualquier intento de acceso no autorizado a datos o recursos, informar de posibles debilidades en los controles, y no poner en peligro la disponibilidad de los datos, ni la confidencialidad o integridad de los mismos,
- ✓ Guardar secreto sobre los datos que pueda conocer, así como sobre controles y posibles debilidades, incluso después de haber causado baja en la entidad.
- ✓ Usar de forma adecuada según la normativa los mecanismo de identificación y autenticación ante los sistemas de información, tanto sean contraseñas como sistemas más avanzados: biométricos y otros y en ambos casos: mediante acceso local o a través de redes de comunicaciones, cuando esté así previsto. En el caso de contraseñas cumplir lo recogido en la normativa, especialmente en cuanto a asignación, sintaxis, distribución, custodia y almacenamiento de las mismas, así como el cambio con la periodicidad que se determine.
- ✓ No ceder ni comunicar a otros las contraseñas, que son personales, que no estarán almacenadas en claro, y que serán transmitidas por canales seguros; los usuarios serán responsables ante la entidad de todos los accesos y actividades que se puedan haber realizado utilizando su código de usuario y contraseña.
- ✓ Evitar transmitir o comunicar datos considerados sensibles por medios poco fiables sin protección (telefonía de voz, correo electrónico, fax).
- ✓ Realizar las copias de los datos que en cada caso se establezcan en la normativa así como proteger las copias obtenidas.
- ✓ Cumplir la normativa en cuanto a gestión de soportes informáticos que contengan datos de carácter personal, así como tomar precauciones en el caso de soportes que vayan a desecharse o ser reutilizados, mediante la destrucción, inutilización o custodia. En el caso de averías que

requieran su transporte fuera de las instalaciones se intentará borrar previamente su contenido o se exigirán garantías escritas de que se hará así.

- ✓ No sacar equipos o soportes de las instalaciones sin la autorización necesaria, y en todo caso con los controles que se hayan establecido.

4.8. Funciones y Obligaciones de los Usuarios de la Organización

A continuación se describen las principales funciones y obligaciones de los usuarios de la organización, las cuales afectarán a cada uno en función de su puesto de trabajo.

4.8.1. Funciones

- ✓ Accederá a los datos de carácter personal a los que esté autorizado necesarios para la función que realice.
- ✓ Realizará las funciones propias del puesto de trabajo.

4.8.2. Obligaciones

- ✓ Guardar secreto de la información de carácter personal que conozca en el desempeño de su función aún después de haber abandonado la organización (artículo 10 Ley).
- ✓ Conocer la normativa interna en materia de seguridad, y especialmente la referente a protección de datos de carácter personal. Dicha normativa puede consistir en: normas, procedimientos, reglas y estándares, así como posibles guías.
- ✓ Cumplir lo dispuesto en la normativa interna vigente en cada momento.
- ✓ Conocer las consecuencias que se pudieran derivar y responsabilidades en que pudiera incurrir en caso de incumplimiento de la normativa, que podrían derivar en sanciones.
- ✓ No intentar saltar los mecanismos y dispositivos de seguridad, evitar cualquier intento de acceso no autorizado a datos o recursos, informar de posibles debilidades en los controles, y no poner en peligro la disponibilidad de los datos, ni la confidencialidad o integridad de los mismos.
- ✓ Usar de forma adecuada según la normativa los mecanismos de identificación y autenticación ante los sistemas de información, tanto sean contraseñas como sistemas más avanzados: biométricos u otros, y en ambos casos: mediante acceso local o a través de redes de comunicaciones, cuando esté así previsto. En el caso de contraseñas cumplir lo recogido en la normativa, especialmente en cuanto a asignación, sintaxis, distribución, custodia y almacenamiento de las mismas, así como el cambio con la periodicidad que se determine.
- ✓ No utilizar el correo electrónico u otros medios de comunicación interna o con el exterior para transmitir mensajes que contengan o lleven adjuntos datos de carácter personal que por sus características, volumen o destinatarios pueden poner en peligro la confidencialidad o la integridad de los datos.
- ✓ No realizar transferencias de ficheros con datos de carácter personal entre sistemas o descargas en equipos salvo en los casos expresamente autorizados, y protegiendo después los contenidos para evitar difusión o copias no autorizadas.
- ✓ Dirigir a impresoras protegidas los listados que contengan datos de carácter personal que requieran protección, y recogerlos con celeridad para evitar su difusión, copia o sustracción.

- ✓ No sacar equipos o soportes de las instalaciones sin autorización necesaria, y en todo caso con los controles que se hayan establecido.
- ✓ Proteger los datos personales de la entidad que excepcionalmente tuvieran que almacenarse o usarse fuera del lugar de trabajo: en clientes, en el propio domicilio o en otras instalaciones alternativas tanto en sistemas fijos como en portátiles.
- ✓ Salir de los ordenadores personales o terminales cuando vaya a estar ausente de su puesto durante un tiempo superior al fijado en los procedimientos par cada caso, de modo que el sistema le pida alguna clave.
- ✓ Entregar cuando se le requiera por la Dirección, y especialmente cuando vaya a causar baja en la entidad, las claves, tarjetas de identificación, material, documentación, equipos, contraseñas y cuantos activos sean propiedad de la entidad.
- ✓ Para el resto del personal de la Excma. Diputación Provincial de Ourense nos remitiremos a la descripción de puestos de trabajo y a la información que existe en el Departamento de Recursos Humanos.

DOCUMENTACIÓN AGENCIA DE PROTECCIÓN DE DATOS

5.1. INTRODUCCIÓN

La aplicación práctica de la Ley Orgánica 15/1999, de 13 de diciembre, de *Protección de Datos de carácter Personal*, obliga al intercambio de una serie de documentos con la Agencia Española de Protección de Datos. En ningún artículo del Reglamento se obliga a que dicha documentación forme parte del Documento de Seguridad, pero sí es conveniente hacerlo.

En los apartados que se presentan a continuación, se muestran los modelos que dispone la ***Excma. Diputación Provincial de Ourense*** para almacenar la información relevante.

5.2. NOTIFICACIONES DE ALTAS, BAJAS Y MODIFICACIONES.

NOTIFICACIONES DE ALTAS, BAJAS Y MODIFICACIONES		
ORGANIZACIÓN: DIPUTACIÓN PROVINCIAL DE OURENSE		*01/02/2015*
Nombre del Fichero	**Tipo de Notificación**	**Fecha de la Operación**

5.3. OFICIOS DE INSCRIPCIÓN

OFICIOS DE INSCRIPCIÓN		
ORGANIZACIÓN: DIPUTACIÓN PROVINCIAL DE OURENSE		*01/02/2015*
Nombre del Fichero	**Tipo de Notificación**	**Fecha de la Operación**

5.4. PUBLICACIÓN EN EL DIARIO OFICIAL (SÓLO FICHEROS DE TITULARIDAD PÚBLICA)

PUBLICACIÓN EN DIARIO OFICIAL (FICHEROS TITULARIDAD PÚBLICA)		
ORGANIZACIÓN: DIPUTACIÓN PROVINCIAL DE OURENSE		*01/02/2015*
Nombre del Fichero	**Tipo de Notificación**	**Fecha de la Operación**

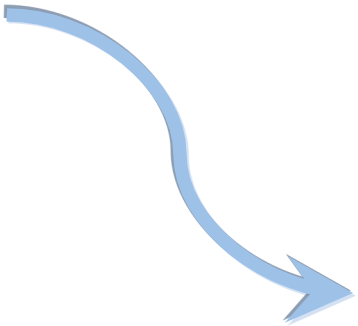
5.5. ACTUACIÓN ANTE EL EJERCICIO DE UN DERECHO POR EL INTERESADO

ACTUACIÓN ANTE EL EJERCICIO DE UN DERECHO DEL INTERESADO	
ORGANIZACIÓN: ***DIPUTACIÓN PROVINCIAL DE OURENSE***	***01/02/2015***

El sistema debe ser conocido por todo el personal de atención al público o de recepción de correo postal, telegramas, e-mail.

Envío urgente

Recepción de la Petición



Asesoría Jurídica o persona encargada de la atención en la AEPD

LEGISLACIÓN VIGENTE

6.1. LEGISLACIÓN DE PROTECCIÓN DE DATOS

No existe obligación de archivar dentro del Documento de Seguridad la Legislación vigente sobre protección de datos, pero se ha considerado oportuno incluirla, para que sirva de ayuda a los depositarios no juristas del mismo.

- *Real Decreto 428/1993*, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos (subsistente según la disposición transitoria tercera de la LOPD).
- *Real Decreto 1332/1994*, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de carácter personal (subsistente según la disposición transitoria tercera de la LOPD).
- *Ley Orgánica 15/1999*, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).
- *Sentencia del Tribunal Constitucional número 290/2000*, de 30 de noviembre (BOE número 4, de 4 de enero de 2001).
- *Sentencia del Tribunal Constitucional número 292/2000*, de 30 de noviembre (BOE número 4, de 4 de enero de 2001).
- *Resolución*, de 30 de mayo de 2000, de la Agencia Española de Protección de Datos, por la que se aprueban los modelos normalizados en soporte papel, magnético y telemático a través de los que deberán efectuarse las solicitudes de inscripción en el Registro General de Protección de Datos.
- *Instrucción 1/2000*, de 1 de diciembre, de la Agencia Española de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos.
- *Real Decreto 1720/2007*, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

GLOSARIO DE TÉRMINOS DE PROTECCIÓN DE DATOS

A continuación figuran, por orden alfabético, las definiciones aparecidas en el Convenio 108 del Consejo de Europa, la Ley Orgánica 15/1999. Real Decreto 1332/1994, Resolución de 22 de junio, Directiva 95/46/CE, Reglamento 1720/2007 e Instrucción 1/2000.

GLOSARIO DE TÉRMINOS DE PROTECCIÓN DE DATOS	
ORGANIZACIÓN: DIPUTACIÓN PROVINCIAL DE OURENSE	***01/02/2015***
TÉRMINO	**DEFINICIÓN**
Accesos autorizados	Autorizaciones concedidas a un usuario para la utilización de los diversos recursos.
Afectado	Persona física titular de los datos que sean objeto del tratamiento automatizado.
Autenticación	Procedimiento de comprobación de la identidad de un usuario.
Bloqueo de datos	La identificación y reserva de datos con el fin de impedir su tratamiento.
Cesión de datos	Toda revelación de datos realizada a una persona distinta del interesado. Toda obtención de datos resultante de la consulta de un fichero, la publicación de los datos contenidos en el fichero, su interconexión con otros ficheros y la comunicación de datos realizada por una persona distinta de la afectada.
Comunicación de datos	Toda revelación de datos realizada a una persona distinta del interesado.
Consentimiento del interesado	Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consiente el tratamiento de datos personales que le conciernen. Toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consiente el tratamiento de datos personales que le conciernan.
Contraseña	Información confidencial frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.
Control de acceso	Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.
Copia de respaldo	Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.
Datos accesibles al público	Los datos que se encuentran a disposición del público en general, no impedida por cualquier norma limitativa, y están recogidos en medios tales como censos, anuarios, bases de datos públicas, repertorios de jurisprudencia, archivos de prensa, repertorios telefónicos o análogos, así como los datos publicados en forma de listas de personas pertenecientes a grupos profesionales que contengan únicamente los nombres, títulos, profesión, actividad, grados académicos, dirección e indicación de su pertenencia al grupo. Los datos que figuren en censos, anuarios, bases de datos públicas, repertorios telefónicos o análogos, así como los datos publicados en forma de listas de personas pertenecientes a grupos profesionales que contengan únicamente los

	nombres, títulos, profesión, actividad, grados académicos, dirección e indicación de su pertenencia al grupo.
Datos de carácter personal	Cualquier información concerniente a personas físicas identificadas o identificables. Toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable. Significa cualquier información relativa a una persona física identificada o identificable.
Datos personales	Toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular, mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.
Destinatario	La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios. Persona física o jurídica, pública o privada, situada fuera del territorio español que recibe los datos transferidos (Instrucción).
Encargado del tratamiento	La persona física o jurídica, autoridad pública o servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento. La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.
Fichero	Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
Fichero automatizado	Todo conjunto organizado de datos de carácter personal que sean objeto de un tratamiento automatizado cualquiera que fuera la forma o modalidad de su creación, almacenamiento, organización y acceso. Significa cualquier conjunto de informaciones que sea objeto de un tratamiento automatizado.
Fichero de datos personales	Todo conjunto estructurado de datos personales accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado, o repartido de forma funcional o geográfica.
Fuentes accesibles al público	Aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación.
Identificación	Procedimiento de reconocimiento de la identidad de un usuario.
Identificación del afectado	Cualquier elemento que permita determinar directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de la persona física afectada.
Incidencia	Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

Interesado	Persona física titular de los datos que sean objeto del tratamiento.
Recurso	Cualquier parte componente de un sistema de información.
Responsable del fichero o tratamiento	Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.
Responsable de seguridad	Persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.
Responsable del tratamiento	La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o conjuntamente con otros determine los fines y los medios del tratamiento de los datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario.
Sistema de información	Conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.
Soporte	Objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.
Tercero	La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento.
Transferencia de datos	El transporte de datos entre sistemas informáticos por cualquier medio de transporte, así como el transporte de soportes de datos por correo o por cualquier otro medio convencional.
Transferencia internacional de datos	Transporte de datos entre sistemas informáticos por cualquier medio de transmisión así como el transporte de soportes de datos por correo o por cualquier otro medio convencional. Toda transmisión de los mismos fuera del territorio español. En particular se consideran como tales las que constituyan una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero.
Tratamiento automatizado	Se entiende las operaciones que a continuación se indican efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados: registro de datos, aplicación de esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión.
Tratamiento de datos personales (tratamiento)	Cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados y aplicables a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.
Usuario	Sujeto o proceso autorizado para acceder a datos o recursos.

ANEXO I. COMPROMISO DE CONFIDENCIALIDAD

COMPROMISO DE CONFIDENCIALIDAD	
ORGANIZACIÓN: *DIPUTACIÓN PROVINCIAL DE OURENSE*	***01/02/2015***

Don/Doña:

Se compromete, durante su relación laboral con la Excma. Diputación Provincial de Ourense a:

- *Conocer y cumplir lo establecido en el Documento de Seguridad de Datos Personales así como en otros documentos de régimen interior en la medida que le sean aplicables, por la naturaleza de las actividades, funciones y responsabilidades que se le encomienden.*
- *No realizar ninguna actividad que sea incompatible con su independencia de juicio e integridad profesional en relación con las actividades de la DIPUTACIÓN.*
- *Mantener absoluta confidencialidad y discreción sobre la información obtenida en el ejercicio de su trabajo acerca de las actividades de la institución, de sus clientes, personal y organismos relacionados. Especialmente en lo que se refiere a Datos de Carácter Personal, incluso tras la extinción de su relación laboral con la Entidad.*
- *Observar y cumplir los criterios establecidos en el Documento de Seguridad, en lo que se refiere a "Funciones y Obligaciones del Personal".*

En Ourense, a de de	*Firmado:*

ANEXO II. INFORME DE INCIDENCIAS

AII.1. INTRODUCCIÓN

La ***Excma. Diputación Provincial de Ourense*** dispone de un procedimiento de notificación, gestión y respuesta de las incidencias, entendiendo por "*incidencia*" cualquier anomalía que afecte o pueda afectar a la seguridad de los datos, tales como pérdida o deterioro de datos en cualquier transmisión, caída de los Sistemas informáticos, pérdida de cualquier soporte físico o automatizado que pudiera contener datos de carácter personal.

AII.1.1. Ámbito

Todas las áreas, divisiones, departamentos, servicios y dependencias, y tanto a sus directivos como a otros empleados, y también entidades y profesionales contratados bajo otras modalidades cuando en sus contratos se especifique.

AII.1.2. Contenido

A los efectos de este procedimiento se puede definir incidencia como cualquier evento que pueda producirse esporádicamente y que suponga un peligro para la seguridad del fichero, entendida en sus tres vertientes de confidencialidad, integridad y disponibilidad.

El mantener un ***registro de incidencias*** que comprometan la seguridad de un fichero es una condición que regula el artículo 10 del Reglamento y que se convierte en una herramienta indispensable para la prevención y detección de posibles ataques a la seguridad, así como la persecución de los responsables de los mismos.

- El responsable del fichero, o en su caso el responsable de seguridad habilitará un ***Registro de Incidencias*** a disposición de todos los usuarios y administradores del fichero con el fin de que se registre en él cualquier incidencia que pueda suponer un peligro para la seguridad del mismo.

- Cualquier usuario que tenga conocimiento de una incidencia es responsable de la anotación de la misma en el ***Registro de Incidencias*** del Fichero o, en su caso, de la comunicación por escrito al responsable del fichero o a quien se disponga.

- El conocimiento y la no notificación o registro de una incidencia por parte del usuario será considerado como una falta contra la seguridad del Fichero por parte de ese usuario.

- La notificación o registro de una incidencia deberá constar al menos de los siguientes datos: tipo de incidencia, fecha y hora en que se produjo, persona que realiza la notificación, persona a quien se comunica, efectos que puede producir, descripción detallada de la misma.

AII.2. PROCEDIMIENTO DE REGISTRO DE INCIDENCIAS

Se habilitará un registro, preferentemente en soporte electrónico, en el que se recoja información de las incidencias que pudieran afectar a la seguridad de los datos de carácter personal, y que tendrá orden cronológico.

Los campos previstos por cada incidencia serán los siguientes, tratando de cubrir todos, aunque sea posteriormente:

- Fecha y hora en que se conoce la incidencia.
- Fecha y hora en que se produjo si es descrita. (*)
- Descripción del tipo de incidencia: acceso indebido, pérdida de datos, copia no autorizada, corrupción de datos, etc. y explicación así como recursos afectados. (*)
- Posible inclusión o referencia de documentos, memoranda, registros de ordenador (log), manuales técnicos, comunicaciones del personal de seguridad del edificio, en definitiva, cualquier información que pueda resultar válida.
- Persona que ha realizado la notificación de la incidencia. (*)
- Persona a la que se ha comunicado. (*)
- Persona que ha incorporado la incidencia al registro.
- Posibles causas de la incidencia si se conocen.
- Efectos derivados de la incidencia. (*)
- Medidas adoptadas y controles implantados o reforzados.
- Fecha de «cierre» de la incidencia.
- Persona que ha cerrado la incidencia.

(*) Estos campos son obligatorios según exigen en el Reglamento.

AII.3. PROCEDIMIENTO DE NOTIFICACIÓN DE INCIDENCIAS

Cualquier persona que conozca hechos o circunstancias que puedan constituir una incidencia, especialmente si implica un riesgo respecto a la seguridad de los datos automatizados de carácter personal, los pondrá en conocimiento, preferentemente por escrito (considerándose válido el correo electrónico como medio), de la persona responsable del fichero y/o de la persona responsable de seguridad quienes recabarán las información complementaria necesaria en cada caso.

AII.4. PROCEDIMIENTO DE GESTIÓN DE INCIDENCIAS

Cualquier hecho que constituya una incidencia se incorporará al ***Registro de Incidencias*** por parte de la persona designada (***Gestor de Incidencias***) por la persona responsable de seguridad y con el conocimiento de la persona responsable del fichero.

Dicho Gestor de Incidencias recabará la información necesaria para cubrir los diferentes campos del Registro de Incidencias y realizará las gestiones y análisis necesarios en su caso.

Deberá notificar los hechos a la persona responsable de seguridad, sin perjuicio de que, según las circunstancias, incidencia y horario, pueda iniciar o sugerir acciones de control, especialmente de carácter técnico, recuperación de ficheros, bloqueo de usuarios.

La persona designada para gestionar las incidencias, y en función del posible impacto, habrá comunicado la incidencia, con mayor celeridad si el impacto o el riesgo pueden ser mayores.

Según las características de la incidencia, la persona responsable del fichero y/o la persona responsable de seguridad, habrán tomado las decisiones correspondientes y/o habrán comunicado la incidencia a otras personas o unidades: Seguridad Corporativa, Recursos Humanos, Policía, Persona a cargo del usuario o Entidad que procesa los datos.

En todo caso, se habrán analizado y registrado las causas y los efectos y se analizarán los controles a establecer o reforzar, y se verificará después su implantación y efectos.

En el caso de tratamiento de niveles de seguridad ***medio*** y ***alto*** deberá incorporarse al registro de incidencias la siguiente información:

- *Procedimientos realizados de recuperación de los datos.*
- *Persona que ejecuta el proceso.*
- *Datos restaurados.*
- *Datos que ha sido necesario grabar manualmente en el proceso de recuperación.*

AII.5. SISTEMA DE INCIDENCIAS DE LA ENTIDAD

AII.5.1. Introducción

En el Servicio de Informática y Nuevas Tecnologías se registran las incidencias utilizando una aplicación desarrollada en Access, denominada: Sistema de control de los datos de carácter personal.

En este sistema se registran todas las incidencias que han tenido un impacto importante en la actividad de la entidad.

El listado de incidencias se encuentra en el documento ***"INCIDENCIAS – Documento Seguridad"***, que se guarda en el mismo directorio que este documento de seguridad.

AII.6. Notificación Manual de Incidencias de Nivel Básico

<table>
<tr><th colspan="4">INFORME DE INCIDENCIAS</th></tr>
<tr><td colspan="2">NOMBRE DEL FICHERO:</td><td rowspan="2">NIVEL DELFICHERO:</td><td rowspan="2">☐ Básico
☐ Medio
☐ Alto</td></tr>
<tr><td colspan="2">DOCUMENTO DE SEGURIDAD: DS_DPO</td></tr>
<tr><td colspan="2">DETECTADA POR:</td><td colspan="2">RESPONSABLE DEL FICHERO:</td></tr>
<tr><td colspan="4">DESCRIPCIÓN:</td></tr>
<tr><td colspan="2">ACCIONES A EMPRENDER</td><td colspan="2">CIERRE DE LAS ACCIONES</td></tr>
<tr><td colspan="2">☐ Preventiva ☐ Correctora
Descripción:
Responsable de la acción:</td><td colspan="2">Fecha Cierre: / /
Firma del responsable:</td></tr>
<tr><td colspan="2">☐ Preventiva ☐ Correctora
Descripción:
Responsable de la acción:</td><td colspan="2">Fecha Cierre: / /
Firma del responsable:</td></tr>
<tr><td colspan="2">☐ Preventiva ☐ Correctora
Descripción:
Responsable de la acción:</td><td colspan="2">Fecha Cierre: / /
Firma del responsable:</td></tr>
<tr><td colspan="4">Si la acción a tomar implicase la recuperación de datos, ésta se realiza conforme al Procedimiento de Realización de Copias de Respaldo y Recuperación de Datos, describiendo la persona que realiza el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.</td></tr>
<tr><td colspan="2">CONCLUSIÓN DEL RESPONSABLE DEL FICHERO:</td><td colspan="2">Firma del Responsable del Fichero:

Fecha : / /</td></tr>
</table>

ANEXO III. ESTRUCTURA DE LOS FICHEROS

AIII.1. RECURSOS HUMANOS

Nivel Seguridad	**ALTO**
Número Publicación AGPD	255
Fecha Publicación BOP	05/11/2003
Finalidad y Usos Previstos	Gestión del personal. Elaboración de Nóminas. Declaración de retenciones y renta. Obtención de estadísticas internas. Formación de Personal. Gestión de anticipos, pensiones, subsidios y otras prestaciones económicas. Procedimientos administrativos. Concesión y gestión de permisos. Gestión de los modelos de la Seguridad Social. Gestión de asistencia sanitaria.
Personas o colectivos sobre los que se obtienen datos	Personal al servicio de la Diputación Provincial de Ourense.
Procedimiento de recogida datos	Declaraciones recogidas directamente en el ordenador o en formularios en papel.
Estructura básica del fichero	*Datos de carácter identificativo*: D.N.I./N.I.F., Nº S.S. / Mutualidad, Nombre y Apellidos, Dirección postal, Teléfono. *Datos de características personales*: Datos de estado civil, Datos de familia, Fecha de nacimiento, Edad, Sexo, Nacionalidad. *Datos académicos y profesionales*: Formación, Titulaciones. *Datos de detalle de empleo*: Cuerpo / escala, Categoría / grado, Puestos de trabajo, Datos no económicos de nómina. *Datos económicos-financieros y de seguros*: Datos bancarios, Datos económicos de nómina, Datos deducciones impositivas/impuestos, Seguros, Subsidios, Beneficios.
Ubicación	S44BB203\ABDEUR\PERSOFFF (Más los ficheros relacionados)
Aplicaciones tratamiento	GESNOM
Departamentos con acceso	Personal, Intervención
Cesiones previstas a tercetos	✓ ADESLAS ✓ AGENCIA ESTATAL DEADMINISTRACION TRIBUTARIA ✓ CAIXANOVA ✓ TESORERIA TERRITORIAL DE LA SEGURIDAD SOCIAL ✓ A28013050 CASER

AIII.2. CONTABILIDAD

Nivel Seguridad	**MEDIO**
Número Publicación AGPD	255
Fecha Publicación BOP	05/11/2003
Finalidad y Usos Previstos	Gestión contable de la Diputación Provincial de Ourense. Gestión personal y económica con terceros.
Personas o colectivos sobre los que se obtienen datos	Terceros que tienen relación con la Diputación Provincial de Ourense.
Procedimiento de recogida datos	Declaraciones recogidas directamente en el ordenador o en formularios en papel.
Estructura básica del fichero	*Datos de carácter identificativo*: D.N.I./N.I.F., Nombre y Apellidos, Dirección postal, Teléfono. *Datos de información comercial*: Actividades y negocios. *Datos económicos-financieros*: Datos bancarios. *Datos de transacciones*: Bienes y servicios suministrados por el afectado, Transacciones financieras.
Ubicación	Servidor: oracle.depourense.es Ruta: /home/oracle/10.2.0/oradata/
Aplicaciones tratamiento	Sistema de Gestión de BD: Oracle 10g Aplicación de contabilidad: Sical-Win
Departamentos con acceso	Intervención, Tesorería, Informática
Cesiones previstas a tercetos	✓ AGENCIA ESTATAL DE ADMINISTRACION PUBLICA ✓ CAIXANOVA

AIII.3. RIESGOS LABORALES

Nivel Seguridad	**MEDIO**
Número Publicación AGPD	255
Fecha Publicación BOP	05/11/2003
Finalidad y Usos Previstos	Gestión de servicios orientados a la prevención de riesgos laborales.
Personas o colectivos sobre los que se obtienen datos	Personal al servicio de la Diputación Provincial de Ourense.
Procedimiento de recogida datos	Declaraciones recogidas directamente en el ordenador o en formularios en papel.
Estructura básica del fichero	*Datos de carácter identificativo*: D.N.I./N.I.F., Nº S.S. / Mutualidad, Nombre y Apellidos, Dirección postal, Teléfono. *Datos de características personales*: Fecha de nacimiento. *Datos de detalle de empleo*: Clase de personal, Puesto de trabajo.
Ubicación	Servidor: datos.depourense.es Ruta: / datos.depourense.es\Riscos
Aplicaciones tratamiento	Aplicación ofimática de Windows (Access): "Relacion_Trabajadores.mdb"
Departamentos con acceso	Riesgos laborales, Informática
Cesiones previstas a tercetos	✓ No está prevista

AIII.4. ASISTENCIA SOCIAL

Nivel Seguridad	**ALTO**
Número Publicación AGPD	255
Fecha Publicación BOP	05/11/2003
Finalidad y Usos Previstos	Administración de asistencia social.
Personas o colectivos sobre los que se obtienen datos	Personas de tercera edad o con minusvalías solicitantes de servicios de asistencia social.
Procedimiento de recogida datos	Formularios en papel.
Estructura básica del fichero	*Datos de carácter identificativo*: D.N.I./N.I.F, Nombre y Apellidos, Dirección postal, Teléfono. *Datos de características personales*: Datos de estado civil, Fecha de nacimiento, Edad, Sexo, Discapacidades, Salud. *Datos de circunstancias sociales:* Características de alojamiento, Vivienda. *Datos académicos y profesionales:* Tipo d estudios. *Datos económicos-financieros:* Renta.
Ubicación	Servidor: datos.depourense.es Ruta: \\datos.depourense.es\Asocial
Aplicaciones tratamiento	Aplicación ofimática de Windows (Access): "Teleasistencia.mdb"
Departamentos con acceso	Asistencia Social, Informática
Cesiones previstas a tercetos	✓ EULEN

AIII.5. FORMADORES

Nivel Seguridad	**MEDIO**
Número Publicación AGPD	255
Fecha Publicación BOP	05/11/2003
Finalidad y Usos Previstos	Gestión de los datos del profesorado que imparte los cursos de formación continua.
Personas o colectivos sobre los que se obtienen datos	Profesores que imparten los cursos de formación continua.
Procedimiento de recogida datos	Formularios en papel.
Estructura básica del fichero	*Datos de carácter identificativo*: D.N.I./N.I.F, Nombre y Apellidos, Dirección postal, Teléfono. *Datos académicos y profesionales:* Formación. *Datos de detalle de empleo:* Puesto de trabajo. *Datos económicos-financieros:* Datos bancarios.
Ubicación	Servidor: datos.depourense.es Ruta: \\datos.depourense.es\formacion
Aplicaciones tratamiento	Aplicación ofimática de Windows (Word): "Formadores.doc".
Departamentos con acceso	Formación continua (Centro Cultural Simeón)
Cesiones previstas a tercetos	✓ No está prevista

AIII.6. ALUMNOS FORMACIÓN

Nivel Seguridad	**MEDIO**
Número Publicación AGPD	255
Fecha Publicación BOP	05/11/2003
Finalidad y Usos Previstos	Gestión del personal de la administración local que realiza los cursos de formación continua.
Personas o colectivos sobre los que se obtienen datos	Personal de la administración local que realiza los cursos de formación continua.
Procedimiento de recogida datos	Formularios en papel.
Estructura básica del fichero	*Datos de carácter identificativo*: D.N.I./N.I.F, Nombre y Apellidos, Dirección postal, Teléfono. *Datos de detalle de empleo:* Cargo que desempeña.
Ubicación	Servidor: datos.depourense.es Ruta: \\datos.depourense.es\formacion
Aplicaciones tratamiento	Aplicación ofimática de Windows (Access): "Formacion.mdb".
Departamentos con acceso	Formación continua (Centro Cultural Simeón)
Cesiones previstas a tercetos	✓ No está prevista

AIII.7. ACTIVIDADES CULTURALES

Nivel Seguridad	**BÁSICO**
Número Publicación AGPD	255
Fecha Publicación BOP	05/11/2003
Finalidad y Usos Previstos	Gestión de los datos de las personas que participan en las actividades del Centro Cultural de la Diputación de Ourense.
Personas o colectivos sobre los que se obtienen datos	Personal que participan en actividades culturales.
Procedimiento de recogida datos	Formularios en papel.
Estructura básica del fichero	*Datos de carácter identificativo*: D.N.I./N.I.F, Nombre y Apellidos, Dirección postal, Teléfono. *Datos de detalle de empleo:* Puesto de trabajo, Clase de personal, Grupo, Nivel.
Ubicación	Servidor: datos.depourense.es Ruta: \\datos.depourense.es\Centro_Cultural
Aplicaciones tratamiento	Aplicación ofimática de Windows (Excel): "Formacion.mdb".
Departamentos con acceso	Centro Cultural Simeón
Cesiones previstas a tercetos	✓ No está prevista

AIII.8. PAGO ANUNCIOS BOP

Nivel Seguridad	**MEDIO**
Número Publicación AGPD	255
Fecha Publicación BOP	05/11/2003
Finalidad y Usos Previstos	Gestión de los anuncios que se publican en el B.O.P.
Personas o colectivos sobre los que se obtienen datos	Personas que desean publicar anuncios en el B.O.P.
Procedimiento de recogida datos	Declaraciones recogidas directamente en el ordenador o formularios en papel.
Estructura básica del fichero	*Datos de carácter identificativo*: D.N.I./N.I.F., Nombre y Apellidos, Dirección postal. *Datos económicos-financieros:* Datos bancarios.
Ubicación	S44BB203\ANUNCIO\CODIGOP
Aplicaciones tratamiento	Módulo "Sección de Arbitrios y BOP", herramientas Query y DFU.
Departamentos con acceso	Arbitrios
Cesiones previstas a tercetos	✓ CAIXANOVA

AIII.9. USUARIOS PAZO DOS DEPORTES

Nivel Seguridad	**MEDIO**
Número Publicación AGPD	255
Fecha Publicación BOP	05/11/2003
Finalidad y Usos Previstos	Gestión personal y económica de los usuarios del Pazo de los Deportes Paco Paz.
Personas o colectivos sobre los que se obtienen datos	Usuarios de los servicios proporcionados por el Pazo de los Deportes Paco Paz.
Procedimiento de recogida datos	Declaraciones recogidas directamente en el ordenador o formularios en papel.
Estructura básica del fichero	*Datos de carácter identificativo*: D.N.I./N.I.F., Nombre y Apellidos, Dirección postal y electrónica, Teléfono. *Datos de características personales*: Fecha de nacimiento, Sexo. *Datos económicos-financieros:* Datos bancarios.
Ubicación	\\Pc-Alberto\Paz_gimn
Aplicaciones tratamiento	Aplicación ofimática de Windows (Access): "Paz_gimn.mdb".
Departamentos con acceso	Administración del Pazo de los deportes Paco Paz
Cesiones previstas a tercetos	✓ CAIXANOVA

AIII.10. ALUMNOS ESCUELA DE GAITAS

Nivel Seguridad	**MEDIO**
Número Publicación AGPD	255
Fecha Publicación BOP	05/11/2003
Finalidad y Usos Previstos	Gestión de los alumnos matriculados en la Escuela de Gaitas de la Diputación Provincial de Ourense.
Personas o colectivos sobre los que se obtienen datos	Alumnos de la Escuela de Gaitas de la Diputación Provincial de Ourense.
Procedimiento de recogida datos	Declaraciones recogidas directamente en el ordenador o formularios en papel.
Estructura básica del fichero	*Datos de carácter identificativo*: D.N.I./N.I.F, Nombre y Apellidos, Dirección postal y electrónica, Teléfono. *Datos de características personales*: Fecha de nacimiento. *Datos de detalle de empleo:* Profesión.
Ubicación	
Aplicaciones tratamiento	Aplicación ofimática de Windows (Access): "Escola Provincial de Gaitas.mdb"
Departamentos con acceso	Administración de la Escuela de Gaitas.
Cesiones previstas a tercetos	✓ No está prevista

AIII.11. EMIGRANTES RETORNADOS

Nivel Seguridad	**MEDIO**
Número Publicación AGPD	255
Fecha Publicación BOP	05/11/2003
Finalidad y Usos Previstos	Gestión de datos de emigrantes retornados para proporcionarles información y asesoramiento.
Personas o colectivos sobre los que se obtienen datos	Emigrantes retornados.
Procedimiento de recogida datos	Declaraciones recogidas directamente en el ordenador o formularios en papel.
Estructura básica del fichero	*Datos de carácter identificativo*: Pasaporte, Nombre y Apellidos, Dirección postal y electrónica, Teléfono. *Datos de características personales*: Estado civil, Datos de Familia, Fecha de nacimiento, Lugar de nacimiento, Sexo, Nacionalidad actual y anterior, País de procedencia. *Datos de circunstancias sociales:* Datos permiso de residencia, Datos permiso de trabajo, Datos del visado, Situación laboral. *Datos académicos y profesionales:* Nivel de estudios.
Ubicación	Servidor: datos.depourense.es Ruta: \\datos.depourense.es\UPD
Aplicaciones tratamiento	Aplicación ofimática de Windows (Access).
Departamentos con acceso	Fomento de Empleo
Cesiones previstas a tercetos	✓ No está prevista

AIII.12. TÉCNICOS DE EMPLEO

Nivel Seguridad	**MEDIO**
Número Publicación AGPD	255
Fecha Publicación BOP	05/11/2003
Finalidad y Usos Previstos	Gestión de datos de emigrantes retornados para proporcionarles información y asesoramiento.
Personas o colectivos sobre los que se obtienen datos	Emigrantes retornados.
Procedimiento de recogida datos	Declaraciones recogidas directamente en el ordenador o formularios en papel.
Estructura básica del fichero	*Datos de carácter identificativo*: Pasaporte, Nombre y Apellidos, Dirección postal y electrónica, Teléfono. *Datos de características personales*: Estado civil, Datos de Familia, Fecha de nacimiento, Lugar de nacimiento, Sexo, Nacionalidad actual y anterior, País de procedencia. *Datos de circunstancias sociales:* Datos permiso de residencia, Datos permiso de trabajo, Datos del visado, Situación laboral. *Datos académicos y profesionales:* Nivel de estudios.
Ubicación	Servidor: datos.depourense.es Ruta: \\datos.depourense.es\UPD
Aplicaciones tratamiento	Aplicación ofimática de Windows (Access).
Departamentos con acceso	Fomento de Empleo
Cesiones previstas a tercetos	✓ No está prevista

AIII.13. ALUMNOS SUSCRIPTORES

Nivel Seguridad	**MEDIO**
Número Publicación AGPD	255
Fecha Publicación BOP	05/11/2003
Finalidad y Usos Previstos	Gestión de datos de los Técnicos de empleo de las administraciones locales.
Personas o colectivos sobre los que se obtienen datos	Técnicos de empleo de las administraciones locales.
Procedimiento de recogida datos	Declaraciones recogidas directamente en el ordenador o en formularios en papel.
Estructura básica del fichero	*Datos de carácter identificativo*: D.N.I./N.I.F, Nombre y Apellidos, Dirección postal y electrónica, Teléfono. *Datos de características personales*: Fecha de nacimiento. *Datos de circunstancias sociales:* Situación laboral. *Datos académicos y profesionales:* Formación. *Datos de detalle de empleo:* Ocupación
Ubicación	Servidor: datos.depourense.es Ruta: \\datos.depourense.es\UPD
Aplicaciones tratamiento	Aplicación ofimática de Windows (Access).
Departamentos con acceso	Fomento de Empleo
Cesiones previstas a tercetos	✓ No está prevista

AIII.14. DIETAS DE VÍAS Y OBRAS

Nivel Seguridad	**BÁSICO**
Número Publicación AGPD	255
Fecha Publicación BOP	05/11/2003
Finalidad y Usos Previstos	Gestión de las personas matriculadas y/o suscritas a la revista informativa de la Escuela de Danza de la Diputación Provincial de Ourense
Personas o colectivos sobre los que se obtienen datos	Alumnos de la Escuela de Danza de la Diputación Provincial de Ourense.
Procedimiento de recogida datos	Declaraciones recogidas directamente en el ordenador o en formularios en papel.
Estructura básica del fichero	*Datos de carácter identificativo*: D.N.I./N.I.F., Pasaporte, Nombre y Apellidos, Dirección postal y electrónica, Teléfono.
Ubicación	
Aplicaciones tratamiento	Aplicación ofimática de Windows (Access): "alumnos.mdb" y "raigame.mdb".
Departamentos con acceso	Administración de la Escuela de Danza.
Cesiones previstas a tercetos	✓ No está prevista

AIII.15. DIRECTORES DE OBRAS

Nivel Seguridad	**MEDIO**
Número Publicación AGPD	255
Fecha Publicación BOP	05/11/2003
Finalidad y Usos Previstos	Mantener datos sobre los directores de obras. Permite seguir las obras dirigidas por los directores y se utiliza en todos los temas de gestión de los planes de obras relacionándolo con el fichero de obras.
Personas o colectivos sobre los que se obtienen datos	Directores de obras de la Diputación de Ourense.
Procedimiento de recogida datos	Declaraciones recogidas directamente en el ordenador o en formularios en papel.
Estructura básica del fichero	*Datos de carácter identificativo*: D.N.I / N.I.F., Nombre y Apellidos, Dirección postal, Teléfono. *Datos académicos y profesionales:* Formación, Titulaciones. *Datos económicos-financieros:* Datos bancarios.
Ubicación	S44BB203\PLAN\OPODIRP
Aplicaciones tratamiento	Módulo: "Búsqueda de directores, autores y técnicos", herramientas Query, SQL y DFU.
Departamentos con acceso	Vías y obras, Planes provinciales, Cooperación
Cesiones previstas a tercetos	✓ No está prevista

AIII.16. SUSCRIPTORES BOP

Nivel Seguridad	**MEDIO**
Número Publicación AGPD	255
Fecha Publicación BOP	05/11/2003
Finalidad y Usos Previstos	Mantener datos sobre los suscriptores al boletín oficial de la provincia. Se utiliza para hacerlo llegar y controlar el cobro.
Personas o colectivos sobre los que se obtienen datos	Suscriptores al boletín oficial de la provincia.
Procedimiento de recogida datos	Declaraciones recogidas directamente en el ordenador o en formularios en papel.
Estructura básica del fichero	*Datos de carácter identificativo*: Nombre y Apellidos, Dirección postal. *Datos económicos-financieros:* Datos bancarios.
Ubicación	S44BB203\IMPRENTA\BOLSUSP
Aplicaciones tratamiento	Módulo "Sección Arbitrios y BOP", herramientas Query y DFU.
Departamentos con acceso	Arbitrios
Cesiones previstas a tercetos	✓ No está prevista

AIII.17. INVESTIGADORES

Nivel Seguridad	**MEDIO**
Número Publicación AGPD	255
Fecha Publicación BOP	05/11/2003
Finalidad y Usos Previstos	Se utiliza para realizar un control interno de los fondos, y para estadísticas dentro de la propia biblioteca (fotocopias, fondos más utilizados…).
Personas o colectivos sobre los que se obtienen datos	Investigadores que utilizan la biblioteca de la Diputación.
Procedimiento de recogida datos	Declaraciones recogidas directamente en el ordenador o en formularios en papel.
Estructura básica del fichero	*Datos de carácter identificativo*: Nombre y Apellidos *Datos académicos y profesionales:* Formación, Titulaciones, Profesión.
Ubicación	Servidor: datos.depourense.es Ruta: \\datos.depourense.es\UPD
Aplicaciones tratamiento	Aplicación ofimática de Windows (Access): "Investigadores.mdb"
Departamentos con acceso	Biblioteca
Cesiones previstas a tercetos	✓ No está prevista

AIII.18. APOYO TELEMÁTICO A ENTIDADES

Nivel Seguridad	**ALTO**
Número Publicación AGPD	
Fecha Publicación BOP	2008
Finalidad y Usos Previstos	Herramienta telemática de apoyo a las entidades locales en la gestión administrativa integral a las personas en situación de dependencia.
Personas o colectivos sobre los que se obtienen datos	Integra los datos de carácter personal de las personas o colectivos en situación de dependencia, y miembros de la unidad familiar, en los términos definidos por la Ley de Dependencia.
Procedimiento de recogida datos	Entorno Web de la herramienta, mediante formularios dedicados a tal finalidad y serán remitidos por los propios interesados.
Estructura básica del fichero	*Características personales*: Edad, DNI, estado civil, domicilio, profesión, nº SS, teléfonos. *Datos relacionados con la salud*: Grado de minusvalía. Actividades para las que necesita ayuda de otra persona. *Circunstancias sociales*: Recursos e servicios sociales que percibe. Apoyo de voluntario y tipo de servicios. Tipo de vivienda, régimen, etc. *Económicos y financieros*: Ingresos netos. Rendimientos de capital mobiliario. Otro rendimiento. Ganancias y pérdidas patrimoniales. Bienes inmuebles. Capital mobiliario. *Transacciones de bienes y servicios*: Transmisiones patrimoniales con su valor catastral.
Ubicación	Servidor: datos.depourense.es Ruta: \\datos.depourense.es\UPD
Aplicaciones tratamiento	
Departamentos con acceso	Fomento de Empleo
Cesiones previstas a tercetos	✓ No está prevista

AIII.19. VIDEOVIGILANCIA

Nivel Seguridad	**ALTO**
Número Publicación AGPD	
Fecha Publicación BOP	2010
Finalidad y Usos Previstos	Se emplea para la captura grabación y conservación temporal de imágenes captadas por las cámaras de videovigilancia situadas en las dependencias del Pazo Provincial de la Diputación de Ourense, Centro Cultural, Pazo de los Deportes Paco Paz y en plantas de transferencia y puntos limpios de ayuntamientos todos ellos en el municipio de Ourense.
Personas o colectivos sobre los que se obtienen datos	Datos de carácter personal consistentes en imágenes capturadas de personas que transiten por los lugares públicos sometidos a videovigilancia, indicados en el artículo 2.
Procedimiento de recogida datos	Cámaras y dispositivos del sistema de videovigilancia.
Estructura básica del fichero	*Datos de carácter identificativo*: Imagen y voz, silueta y matrículas de vehículos. Las grabaciones serán destruidas en un plazo máximo de un mes, excepto cuando se requieran por las autoridades gobernativas o judiciales.
Ubicación	Cámaras y dispositivos del sistema de videovigilancia.
Aplicaciones tratamiento	
Departamentos con acceso	Gobierno Interior
Cesiones previstas a tercetos	✓ ORGANOS JUDICIALES ✓ FUERZAS Y CUERPOS DE SEGURIDAD

AIII.20. BECARIOS DE LA DIPUTACIÓN DE OURENSE

Nivel Seguridad	**MEDIO**
Número Publicación AGPD	
Fecha Publicación BOP	2010
Finalidad y Usos Previstos	Gestión de los beneficiarios de becas de estudios e investigación concedidas por la Diputación Provincial de Ourense.
Personas o colectivos sobre los que se obtienen datos	Datos de carácter personal de las bolsas ofertadas por la Diputación Provincial de Ourense.
Procedimiento de recogida datos	Formularios y solicitudes (vía web e impresos en papel), presentados por los interesados en las bolsas ofertadas por la Diputación Provincial de Ourense
Estructura básica del fichero	*Datos de carácter identificativo*: Nombre, apellidos, NIF/DNI, dirección, teléfono, correo electrónico. *Datos académicos y profesionales:* Formación, Titulaciones, Profesión. *Datos económicos-financieros:* Datos bancarios. *Datos tributarios y Seguridad Social:* cumplimiento de las obligaciones tributarias y de seguridad social.
Ubicación	Cámaras y dispositivos del sistema de videovigilancia.
Aplicaciones tratamiento	
Departamentos con acceso	Promoción de Empleo
Cesiones previstas a tercetos	✓ ORGANOS JUDICIALES ✓ ÓRGANOS DE LA ADMINISTRACIÓN DEL ESTADO ✓ ÓRGANOS DE LA COMUNIDAD AUTÓNOMA ✓ OTROS ÓRGANOS DE LA ADMINISTRACIÓN LOCAL ✓ INSTITUCIONES EUROPEAS QUE COFINANCIEN LAS BECAS

AIII.21. CENTRO DE CULTURA POPULAR

Nivel Seguridad	**BASICO**
Número Publicación AGPD	
Fecha Publicación BOP	2010
Finalidad y Usos Previstos	Gestión de los usuarios del centro de cultura popular de la Diputación Provincial de Ourense.
Personas o colectivos sobre los que se obtienen datos	Datos de carácter personal de las personas físicas, y si es el caso, personas jurídicas, que se inscriban como alumnos o participantes en las actividades organizadas por el centro de cultura popular Xaquín Lorenzo.
Procedimiento de recogida datos	Formularios y solicitudes (vía web e impresos en papel), presentados por los interesados en participar en las actividades organizadas por el centro de cultura popular Xaquín Lorenzo.
Estructura básica del fichero	*Datos de carácter identificativo*: Nombre, apellidos, NIF/DNI, dirección, teléfono, correo electrónico (del interesado o representante). *Datos personas jurídicas:* razón social, CIF, domicilio social, teléfono, correo electrónico, nombre, apellidos, DNI (del interesado o representante).
Ubicación	Centro de cultura popular Xaquín Lorenzo
Aplicaciones tratamiento	
Departamentos con acceso	Centro de cultura popular Xaquín Lorenzo
Cesiones previstas a tercetos	✓ No está prevista

AIII.22. SOLICITANTES Y BENEFICIARIOS DE SUBVENCIONES

Nivel Seguridad	**ALTO**
Número Publicación AGPD	
Fecha Publicación BOP	2010
Finalidad y Usos Previstos	Gestión del registro de datos de los expedientes correspondientes a las subvenciones tramitadas y concedidas por la Diputación Provincial de Ourense.
Personas o colectivos sobre los que se obtienen datos	Datos de carácter personal de las personas físicas, y si es el caso, personas jurídicas, residentes y solicitantes que figuran en algún expediente obtenido por la concesión de subvenciones ofrecidas por la Diputación Provincial de Ourense.
Procedimiento de recogida datos	Formularios y solicitudes presentados por los interesados en participar en los procedimientos administrativos tramitados por la Diputación.
Estructura básica del fichero	*Datos de carácter identificativo*: Nombre, apellidos, razón social, NIF/DNI, dirección, teléfono, correo electrónico (del interesado o representante). *Datos personas jurídicas:* razón social, CIF, domicilio social, teléfono, correo electrónico, nombre, apellidos, DNI (del interesado o representante). *Datos bancarios:* para el pago de la subvención, así como los ingresos y gastos del solicitante, incluidos, sí es el caso, datos fiscales y patrimoniales. *Datos tributarios y seguridad social:* datos sobre el cumplimiento de las obligaciones tributarias y seguridad social. *Datos actividad:* datos relativos a las situaciones, conductas o actividades que motivan la solicitud, y si es el caso, concesión de la subvención.
Ubicación	Diputación Provincial de Ourense
Aplicaciones tratamiento	
Departamentos con acceso	Departamento de Subvenciones
Cesiones previstas a tercetos	✓ ORGANOS JUDICIALES ✓ OTROS ÓRGANOS DE LA ADMINISTRACIÓN LOCAL ✓ INTERESADOS LEGÍTIMOS ✓ PUBLICACION EN DIARIOS OFICIALES CORRESPONDIENTES Y EN SEDE ELECTRONICA DE LA DIPUTACION PROVINCIAL

AIII.23. USUARIOS DEL CENTRO ECUESTRE Y ESCUELA DE HÍPICA

Nivel Seguridad	**MEDIO**
Número Publicación AGPD	
Fecha Publicación BOP	2010
Finalidad y Usos Previstos	Gestión para la prestación de servicios a los usuarios del servicio de equitación de la Diputación Provincial de Ourense y de la escuela de hípica.
Personas o colectivos sobre los que se obtienen datos	Datos de carácter personal de los ciudadanos, residentes y solicitantes que desean acceder a las instalaciones y medios propuestos por el servicio de equitación.
Procedimiento de recogida datos	Formularios y solicitudes presentados por los interesados en las instalaciones y medios propuestos por el servicio de equitación.
Estructura básica del fichero	*Datos de carácter identificativo*: Nombre, apellidos, razón social, NIF/DNI, dirección, teléfono, correo electrónico (del interesado o representante). *Datos personas jurídicas:* razón social, CIF, domicilio social, teléfono, correo electrónico, nombre, apellidos, DNI (del interesado o representante). *Datos bancarios:* para el pago de servicios.
Ubicación	Centro Ecuestre de la Diputación Provincial de Ourense
Aplicaciones tratamiento	
Departamentos con acceso	Centro Ecuestre de la Diputación Provincial de Ourense
Cesiones previstas a tercetos	✓ No está prevista

AIII.24. USUARIOS DEL SERVICIO DE DEPORTES

Nivel Seguridad	**BASICO**
Número Publicación AGPD	
Fecha Publicación BOP	2010
Finalidad y Usos Previstos	Gestión de la prestación de servicios a las personas usuarios o participantes de las actividades gestionadas promovidas u organizadas por el servicio de deportes de la Diputación de Ourense.
Personas o colectivos sobre los que se obtienen datos	Datos de carácter personal de personas físicas y jurídicas que, por propia voluntad, utilicen los servicios o participen en las actividades gestionadas, organizadas o promovidas por el Servicio de Deportes de la Diputación Provincial de Ourense.
Procedimiento de recogida datos	Formularios y solicitudes presentados por los interesados en las instalaciones y actividades gestionadas, organizadas o promovidas por el Servicio de Deportes de la Diputación Provincial de Ourense.
Estructura básica del fichero	*Datos de carácter identificativo*: Nombre, apellidos, razón social, NIF/DNI, dirección, teléfono, correo electrónico (del interesado o representante). *Datos personas jurídicas:* razón social, CIF, domicilio social, teléfono, correo electrónico, nombre, apellidos, DNI (del interesado o representante). *Datos bancarios:* para el pago de servicios.
Ubicación	Servicio de Deportes
Aplicaciones tratamiento	
Departamentos con acceso	Pazo de los Deportes Paco Paz
Cesiones previstas a tercetos	✓ No está prevista

AIII.25. REGISTRO DE INTERESES DE CARGOS PÚBLICOS

Nivel Seguridad	**ALTO**
Número Publicación AGPD	
Fecha Publicación BOP	2010
Finalidad y Usos Previstos	Gestión del registro de los datos de los interesados en expedientes administrativos gestionados por los distintos servicios de la Diputación provincial de Ourense para los que no existan ficheros automatizados específicos.
Personas o colectivos sobre los que se obtienen datos	Datos de carácter personal de personas físicas que ocupen cargos públicos sujetos a declaración de actividades y bienes en los registros de actividades y bienes previstos en el artículo 75.7 de la Ley de bases del régimen local. Además incluirá información sobre las sociedades de todo tipo participantes por dichas personas físicas, y por las sociedades participantes a su vez por ellas.
Procedimiento de recogida datos	Formularios y solicitudes presentados por los interesados en las instalaciones y actividades gestionadas, organizadas o promovidas por el Servicio de Deportes de la Diputación Provincial de Ourense.
Estructura básica del fichero	*Datos de carácter identificativo*: Nombre, apellidos, razón social, NIF/DNI, dirección, teléfono, correo electrónico (del interesado o representante). *Otros datos:* - Declaración sobre causas de posible incompatibilidades con los cargos públicos ocupados. - Declaración sobre cualquier actividad que les proporcione o pueda proporcionar ingresos económicos. - Declaración de sus bienes patrimoniales, incluyendo su identificación, descripción y valoración. - Declaración de acciones o participaciones en sociedades de todo tipo, con información de las sociedades en las que participan. - Liquidaciones de los impuestos sobre la renta, patrimonio y, si es el caso, sociedades de las que sean socios.
Ubicación	Diputación Provincial de Ourense
Aplicaciones tratamiento	
Departamentos con acceso	Diputación Provincial de Ourense
Cesiones previstas a tercetos	✓ ORGANOS JUDICIALES ✓ OTROS ÓRGANOS DE LA ADMINISTRACIÓN DEL ESTADO ✓ OTROS ÓRGANOS DE LA COMUNIDAD AUTÓNOMA ✓ OTROS ÓRGANOS DE LA ADMINISTRACIÓN LOCAL ✓ INTERESADOS LEGÍTIMOS ✓ PUBLICACION EN LOS TERMINOS PREVISTOS EN EL ART. 75.7 DE LA LEY DE BASES DE REGIMEN LOCAL

AIII.26. INTERESADOS EN EXPEDIENTES ADMINISTRATIVOS

Nivel Seguridad	**BAJO**
Número Publicación AGPD	
Fecha Publicación BOP	2010
Finalidad y Usos Previstos	Gestión del registro de los datos de los interesados en expedientes administrativos gestionados por los distintos servicios de la Diputación provincial de Ourense para los que no existan ficheros automatizados específicos.
Personas o colectivos sobre los que se obtienen datos	Datos de carácter personal de personas físicas y jurídicas, residentes y solicitantes, que figuran en algún procedimiento administrativo de la Diputación Provincial de Ourense.
Procedimiento de recogida datos	Formularios y solicitudes presentados por los interesados mediante formularios y solicitudes en los procedimientos administrativos que se presentan en la Diputación.
Estructura básica del fichero	*Datos de carácter identificativo*: Nombre, apellidos, razón social, NIF/DNI, CIF, dirección, teléfono, correo electrónico (del interesado o representante).
Ubicación	Diputación Provincial de Ourense
Aplicaciones tratamiento	
Departamentos con acceso	Diputación Provincial de Ourense
Cesiones previstas a tercetos	✓ No está prevista

ANEXO IV. COPIAS DE SEGURIDAD

AIV.1. REGLAMENTO SEGÚN LOPD

La seguridad que contempla tanto la LOPD como su desarrollo reglamentario se refiere a la confidencialidad, la integridad de los datos y la autenticación de los usuarios así como el control de accesos.

El Reglamento de Desarrollo de la LOPD contempla la obligación de realizar copias de respaldo de la siguiente forma (artículo 94):

1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

    - ✓ Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.

    - ✓ La periodicidad mínima con que se deben realizar las copias de respaldo es semanal, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

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

4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.

    - ✓ Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

El artículo 102 amplía estas obligaciones para los ficheros de nivel alto, estableciendo que se debe conservar una copia de respaldo en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, siendo éste la ***Excma. Diputación Provincial de Ourense,*** cumpliendo las medidas de seguridad exigidas en el Reglamento. En el ***Edificio Simeón*** se dispone de un espacio de seguridad en el que salvaguardan las copias de respaldo para cumplir con la Ley.

En los siguientes apartados se presentan los distintos procedimientos que hay que llevar a cabo:

- *Procedimiento de Copias de respaldo.*
- *Procedimiento de Recuperación.*
- *Procedimiento de puesta al día del Documento*
- *Procedimiento de Registro de Accesos.*
- *Procedimiento de Cifrado.*
- *Procedimiento de Almacenamiento de Copias de Seguridad.*

AIV.2. PROCEDIMIENTO DE COPIAS DE RESPALDO

PROCEDIMIENTO DE COPIAS DE RESPALDO	
ORGANIZACIÓN: DIPUTACIÓN PROVINCIAL DE OURENSE	**01/02/2015**
Ámbito	*Todas las áreas, divisiones, departamento, servicios y dependencias, y tanto a sus directivos como al resto de usuarios, y también entidades y profesionales contratados bajo otras modalidades cuando en sus contratos se especifique.*
Contenido	*Está implantada una política de copias de seguridad de los datos de carácter personal. Esta política es incremental, haciéndose copias diarias, semanales y mensuales. Esto implica que en una operación de copia incremental sólo son volcados archivos que hayan sufrido cambios desde la última copia de seguridad del mismo nivel o superior.* *La gestión de las copias de seguridad de los ficheros de datos de carácter personal ubicados en los sistemas Windows Server se realiza mediante un robot de cintas del fabricante Adic y gestionado por un software de "Legato Software (EMC) ". Las aplicaciones de gestión se llaman Networker Administrador y Networker user, y se encuentran instaladas en el servidor "backup.depourense.es" En el robot de cintas automático, las copias diarias y semanales se reutilizan, guardándose la copia mensual de los últimos durante un periodo mínimo.* *Estas cintas se guardan en una caja de seguridad ignífuga cerrada con clave de un número determinado de cifras.* *El procedimiento es el siguiente:* 1. *Se harán diariamente copias de respaldo de la base de datos donde residen los datos de carácter personal.* 2. *Se hará una copia de respaldo inmediatamente antes de empezar los procesos de actualización semanal.* 3. *Los soportes a utilizar estarán etiquetados convenientemente para que exista un soporte para cada día de la semana, uno para la copia previa a la*

	actualización y otro para la copia posterior a la misma.

AIV.3. PROCEDIMIENTO DE RECUPERACIÓN

PROCEDIMIENTO DE RECUPERACIÓN	
ORGANIZACIÓN: *DIPUTACIÓN PROVINCIAL DE OURENSE*	***01/02/2015***
Ámbito	*Todas las áreas, divisiones, departamento, servicios y dependencias, y tanto a sus directivos como al resto de usuarios, y también entidades y profesionales contratados bajo otras modalidades cuando en sus contratos se especifique.*
Contenido	*(La recuperación se refiere sólo a los datos, no a la recuperación de librerías de programas o del propio sistema.)* *Aquí no se detallan las recuperaciones que el sistema pueda realizar de forma automática, como es el caso de relanzamiento de procesos, o restauración de ficheros o bases de datos a partir de copias anteriores, cuando ha habido fallos de cualquier tipo que hagan necesaria la restauración.* *En dichas recuperaciones automatizadas se establecerán controles que permitan verificar el resultado, al menos por excepción: incluso de alertas que avisen cuando se ha producido algún problema: cancelación, interrupción provocada, resultado no esperado por falta de espacio...* *Especialmente en los casos más críticos y menos automatizados una vez identificados los soportes desde los que se va a producir la recuperación, éstos deben protegerse contra escritura accidental, si dicha protección es técnicamente posible, y se debe considerar la obtención inmediata de alguna copia adicional muy controlada del soporte antes de su uso.* *En los casos necesarios se verificará la fecha en que se realizó la copia del fichero, base de datos u otro objeto en general, así como el contenido previamente a la recuperación.* *Si la restauración no es total, se buscará el objeto a recuperar, preferiblemente de forma automática, como sería usando funciones tipo "search".* *Si del objeto existen varias versiones, se seleccionará la que corresponda, verificando fecha y hora, incluso tamaño u otros parámetros que contribuyan a asegurar que se está restaurando la que se quiere.* *En el caso de respaldos incrementales, se analizará la forma de hacer la restauración de dichas copias incrementales, según el sistema, para llegar a la situación deseada, que debe verificarse posteriormente.* *Si se produjera un error en el soporte, se sopesarán varias opciones según las circunstancias: realizar otros intentos, copiar el soporte con cuidado y reintentarlo, o usar otra copia que se hubiera realizado, que puede estar en el mismo lugar o en el sitio*

	de almacenamiento alternativo, en otro edificio. *Los soportes utilizados se volverán a guardar en el lugar correspondiente lo antes posible, y se cubrirán los formularios o notificaciones en su caso, así como se abrirá/cerrará incidencia, si la recuperación está relacionada con algún tipo de incidencia.* *A efectos de cumplimiento del punto 3 del artículo 94 del Reglamento de medida de seguridad, «El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos», por lo que, según el fichero, se llevará a cabo la verificación correspondiente, notificando al responsable de seguridad en el caso de ficheros de nivel medio y alto.* *En cuanto al punto 2 del artículo 94: «se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción».* *En la medida en que sea posible, se conciliará con información de las áreas usuarios correspondientes el proceso de recuperación y actualización; en determinados casos, y con el debido control, los usuarios podrían tener que repetir las últimas transacciones.* ***Ficheros de nivel Medio**: A efectos de cumplimiento del artículo 100 «... en el registro de incidencias deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación. Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos».* ***Ficheros de nivel Alto**: A fin de cumplir lo establecido en el artículo 102 del Reglamento de medidas de seguridad: «Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación». Como ya se ha comentado anteriormente, en el Edificio Simeón se mantiene una copia de respaldo para mayor seguridad y cumplir con lo estipulado en la Ley.*

AIV.4. PROCEDIMIENTO DE PUESTA AL DÍA DEL DOCUMENTO DE SEGURIDAD

PROCEDIMIENTO DE PUESTA AL DÍA DEL DOCUMENTO	
***ORGANIZACIÓN:** DIPUTACIÓN PROVINCIAL DE OURENSE*	***01/02/2015***
Ámbito	*Todas las áreas, divisiones, departamento, servicios y dependencias, y tanto a sus directivos como al resto de usuarios, y también entidades y profesionales contratados*

	bajo otras modalidades cuando en sus contratos se especifique.
Contenido	*El Documento de Seguridad ha de estar siempre al día, por lo cual ha de recibir cualquier tipo de modificación relevante que se produzca tanto desde el punto de vista técnico y organizativo como jurídico.* ***A. Modificaciones*** 1. *Hardware* 2. *Software* 3. *Bases de datos* 4. *Estructura de los ficheros* ***B. Variaciones*** 1. *Procedimientos* 2. *Funciones y obligaciones del personal* ***C.*** *Nuevas normas jurídicas: La Asesoría Jurídica deberá comunicar todas las disposiciones, de cualquier rango, aunque puedan parecer no relevantes, que se publiquen respecto a los datos de carácter personal.* ***D.*** *Relaciones con la Agencia Española de Protección de Datos. De cualquier documento que se envíe o reciba de la AGPD debe constar una fotocopia en el apartado correspondiente del Documento de Seguridad.*

AIV.5. PROCEDIMIENTO DE REGISTRO DE ACCESOS

PROCEDIMIENTO DE REGISTRO DE ACCESOS	
ORGANIZACIÓN: *DIPUTACIÓN PROVINCIAL DE OURENSE*	***01/02/2015***
Ámbito	*Todas las áreas, divisiones, departamento, servicios y dependencias, y tanto a sus directivos como al resto de usuarios, y también entidades y profesionales contratados bajo otras modalidades cuando en sus contratos se especifique.*
Contenido	*De todos los accesos a datos de nivel alto se guardará un registro de accesos que cumpla lo que se establece en el artículo 103 del Reglamento. Para ello se considerará acceso no sólo la creación, modificación o borrado de datos, sino también el acceso en modo lectura, aunque el usuario no varíe o incluso no pueda variar ningún contenido.* *Aunque en una pantalla/vista aparezca sólo un dato de nivel alto, se considerará acceso a registrar, aunque el usuario haya seleccionado el acceso (o haya modificado) sólo otros datos de nivel inferior.* *Los datos que se deben guardar son los siguientes:*

- *La identificación del usuario: debe ser inequívoca y personalizada por ser datos de nivel alto.*
- *La fecha y hora en que se realizó el acceso.*
- *El fichero accedido, entendiéndose como tal el declarado, que puede comprender varios ficheros desde el punto de vista técnico, pero que puede ser una parte de él más específica, como tabla concreta o una vista.*
- *El tipo de acceso: lectura/consulta, creación, modificación, borrado, etc.*
- *Si ha sido denegado o autorizado el acceso, circunstancia que a veces, especialmente si ha sido denegado, constará en otra plataforma, como puede ser en lo que haya recogido el sistema operativo, el sistema de gestión de bases de datos, el software o paquete de control de accesos, la herramienta single sing-on o incluso un cortafuegos.*
- *En algunos sistemas algún dato permitirá conocer otros, como el tipo de transacción que puede indicar el fichero accedido y el tipo de acceso.*

Es necesario guardar la información que permita identificar el registro accedido, considerando que se puede requerir pasado tiempo, por lo que no sería válido algo variable, como el número de orden dentro del fichero, y sí podría serlo el DNI o número de empleado, si no varía.

Al menos se deben guardar los datos de identificación y de nivel alto de todos los accesos individualizados, incluidas consultas, durante un periodo de tiempo.

Los mecanismos que permitan el registro de los datos citados estarán bajo el control directo del responsable de seguridad competente (correspondiente al fichero en cuestión), sin que deba permitir en ningún caso, la desactivación de los mismos.

Los mecanismos correspondientes estarán protegidos, o bien las aplicaciones o paquetes y sus programas, en librerías con acceso restringido, o los sistemas que produzcan el registro.

El responsable de seguridad del fichero se encargará de revisar, al menos una vez al mes, la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos con esa misma periodicidad.

AIV.6. PROCEDIMIENTO DE CIFRADO

PROCEDIMIENTO DE CIFRADO	
ORGANIZACIÓN: DIPUTACIÓN PROVINCIAL DE OURENSE	**01/02/2015**
Ámbito	*Todas las áreas, divisiones, departamento, servicios y dependencias, y tanto a sus directivos como al resto de usuarios, y también entidades y profesionales contratados*

	bajo otras modalidades cuando en sus contratos se especifique.
Contenido	*El cifrado constituye una medida técnica muy conveniente, que si bien puede tener un coste e incrementar la duración de los procesos, es imprescindible cuando se quiere garantizar la confidencialidad y la integridad de los datos que estén clasificados por la entidad como que requieren medidas de seguridad especiales, y en todo caso cuando se transmitan o estén contenidos en los soportes de datos personales de nivel alto y no se puedan aplicar otras medidas o mecanismos que garanticen:* ♦ *En el caso de **distribución de soportes**, que dicha información no sea inteligible ni manipulada durante su transporte, lo que se podría conseguir, en caso de almacenamiento, mediante copias de seguridad: los soportes estarán en todo caso debidamente protegidos y entregándose sólo a las personas expresamente autorizadas.* ♦ *En cuanto a **comunicaciones**, que la información no sea inteligible ni manipulada por terceros, porque se realicen en redes/líneas privada o virtualmente privadas estableciéndose túneles, o bien porque por el uso de protocolos, tecnologías o infraestructuras puedan garantizar el cumplimiento de lo exigido en el Reglamento.* *Distribución de soportes:* ♦ *En principio no se considerará protección suficiente, por lo que se estará a lo que recomiende Seguridad de la Información, que la obtención de soportes sea a través de paquetes o productos de copia específicos o que los soportes sean grabados por robots porque se podrían leer en sistemas similares o bien mediante conversiones o utilidades, aún sin conocer estructura o formato. En el caso de la Excma. Diputación Provincial de Ourense, como ya se ha indicado anteriormente, se cuenta con un robot de cintas que realiza el proceso de copias de seguridad.* ♦ *En el caso de copia o bajada de datos a PCs portátiles o a dispositivos móviles o PDAs, se aplicará el cifrado u otra protección suficiente, y en caso de duda se consultará con Seguridad de la Información antes de la copia o extracción de datos de nivel alto.* ♦ *Es preferible aplicaciones, paquetes o sistemas que mantengan los datos cifrados también cuando están almacenados, por lo que se evitará problemas en el caso de soportes desechados, o en el caso de salida de los soportes por operaciones de mantenimiento.* *Comunicaciones:* ♦ *El cifrado podrá producirse por el sistema operativo, por el gestor de bases de datos o sus componentes, a través del propio sistema de comunicaciones.* ♦ *En el caso de redes abiertas, como Internet, se usarán sistemas o protocolos que de forma aislada o en conjunto puedan contribuir a garantizar el cumplimiento del Reglamento, como pueden ser: SSL, TLS, SSH, FTP seguro, etc. y se evitarán aquellos que presentan debilidades como FTP no seguro,*

	TELNET y otros. ♦ *Respecto al correo electrónico externo, al menos se usará cifrado en aquellos mensajes que en su texto o en los anexos contengan datos personales de nivel alto, mediante sistemas y opciones que cumplan el Reglamento según la Seguridad de la Información, como podrían ser: S/MIME, PGP, etc. Mientras los correos sean internos y haya un nivel de protección adecuado en la red interna, no será necesario que haya medidas como las exigidas para correos externos.* ♦ *Deberán existir medidas también en los sistemas de ofimática que envíen o reciban ficheros con datos personales de nivel alto fuera de la red interna.* ♦ *En el caso de conexiones remotas desde el exterior de las instalaciones de la entidad, a través de PCs portátiles, teléfonos móviles o PDAs se establecerán VPNs y otros mecanismos que garanticen el cumplimiento del Reglamento, además de una autenticación adecuada.* ♦ *En el caso de redes locales, y especialmente inalámbricas, se seguirán los estándares de la organización, en cuanto a segmentos o dominios aislados, o dispositivos, protocolos o herramientas que refuercen la seguridad.*

AIV.7. PROCEDIMIENTO DE ALMACENAMIENTO DE COPIAS DE SEGURIDAD

PROCEDIMIENTO DE ALMACENAMIENTO DE COPIAS DE SEGURIDAD	
ORGANIZACIÓN: *DIPUTACIÓN PROVINCIAL DE OURENSE*	***01/02/2015***
Ámbito	*Todas las áreas, divisiones, departamento, servicios y dependencias, y tanto a sus directivos como al resto de usuarios, y también entidades y profesionales contratados bajo otras modalidades cuando en sus contratos se especifique.*
Contenido	*Debe conservarse una copia de respaldo y de los procedimientos de recuperación de los datos de nivel alto en un lugar diferente de aquel en el que se encuentren los equipos informáticos que los tratan, cumpliendo en todo caso las medidas de seguridad exigidas en el Reglamento de medidas de seguridad. Así pues, la Excma. Diputación Provincial de Ourense guarda las copias de seguridad en dos ámbitos:* ♦ *Una caja fuerte de seguridad, con clave de dígitos e ignífuga, situada en una parte del Servicio de Informática y Nuevas Tecnologías, pero alejada de la cabina de servidores y equipos de red.* ♦ *Una caja de seguridad en el edificio Simeón, situado próximo a la entidad pero cumpliendo las distancias y requisitos exigidos.* *Estos lugares disponen de medidas de seguridad adecuada y acceso restringido, y el transporte de soportes se realiza bajo medidas de seguridad adecuadas, que cumplan el artículo 92 del Reglamento.*

	Las copias de respaldo estarán en soportes informáticos, y los procedimientos de recuperación podrán estar en soportes informáticos o en papel, y preferentemente en ambos para facilitar su uso. *Es el caso de copias mediante transmisión de datos se cumplirá el artículo 85 del Reglamento.* *Especialmente las copias de respaldo estarán protegidas y sólo las personas autorizadas podrán acceder a los soportes. En el caso de recuperación, se protegerán los soportes contra escritura o borrado no autorizado, y preferentemente se obtendrá una copia adicional controlada previamente a su uso.* *Se verificarán periódicamente los procedimientos de copia así como los de recuperación, para garantizar que permiten la recuperación en caso necesario.* *Los soportes de copia se almacenarán en lugares y condiciones ambientales adecuados, y periódicamente se volcarán para poder verificar que son legibles y en las unidades y con los paquete o aplicaciones existentes en el momento.* *Se mantendrán las generaciones o ciclos de soportes adecuados previendo errores de lectura o en el proceso de recuperación.*

ANEXO V. MEDIDAS DE SEGURIDAD APLICABLES A LOS FICHEROS Y TRATAMIENTOS NO AUTOMATIZADOS

El Reglamento de Desarrollo de la LOPD (Real Decreto 1720/2007, de 21 de diciembre) define una serie de medidas aplicables a los ficheros en soporte no automatizado (artículos 105 y siguientes).

Por este motivo, la Diputación Provincial de Ourense ha decidido implantar las siguientes medidas de seguridad relacionadas con los datos personales que se encuentren en soporte papel:

- Definición de criterios de archivo de los documentos, que permiten garantizar la correcta conservación de estos documentos, así como la localización y consulta de la información para facilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación de los interesados (art. 106 del Reglamento).

- Seguridad de los dispositivos de almacenamiento: los documentos siempre serán guardados en un cuarto o en un armario cerrado bajo llave. Los dispositivos de almacenamiento (cajoneras, armarios, etc.) deberán disponer de mecanismos que obstaculicen su apertura (art. 107 del Reglamento).

- Custodia de los documentos: la persona que tenga acceso a estos documentos debido a las tareas que desempeñe en cumplimiento de sus funciones y obligaciones actuando como empleado de la Diputación Provincial de Ourense, deberá responsabilizarse de su custodia y protección, impidiendo que estos documentos puedan ser entregados a terceros sin la debida autorización. Asimismo, se encargará de conservarlos de forma segura, guardándolos en un cajón o armario bajo llave si por alguna circunstancia tuviera que ausentarse de su despacho o mesa de trabajo (art. 108 del Reglamento).

- Traslado de la documentación: siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado (art. 114 del Reglamento).

Los documentos que ya no tengan que ser conservados por la Diputación Provincial de Ourense deberán ser devueltos a su titular o, en otro caso, serán destruidos de forma segura, mediante una máquina trituradora de papel o procediendo a su incineración (con las adecuadas medidas de protección para evitar el riesgo de incendio).

En el caso de los ficheros declarados de nivel alto, se deberán adoptar asimismo las siguientes medidas de seguridad adicionales:

- Almacenamiento de la información: Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad (artículo 111 del Reglamento).

- La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad. Deberá

procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior (artículo 112 del Reglamento).

- El acceso a la documentación se limitará exclusivamente al personal autorizado. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad (artículo 113 del Reglamento).

ANEXO VI. AUDITORÍA DE LAS MEDIDAS DE SEGURIDAD

Para cumplir con lo establecido en el artículo 96 del Reglamento de la LOPD, la DIPUTACIÓN realizará con una periodicidad bianual una auditoría interna o externa sobre la seguridad informática, el nivel de protección de sus datos de carácter personal y el cumplimiento de lo dispuesto en el presente Documento de Seguridad.

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al Reglamento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

El informe de auditoría será analizado por el responsable de seguridad, quien propondrá al responsable de los ficheros las medidas correctoras correspondientes.

Los principales aspectos que deben ser verificados en esta auditoría son los que se indican a continuación:

- Características técnicas del sistema informático de la organización: locales y puestos de trabajo, equipamiento hardware, software y aplicaciones informáticas, infraestructura de red y de comunicaciones.
- La lista actualizada de usuarios que tienen acceso a los ficheros se corresponde con la lista de los usuarios realmente autorizados por el responsable de los ficheros.
- Procedimiento de registro de incidencias, y revisión de las incidencias registradas en los últimos meses por la organización para que, independientemente de las medidas particulares que se hayan adoptado en el momento que se produjeron, se puedan adoptar las medidas correctoras que limiten esas incidencias en el futuro.
- Procedimiento de gestión de soportes informáticos.
- La existencia de copias de respaldo que permitan la recuperación de los datos de los ficheros, así como la correcta realización del procedimiento periódico de generación de copias de seguridad.
- Procedimiento de registro y autorización de entradas y salidas de datos de carácter personal, ya sea por red o por medio de algún soporte informático.
- Medidas de seguridad físicas, técnicas y organizativas implantadas por la organización.
- Nivel de sensibilización y formación de los usuarios con acceso a datos de carácter personal.
- Tratamientos de datos encargados a terceros: regulación mediante un contrato de prestación de servicios, que incluya las correspondientes cláusulas de seguridad y protección de datos.
- Comunicaciones de datos a otras personas jurídicas.

- Cumplimiento de la obligación de información del tratamiento de datos de carácter personal a los afectados, así como del respecto de sus derechos de acceso, rectificación, cancelación y oposición.

La metodología propuesta para llevar a cabo esta auditoría es la que se presenta a continuación:

1. Identificación de los sistemas a auditar. Incluirán los servicios contratados a terceros como parte del sistema auditado.

2. Organización de los papeles de trabajo y check-lists para realizar la auditoría.

3. Elaboración del calendario de entrevistas, especificando el contenido y la duración aproximada.

4. Entrega al responsable del fichero, al responsable de informática y al responsable de seguridad de un memorando formal en el que se detallarán los temas y datos específicos necesarios para llevar a cabo la auditoría.

5. Evaluación objetiva del funcionamiento operativo y de la información del aspecto de seguridad o procedimiento auditado.

6. Información al responsable de seguridad y al responsable de informática de la organización del transcurso de la auditoría.

7. Redacción del informe final, que incluirá los motivos de la evaluación efectuada, así como los comentarios clasificados y las recomendaciones o acciones a realizar. Dicho informe también incluirá las siguientes conclusiones:

    a. Exposición de las normas o procedimientos (propios o legales) que han sido violados, indicando las causas.

    b. Descripción del riesgo potencial que entraña la debilidad y su impacto en la organización.

8. Distribución del informe final al responsable del fichero, al responsable de seguridad y al responsable de informática.

9. Seguimiento de las acciones correctoras propuestas como conclusión del trabajo de auditoría.