DOCUMENTO DE SEGURIDAD
PARA FICHERO DE INSCRITOS Y AFILIADOS AL PARTIDO POLÍTICO LEGANEMOS

NIVEL ALTO DE SEGURIDAD

Versión: 1.1 14 de Mayo de 2018

HOJA DE CONTROL DE VERSIONES DEL DOCUMENTO

Versión	Fecha	Realizado por	Cambios (respecto a la versión anterior)	Aprobado por
1.0	01/11/2016	Responsable de Seguridad	Documento base	Responsable del Fichero
1.1	14/05/2018	Responsable de Seguridad	Revisión nueva normativa	Responsable del Fichero

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El presente Documento y sus Anexos, redactados en cumplimiento de lo dispuesto en el RLOPD, responde a la obligación establecida en el artículo 88 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/19999, de 13 de diciembre, y el Reglamento General de Protección de Datos (RGPD) aprobado el 25 de Mayo de 2016, de protección de datos de carácter personal, en el que se regulan entre otras, las medidas de seguridad para los ficheros y tratamientos automatizados que contengan datos de carácter personal.

Los ficheros de datos a los que se refiere el presente documento, que en adelante denominaremos FICHERO, dado de alta en la Agencia Española de Protección de Datos a 25 de Octubre de 2016 como nivel de seguridad ALTO atendiendo a las condiciones descritas en el artículo 81 del Real Decreto citado.

El contenido de este documento queda estructurado como sigue:

1. Ámbito de aplicación del documento.
2. Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento.
3. Información y obligaciones del personal.
4. Procedimientos de notificación, gestión y respuestas ante las incidencias.
5. Procedimientos de revisión.
6. ANEXOS.

2. ÁMBITO DE APLICACIÓN DEL DOCUMENTO

El presente documento ha sido elaborado bajo la responsabilidad de las personas descritas en portada (Responsables de Seguridad y Fichero) que encargadas del tratamiento interno, se comprometen a implantar, revisar y actualizar el cumplimiento del documento así como la actualización de esta Normativa de Seguridad de obligado cumplimiento para todo personal con acceso a los datos protegidos o a los sistemas de información que permiten el acceso a los mismos.

Todas las personas que tengan acceso a los datos del Fichero, ya sea del automatizado o del registro en papel, se encuentran obligados por ley a cumplir lo establecido en este documento. Una copia de este documento, le será entregada, para su conocimiento, a cada una de las personas autorizadas para acceder o manipular los datos del Fichero, siendo obligatoria al haber firmado la recepción del mismo.

Los ficheros sujetos a las medidas de seguridad establecidas en este documento, con indicación del nivel de seguridad ALTO, son los siguientes:

- FICHERO automatizado en formato electrónico
- Registro de FICHERO en papel

En el Anexo I se describen detalladamente cada uno de los ficheros o tratamientos, junto con los aspectos que les afecten de manera particular.

Este Documento deberá mantenerse permanentemente actualizado. Cualquier modificación relevante conllevará la revisión de la normativa incluida y si procediera, su modificación total o parcial, siendo reflejado en el control de versiones del documento. Dado el continuo seguimiento de las distintas tablas existentes en los ANEXOS, el rellenado de estas tablas ante las distintas peticiones, no supondrán un cambio en el control de versiones del presente documento.

3. FUNCIONES Y OBLIGACIONES DEL PERSONAL

Además del **Responsable del fichero**, el personal afectado por esta normativa se podría clasificar en algunas de las categorías siguientes:

1. **Responsable del Fichero**, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal en su artículo 3, apartado d), define al responsable del fichero o tratamiento de la siguiente forma: "Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento". Según firmado en el registro de la AGPD sobre el alta del Fichero para Leganemos.

2. **Encargados Interno del tratamiento,** serán designados por Responsable de los ficheros, de entre el personal adscrito al partido que modificará el fichero, supervisará la aplicación a los datos contenidos en el fichero, así como las aplicaciones de las medidas organizativas y de seguridad plasmadas en el Documento de seguridad.

3. **Responsable de Seguridad**, tendrá las responsabilidades fijadas en la LOPD y su Reglamento de Desarrollo. Si no se explicita que sus funciones recaigan en una persona distinta, será el Encargado Interno del Tratamiento el que las asuma.

Es importante destacar que no se procederá a ningún tipo de tratamiento de datos por personas ajenas. Este documento es de obligado cumplimiento para todos ellos.

4. MEDIDAS, NORMAS, PROCEDIMIENTOS, REGLAS Y ESTÁNDARES

El acceso a los datos del Fichero se realizará ateniéndose a las medidas, normas, procedimientos, reglas y estándares que se describen en este capítulo y que serán de obligado cumplimiento para todo el personal relacionado. Si bien cabe destacar que este personal siempre será personal propio y nunca ajeno.

4.1.- Identificación y autenticación del personal

Solamente el personal expresamente autorizado por el responsable del Fichero y los nombrados en el Anexo II, según sus cargos, podrán tener acceso a los datos del Fichero siguiendo los distintos procedimientos a rellenar en los Anexos III y IV.

El responsable del Fichero establecerá un mecanismo que proteja el acceso a los datos del Fichero de parte de personal no identificado. Medidas y normas relativas a la identificación y autenticación del personal autorizado para acceder a los datos personales.

FICHERO AUTOMATIZADO

El fichero se encontrará cifrado en un servidor privador perteneciente a la organización. Por tanto se dotará a la persona responsable de este fichero un acceso único a este servidor para el acceso a este Fichero así como la contraseña de cifrado MD5 correspondiente. Estas contraseñas serán renovadas mediante un mecanismo de periodicidad y ante posibles vulnerabilidades descubiertas.

Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia para su modificación.

REGISTRO DE FICHERO EN PAPEL

Este registro de fichero se encontrará ubicado en un armario cerrado con llave dentro de un espacio privado del local establecido para el Grupo. Por tanto se dotará a la persona responsable de este fichero de una llave para poder acceder al recurso.

Cada usuario será responsable de la pertenencia de la llave y, en caso de pérdida o robo de la misma, deberá registrarlo como incidencia para su pronta corrección.

4.2.- Control de acceso

El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados mediante el cifrado y gestión de contraseñas y llaves para el acceso.

Exclusivamente el Responsable del Fichero está autorizado para conceder, alterar o anular el acceso sobre los datos y los recursos, conforme a los criterios establecidos.

Se podrá solicitar una autorización al Responsable del Fichero mediante solicitud firmada por el órgano competente del Partido Político siendo registrada su solicitud previa.

En el Anexo I, se incluye la relación de usuarios actualizada con acceso autorizado a cada sistema de información. Asimismo, se incluye el tipo de acceso autorizado para cada uno de ellos. Esta lista deberá mantenerse actualizada con una periodicidad mínima mensual por el Responsable de Seguridad.

4.3.- Registro de accesos

FICHERO AUTOMATIZADO

El fichero se encuentra alojado en un servidor seguro contratado por Leganemos. Por tanto, se registra dispone de un registro de accesos completos facilitado por el propio servidor.

Para ello solo se podrá acceder al servidor UNIX via web con un usuario y contraseña facilitados a las personas encargadas. Estas contraseñas podrán y deberán ser modificadas regularmente.

El responsable de seguridad revisará al menos una vez al mes la información de control registrada y elaborará un informe en caso de que sea necesario.

No será necesario el registro de accesos cuando:

- Solamente haya una persona con acceso al fichero.
- el responsable del fichero garantice que sólo él tiene acceso y trata los datos personales, y se haga constar en el documento de seguridad.

REGISTRO DE FICHERO EN PAPEL

El acceso a la documentación se limita exclusivamente al personal autorizado. El local donde se encuentra este registro de Fichero deberá contar con los medios mínimos de seguridad en su entrada. Además el registro se ubicará en una zona privada y con mayor seguridad donde solo podrán acceder al Responsable del Fichero y el encargado autorizado a ello.

4.4.- Gestión de soportes y documentos

Los soportes que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y serán almacenados en en formato papel en un lugar de acceso restringido dentro del Grupo Municipal y el Fichero automatizado será cifrado en un servidor seguro, lugar de acceso restringido al que solo tendrán acceso las personas con autorización que se relacionan a continuación:

- Responsable de Fichero
- Encargados internos de tratamiento del Fichero

Los siguientes soportes "Registro de Fichero en Papel" se identificarán utilizando los sistemas de etiquetado siguientes por carpetas:

- Alta_Año_Mes; Contendrá las fichas de altas recibidas y tramitadas durante el mes y indicado.
- Baja_Año_mes: Contendrá las fichas dadas de baja, junto con la justificación firmada por la persona dada de baja en los casos necesarios.

El soporte "Fichero automatizado" será almacenado en el servidor privado del Partido Leganemos dado de alta por el Responsable de Fichero. Para ello se creará una base de datos MySql que solo podrá ser accesible por usuarios creados para el Responsable del Fichero y por el Encargadx interno del tratamiento, además solo se podrá acceder desde el cuadro de gestión del hosting, asegurando la trazabilidad de los accesos y la recuperación ante pérdida de datos. Esta base de datos será cifrada mediante protocolos de cifrado accesibles en MySQL tipo MD5, SHA o SHA1, siendo conocidas únicamente las contraseñas por el responsable del fichero y renovadas mes a mes. La información privada almacenada en este medio se actualizará únicamente al comienzo de cada mes.

El soporte del Registro de Fichero en papel se almacenará en un lugar de acceso restringido dentro del local perteneciente al Grupo Municipal. Allí se habilitará un acceso mediante llave única que será responsabilidad del Responsable del Fichero.

La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos en correos electrónicos, fuera de los locales bajo el control del responsable del tratamiento, deberá ser autorizada por el responsable del fichero o aquel en que se hubiera delegado de acuerdo al siguiente procedimiento:

- Dada la necesidad eventual de necesitar un listado de las personas censadas en el registro a modo de comprobante en Asambleas de Inscritos, se procederá a realizar una copia del Fichero automatizado con la información mínima y necesaria para poder reconocer a una persona (véase nombre, apellidos y dni).

En el Anexo III se incluirán los documentos de autorización relativos a la salida de soportes que contengan datos personales.

Los soportes que vayan a ser desechados, deberán ser previamente bloqueados de forma que no sea posible el acceso a la información contenida en ellos o su recuperación posterior. Una vez cesa la finalidad, la legislación precisa que hay que proceder a la cancelación. La cancelación dará lugar, al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión. Se

entiende por bloqueo de datos la identificación y reserva de datos con el fin de impedir su tratamiento. Mientras los datos están bloqueados es como si estuvieran cancelados a todos los efectos.

Por tanto, una vez cesa la finalidad los datos antes de desaparecer porque se bloquean. Podría entenderse este bloqueo como una "congelación" del dato. Éste queda congelado en la fecha de cancelación, nadie lo puede usar, consultar o modificar salvo para casos de responsabilidad. Por ello, no pueden estar disponibles ni siquiera para el ejercicio de derechos como el derecho de acceso.

En el traslado de la documentación exportada será realizado por el Responsable de Fichero o en su defecto la persona delegada para tal uso. Para tal uso, se realizará una copia del Fichero automatizado minutos antes del traslado al lugar destinado para su uso. En el caso del traslado de fichas de alta para el Registro de Fichero en papel, éstas serán trasladadas una vez validadas por el Responsable del Fichero o en su defecto la persona Encargada para el tratamiento interno de datos.

REGISTRO DE ENTRADA Y SALIDA DE SOPORTES

Las salidas y entradas de soportes correspondientes a los ficheros de nivel alto, serán registradas de acuerdo al siguiente procedimiento:

Entradas

- REGISTRO EN PAPEL
    - Serán consideradas entradas las fichas de alta validas por el Responsable de Ficheros.
    - Quincenalmente o mensualmente se validarán las fichas de altas recibidas correctamente y se procederán a su registro en el lugar habilitado para ello.
- AUTOMATIZADO
    - Mensualmente se procederá a automatizar las altas validadas en el registro en papel.
    - El Responsable de Fichero o Encargado de tratamiento interno de datos procederá a actualizar el registro automatizado con las nuevas altas.
    - Para ello actualizará el registro con los nuevos datos personales cifrados con la tecnología adecuada. En el caso del Encargado de tratamiento de datos tendrá que facilitar la contraseña de cifrado al Responsable de Fichero.

Salidas

- AUTOMATIZADO
    - Ante Asambleas o actos destinados a inscritos se procederá a exportar los datos mínimos de personas del registro para su correcta verificación en el lugar indicado.

El registro de entrada y salida de soportes se gestionará mediante el formulario del ANEXO VIII – Registro de Entrada y Salida de Soportes, donde se registrará la hora, fin y personas que realizarán la entrada/salida.

CRITERIOS DE ARCHIVO

El archivo de los soportes o documentos se realizará de acuerdo con los criterios descritos anteriormente.

- REGISTRO EN PAPEL
    - Serán consideradas entradas las fichas de alta validas por el Responsable de Fichero.
    - Quincenalmente o mensualmente se validarán las fichas de altas recibidas correctamente y se procederán a su registro en el lugar habilitado para ello.
- AUTOMATIZADO
    - Mensualmente se procederá a automatizar las altas validadas en el registro en papel.
    - El Responsable de Fichero o Encargado de tratamiento interno de datos procederá a actualizar el registro automatizado con las nuevas altas.
    - Para ello actualizará el registro con los nuevos datos personales cifrados con la tecnología adecuada. En el caso del Encargado de tratamiento de datos tendrá que facilitar la contraseña de cifrado al Responsable de Fichero.

ALMACENAMIENTO DE LA INFORMACIÓN

Los siguientes dispositivos; carpetas etiquetadas para altas y carpetas etiquetadas para bajas se utilizarán para guardar los documentos con datos personales.

Estos elementos de almacenamiento respecto de los documentos con datos personales, se encuentran en ubicados en el local designado al Grupo Municipal, bajo un acceso restringido por una llave distinta a la entrada del local.

CUSTODIA DE SOPORTES

En tanto los documentos con datos personales no se encuentren archivados en los dispositivos de almacenamiento indicados en el punto anterior, por estar en proceso de tramitación, las personas que se encuentren a su cargo deberán custodiarlos e impedir el acceso a personas no autorizadas.

4.5.- Acceso a datos a través de redes de comunicaciones

Las medidas de seguridad exigibles a los accesos a los datos de carácter personal a través de redes de comunicaciones, sean o no públicas, garantizarán un nivel de seguridad equivalente al exigido para los accesos en modo local.

Los datos personales correspondientes a los ficheros de nivel alto correspondientes al Fichero Automatizado, que se transmitan a través de redes públicas o inalámbricas de comunicaciones electrónicas se realizará cifrando previamente estos datos mediante el protocolo MD5, SHA o SHA1 con una contraseña individual.

4.6.- Régimen de trabajo fuera de los locales de la ubicación del fichero

Únicamente se podrán llevar a cabo los siguientes tratamientos de datos personales sobre las fichas de registro fuera de los locales del responsable del;

Validar fichas de altas recibidas

Recibir bajas de fichas,

La validación de estas fichas serán realizadas siempre por el Responsable del Fichero o en su defecto la persona delegada o encargada del tratamiento. La recepción de datos para bajas serán recibidos por el responsable del fichero en caso de recepción electrónica o por personal autorizado del partido en el caso de recepción física. En este caso, la persona que los recoja tendrá que informar obligatoriamente del procedimiento y normativa vigente de bajas.

4.7.- Ficheros temporales o copias de trabajo de documentos

Los ficheros temporales o copias de documentos creados exclusivamente para trabajos temporales o auxiliares como pueden ser la exportación del registro, deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el Reglamento de medidas de seguridad, y serán bloqueados una vez que hayan dejado de ser necesarios para los fines que motivaron su creación, manteniéndoles en el propio registro el tiempo necesario que cubra las necesidades legales ante trámites judiciales que pudieran darse.

4.8.- Copia o reproducción

La realización de copias o reproducción de los documentos con datos personales sólo se podrán llevar a cabo bajo el control del siguiente personal autorizado Responsable de Fichero y/o Encargado interno de tratamiento de Datos.

Las copias desechadas deberán ser destruidas imposibilitando el posterior acceso a la información contenida.

4.9.- Copias de respaldo y recuperación

Se realizarán copias de respaldo, salvo que no se hubiese producido ninguna actualización de los datos, con periodicidad mensual. Además, el propio servidor donde se ubica el registro automatizado dispone de políticas de respaldo completas, por tanto siempre se dispone de copias de respaldo del fichero de los últimos meses, como mínimo.

Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. En el caso de los ficheros parcialmente automatizados, se grabarán manualmente los datos, pudiéndose recuperar del registro automatizado.

El responsable del fichero verificará semestralmente los procedimientos de copias de respaldo y recuperación de los datos.

Las pruebas anteriores a la implantación o modificación de sistemas de información se realizarán con datos reales previa copia de seguridad, y garantizando el nivel correspondiente al tratamiento realizado.

En el Anexo I se detallan los procedimientos de copia y recuperación de respaldo para cada fichero.

4.10.- Responsable de seguridad

Se designa como responsable de seguridad que con carácter general se encargará de coordinar y controlar las medidas definidas en este documento de seguridad.

En ningún caso, la designación supone una exoneración de la responsabilidad que corresponde al Responsable de Fichero como responsable del fichero de acuerdo con el RLOPD.

El responsable de seguridad desempeñará las funciones encomendadas durante el periodo de desempeño del cargo. Una vez transcurrido este plazo *el Responsable del Fichero* podrá nombrar al mismo responsable de seguridad o a otro diferente.

En el Anexo II se encuentran las copias de los nombramientos de responsables de seguridad.

5. INFORMACIÓN Y OBLIGACIONES DEL PERSONAL

INFORMACIÓN AL PERSONAL

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias del incumplimiento de las mismas, serán informadas de acuerdo con el siguiente procedimiento:

- Toda persona que ocupe un cargo designado en ese documento tendrá copia de ese documento.
- El receptor de cada copia firmará la recepción de la misma.
- El responsable de seguridad podrá efectuar preguntas a los distintos encargados sobre el contenido del documento periódicamente.

FUNCIONES Y OBLIGACIONES DEL PERSONAL

Todo el personal que acceda a los datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.

Constituye una obligación del personal notificar Responsable de Fichero y al Responsable de Seguridad las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este Documento, y en concreto en el apartado de "Procedimientos de notificación, gestión y respuesta ante las incidencias."

Todas las personas deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo.

Funciones y obligaciones de Responsable de Fichero:

- Absoluta confidencialidad en cuanto a los datos del Fichero
- Conocer todas las medidas, normas, procedimientos y reglas descritas en este documento.
- Mensualmente actualizar el Fichero con los nuevos datos
- Absoluta confidencialidad con las contraseñas de cifrado del Fichero automatizado.
- Delegar autorizadamente a otra persona en caso donde no puede ejercer alguna tarea.

Funciones y obligaciones de los Encargados Internos del Tratamiento de datos:

- Absoluta confidencialidad en cuanto a los datos del Fichero
- Conocer todas las medidas, normas, procedimientos y reglas aplicables a su ámbito.
- Informar al Responsable del Fichero de todo el tratamiento realizado.

El personal que realice trabajos que no impliquen el tratamiento de datos personales tendrán limitado el acceso a estos datos, a los soportes que los contengan, o a los recursos del sistema de información.

CONSECUENCIAS DEL INCUMPLIMIENTO DEL DOCUMENTO DE SEGURIDAD

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente documento por el personal afectado, se sancionará conforme a Código Ético del partido y a la normativa vigente.

6. PROCEDIMIENTOS DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS

Se considerarán como "incidencias de seguridad", entre otras, cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como a cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal del Fichero, entendiendo bajo como anomalías tres vertientes; confidencialidad, integridad y disponibilidad de los datos.

El mantener un registro de incidencias que comprometan la seguridad del Fichero es una herramienta imprescindible para hacer un correcto seguimiento y corrección de las anomalías que surjan y posibilitar la prevención de posibles ataques a la seguridad establecida.

Por tanto;

- Se habilita un registro de incidencias, Anexo VI, con el fin de registrar 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 hacerla saber al Responsable de Seguridad o Responsable de Fichero para su registro.
- El conocimiento y no notificación de una incidencia por parte de un usuario será considerado una falta contra la seguridad del Fichero.
- 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.

En el registro de incidencias se consignarán también los procedimientos de recuperación de datos que afecten a los ficheros, pudiendo llegar a proceder a una recuperación completa de datos así como a cambios o revisión de procedimientos, contraseñas…etc.

Para ejecutar los procedimientos de recuperación de datos en los ficheros mencionados en el párrafo anterior, será necesaria la autorización por escrito del responsable del fichero.

En el Anexo III se incluirán los documentos de autorización del responsable del fichero relativos a la ejecución de procedimientos de recuperación de datos.

7. PROCEDIMIENTOS DE REVISIÓN

El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información, en el contenido de la información incluida en los ficheros o como consecuencia de los controles periódicos realizados por el Responsable de Seguridad. En todo caso se entenderá como cambio relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

Así mismo, deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

AUDITORÍA

Con una periodicidad al menos semestral, se procederá a realizar una auditoría interna para comprobar el correcto cumplimiento del seguimiento de este documento:

- Se comprobará que la lista de autorizados del Anexo II se corresponde con la lista de usuarios realmente autorizados.
- Se comprobará la existencia de copias de respaldo del Fichero automatizado
- Los encargados del tratamiento y responsable de Fichero indicarán los cambios realizados en las contraseñas durante ese período
- Analizará el registro de incidencias tomando medidas oportunas
- Comprobará el correcto funcionamiento del traslado y exportación de datos en este período
- Los resultados de estos controles serán registrados en el Anexo IX.

Con carácter extraordinario deberá realizarse cuando se lleven a cabo modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas, con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado.

El informe analizará la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificará las deficiencias y propondrá las medidas correctoras o complementarias necesarias.

Los informes de auditoría han de ser analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras y quedará a disposición de la Agencia Española de Protección de Datos, o en su caso de las autoridades de control de las comunidades autónomas.

ANEXOS

DOCUMENTO DE SEGURIDAD

ANEXO I: DESCRIPCIÓN DE FICHEROS

Actualizado a*:*

<Se incluirá un anexo de este tipo por cada fichero incluido en el ámbito del

Documento de seguridad, podrían denominarse ANEXO I a, b, c, etc .>.

- Nombre del fichero o tratamiento: *<rellenar con nombre del fichero >.*
- Unidad/es con acceso al fichero o tratamiento: *<especificar departamento unidad con acceso al fichero, si aporta alguna información >.*
- Identificador y nombre del fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos: *<rellenar los siguientes campos con los datos relativos a la inscripción del fichero en el Registro General de Protección de Datos (RPGD) >.*
  - Identificador: *<código de inscripción >*
  - Nombre: *<nombre inscrito >*
  - Descripción: *<descripción inscrita >*
- Estructura del fichero principal: *<incluir los tipos de datos personales contenidos en el fichero, especificando aquellos que, por su naturaleza, afectan al nivel de medidas de seguridad a adoptar, según lo indicado en el artículo 81 del Reglamento de desarrollo de la LOPD >.*
- Información sobre el fichero o tratamiento
  - Procedimiento de recogida: *<encuestas, formularios en papel, Internet. ..>.*
  - Sistema de tratamiento: *<automatizado, manual o mixto >.*
  - Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición: *<indicar la unidad y/o dirección. Deben preverse además, los procedimientos internos para responder a las solicitudes de ejercicio de derechos de los interesados >.*
  - Descripción detallada de las copias de respaldo y de los procedimientos de recuperación *<Especificar la periodicidad de las copias (que debe ser al menos semanal). Si se trata de ficheros manuales y tienen prevista alguna medida en este sentido, detallarla >.*
  - Funciones del personal con acceso a los datos personales: *<Especificar las diferentes funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y sistema de información específicos de este fichero >.*
  - Descripción de los procedimientos de control de acceso e identificación: *<Cuando sean específicos para el fichero >.*
  - Relación actualizada de usuarios con acceso autorizado: *<Relacionar todos los usuarios que acceden al fichero, con especificación del tipo o grupo de usuarios al que pertenecen, su clave de identificación, nombre y apellidos, unidad, fecha de alta y fecha de baja. Si la relación se mantiene de forma informatizada, indicar aquí cual es el sistema utilizado y la forma de obtener el listado. No*

obstante, siempre que sea posible, es conveniente imprimir la relación de usuarios y adjuntarla periódicamente a este Anexo >.

ANEXO II: NOMBRAMIENTOS

<Adjuntar original o copia de los nombramientos que afecten a los diferentes perfiles incluidos en este documento, como el del responsable de seguridad >.

Función	Persona	Fecha de Alta	Fecha de Baja
Responsable de Fichero			
Responsable de Seguridad			
Encargada de Tratamiento			

ANEXO III: AUTORIZACIONES DE SALIDA O RECUPERACIÓN DE DATOS

<Adjuntar las autorizaciones que el responsable del fichero ha firmado para la salida de soportes que contengan datos de carácter personal, incluyendo aquellas que se refieran a salidas que tengan un carácter periódico o planificado. Incluir asimismo, las autorizaciones relativas a la ejecución de los procedimientos de recuperación de datos >.

Persona encargada	Descripción (Soporte, contenido, finalidad, destino, medio de envío)	Fecha autorización

ANEXO IV: DELEGACIÓN DE AUTORIZACIONES

<En su caso, personas en las que el responsable del fichero ha delegado. Indicar las autorizaciones, tales como: salida de dispositivos portátiles, la copia o reproducción de documentos en soporte papel,… >.

Persona delegada	Cargo delegado	Descripción	Fecha de Alta	Fecha de Baja

ANEXO V: INVENTARIO DE SOPORTES

<Si el inventario de soportes no está informatizado, recoger en este anexo la información al efecto, según lo indicado en el apartado de "Gestión de soportes y Documentos" de este documento. Los soportes deberán permitir identificar el tipo de información, que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en este documento >.

<Si el inventario de soportes está informatizado, indicar la aplicación o ruta de acceso del archivo que lo contiene >.

Soporte	Descripción	Etiqueta	Lugar	Fecha de Alta

ANEXO VI: REGISTRO DE INCIDENCIAS

<Si el registro de incidencias no está informatizado, recoger en este anexo la información al efecto, según lo indicado en el apartado de "Procedimientos de notificación, gestión y respuesta ante las incidencias" de este documento>.

<Si el registro de incidencias está informatizado, indicar la aplicación o ruta de acceso del acceso del archivo de lo contiene >.

Nivel incidencia	Fecha encontrada	Persona	Descripción detallada	Procedimiento de gestión

ANEXO VII: REGISTRO DE ENTRADA Y SALIDA DE SOPORTES

<Si el registro de entrada y salida de soportes al que se refiere el apartado de "Gestión de soportes y documentos", y que es obligatorio a partir del nivel medio, no está informatizado, recoger en este anexo la información al efecto, según lo indicado el artículo 97 del RLOPD >.

<Si el registro de entrada y salida está informatizado, indicar la aplicación o ruta de acceso del acceso del archivo de lo contiene >.

Persona encargada	Descripción (Soporte, contenido, finalidad, destino, medio de envío)	Fecha autorización

ANEXO VIII: MEDIDAS ALTERNATIVAS

<En el caso de que no sea posible adoptar las medidas exigidas por el RLOPD en relación con la identificación de los soportes, los dispositivos de almacenamiento de los documentos o los sistemas de almacenamiento de la información, indicar las causas que justifican que ello no sea posible y las medias alternativas que se han adoptado >.

Persona encargada	Descripción detallada (soporte, causas)	Fecha

ANEXO IX. CONTROLES PERIÓDICOS Y AUDITORÍAS

<<Contendrá los resultados de los controles periódicos descritos en el apartado 10 y de las auditorías realizadas por el responsable de Seguridad>>

Usuarios correctos	Copias de respaldo	Cambio de contraseñas	Registro de incidencias	Traslado de datos	Fecha