**PLAN DE AUDITORÍA**



**ÍNDICE**

1. **OBJETIVO…………………………………………………………………………………....2**
2. **DETERMINACIÓN DEL ALCANCE DE AUDITORÍA………………………………….3**
3. **PLANIFICACIÓN…………………………………………………………………………….3**
4. **RECOLECCIÓN DE DATOS………………………………………………………………..4**
5. **EVALUACIÓN DE PRUEBAS……………………………………………………………....6**
   1. Nivel de seguridad (BÁSICO, ALTO, MEDIO)
6. **OBJETIVO**

*Determinar si se han establecido, si son adecuadas y si se cumplen las medidas de seguridad recogidas en el Título VIII del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Su realización es obligatoria para ficheros de nivel medio y alto. Puede ser interna o externa. Debe realizarse al menos cada dos años. Excepcionalmente, si se han realizado modificaciones sustanciales en el sistema de información, deberá realizarse una auditoría para comprobar la adecuación, adaptación y eficacia de las medidas de seguridad. Esta auditoría iniciará el cómputo de dos años.*

Por consiguiente, se evaluará el sistema de ficheros de carácter personal, con el propósito de determinar su estado, el cumplimiento de las normas, nivel de fiabilidad… además de verificar si los métodos de control que se utilizan en todos los casos son eficaces para la protección de los datos. Se tendrá en cuenta la normativa vigente de la Protección de los Datos de Carácter Personal.

Además de lo anteriormente mencionado se tendrán en cuenta los siguientes puntos:

1. En el caso de posibles deficiencias se propondrán soluciones que mejoren su propósito.
2. Se conseguirá una mejora en cuanto a las medidas de seguridad que serán auditadas para conseguir un proceso de mejora continua.
3. En cuanto a lo que se refiere a datos personales se prestará especial atención, comprobando si cumplen lo recogido en el Título VIII del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y ajustar a dicha normativa.
4. Se concienciará al personal sobre la importancia de asegurar los datos personales para evitar su uso incorrecto y asegurando así que dichos datos se encuentren protegidos.
5. La auditoría se realizará cada dos años.
6. **DETERMINACIÓN DEL ALCANCE DE AUDITORÍA**

El presente informe corresponde al período comprendido entre el 15/04/2019 y 3/05/2019 se analiza el documento de seguridad del ministerio de hacienda relacionado con los ficheros de datos de carácter personal.

Es decir el grado de adaptación de la entidad según lo establecido al Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) .

La finalidad de la auditoría es comprobar las medidas y verificación de las normativas según lo establecido en la RGPD , también se proporcionarán medidas, observaciones y propuestas para la correcta adecuación

Ficheros a analizar:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Fichero** | Ayuda  a  autónomos | Proveedores | Empleados | Nóminas | Gestión Económico administrativa | Control de visitas | Video  Vigilancia | Video  Vigilancia CPD | Historiales clínicos |
| **Nivel/**  **Criterio** | Básico | Básico | Básico | Básico | Básico | Básico | Básico | Básico | Alto |

1. **PLANIFICACIÓN**

La auditoría realizada en este documento estará basada en el Documento de Seguridad de una Agencia Pública de

Gestión de Ayudas, en este caso, el ministerio de Hacienda. Dicho documento fue entregado por el profesor de la

asignatura a los alumnos que figuran como realizadores de esta auditoría, con el objetivo de su posterior análisis.

Para llevar a cabo la auditoría, será necesario contar con una serie de recursos indispensables para su realización.

Entre estos recursos cabría destacar elementos de software y hardware como ordenadores, y entornos de trabajo como en Word o Google Drive.

En cuanto a las instalaciones, dispondremos de entornos de trabajo adecuados como la biblioteca de la facultad de

informática de la UCM.

A su vez, todo el contenido de la auditoría estará basado en la Guía de Seguridad de Datos de la Agencia Española de Protección de datos, que asienta las bases y objetivos a cumplir por los documentos de seguridad de las distintas agencias y empresas, así como la forma correcta en la que se debe realizar su correspondiente auditoría.

A continuación se detallarán las distintas tareas a realizar junto con los miembros del equipo que las desempeñarán:

|  |  |
| --- | --- |
| **TAREA** | **MIEMBROS DEL EQUIPO** |
| Objetivo | Carla |
| Determinación del alcance de auditoría | Rocío |
| Planificación | Laura |
| Recolección de datos | Evald Alin |
| Evaluación de pruebas | Laura |
| Elaboración del informe | Todo el equipo |
| Adaptación a la nueva LOPD | Rocío y Carla |

1. **RECOLECCIÓN DE DATOS**

En cuanto a los datos recabados, los cuales están descritos en el Documento de Seguridad, se tendrán clasificados según lo siguiente:

* Relación de ficheros, estructura y contenido: los datos están divididos en nueve ficheros de carácter personal. A continuación se presenta el nombre, la estructura, el contenido, el administrador y el nivel de las medidas a adoptar de cada uno de ellos.
  + 1-Fichero “Ayuda a autónomos”: la estructura y el contenido del fichero es lo siguiente: nombre y apellidos, NIF, N.o de afiliación a la seguridad social, últimos tres recibos abonados a la seguridad social como autónomos, teléfono, dirección completa y fotografía reciente. El administrador es el director general de la agencia pública de ayudas y el nivel de seguridad a adoptar es básico.
  + 2-Fichero “Proveedores”: la estructura y el contenido del fichero es lo siguiente: télefono, mail, puesto desempeñado. El administrador es el director general de la agencia pública de ayudas y el nivel de seguridad a adoptar es básico.
  + 3-Fichero “Empleados”: la estructura y el contenido del fichero es lo siguiente: nombre y apellidos, NIF. El administrador es el director general de la agencia pública de ayudas y el nivel de seguridad a adoptar es básico.
  + 4-Fichero “Nóminas”: la estructura y el contenido del fichero es lo siguiente: nombre y apellidos, NIF, grado de discapacidad(si procede). El administrador es el director general de la agencia pública de ayudas y el nivel de seguridad a adoptar es básico.
  + 5-Fichero “Gestión económica administrativa”: la estructura y el contenido del fichero es lo siguiente: datos administrativos. El administrador es el director general de la agencia pública de ayudas y el nivel de seguridad a adoptar es básico.
  + 6-Fichero “Control de visitas”: la estructura y el contenido del fichero es lo siguiente: DNI de la persona que accede. El administrador es el director general de la agencia pública de ayudas y el nivel de seguridad a adoptar es básico.
  + 7-Fichero “Videovigilancia”: no hay fichero. El administrador es el director general de la agencia pública de ayudas y el nivel de seguridad a adoptar es básico.
  + 8-Fichero “Videovigilancia CPD”: la estructura y el contenido del fichero es lo siguiente: fotogramas . El administrador es el director general de la agencia pública de ayudas y el nivel de seguridad a adoptar es básico.
  + 9-Fichero “Historiales clínicos empleados”: la estructura y el contenido del fichero es lo siguiente: datos de la salud de los empleados. El administrador es el director general de la agencia pública de ayudas y el nivel de seguridad a adoptar es básico.
* Políticas de seguridad y procedimientos: se tienen políticas de seguridad y procedimientos en los siguientes aspectos:
  + Registro de incidencias: se consideran “incidencias de seguridad” cualquier incumplimiento de la normativa desarrollada en el Documento de Seguridad. El procedimiento a seguir será que el jefe de departamento donde se haya producido la incidencia emita un informe explicando detalladamente la incidencia. El registro se realizará mediante una aplicación informática enlazada a una base de datos de uso exclusivo para las incidencias.
  + Copias de respaldo y recuperación: se realizan copias de respaldo una vez a la semana(salvo actualización de los datos). Para la recuperación de los datos, se tiene una herramiento de reconstrucción de documentos que garantizan su recuperación en el estado inmediatamente anterior a la pérdida de estos. El responsable del fichero revisa semestralmente los procedimientos de copias de respaldo y recuperación de datos.
  + Identificación y cifrado: toda persona con acceso a datos de carácter personal debe ser validada por una persona autorizada del responsable del fichero. Toda persona que quiera acceder a datos de carácter personal debe loguearse correctamente mediante una contraseña validada por el Sistema. Dichas contraseñas están en formato hash con un nivel SHA2 o superior. La contraseña debe contener un mínimo de 8 caracteres, formados por dígitos, letras y caracteres especiales. Cada contraseña es cambiada en un periodo entre 3 y 6 meses. No se usan palabras que aparecen en diccionarios. No se usan elementos personales. Se evitan secuencias fáciles de teclado.
  + Ficheros temporales o copias de trabajo de documentos: los documentos creados exclusivamente para trabajos temporales o auxiliares son destruidos una vez que han dejado de ser necesarios para los fines que motivaron su creación.
  + Régimen de trabajo fuera de los locales de la ubicación del fichero: el nivel de seguridad es estableciendo una conexión VPN para cifrar toda la información.
  + Traslado de documentación: se lleva a cabo con maletines con llave o clave secreta.
  + Acceso de datos a través de redes de telecomunicaciones: Todas las conexiones son llevadas en un circuito lógico local a nivel de red. Las conexiones desde el exterior, son llevadas a cabo mediante VPN. Se usarán cortafuegos, proxys y otros mecanismos de seguridad a nivel de equipo.

* Relación de usuarios, accesos autorizados y sus funciones: hay tres tipos de usuarios dentro del sistema:
  + Usuarios: usan los datos personales a los que están autorizados a hacerlo únicamente para el desempeño laboral. No está permitido que alteren o destruyan información contenida en los SI sin autorización expresa por parte del responsable del fichero. Están obligados a informar de cualquier anomalía o error que detecten en los SI.
  + Responsables de seguridad: coordinan y controlan las medidas de seguridad establecidas en el documento de seguridad. Verifican el correcto funcionamiento de los SI. Gestionan tanto el registro de incidencias como las copias de respaldo y recuperación de datos.
  + Administrador: colabora con los responsables de seguridad para la implantación y el cumplimiento de las medidas de seguridad recogidas en el documento de seguridad. Proponen y desarrollan procedimientos y estándares de seguridad relacionados con los SI. Dan soporte a los usuarios en materia de seguridad. Gestionan los perfiles de los usuarios de los SI y los accesos de cada uno.
* Inventario soportes, registro de entrada y salida de soportes: los soportes se identifican mediante el sistema de etiquetado interpuesto por la AEPD.

Se gestiona mediante registro de acceso, de entrada y de salida y un formulario en el que consta el tipo de documento o soporte , la fecha y la hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contiene,la forma de envío y la persona autorizada responsable de la recepción; y en el caso de las salidas, el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona autorizada responsable de la entrega.

* Registros de acceso e informes de revisión de los mismos: Se registran de forma automática los accesos a los datos de los ficheros de nivel alto. Por cada acceso se guarda la información de dicho acceso. Este registro de accesos se conservan durante la actividad principal de la empresa y la vida útil del documento. Es función del responsable de seguridad revisar al menos una vez cada 2 meses la información de control registrada y elaborará un informe anual de los mismos.

.

1. **EVALUACIÓN DE** **PRUEBAS**

|  |  |  |
| --- | --- | --- |
| **TIPO** | **COMPROBACIONES A REALIZAR** | **NIVEL** |
| **Aspectos generales** | ¿La clasificación del nivel de seguridad es adecuada respecto a la naturaleza de la información contenida en cada uno de los ficheros y su finalidad?  **RESPUESTA:**La mayor parte de los niveles de seguridad adoptados son básicos y adecuados al tipo de información, sin embargo hay casos como el de la videovigilancia que deberían tener un nivel de seguridad más alto, ya que con un nivel básico sería fácil acceder a los videos y robar información de la agencia.  Por otra parte, se considera que el historial clínico de los empleados, cuyo nivel de seguridad es alto, tiene la misma relevancia que otros de sus datos de carácter personal, por lo que deberían tener el mismo nivel de seguridad (nivel recomendado:medio). | **Básico** |
| **Encargado de tratamiento** | ¿Se realiza el tratamiento por persona distinta al responsable del fichero?, ¿se ha formalizado mediante contrato conforme a lo establecido en el artículo 12 de la LOPD y artículos 20 a 22 del RLOPD?  **RESPUESTA:** Sí, se realiza pero únicamente con una autorización por escrito del responsable de fichero. Por otra parte, dicha autorización no hace ninguna referencia a los artículos mencionados anteriormente, por lo que se considera que no está debidamente formalizada. | **Básico** |
| **Prestación de servicio sin acceso a datos personales** | Si el tratamiento no afecta a datos personales ¿se han adoptado las  medidas necesarias para limitar el acceso del personal a los datos  personales, soportes y recursos?  **RESPUESTA:** Sí, esas medidas han sido adoptadas mediante el registro de accesos, donde la petición de acceder a los documentos puede ser aceptada o denegada según el nivel de seguridad al que esté autorizado a acceder el usuario en cuestión. | **Básico** |
| **Delegación de autorizaciones** | ¿Se han delegado las autorizaciones que el Reglamento atribuye al responsable en otras personas?, ¿se ha hecho constar en el Documento  de Seguridad las personas habilitadas para otorgar estas autorizaciones y las personas en quienes recae dicha delegación?  **RESPUESTA:** Sí, pero dichas autorizaciones aparecen reflejadas en el control de visitas del Documento de Seguridad. | **Básico** |
| **Régimen de trabajo fuera de los locales de la ubicación del fichero** | ¿Se garantiza el nivel de seguridad correspondiente al tipo de fichero  tratado?  **RESPUESTA:** Sí se garantiza, ya que el nivel de seguridad sería a través de internet, pero estableciendo una conexión VPN previamente para cifrar toda la información. | **Básico** |
| **Ficheros temporales o copias de trabajo de documentos** | ¿Cumplen el nivel de seguridad correspondiente?¿Se han destruido o borrado cuando ya no han sido necesarios para los fines que motivaron su creación?  **RESPUESTA:** Sí, cumplen el nivel de seguridad que les corresponde según el Reglamento de medidas de seguridad. A su vez, han sido borrados cuando ya no fueron necesarios. | **Básico** |
| **Documento de seguridad** | ¿Establece la identidad del responsable o responsables de seguridad?,  ¿Se especifica si la designación es única para todos los ficheros o está  diferenciada según el sistema de tratamiento utilizado?  **RESPUESTA:** Sí, se establece como responsable de seguridad a Guillermo Jesús Díaz Núñez. Aunque se entiende que la designación es única al aparecer su nombre en todos los ficheros sin diferenciar en el tratamiento utilizado, dicha designación no está debidamente especificada. | **Medio** |
| **Funciones y obligaciones del personal** | Están las funciones y obligaciones del personal con acceso a datos de  carácter personal y los sistemas de información claramente definidas?  **RESPUESTA:** Sí, dichas funciones están definidas para cada uno de los procedimientos que se especifican en el documento. | **Básico** |
| **Registro de incidencias** | ¿Se han anotado las ejecuciones de los procedimientos de recuperación de datos realizados?  **RESPUESTA:** Sí, se han anotado y detallado dichas ejecuciones según su ámbito correspondiente. | **Medio** |
| **Identificación y autenticación** | ¿Se limita el intento reiterado de acceso no autorizado al sistema?,  ¿Se anotan estos intentos en el registro de incidencias?  **RESPUESTA:** Sí, ya que todo acceso indebido, deberá ser detectado en el menor tiempo posible mediante mecanismos de alarmas y notificado al momento. Estos intentos serán registrados en el registro de incidencias, donde el responsable de seguridad deberá elaborar un informe. | **Medio** |
| **Control de acceso** | ¿Se encuentran los archivadores u otros elementos de almacenamiento en áreas de acceso restringido dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente?, ¿están cerradas estas áreas mientras no sea preciso el acceso a los documentos incluidos en el fichero?  **RESPUESTA:** Sí, los archivos están en cámaras aisladas e ignífugas. Los elementos de almacenamiento son armarios archivadores con clave secreta y llave maestra respecto de los documentos con datos personales | **Alto** |
| **Gestión de soportes y documentos** | ¿La distribución de soportes se realiza de forma cifrada, o por otro  mecanismo que garantice que no sea inteligible o manipulable durante  el transporte?  **RESPUESTA:** Sí, la distribución y salida de soportes que contengan datos de carácter personal de los ficheros de nivel alto se realizará mediante encriptación de datos con algoritmos de clave simétrica fuertes. | **Alto** |
| **Identificación y autenticación** | ¿Se limita el intento reiterado de acceso no autorizado al sistema?,  ¿Se anotan estos intentos en el registro de incidencias?  **RESPUESTA:** Sí, ya que todo acceso indebido, deberá ser detectado en el menor tiempo posible mediante mecanismos de alarmas y notificado al momento. Estos intentos serán registrados en el registro de incidencias, donde el responsable de seguridad deberá elaborar un informe. | **Medio** |
| **Copias de respaldo y recuperación** | ¿Se conserva una copia de respaldo y de los procedimientos de recuperación de datos en lugar diferente al de los equipos que los tratan?  **RESPUESTA:** Sí, ya que se mantienen copias de las salvaguardas de la información en una ubicación auxiliar distantes 50Km de la sede central. Los soportes con las copias se trasladan de forma semanal. | **Alto** |
| **Registro de accesos** | ¿Existe el registro de accesos?¿Los mecanismos que permiten el registro de estos accesos están directamente bajo el control del responsable de seguridad?  **RESPUESTA:** Sí, existe el registro de accesos bajo el control del responsable de seguridad. El responsable de seguridad revisará al menos una vez cada 2 meses la información de control registrada y elaborará un informe anual de los mismos. | **Alto** |
| **Acceso a datos a través de redes de comunicaciones** | ¿La transmisión de datos a través de redes se realiza de forma cifrada  (o por cualquier otro mecanismos que garantice que la información  no sea inteligible ni manipulada por terceros)?, ¿este mecanismo de  cifrado es eficaz?  **RESPUESTA:** Parece que el mecanismo de seguridad utilizado en este caso no es tan seguro como debería, ya que las conexiones desde el exterior, serán llevadas a cabo mediante VPN y simplemente se usarán cortafuegos, proxys y otros mecanismos de seguridad a nivel de equipo. | **Alto** |
| **Auditoría** | ¿Se realiza la actual auditoría en el plazo establecido desde la anterior?  **RESPUESTA:** Dado que esta es la primera auditoría realizada, no existe dicho plazo establecido. | **Medio** |
| **Criterios de archivo** | ¿Existe legislación específica con criterios para el archivo de soportes o documentos?  **RESPUESTA:** Sí, existe una legislación específica para cada tipo de soporte, tal y como se expone en el el punto 2.4 (Gestión de soporte y documentos) del Documento de Seguridad. | **Básico** |
| **Almacenamiento de la información** | ¿Los dispositivos de almacenamiento de documentos disponen de  mecanismos que obstaculicen su apertura?  **RESPUESTA:** Sí, disponen de dichos mecanismos tal y como se ha mencionado anteriormente. | **Básico** |
| **Custodia de soportes** | ¿Se custodia correctamente la documentación cuando ésta no se  encuentra archivada en los dispositivos de almacenamiento por estar  en revisión o tramitación?, ¿se impide en todo momento que sea accedida por persona no autorizada?  **RESPUESTA:** Sí,cuando los documentos con datos personales no se encuentren archivados en los dispositivos de almacenamiento indicados, por estar en proceso de tramitación, las personas que se encuentren a su cargo deberán custodiarlos e impedir el acceso a personas no autorizadas. | **Básico** |