Auditoría del RGPD/RMS

ASLEPI

Escuela de Ingeniería Informática
Universidad de Oviedo

Profesor asignado: Hugo Lebredo Buján
Código: PF2
Blanco Bielsa Eduardo – 41012833S
Coya Abajo Francisco – 71559542X
Diez Fernández Carlos – 71807062G

Tabla de contenidos

Hoja de declaraciones

En este apartado se muestran, a modo de conversación, las aclaraciones aportadas por el cliente. Se usarán las siguientes abreviaturas:

C – Cliente

A – Equipo auditor

A	**¿Podría indicar si existe alguna medida de seguridad (contraseñas, claves privadas...) para el acceso al ordenador donde se introducen los datos personales de los interesados en comprar un turismo?**
C	**Existe un usuario genérico con su contraseña:** ***Usuario: Comercial*** ***Contraseña: Alonso33***

A	**¿Podría indicar si existe alguna medida de respaldo o de realización de copias de seguridad de los datos almacenados en la Base de datos?**
C	**Se realizan copias de seguridad una vez a la semana de la base de datos. Tenemos ese servicio contratado con una consultora. Las copias se realizan en la nube.**

A	**¿Podría indicar los estándares de calidad y la reputación de la empresa a la que se subcontrata la administración de la página web?**
C	**No. Simplemente la contratamos porque nos hicieron un presupuesto muy generoso.**

A	**¿Se ha declarado en algún momento algún fichero relacionado con la LOPD?**
C	**No.**

A	**¿Se lleva de algún modo el registro de actividades del tratamiento?**
C	**Ninguno.**

A	**¿Podría indicar qué software utiliza la empresa para la gestión de las cámaras de seguridad, así como qué base de datos se utiliza?**
C	**No. El servicio de las cámaras de seguridad está contratado a AsturSegur. Instalaron las cámaras y la señal de estas van a sus servidores. Nosotros podemos acceder a través de su web con el usuario y la contraseña proporcionada por ellos. Todos los vídeos se almacenan en sus servidores.**

A	**¿Podrías indicar qué tipo de red utiliza la empresa (wifi, cable, satélite...) y de qué compañía?**
C	**Tenemos contratada 1 GB de fibra óptica con Telefónica.**

A	**¿Cuáles son los datos de la empresa (CIF, domicilio fiscal)?**

C	**El CIF es C49087604. Dirección Fiscal: Avda Los telares 57.**

A	**¿Hay algún procedimiento establecido para la destrucción de la documentación almacenada? Si es así, indicarlo**
C	**La documentación almacenada la eliminamos triturando el papel y tirándolo al contenedor correspondiente.**

A	**¿Se realizan copias de seguridad periódicas? En caso afirmativo, indicar cada cuánto y sobre qué archivos.**
C	**Se realiza una copia mensual sobre todos nuestros servidores.**

A	**En adición ¿Se eliminar las copias de seguridad una vez pasado un intervalo de tiempo determinado?**
C	**Las copias de seguridad se guardan durante un año.**

Auditoría de la empresa

1. Alcance

1.1. Objeto

El presente documento establece un informe detallado acerca de las medidas de seguridad implantadas del concesionario **BestAuto** (En adelante, el **Cliente**), ubicado en Lugones, encargado de la venta de turismos, conforme a la norma *ISO/IEC 27001:2022*, recogiendo toda la información relativa a la protección de datos del Cliente.

1.2. Normativa vigente

Este documento se basará en la información consulta en la normativa vigente que procede:

- ISO/IEC 27001:2022.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 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).
- Ley Autonómica de Creación de la Agencia Vasca de Protección de Datos (LAVPD, Ley 2/2004).
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.

1.3. Fecha de la auditoría

La auditoría de protección de datos se realizó, a fecha efectiva, el día 6 de mayo del año 2024.

1.4. Identificación del responsable del tratamiento

El responsable del tratamiento es la empresa de servicio informáticos **AsturWeb**.

Nombre: BestAuto
CIF: C49087604
Dirección Fiscal: Avda Los telares 57

2. Solicitud de inscripción en la AEPD

No consta una solicitud de inscripción. Según argumenta la empresa, no se ha declarado en algún momento algún fichero relacionado con la LOPD, ni tampoco se lleva de algún modo el registro de actividades del tratamiento.

3. Situación actual

3.1. Actividad actual de la empresa

La empresa por auditar, *BestAuto* (concesionario en Lugones), trata los datos relacionados con la venta de turismos, los comerciales, las solicitudes de empleo y las nóminas de sus empleados. Se detalla a continuación la situación de los datos tratados por la empresa.
En **primer** lugar, la empresa cuenta con una página web (subcontratada al tercero *AsturWeb*) donde se recaban los datos personales de las personas que solicitan un puesto, de forma que a la empresa por auditar sólo le llega un correo por cada solicitante de empleo. Por tanto, estos datos personales se dejan en manos de *AsturWeb*.
En **segundo** lugar, los datos de las personas con interés en la compra de un vehículo quedan registrados al principio en papel (formato físico) y posteriormente son entregados al gerente, quien los introduce en la Base de Datos.
En **tercer** lugar, los datos de compradores de vehículos (incluyendo los datos bancarios) así como los propios contratos de venta son registrados en papel (formato físico) y una de las copias es almacenada en un archivador dentro de un armario sin llave (siendo la otra copia entregada al propio comprador).
En **cuarto** lugar, el gerente introduce directamente los datos de los comerciales en la Base de Datos.
En **quinto** lugar, se recoge la firma del contrato laboral en papel y es guardada en un armario sin llave.
En **sexto** lugar, existen cámaras de videovigilancia que son revisadas por el gerente.
Por último, se envían los datos de las nóminas a una Consultoría externa (*Consultoría Pérez*).

3.2. Organización

La empresa tiene un tamaño pequeño, pues cuenta con 4 empleados (3 comerciales y 1 gerente).

Datos

Los datos de las personas solicitantes de empleo, así como los contratos de venta, los datos de los interesados en comprar un vehículo y los de los comerciales son almacenados digitalmente. El gerente se encarga de introducir estos datos manualmente en la Base de Datos.
Los datos de los interesados son en primer lugar recabados por los comerciales manualmente a papel.
Los contratos de venta son almacenados en un archivador en un armario poco protegido. De esta forma, cualquier persona con acceso al ordenador del gerente o mismamente al armario donde se almacenan los contratos, puede editar dichos contratos o incluso robarlos.

Espacios

La empresa se encuentra ubicada en Lugones donde únicamente el gerente cuenta con un despacho propio, mientras que los comerciales trabajan en una sala conjunta. Además, el concesionario cuenta con una sala de espera para las personas interesadas en la compra de un turismo, al lado de los vehículos expuestos.

3.3. Equipamiento

Software

No se usa ningún software en específico. El gerente no tiene constancia del software utilizado por las empresas subcontratadas (la de videovigilancia y la de administración de los datos). Accede directamente a través de la web.

Hardware

La empresa únicamente cuenta con un portátil (de marca HP) con una contraseña fácil de adivinar (**Alonso33**). Pese a contar con el hardware de videovigilancia (las cámaras) son seleccionadas por otra empresa subcontratada.

Red

La red que se utiliza en las instalaciones de la empresa es 1gb de fibra óptica contratado a Telefónica. No hacen uso de WiFi ni otras tecnologías.

4. Ficheros objeto de la auditoría

Fichero	Tratamiento	Formato	Finalidad	Nivel de seguridad
Datos de los clientes interesados en un vehículo	Gestión de clientes	En digital (base de datos)	Gestionar los datos personales de los clientes	Medio
Contratos de compra	Gestión de clientes	En físico (documento guardado en armario son llave)	Gestionar los datos personales de los clientes incluidos en	Bajo

			su contrato de compra	
Contratos de los empleados	Gestión de empleados	En físico (documento guardado en armario sin llave)	Gestionar los datos personales de los empleados incluidos en su contrato laboral	Bajo
Nóminas de los empleados	Gestión de nóminas	En digital (base de datos)	Gestionar los datos personales bancarios de los empleados	Medio
Control de acceso físico	Control de los accesos al establecimiento	Mediante cámaras de videovigilancia	Controlar quién y cuándo accede a cada una de las salas del establecimiento	Medio

5. Medidas de seguridad

A continuación, se procederá a realizar la auditoría. Para ello se realizará un control exhaustivo, articulado, con todos aquellos aspectos que atañen a la Protección de Datos del Cliente.

5.1. Identificación y autentificación de usuarios

Definición

Este apartado se rige mediante los siguientes artículos de la RGPD:

- **Artículo 93**. Identificación y autenticación.
  - **Art. 93.1**. "*El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios."*
  - **Art. 93.2**. "*La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad."*
  - **Art. 93.3**. *"En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte."*
  - **Art. 93.4**. "*Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior."*
  - **Art. 93.5**. "*La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas."*

- **Artículo 98**. Identificación y autenticación.
  "El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información."

  No consta.

Verificación de su cumplimiento

Con lo que atañe al art. 93, el cliente asegura que la documentación almacenada se elimina triturando el papel y tirándolo al contenedor correspondiente. Sin embargo, no se proporciona más información acerca de cómo se identifican y autentican los usuario, si bien es cierto que existe una única cuenta de acceso, gestionada por el responsable del establecimiento. No se alude al procedimiento de traslado de documentación. Por consiguiente, el art. 98 no consta.

Medidas correctoras propuestas

Incluir un procedimiento detallado del traslado de documentación. Para cumplir con el art.98, es necesario implantar un mecanismo de repeticiones de inicio de sesión. Por ejemplo, un mecanismo de inicio de sesión con tres intentos, donde al tercer intento se bloquee el acceso al sistema de información a la IP que intenta acceder. Todos los intentos se deben de registrar en un fichero de log, bien sea genérico o de accesos a recursos.

5.2. Control y registro de accesos

Definición

Este apartado se rige mediante los siguientes artículos de la RGPD:

- Artículo 91. Control de acceso.
  - Art. 91.1. *"Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones"*.
  - Art. 91.2. *"El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos".*
  - Art. 91.3. *"El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados".*
  - Art. 91.4. *"Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero".*
  - Art. 91.5. *"En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio"*.
- Artículo 99. Control de acceso físico.
  "Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información".
- Artículo 103. Registro de accesos.
  - Art. 103.1. *"De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado".*
  - Art. 103.2. *"En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido".*
  - Art. 103.3. *"Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos".*
  - Art. 103.4. *"El período mínimo de conservación de los datos registrados será de dos años".*
  - Art. 103.5. *"El responsable de seguridad 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".*

- Art. 103.6. *"No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:*
- *a) Que el responsable del fichero o del tratamiento sea una persona física.*
- *b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales."*

Verificación de su cumplimiento

En primer lugar, relativo al art. 91, no se cumple esta medida, puesto que en el sistema solo se precisa de un usuario genérico para acceder a los recursos, en el ordenador del comercial.

En segundo lugar, con respecto al art. 99, no se cumple. Los datos se almacenan en un armario que no dispone de cerradura con llave. Además, no se indica quién está autorizado al acceso a dicho armario. Se especifica "un armario", de forma genérica, ha de ser más conciso. Establecer e indicar, de forma unívoca, por escrito, el personal autorizado para acceder a los equipos físicos, así como establecer un protocolo de acceso, mediante identificación del personal, llevando un registro de todos los accesos realizados a dicha instalación.

Por último, del art. 103 no consta información acerca de si esta medida está implementada en la empresa.

Medidas correctoras propuestas

Llevar a cabo un registro de accesos (Registro log), tanto a aplicaciones de la empresa, como de accesos físicos a lugares concretos de la empresa, que contengan información sensible.

5.3. Procedimientos de realización de copias de recuperación y respaldo

Definición

Este apartado se rige mediante los siguientes artículos de la RGPD:

- Artículo 94.
  - Art. 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".*
  - Art. 94.2. *"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".*
  - Art. 94.3. *"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".*
  - Art. 94.4. *"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".*

Verificación de su cumplimiento

La medida de seguridad se cumple, puesto que el cliente asegura que se realizan copias de seguridad con carácter mensual. Además, las copias se almacenan en los servidores internos de la empresa durante un periodo de un año. Posteriormente, se eliminan del sistema.

Medidas correctoras propuestas

Especificar un procedimiento de recuperación de datos, si este no está presente actualmente. De igual forma, realizar las pruebas con datos que no estén en producción, ni sean reales, para evitar graves incidencias.

5.4. Control de acceso a ficheros, ficheros temporales

Definición

Este apartado se rige mediante los siguientes artículos de la RGPD:

- Artículo 87: Ficheros temporales o copias de trabajo de documentos.
  - Art. 87.1. *"Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda conforme a los criterios establecidos en el artículo 81".*
  - Art. 87.2. *"Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación".*
- Artículo 91: Control de acceso.
  - Art. 91.1. *"Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones".*
  - Art. 91.2. *"El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos".*
  - Art. 91.3. *"El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados".*
  - Art. 91.4. *"Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero".*
  - Art. 91.5. *"En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio".*

Verificación de su cumplimiento

En primer lugar, si analizamos las políticas de ficheros temporales y de copias de trabajo podemos concluir que no se está cumpliendo, ya que no se realiza ningún borrado de las copias de los documentos creados.

En segundo lugar, si analizamos los controles de acceso podemos concluir que se cumple para los datos de los clientes interesados y los datos bancarios de los empleados, ya que estos se guardan en base de datos y solo tienen acceso el responsable y la empresa auditora encargada de gestionarlos. Pero, por otro lado, si analizamos los contratos de compra y los datos de contrato de los empleados, podemos afirmar que no se cumple, ya que estos se guardan en un armario sin llave, por lo que cualquier persona con acceso a la sala podría entrar y consultarlo. Cabe destacar, que la única medida de seguridad empleada es el uso de cámaras de videovigilancia que revisa el responsable.

Medidas correctoras propuestas

Se deben implementar medidas de seguridad de acceso a los ficheros mediante las que se controle que solamente los usuarios autorizados puedan acceder a estos ficheros.

Además, en el caso de que se almacenen de forma física se deberá implementar alguna medida de seguridad de acceso.

5.5. Redes de comunicaciones

Definición

Este apartado se rige mediante los siguientes artículos de la RGPD:

- Artículo 85: Acceso a datos a través de redes de comunicaciones.
  - Art. 85.1. *"Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 80".*
- Artículo 104: Telecomunicaciones.
  - Art. 104.1. *"Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros".*
  -

Verificación de su cumplimiento

En cuanto al Artículo 85, BestAuto aloja su página web en un servidor en la nube y permite que el público acceda para consultar el catálogo de automóviles y enviar formularios, pero no se mencionan explícitamente las medidas de seguridad específicas que se han implementado para garantizar un nivel de seguridad de accesos.
En relación con el Artículo 104, se menciona que los datos personales se recopilan a través de la página web, pero no se especifica si la transmisión de estos datos se realiza cifrando los datos o utilizando cualquier otro mecanismo para garantizar que la información no sea inteligible ni manipulada por terceros durante la transmisión a través de redes públicas o inalámbricas.
Como no se menciona se considera que no se están cumpliendo las medidas de seguridad exigidas por la RGPD.

Medidas correctoras propuestas

Para cumplir las medidas de seguridad impuestas por la RGPD referentes a las telecomunicaciones, BestAuto debe realizar un cifrado de las comunicaciones, utilizando, por ejemplo, protocolos de cifrado como SSL/TLS para asegurar que la información transmitida esté protegida contra la interceptación por parte de terceros. Además, cuando se transmitan datos personales se debe garantizar que estos datos estén cifrados para proteger su confidencialidad e integridad.

5.6. Responsable del tratamiento

Definición

Este apartado se rige mediante los siguientes artículos de la RGPD:

- Artículo 82: Encargado del tratamiento.
  - Art. 82.1. *"Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho*

responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento. Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento".

- Art. 82.2. *"Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad en los términos exigidos por el artículo 88 de este reglamento o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento".*
- Art. 82.3. *"En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este reglamento".*

Verificación de su cumplimiento

El responsable del tratamiento cabe pensar que es el gerente, pero no se especifica que este aplique ninguna medida de seguridad en la gestión de los datos. Además, estos datos se proporcionan a la Consultoría Pérez. Por otro lado, los datos en algunos casos los guarda de forma poco segura.
Por ello, podemos concluir que no se cumplen estos artículos de la RGPD.

Medidas correctoras propuestas

Se debe verificar que la empresa consultora a la que se le facilitan los datos personales realiza un correcto tratamiento de estos para comprobar que se están aplicando medidas de seguridad.
Por otro lado, para los datos que el encargado del tratamiento guarde de forma física, se deberían implementar medidas de control de accesos.

5.7. Documento de seguridad

Definición

Este apartado se rige mediante los siguientes artículos de la RGPD:

- Artículo 88: El documento de seguridad.
  - Art. 88.1. *"El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información".*
  - Art. 88.1. *"El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización".*
  - Art. 88.1. *"El documento deberá contener, como mínimo, los siguientes aspectos:*
    - *a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.*
    - *b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.*
    - *c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.*

        - *d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.*
        - *e) Procedimiento de notificación, gestión y respuesta ante las incidencias.*
        - *f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.*
        - *g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.".*
    - Art. 88.1. *"En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:*
        - *a) La identificación del responsable o responsables de seguridad.*
        - *b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento".*
    - Art. 88.1. *"Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo".*
    - Art. 88.1. *"En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá. anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados. En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento".*
    - Art. 88.1. *"El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas".*
    - Art. 88.1. *"El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal".*

Verificación de su cumplimiento

La empresa auditada no cuenta con un documento de seguridad según lo expuesto en el artículo 88 de la RGPD.

Medidas correctoras propuestas

El responsable del tratamiento debe elaborar el documento de seguridad en el que se detallen las medidas de seguridad que se llevan a cabo para asegurar la protección de los datos personales.

Este documento de seguridad debería contemplar los siguientes puntos:

- El documento debe especificar el ámbito de aplicación con detalle de los recursos protegidos.

- Debe incluir medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en el RGPD.
- Las funciones y obligaciones del personal en relación con el tratamiento de datos personales deben estar claramente definidas.
- Se debe describir la estructura de los ficheros con datos personales y los sistemas de información que los tratan.
- Se deben establecer procedimientos de notificación, gestión y respuesta ante incidencias.
- Debe haber procedimientos para realizar copias de respaldo y recuperación de datos, así como medidas para el transporte y destrucción segura de soportes y documentos.

Referencias

- ISO/IEC 27001:2022. ISO. Recuperado 6 de mayo de 2024, de https://www.iso.org/standard/27001
- BOE-A-1999-23750 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. (s. f.). Recuperado 6 de mayo de 2024, de https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750
- BOE-A-2008-979 Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. (s. f.). Recuperado 6 de mayo de 2024, de https://www.boe.es/buscar/act.php?id=BOE-A-2008-979
- BOE.es—DOUE-L-2016-80807 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 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). (s. f.). Recuperado 6 de mayo de 2024, de https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807
- Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos. (s. f.).