UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Informática

Guía para el cumplimiento normativo en una pequeña organización de la protección de las bases de datos.

Trabajo Fin de Grado

Grado en Ingeniería Informática

AUTOR/A: Sahuquillo Ejarque, Miguel

Tutor/a: Oltra Gutiérrez, Juan Vicente

CURSO ACADÉMICO: 2023/2024

Escola Tècnica Superior d'Enginyeria Informàtica

Universitat Politècnica de València

Guía para el cumplimiento normativo en una pequeña organización de la protección de las bases de datos

Trabajo Fin de Grado

Grado en Ingeniería Informática

Autor: Miguel Sahuquillo Ejarque

Tutor: Juan Vicente Oltra

Curso: 2023/2024

Resumen

En ocasiones las empresas pueden tener ciertas dudas a la hora de proteger las bases de datos que contienen la información clave para que su empresa funcione, para ello se elaborará una guía o herramienta que nos ayudará a cumplir con las leyes de protección de datos y evitar problemas legales. Con este fin se consultarán las principales leyes, que son, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 además, de otras guías que podemos encontrar en la web de la Agencia Española de Protección de Datos o AEPD. De entre estas guías destacaremos un par que tocan temas más relevantes o de actualidad, una guía para teletrabajar con seguridad y otra guía que nos indica qué tener en cuenta a la hora de implementar el control de acceso por biometría. También se debe proteger el lugar físico dónde se almacenan estos datos, el Centro de Procesamiento de Datos o CPD, para ello nos basaremos una norma de diseño y construcción de CPD, la norma TIA 942, además tendremos en cuenta un par de aspectos de las leyes de protección de datos que son la videovigilancia y el control de acceso mediante biometría. Para elaborar la guía utilizaremos el programa de ofimática llamado Excel, con el cual crearemos un libro que deberemos cumplimentar con información sobre nuestra organización y que nos dará directrices para el cumplimiento de las normativas. Con todo esto podremos garantizar que superaremos una auditoría externa de protección de datos y además los datos de la organización estarán seguros.

Palabras clave: bases de datos, legalidad, AEPD, empresas

Abstract

Occasionally, companies may face uncertainties regarding the safeguarding of databases that contain critical information, essential to their operations. To address these concerns, a comprehensive guide or tool will be developed to ensure compliance with data protection laws, and to mitigate potential legal risks. In this endeavor, the primary legislative references will include the Organic Law 3/2018, of December 5, on Personal Data Protection and the guarantee of digital rights, and Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016. Additionally, we will consult various guides available on the website of the Spanish Data Protection Agency (AEPD). Noteworthy among these guides are those addressing current and relevant topics: a guide for secure remote working, and another one outlining considerations for implementing biometric access control. Furthermore, it is imperative to secure the physical location where data is stored, namely the Data Processing Center (DPC). To this end, we will adhere to the TIA 942 standard for the design and construction of DPCs, while also integrating specific aspects of data protection laws, such as video surveillance and biometric access control. The guide will be developed using the office software Excel, wherein a workbook will be created to be filled with organizational information, providing detailed guidelines to ensure regulatory compliance. By following this comprehensive approach, we can confidently ensure that the organization will successfully pass an external data protection audit and, more importantly, that the organization's data will remain secure.

Keywords: databases, legality, AEPD, companies

Tabla de contenidos

Contenido

Índice de figuras

Índice de tablas

1. Introducción

Hoy en día vivimos en una era muy digitalizada donde los datos han cobrado una gran importancia. Los datos son el equivalente a dinero para todas las empresas. Estos se tratan y se extraen conclusiones que ayudan a conocer más y mejor a los clientes. Con el conocimiento de las necesidades y hábitos de los clientes se puede hacer un gran trabajo de mercadotecnia para subir las ventas de cualquier empresa. Por ejemplo, se puede segmentar a los clientes por grupos y tratarlos de forma distinta en función de sus gustos y necesidades.

Los datos se almacenan en bases de datos de forma que estén ordenados y estructurados. Una base de datos puede esta digitalizada y gestionada por un sistema de gestión de bases de datos como Oracle, MongoDB, un documento xlsx e incluso una libreta en la cual el propietario de un pequeño negocio tiene las cuentas, los datos de los proveedores etc.

Con el nacimiento de la era digital los países han tenido que legislar sobre internet y lo que sucede en él. Uno de los temas sobre los que han tenido que legislar es sobre los datos en la red. En estos días los datos se encuentran en internet, en distintos servidores, ubicados por todo el mundo y no es tan fácil como antes eliminarlos o utilizarlos. Las personas cuyos datos se alojan en internet y que son tratados deben poder tener la garantía y seguridad de que estos no caerán en malas manos y de que serán bien usados. Para esto se han creado una serie de leyes que regulen esto. En el caso de España tenemos la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales y a nivel europeo tenemos el Reglamento UE 2016/679.

Las distintas organizaciones deben ser conscientes de las normativas que supeditan el tratamiento que hacen de los datos de sus clientes. Como consecuencia de esto ha aparecido la figura del responsable del tratamiento de datos, que como su propio nombre indica se encarga de que los datos sean tratados como toca y decide cómo hacerlo.

En el campo de la informática saber acerca de las leyes que afectan al tratamiento de datos es crucial, ya que muchos informáticos trabajamos con ellos. Para evitar problemas legales cuando se nos haga una auditoría debemos tener en cuenta estas leyes. Además, sería una buena idea hacer una guía o manual que nos dijera los pasos a seguir para comprobar que nuestra organización cumple con todo.

Una auditoría se puede ver como un proceso de mejora continua para la empresa. Ya que al llevarla a cabo se pueden mejorar aspectos como la seguridad de la información, que al verse reforzada evitará problemas con los datos como robos y pérdidas. Al tomar una actitud proactiva frente al tratamiento y cuidado de los datos podemos mejorar la imagen de la empresa haciendo sentir a los clientes que es seguro que nosotros poseamos sus datos.

1.1. Motivación

Lo que me ha llevado a hacer este trabajo de fin de grado han sido las asignaturas cursadas a lo largo de la carrera. Las asignaturas con las que más he disfrutado han sido aquellas relacionadas con bases de datos y leyes. Por este motivo cuando vi el tema de este trabajo que ofrecía el profesor Juan Vicente Oltra decidí escogerlo. Espero poder aplicar lo visto en asignaturas como deontología, donde se nos habló de leyes, en especial la ley que más afecta a los informáticos como es la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales; análisis de requisitos de negocio, donde aprendimos modelado de procesos con diagramas BPMN; gestión y configuración de la arquitectura de los sistemas de información, donde se nos habló de los CPD y de cómo mantener estos a salvo. Con este trabajo pondré en práctica los conocimientos de las asignaturas mencionadas anteriormente junto con lo que aprenda mientras investigo para realizar este trabajo.

1.2. Objetivos

El objetivo principal es la confección de una guía de control interna que permita al profesional realizar una auditoría para verificar que se cumple con la ley. Para llevar a cabo esta guía deberemos cumplir una serie de objetivos secundarios:

- Estudiar y extraer los artículos más relevantes para nosotros de la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales y el Reglamento (UE) 2016/679.
- Indagaremos en las guías y documentos que ofrece la AEPD e incluiremos los que parezcan más relevantes.
- Buscaremos información específica acerca de las amenazas que afectan a las bases de datos y qué medidas tomar.
- Buscaremos información acerca de cómo elaborar apropiadamente una guía de control.
- Finalmente unificaremos todo lo mencionado anteriormente para la creación de nuestra guía. Esta guía se desarrollará utilizando la herramienta Excel con la que crearemos una serie de hojas que contendrán los requisitos para cumplir con las distintas legislaciones y guías.

1.3. Impacto esperado

La guía que crearemos supondrá mejoras en el ámbito del tratamiento de datos en empresas. En concreto:

- La empresa cumplirá con los reglamentos de protección de datos, lo cual evitará sanciones. También ayudará a mantener los datos a salvo lo que hará que la organización tenga buena imagen y genere confianza en los clientes. En cuanto a la relación con los empleados, podremos garantizar que estos cumplen con los horarios y sus deberes laborales.
- Los clientes tendrán la seguridad y tranquilidad de que sus datos son tratados de forma adecuada.

- Los empleados podrán llevar a cabo teletrabajo de forma segura y se protegerán sus derechos laborales gracias al control de acceso.

1.4. Metodología

Para llevar a cabo los objetivos descritos en los párrafos anteriores primero se procederá a la búsqueda de información, la cual sintetizaremos y extraeremos las partes más relevantes para nuestro trabajo. Una vez tengamos esta información procederemos a la creación de la guía.

1.5. Estructura

Este trabajo se divide en distintas partes diferenciables:

1. En el apartado estado del arte se investiga a cerca de las distintas herramientas que ofrecen organizaciones de protección de datos que pueden ser útiles para cumplir con los reglamentos de protección de datos y se buscan otros TFG relacionados con la protección de datos.
2. En el apartado leyes y guías de protección de datos se busca y sintetiza la información de distintas leyes, guías y otros sitios web que luego utilizaremos para elaborar nuestra guía.
3. En el apartado guía de control interno buscaremos información sobre cómo confeccionar esta guía, que temas debe tocar y que apartados debe tener.
4. En el apartado diseño de la solución comentaremos cómo se ha diseñado nuestra guía.
5. Hablaremos también sobre la tecnología utilizada para el desarrollo de la guía, la relación del TFG con los estudios y los futuros trabajos relacionados con este que se podría llevar a cabo.
6. También encontramos un glosario que explica las abreviaturas que encontramos a lo largo del TFG.
7. Después de la bibliografía nos encontramos con una serie de anexos, sobre señales de videovigilancia, cómo funcionan las herramientas que se explican en el estado del arte, cómo funciona la guía que hemos creado, modelos de contrato, algunos conceptos que aparecen la tabla de la TIA y finalmente los ODS.

2. Estado del arte

En este apartado buscaremos información sobre TFG's realizados por otros compañeros en el ámbito de la protección de datos y las distintas herramientas que facilitan los organismos de protección de datos para el cumplimiento de la legislación.

2.1.1. Trabajos relacionados

Buscando en el repositorio de trabajos de fin de grado de la UPV podemos encontrar trabajos previos cuyo objetivo era la creación de una guía o una aplicación que sea de ayuda en materia de protección de datos. Analizaremos algunos de estos trabajos.

1-Creación de una guía para la aplicación del nivel básico, medio y alto del Reglamento de protección de Datos para microempresas

Este TFG tiene como objetivo realizar una guía para aplicar la Ley Orgánica de Protección de Datos en pequeñas empresas. Esta guía será fácil de entender para cualquier trabajador y con bajo coste económico. Para cumplir con la legislación de protección de datos se van cumpliendo con distintos niveles de seguridad, que hacen referencia a las categorías de datos, así pues, los datos de nivel básico son el nombre o el DNI y los de nivel alto son datos de categoría especial, como los datos biométricos, y los pasos para implementarlos. Como ayuda para cumplir con esto tenemos una aplicación móvil.

La ley en la que se basa esta aplicación es la Ley Orgánica 17/1999 de Protección de datos, por lo tanto, este trabajo está desactualizado ya que la ley de protección de datos vigente en la fecha de realización de este trabajo es la LOPDGDD del 2018 y el RGPD 2016/679. De este último se menciona que no entrará en funcionamiento hasta el 2018 debido a que fue aprobado recientemente y no tenían claro cómo afectaría a la protección de datos.

En el apartado de futuras mejoras de este proyecto menciona que se deberá adaptar al por entonces nuevo RGPD, además, también se debe adaptar a la nueva ley española de protección de datos. Así pues, con este trabajo cogeremos el testigo de nuestro compañero, creando una guía adaptada a la legalidad vigente, aunque utilizando otras herramientas y con otros enfoques. (1)

2-Autocheking sobre una auditoría de SI RGPD

Este TGF tiene como objetivo analizar el estado de la empresa para determinar si superaría una auditoría de seguridad. Para llevar a cabo esto hace una introducción sobre ciberseguridad y los posibles ciberataques que podemos sufrir. También trata el tema de la protección de datos y crea una serie de bloques temáticos en los cuales divide los temas de la protección de datos, por ejemplo, un bloque de licitud del tratamiento, un bloque para el delegado de protección de datos, otro para la licitud del tratamiento.

Este autotest consta de 50 preguntas divididas en 21 bloques:

1) Gobierno de la privacidad;
2) Minimización y exactitud de los datos;
3) Responsabilidad proactiva;
4) Corresponsabilidad;
5) Plazos de conservación;
6) Licitud del tratamiento;
7) Transparencia e información;
8) Transparencia e información: web;
9) Transparencia e información: videovigilancia;
10) Limitación de la finalidad;
11) Deber de secreto;
12) Registro de actividades de tratamiento;
13) Derechos de los interesados;
14) Seguridad: violaciones de seguridad;
15) Seguridad: medidas técnicas y medidas organizativas;
16) Seguridad: formación;
17) Delegado de Protección de Datos;

Figura 1: Bloques temáticos. Fuente: (2)

18) Encargado de tratamiento;
19) Categorías especiales de datos;
20) Tratamiento de menores de edad.

Figura 2: Bloques temáticos 2. Fuente: (2)

Para llevar a cabo la auditoría elabora un test llamado Audit AutoQuiz, compuesto por 50 cuestiones, divididas por bloques, que la empresa debe responder y en función de las respuestas autoevaluar si la empresa cumple con las leyes de protección de datos. Para la elaboración de las preguntas la autora del TFG ha analizado los puntos débiles de la empresa donde ejercía como consultora.

A diferencia del trabajo mencionado anteriormente en este ya se tiene en cuenta la normativa actual y puede ser útil el tema de los bloques temáticos en los cuales ha dividido las preguntas de su test y las leyes de protección de datos. (2)

3-Guía Interactiva para el cumplimiento de normas de Protección de Datos en el entorno laboral

Este trabajo consiste en crear una guía interactiva que ayude con el cumplimiento de la normativa de protección de datos. Esta guía está enfocada al tratamiento de datos de los empleados de la empresa y a las personas que están en búsqueda de empleo.

Su guía interactiva fue elaborada en la plataforma CANVA. En la memoria podemos ver una serie de capturas de su guía y vemos de qué trata.

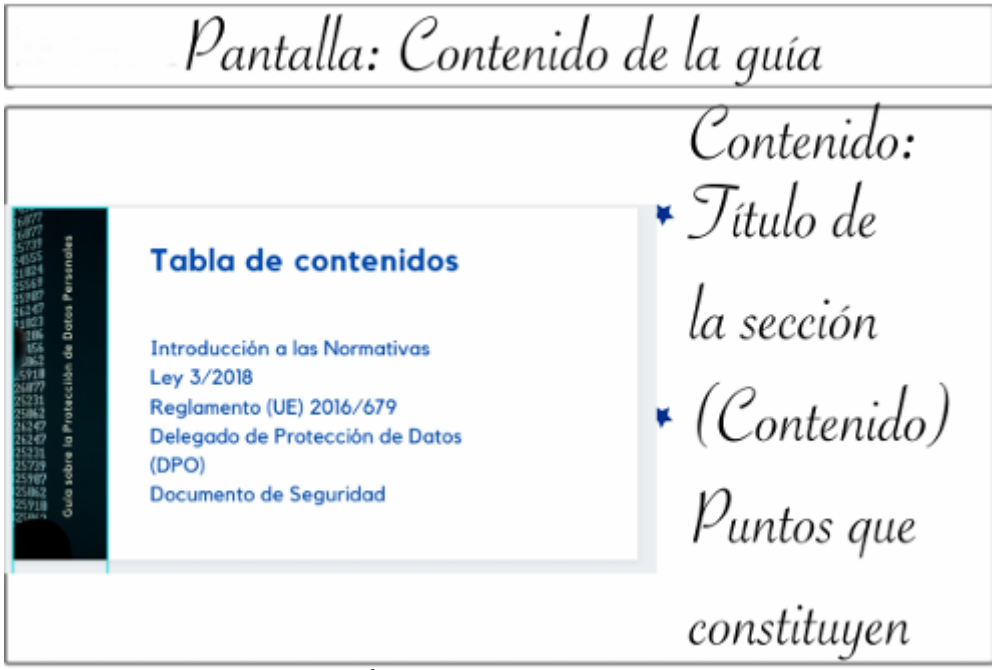


Figura 3: Índice guía interactiva. Fuente: (3)

Según vemos en el índice y en posteriores capturas esta guía introduce la LOPDGDD y el RGPD, además añade ambas leyes para que puedas descargarlas. También nos habla de la figura del Delegado de Protección de datos y sus funciones dentro de la empresa. Para finalizar nos habla del documento de seguridad.

Al investigar sobre el documento de seguridad nos encontramos con que es un documento donde se recogen las medidas técnicas y organizativas adoptadas para proteger los datos. La elaboración de este documento (4) era de carácter obligatorio, con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter personal. En la actualidad, con la LOPDGDD, este documento de seguridad ha sido integrado en el registro de actividades del tratamiento, del cual hablaremos más adelante. (3)

4-Guía sobre protección de datos e implantación de la LOPDGDD en centros sanitarios

Esta guía tiene como objetivo el desarrollo de una guía de buenas prácticas en materia de protección de datos, en concreto para datos relativos a la salud. También se proporcionan herramientas y guías de la AEPD con el fin de garantizar el cumplimiento de las leyes.

En el apartado de trabajos futuros menciona, entre otros, la realización de una guía para el tratamiento de datos especialmente sensibles o categorías de datos especiales, uno de los puntos que trataremos en nuestro trabajo. (5)

5-Guía para la evaluación de impacto requerida en el Reglamento Europeo de Protección de Datos

La entrada en vigor del nuevo reglamento de protección de datos incluyó el análisis de riesgo y la evaluación de impacto previas al tratamiento de los datos. De esta forma se

adopta una actitud proactiva y se previenen los posibles riesgos. Puesto que para el tratamiento de datos biométricos y para llevar a cabo el teletrabajo se recomienda analizar los riesgos y realizar una evaluación de impacto tendremos muy en cuenta este trabajo.

En caso de que los datos conlleven un riesgo bajo para los derechos y libertades de los interesados se realizará un análisis básico de riesgos.

La gestión de riesgos consta de 3 etapas: la identificación de amenazas, la evaluación de riesgos y tratamiento y la mitigación de los riesgos.

		Elementos			
		Operaciones	Datos tratados	Intervinientes	Tecnologías
Etapas del ciclo de vida	Captura de datos				
	Almacenamiento				
	Uso				
	Cesión				
	Destrucción				

Figura 4: Tabla análisis de riesgos en el ciclo de vida de los datos. Fuente: (6)

Cómo podemos ver en la tabla anterior, en el lado derecho vemos el ciclo de vida de los datos y arriba, en elementos, vemos las amenazas a las que estos están expuestos.

	Tipología de riesgo	Riesgo	Medidas de control
Protección de la información	Integridad de los datos		
	Disponibilidad de los datos		
	Confidencialidad de los datos		
Cumplimiento de requisitos regulatorios	Garantizar ejercicio de derechos al interesado		
	Garantizar los principios del tratamiento		

Figura 5: Tabla de análisis de riesgos y medidas de control. Fuente: (6)

En la tabla anterior hemos clasificados los riesgos en 2 grupos, protección de la información, que hace referencia a la integridad, disponibilidad y confidencialidad; el segundo grupo hace referencia al cumplimiento de los requisitos regulatorios, que hace referencia a que el interesado no puede ejercer sus derechos y no se garantizan los principios del tratamiento de datos.

Si los datos suponen un alto riesgo se realizará una AEIPD, también llamada Evaluación de Impacto de Protección de Datos, se debe hacer de forma obligatoria, esto está recogido en el artículo 35.7 del RGPD.
Una AEIPD tiene los siguientes pasos: analizar la necesidad de realizar una EIPD, describir el ciclo de vida de los datos, analizar la necesidad y proporcionalidad del tratamiento, gestionar los riesgos, plan de acción y conclusiones y supervisar y revisar la implementación.

Para la realización de nuestra guía nos apoyaremos en este TFG a la hora de realizar el análisis de riesgos y la evaluación de impacto necesarias a la hora de llevar a cabo el tratamiento de datos. (6)

2.1.2. Agencia Española de Protección de Datos

Facilita RGPD es una herramienta que encontramos en la página web (7) de la AEPD. Esta herramienta nos proporciona unos documentos que nos dicen cómo tratar correctamente los datos, siempre que sean de bajo riesgo. Cabe destacar que el uso de esta herramienta no garantiza el cumplimiento de la LOPDGDD.

Figura 6: Herramienta Facilita RGPD. Fuente: (7)

2.2. Autoridad Catalana de Protección de Datos

Si buscamos información en otras páginas de organizaciones encargadas de la protección de datos podemos encontrar la APdCat o Autoridad Catalana de Protección de Datos (8). En su página web podemos encontrar los principales reglamentos que rigen el tratamiento de datos y algunas guías. En el apartado de recursos, en programas para descargar, podemos encontrar software que puede ser de gran utilidad.

Al igual que en la página web de la AEPD encontramos una herramienta que nos sirve para evaluar el riesgo, la AIPD.

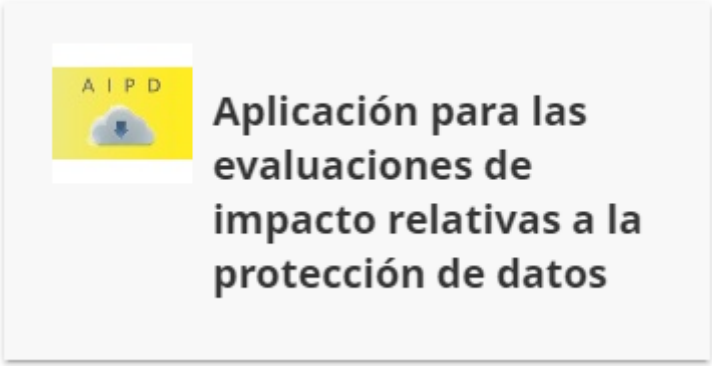


Figura 7: Herramienta de evaluación de impacto. Fuente: (8)

En esta página web hay también un software para gestionar el registro de las actividades del tratamiento. Según el artículo 30 del RGPD el responsable y/o el encargado del tratamiento deberán llevar un registro de las actividades que se llevan a cabo con los datos. Ese registro debe contener cierta información como los datos personales del responsable y/o encargado, los fines del tratamiento, a quienes se comunicarán esos datos, si se realizan transferencias, las categorías de datos que se tratan, las medidas de seguridad que se toman para preservar esos datos y cuando se suprimirán. Este registro

lo deben llevar las empresas que tengan más de 250 empleados o que traten categorías de datos especiales. El software que nos ofrece la APdCat para llevar este registro es la aplicación RAT. Esta herramienta ha sido creada para dar soporte a pequeñas empresas.

Figura 8: Herramienta RAT. Fuente: (8)

2.3. Comisión Nacional de Informática y Libertades

El CNIL (9) es el organismo que se encarga de la protección de datos en Francia. Investigando en su página web encontramos herramientas similares a las ya mencionadas anteriormente. La primera y más destacable es un libro de Excel que sirve para registrar las actividades del tratamiento. Esta herramienta tiene su razón de ser en el artículo 30 del RGPD, como la ya mencionada anteriormente RAT. Tiene la misma funcionalidad solo que esta viene en formato OpenDocument Spreadsheet, que es un formato de hoja de cálculo, en vez de ser un software que se instala.

Figura 9: Documento registro de actividades del tratamiento. Fuente: (9)

Aquí podemos ver un ejemplo una actividad registrada en una de las hojas:

Description of the processing operation							
Name of the processing operation	Payroll management						
N° / REF	1 - Example						
Data of creation of the processing	May 26, 2018						
Update of the processing	May 13, 2019						
Stakeholders	Name	Address	ZIP Code	Town	Country	Phone number	Email address
Controller	Louise DUPONT	1 rue Rivoli	75001	Paris	France	01 xx xx xx xx	example1@ets.com
Data protection officer	Martin HENRI	1 rue Rivoli	75001	Paris	France	01 xx xx xx xx	example2@ets.com
DPO's Organisation (if external DPO)	N/A						

Purpose(s) of the data processing	
Main purpose	Payroll management
Sub-purpose 1	Calculation of remuneration
Sub-purpose 2	Calculation of the amount of payments made to social security organisations
Sub-purpose 3	Transfer orders to the bank

Categories of personal data	Description	Data retention period
Marital status, ID, identification data, images...	Last names, names and addresses	5 years from the payment of the salary
Economic and financial information (income, financial situation, tax situation, etc.)	Bank account details	5 years from the payment of the salary
Social Security Number (or NIR)	Social security numbers of the employees	5 years from the payment of the salary

Figura 10: Ejemplo de actividad registrada. Fuente: (9)

Encontramos también herramientas de evaluación de impacto.

2.4. Comité Europeo de Protección de Datos

El CEPD (10) es el principal organismo europeo e independiente que coordina al resto de autoridades nacionales de protección de datos. Esta organización se asegura de que se cumpla el reglamento general de protección de datos en toda la Unión Europea. En su web podemos encontrar guías de buenas prácticas. También, encontramos una herramienta que nos ayuda a garantizar el cumplimiento del RGPD. En esta ocasión es un software gratuito y de código abierto que permite auditar un sitio web. Esta herramienta facilita mucho este tipo de auditorías ya que es muy sencilla de usar.

Figura 11: Aplicación website-audit. Fuente: (10)

WebsiteAudit analiza un sitio web y recopila información que utiliza el sitio como cookies, información que almacena, el tráfico que tiene etc. Esta herramienta puede ser de gran utilidad a la hora de analizar la web de alguna empresa externa que se quiera contratar o cerciorarnos de que nuestra propia web cumple con la legislación.

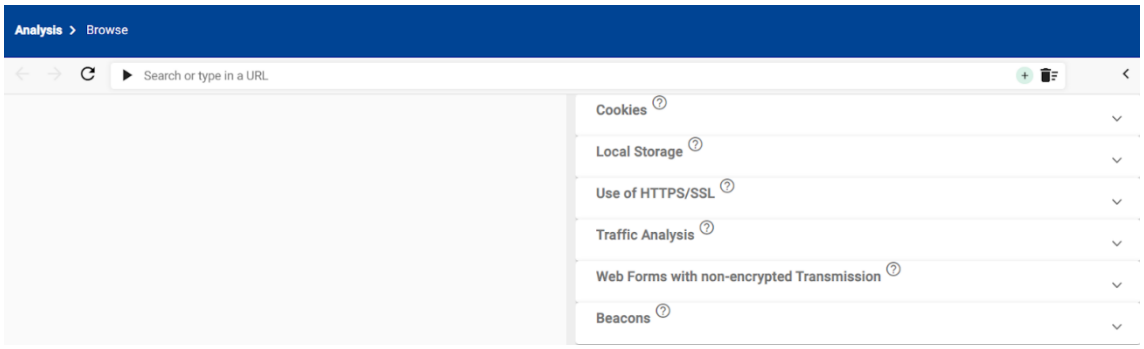


Figura 12: Interfaz principal de la aplicación. Fuente: (10)

2.5. Organismo de protección de datos de Luxemburgo (CNPD)

Investigando en la web de algunos países europeos podemos encontrar otras herramientas útiles y parecidas a las vistas anteriormente. En concreto, en la página del organismo de protección de datos de Luxemburgo (11) (CNPD). Esta organización junto con la Luxembourg House of Cybersecurity han creado un proyecto llamado ALTO (DAta Protection CompLiance SupporT TOolkit) que tiene como objetivo proporcionar a las empresas una herramienta de autoevaluación para asegurarse de que cumplen con el RGPD. Para lograr esto se han desarrollado 2 herramientas: Fit4Cybersecurity y Fit4Privacy.

Estas 2 herramientas son una serie de cuestionarios, muy similares a Facilita RGPD, que en base a la información que facilitamos sobre nuestra organización nos da una serie de pautas. Seguir las recomendaciones de esta herramienta no garantiza el cumplimiento del RGPD, puesto que se dan recomendaciones muy superficiales.

Figura 13: Proyecto ALTO. Fuente: (11)

2.6. Crítica al estado del arte

Esta herramienta puede ser de gran utilidad para cualquier organización, sin embargo, se queda corta en algunos aspectos. Si las actividades que lleva a cabo la empresa trata datos biométricos, relacionados con mercadotecnia o similares esta herramienta no nos dará soporte. Nos saldrá un mensaje que indicará que tenemos que hacer un análisis de riesgos.

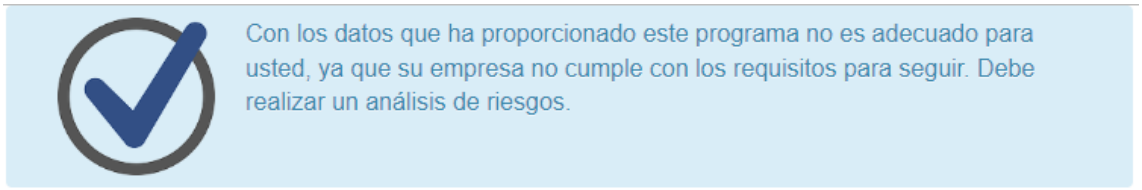


Figura 14: Mensaje análisis de riesgos. Fuente: (7)

Respecto a la evaluación de riesgos, en la misma página de la AEPD (7) podemos encontrar una herramienta que nos ayudará. Evalúa-Riesgo RGPD v2 es una herramienta que evalúa el nivel de riesgo para cada factor de riesgo. El análisis que se hace es de mínimos y se deberán hacer modificaciones para ajustar los resultados a la empresa.

Figura 15: Herramienta Evalúa-Riesgo. Fuente: (7)

El resto de entidades de protección de datos también ofrecen herramientas de evaluación de riesgos que permiten analizar si merece la pena tratar según que tipos de datos, como por ejemplo los datos biométricos.

Todas estas herramientas pretenden garantizar el correcto tratamiento de datos, pero también advierten de que el uso de ellas no asegura al cien por cien el cumplimiento de las leyes de protección de datos.

2.7. Propuesta

Puesto que la herramienta mencionada anteriormente no puede ser usada cuando se usan datos biométricos, mercadotecnia y cuestiones referentes al teletrabajo, crear una herramienta, o en este caso una guía, que contemple también estos aspectos sería de gran utilidad para cualquier organización.

3. Leyes y guías de protección de datos

Antes de comenzar a analizar las distintas guías y leyes es necesario definir algunos conceptos básicos que se mencionarán a lo largo del trabajo.

La protección de datos (12) son el conjunto de estrategias y procesos de seguridad necesarios para proteger datos personales de perdidas, modificaciones ilícitas o robos, además pretende garantizar que el dueño de la información tenga control sobre ella.

Los datos personales (13) son toda información sobre una persona física identificada. Una persona identificada es aquella cuya identidad puede determinarse mediante un identificador como puede ser el DNI, nombre, datos de localización, entre otros.

Una base de datos (14) es una colección estructurada de datos que representa una realidad, en este caso, representará una organización. También cambiará dinámicamente como la organización a la que representa. La base de datos para la cual haremos una guía contendrá: datos de los clientes, datos de los empleados y las cuentas de la empresa entre otras cosas.

El tratamiento de datos (13) es cualquier operación o conjunto de operaciones que se realizan con datos personales mediante procedimientos automatizados o no automatizados. Algunas de estas operaciones pueden ser la recogida de datos, el registro, la estructuración, la modificación, la supresión etc.

El responsable del tratamiento (13) es la persona que se responsabiliza del tratamiento de los datos, decide cómo se llevará a cabo, la finalidad del tratamiento y qué usos se le dará a la información. El encargado del tratamiento es una persona física o jurídica que trabaja para el responsable del tratamiento siguiendo sus directrices respecto a cómo tratar los datos.

Para comenzar a confeccionar nuestra guía analizaremos y extraeremos la información más relevante de una serie de leyes y guías que se encuentran en la web oficial de la AEPD.

3.1. Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales y Reglamento UE 2016/679

La Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (15) establece los derechos y obligaciones en materia de tratamiento de datos en España. Esta ley será uno de los principales pilares en los cuales se basará nuestra guía. Muchos de los artículos de esta ley hacen referencia y se basan en el Reglamento UE 2016/679 o también conocido como RGPD.

A continuación, pasaremos a comentar los artículos más relevantes de la LOPDGDD y los separaremos por bloques:

3.1.1. Delegado de protección de datos

El DPO (data protection officer) o en español DPD (16) (delegado de protección de datos), es la persona encargada de informar al responsable de sus obligaciones en materia de protección de datos. Este deberá supervisar que se cumpla con la normativa y ser el punto de contacto entre la empresa y la autoridad de protección de datos. Los datos de contacto del DPD deben ser públicos para que sea fácil contactar con él. En el RGPD encontramos tres artículos que nos hablan sobre esta figura, los artículos 37, 38 y 39.

En el artículo 39 del RGPD encontramos las funciones de este que son, informar y asesorar al responsable o al encargado del tratamiento y los empleados en materia de protección de datos, comprobar que se cumpla con la normativa, ofrece asesoramiento sobre evaluaciones de impacto, debe cooperar con las autoridades de protección de datos, atender a las consultas de los interesados y ser el enlace entre la autoridad de control y la empresa.

En el artículo 37 se nos dice que debe tener una persona para ser designada delegado de protección de datos. Para ser delegado de protección de datos no es necesario ser jurista, aunque sería recomendable. La persona designada debe tener conocimientos de Derechos, experiencia en el ámbito de la protección de datos y poder llevar a cabo las funciones recogidas en el artículo 39.

En el artículo 34 de la LOPDGDD se nos indica en qué casos es obligatorio tener un delegado de protección de datos. Si una empresa trata datos personales de forma masiva o realiza un tratamiento que puede afectar gravemente a los derechos y libertades de las personas es necesario tener un delegado de protección de datos. Hay ciertas entidades que también están obligadas a tener uno: colegios profesionales y sus consejos, centros docentes, empresas IT que traten datos, prestadores de servicios de la sociedad de la información, entidades financieras, aseguradoras, empresas de inversión, distribuidores de energía eléctrica y gas, entidades que evalúan la solvencia, entidades dedicadas al envío de publicidad, centros sanitarios, entidades que emitan informes comerciales, empresas privadas de seguridad, federaciones deportivas cuando traten datos de menores y operadores que se dediquen a actividades de juegos a través de internet.

El DPO puede ser un externo o bien se puede formar algún trabajador para que lo sea. Aunque no sea obligatorio tener uno, sí es muy recomendable, puesto que ayudará al cumplimiento de la normativa. El responsable o el encargado deben comunicar a la AEPD el nombramiento de un delegado en un plazo de 10 días y publicitar su existencia a través de medios electrónicos[1], también se pueden consultar los DPD que hay registrados.[2]

3.1.2. Principios del tratamiento

Artículo 4. Exactitud de los datos. Los datos deberán ser exactos y estar actualizados. El responsable del tratamiento no podrá ser sancionado si ha adoptado medidas para tener los datos exactos y actualizados. Si los datos inexactos proceden del afectado, proceden de un mediador o intermediario, proceden de otro responsable o proceden de un registro público.

El artículo 5 nos habla del deber de confidencialidad. El responsable del tratamiento y demás personas implicadas están sujetas al deber de confidencialidad. Esto quiere decir que se debe garantizar una cierta seguridad para que los datos sean tratados de forma

[1] Dar de alta al DPD: https://sedeagpd.gob.es/sede-electronica-web/vistas/formDelegadoProteccionDatos/procedimientoDelegadoProteccion.jsf

[2] Consultar DPD: https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/consultaDPD.jsf

correcta y se protejan de pérdidas y daños, usando para ello las técnicas adecuadas. Adicionalmente, también debemos tener en cuenta el secreto profesional. Esta confidencialidad debe mantenerse aun cuando el responsable deje de tratar los datos.

El artículo 6 nos habla del tratamiento basado en el consentimiento del afectado. El afectado da su consentimiento libremente, sabiendo de forma clara para qué fines serán usados sus datos. El consentimiento es expresado de forma clara y sin lugar a duda.

Artículo 11. Transparencia e información del afectado. El responsable deberá facilitar sus datos personales y la finalidad del tratamiento al afectado y este último podrá ejercer los derechos de rectificación, supresión, limitación, portabilidad etc. Para que el afectado pueda acceder a la información se le deberá facilitar una dirección de correo u otro medio con el que acceder de forma rápida y sencilla. Si se quiere utilizar la información para la elaboración de perfiles se deberá notificar previamente al afectado y este deberá dar su consentimiento.

3.1.3. Derechos de los interesados

El artículo 13 nos habla del derecho de acceso. El interesado tiene derecho a la siguiente información con respecto a sus datos: los fines del tratamiento, si son enviados a terceros y quienes son estos, el plazo de conservación o criterios para determinar este, presentar reclamaciones etc. Cuando el afectado solicite acceso a sus datos se le facilitarán en formato electrónico, u otro que se solicite, siempre y cuando el acceso a estos datos afecte a los derechos y libertades de otros.

El artículo 14 nos habla del derecho de rectificación. El afectado podrá solicitar una modificación y/o corrección de sus datos presentando la documentación adecuada que acredite ese cambio.

El artículo 15 nos habla del derecho de supresión o derecho al olvido. El interesado tendrá derecho a que se eliminen sus datos personales en caso de que estos ya no sean necesarios, el interesado retire su consentimiento, se hayan tratado de forma ilícita, cuando el tratamiento tenga por objetivo la mercadotecnia etc.

El artículo 16 habla del derecho a la limitación del tratamiento. El interesado tiene derecho a limitar el tratamiento si los datos tratados no son exactos, el tratamiento es ilícito, se necesiten los datos para una reclamación, entre otros.

El artículo 17 habla del derecho a la portabilidad. El interesado tendrá derecho a recibir sus datos personales y compartirlos con otro responsable. Los datos pueden transmitirse también sin pasar por el interesado. Se podrán compartir estos datos siempre que no afecten a los derechos y libertades de otros.

El artículo 18 nos habla del derecho de oposición. El interesado tendrá derecho a oponerse a que sus datos sean tratados, salvo que deban ser tratados por fuerza de causa mayor. Cuando los datos se traten con fines de mercadotecnia el interesado podrá oponerse en cualquier momento a su tratamiento. Solo si los datos se tratan por razones de interés público será negado el derecho de oposición al tratamiento.

3.1.4. Videovigilancia

El artículo 22 nos habla de la videovigilancia. Se podrá llevar a cabo el tratamiento de imágenes de seguridad con fines de seguridad. Se podrán captar imágenes de la vía pública si estas son necesarias, pero nunca de un domicilio privado. Se deberán suprimir las imágenes en un plazo de un mes, a menos que las autoridades las necesiten para

evidenciar algún delito. Se debe avisar de la captación de estos datos mediante señales[3] que se vean claramente.

3.1.5. Derechos de los clientes

El artículo 23 nos habla de los sistemas de exclusión publicitaría. Se podrán tratar los datos para evitar el envío de publicidad, siempre que se haya solicitado. Las entidades responsables de estos sistemas deben rendir cuentas a la autoridad de control y deben informar[4] sobre cómo unirse a estos sistemas. La autoridad de control publicará una lista de los sistemas de exclusión con toda la información pertinente. Las organizaciones que pretendan enviar publicidad deberán consultar antes la lista Robinson[5]. Si se ha dado el consentimiento para recibir la publicidad no se consultará la lista anterior.

3.1.6. Derechos de los trabajadores

El artículo 87 nos habla del derecho a la intimidad y el uso de dispositivos tecnológicos en el ámbito laboral. Los trabajadores tienen derecho a la intimidad aun cuando usen un dispositivo cedido por la empresa para uso laboral. El empleador tiene derecho a acceder a los dispositivos para controlar que se lleven a cabo las obligaciones laborales y comprobar la seguridad de los dispositivos. Existen unos criterios para el uso de estos dispositivos, los cuales son conocidos por los trabajadores. Si estos dispositivos son usados con fines privados, el empleador solo puede acceder si se especifican los usos autorizados.

El artículo 88 nos habla del derecho de desconexión digital en el ámbito laboral. El trabajador tendrá derecho a la desconexión al finalizar la jornada laboral con el fin de respetar su tiempo de descanso y su intimidad. Se llegan a una serie de acuerdos entre la empresa y los trabajadores o sus representantes para elaborar una política interna que regule esto.

El artículo 89 nos habla del derecho a la intimidad en lo referente a dispositivos de videovigilancia y grabación de sonidos en el lugar de trabajo. Está muy relacionado con el artículo 22. Los empleadores podrán tratar las imágenes para el control de los trabajadores, siempre que se informe a estos últimos de la medida. Los sistemas de videovigilancia no podrán instalarse en aquellos lugares destinados al descanso, aseos, comedores y similares. En cuanto a los sistemas de sonido, se admitirán únicamente cuando sean necesarios para la seguridad y respetando los mismos principios que los sistemas de videovigilancia.

El artículo 90 nos habla del derecho a la intimidad ante los sistemas de geolocalización en el ámbito laboral. Los empleadores podrán tratar los datos obtenidos de geolocalización para el control de los trabajadores. Se debe informar previamente a los empleados.

El artículo 19 nos habla del tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales. Se pueden tratar los datos de contacto y otros

[3] En el anexo 2 podemos encontrar la señal y varios ejemplos de cómo rellenarla.
[4] Información exclusión publicitaria para interesados: https://www.aepd.es/areas-de-actuacion/publicidad-no-deseada

[5] Registro y consulta lista Robinson para empresas: https://www.listarobinson.es/empresas/registro

datos laborales relacionados con el puesto que ocupa la persona siempre que sea para ponerse en contacto con la persona por asuntos de la empresa y la finalidad del tratamiento tenga relación con la organización. Estos datos también podrán ser tratados cuando lo obligue la ley o sea necesario para llevar a cabo su trabajo.

3.1.7. Brechas de seguridad

Una brecha en la seguridad (17) de los datos sucede cuando los datos son destruidos de forma accidental, se pierden, son alterados de forma ilícita o accidental o han caído en manos de personal no autorizado. Estas brechas de seguridad pueden provocar daños y perjuicios a las personas cuyos datos se han visto comprometidos, se debe actuar proactivamente para evitarlas, pero en el caso de que sucedan se deben comunicar.

El artículo 33 del RGPD nos dice cómo se debe notificar a la autoridad de control cuando se produzca una violación en la seguridad de los datos personales. El responsable del tratamiento deberá informar lo antes posible o como máximo en un plazo de 72 horas desde que haya tenido constancia de la brecha, a menos que la violación de seguridad no suponga un riesgo para los derechos y libertades de las personas. Si la notificación por parte del responsable llega pasadas las 72 horas deberá indicar los motivos de la tardanza.
La notificación del responsable deberá documentar la siguiente información sobre la brecha/violación de seguridad:

- describir la naturaleza de la violación de seguridad, las categorías de datos, el número de afectados y su categoría y el número de registros afectados
- el nombre y datos del contacto del delegado de protección de datos u otro método de contacto para obtener información
- describir las consecuencias de la brecha de seguridad
- describir las medidas que el responsable ha adoptado para solucionar la brecha de seguridad y medidas para mitigar las consecuencias

Si no es posible facilitar esta información de forma simultánea se facilitará según se tenga conocimiento de ella.

Si es el encargado del tratamiento quien detecta la brecha de seguridad deberá comunicarlo al responsable a la mayor brevedad posible. En la web de la AEPD encontramos una herramienta[6] que nos ayuda cuando se produce una brecha de seguridad. Los responsables del tratamiento deberán comunicar la brecha de seguridad a la AEPD cuando la empresa esté en territorio español, si su sede se encuentra en España, si tiene a su representante en España o si no tienen establecimiento ni representante en España, pero la brecha afecta a ciudadanos españoles.

Si el responsable considera que el nivel de riesgo de la brecha es muy alto deberá comunicarla a las personas afectadas. El artículo 34 del RGPD nos indica cómo se debe llevar a cabo este proceso. El artículo 34 del RGPD dice que, cuando sea probable que la violación de seguridad conlleve un alto riesgo para los derechos y libertades de las personas el responsable deberá poner en su conocimiento esta situación a la mayor brevedad posible. Se deberá comunicar al interesado de forma clara y sencilla y contendrá la misma información que se ha facilitado a la autoridad de control.
No será necesario comunicar la violación de seguridad al interesado en los siguientes casos:

[6] Herramienta apoyo brecha: https://servicios.aepd.es/AEPD/view/form/MDAwMDAwMDAwMDAwMDUwOTc3NTMxNzE3MDY4NTI2Mzk1?updated=true

- el responsable ha adoptado medidas técnicas y organizativas que se han aplicado a los datos afectados y han hecho que estos sean ininteligibles para cualquier persona no autorizada
- el responsable ha tomado medidas para garantizar que la brecha de seguridad no suponga un alto riesgo para los derechos y las libertades de los afectados
- si comunicar la brecha de seguridad supone un gran esfuerzo se optará por comunicarla vía pública para que la información llegue a todos. Por ejemplo, en las noticias de vez en cuando salen noticias diciendo que los datos de una empresa han sido robados.

En caso de que el responsable no haya comunicado la violación de la seguridad de los datos, la autoridad de control puede exigir que lo haga o que adopte medidas técnicas y organizativas para proteger los datos, como se ha mencionado anteriormente.

Las notificaciones de brechas de datos personales se deben notificar por vía electrónica rellenando un formulario[7] que incluirá los datos que toda comunicación de brecha de seguridad debe tener. Se debe tener en cuenta que, el hecho de no notificar de una brecha de seguridad que afecta a los datos personales es una infracción con su correspondiente sanción económica. Si el responsable considera que no hay riesgos para los derechos y libertades este solo tiene la obligación de documentar la violación de seguridad incluyendo los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas, es decir, lo dicho en el artículo 33 del RGPD.

3.1.8. Transferencias de datos internacionales

Las transferencias internacionales (18) se realizan para datos personales que se estén tratando o se vayan a tratar tras su transferencia a un tercer país u organización internacional.
¿Cuándo se produce una transferencia de datos internacional?
Cuando se comunican datos a países que están fuera de la Unión Europea, Liechtenstein, Islandia y Noruega. Se podrán llevar a cabo estas transferencias cuando existan las garantías adecuadas que protejan los datos equivalentes a nuestra normativa, la autoridad de control lo autorice o haya una excepción. Hay unos artículos que son relevantes a la hora de tratar este tema:

Artículo 45. Este artículo nos habla de transferencias basadas en una decisión de adecuación. Se podrán transferir datos a los países que cuenten con las garantías de protección de datos similares a las del RGPD. Estos países son: Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda, Japón, Reino Unido, Corea del Sur y Estados Unidos.

El artículo 49 del RGPD enumera las excepciones en que se pueden hacer transferencias de datos internacionales. Estas excepciones son: si el interesado ha dado su consentimiento explícito después de haber sido informado de los riesgos, la transferencia es necesaria para la ejecución de un contrato entre el interesado y el responsable, por razones de interés público, para reclamaciones, proteger los intereses de terceros, que la transferencia se realice desde un registro público, la transferencia se haga una sola vez, que afecte a un número limitado de interesados o que sea imprescindible para que el responsable del tratamiento pueda llevar a cabo su cometido, siempre que no atente contra los derechos y libertades de terceros.

[7] Formulario para notificar brechas de seguridad: https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/nbs/guiadoBrechasInicio.jsf;jsessionid=qBJzaqqW1u_KcBageLu8InqHfYgfgNfL02bfYD-U.spvtac-srxsed01

También es posible realizar transferencias internacionales[8] si hay garantías adecuadas o en el caso de normas corporativas vinculantes (BCR).

3.1.9 Noticias sobre protección de datos

Worldcoin

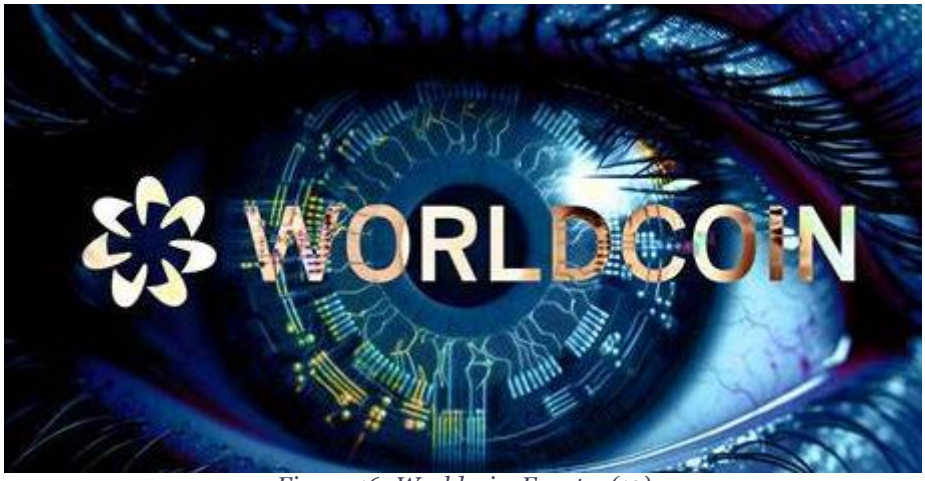


Figura 16: Worldcoin. Fuente: (19)

Prueba de que la protección de datos es un tema de actualidad es que lo encontramos en una noticia reciente. La entidad Tools for Humanit Corporationy está desarrollando un proyecto llamado Worldcoin, el cual consiste en escanear y guardar los datos del iris, a cambio de una remuneración en Worldcoins, la cual se puede canjear por euros. Gracias a que cada iris es único pretenden crear una identificación. Para escanear los iris utilizan un dispositivo llamado Orb. Este dispositivo captura la estructura del iris y genera un código personal. Con este código los usuarios podrán verificar que son humanos y no bots.

¿Cuál es el problema de esto? Pues que se están captando datos de menores de edad que dan su consentimiento sin tener claro para qué. Hay varias reclamaciones que manifiestan que no se informa de que se captan datos biométricos, no se facilita a los interesados el formulario de consentimiento, no se permite retirar el consentimiento ni ejercer los derechos básicos, como el de supresión, tampoco se está informando de los riesgos del tratamiento de datos biométricos. Por estos motivos la AEPD (20) ha interrumpido la recogida de estos datos.

La AEPD ha valorado los hechos mencionados anteriormente y ha estimado que hay indicios razonables de que se están incumpliendo las normativas de protección de datos. Por esto la AEPD le ha prohibido a la empresa continuar con la recogida de datos mediante una medida cautelar el día 6 de marzo de 2024.

Según el informe que ha elaborado la AEPD se están vulnerando los artículos 5.1 a), 6.1, 7, 9, 12, 13 y 17 del Reglamento UE 2016/679. Esto quiere decir que el tratamiento no es lícito, leal y transparente, el consentimiento no es el adecuado, no se tiene en cuenta que se están tratando datos especialmente sensibles, datos biométricos, no se está

[8] Más información sobre transferencias de datos internacionales: https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/garantias-para-las-transferencias-de

comunicando la información adecuada al interesado y no se están atendiendo a las solicitudes de los interesados para ejercer sus derechos.

Desconexión digital (21)

Nos encontramos con otra noticia en la cual un trabajador ha denunciado a su empresa por vulnerar su derecho a la desconexión y facilitar sus datos de contacto a terceras empresas.

El trabajador ha reclamado que su empresa le enviaba mensajes de trabajo a su correo personal fuera del horario laboral. Este hecho vulnera el artículo 88 de la LOPDGDD al violar el derecho al descanso del trabajador y su intimidad personal y familiar. Además, también ha recibido WhatsApp de una academia de formación y de la empresa Quirón, esto significa que su empresa proporcionó su correo a terceros sin su consentimiento y sin informarle de ellos.

Por estos hechos la empresa ha tenido que indemnizar con 300 euros por vulnerar el derecho a la desconexión digital y 700 euros por compartir datos personales del trabajador a terceras empresas.

Minimización de datos (22)

Una empresa de organización de eventos ha sido multada por pedir el DNI de los padres de un menor para poder acceder a un concierto. La madre del menor denunció ante la AEPD que esta empresa además de solicitar la autorización de los padres, también solicitaban copia del DNI de los padres e incluso información del menor.

La AEPD ha dado la razón a la madre ya que considera que vulnera el principio de minimización de los datos, habría bastado con pedir la identificación del menor en el momento de acceder al recinto. Por este motivo se incumple el artículo 5.1 c) que habla del principio de minimización de datos. Otra infracción cometida es que la empresa no informaba adecuadamente en el documento de autorización sobre las leyes de protección de datos y algunas cláusulas estaban desactualizadas.

De estas tres noticias podemos saber cuáles son los puntos débiles de las empresas en materia de protección de datos. Parecen tener problemas a la hora de atender las peticiones de los interesados para atender a los derechos fundamentales de los interesados, no saben muy bien cómo tratar datos especialmente sensibles, como son los datos biométricos, ignoran el derecho a la desconexión de los trabajadores y comparten sus datos de contacto y no incluyen adecuadamente las leyes en los contratos.

3.2. Guía para el teletrabajo

Otro tema importante que ha ido cogiendo fuerza estos últimos años, sobre todo desde la pandemia, es el teletrabajo. Debemos tener claro cómo proteger los datos de la organización cuando se lleva a cabo el teletrabajo. A este respecto hemos buscado y analizado una guía (23) sobre recomendaciones en situaciones de movilidad y teletrabajo, a continuación, analizaremos y comentaremos los aspectos más relevantes:

Primero de todo, se debe hacer un análisis de riesgos para saber si el teletrabajo merece la pena o no. Si se trabaja con una información muy sensible puede que sea mejor que esta información se trate únicamente en la empresa y en un entorno controlado.

El responsable del tratamiento deberá tener en cuenta una serie de cosas:

1-Deberá definir una política específica para las situaciones de movilidad que se verá reflejada en una guía que se facilitará a los empleados y la cual determinará cosas como las formas de acceso remoto permitidas, los dispositivos válidos para acceder y el nivel de acceso de cada empleado. Debe estar claramente indicado qué hacer en caso de incidente. Los empleados deberán firmar un acuerdo de teletrabajo que contenga las responsabilidades cuando teletrabajan.

2-Las aplicaciones y soluciones de teletrabajo deben ser de confianza y seguras, para evitar que se exponga información sensible. Un ejemplo de esto puede ser la aplicación Teams, la cual ha sido muy usada durante la pandemia para reunirse.

3-Se debe restringir la información en función del empleado, su rol y su nivel de acceso. También se deben aplicar restricciones a los distintos tipos de dispositivos con los que se acceda.

4-Los servidores de acceso remoto deben estar actualizados, configurados y se deben revisar periódicamente. Los equipos corporativos deben estar actualizados, tener habilitadas únicamente las aplicaciones que se vayan a usar, tener los privilegios mínimos para llevar a cabo su trabajo, tener activadas las comunicaciones necesarias y tener instaladas las aplicaciones autorizadas por la organización. En el caso de usar dispositivos personales, ya que no se pueden controlar como los corporativos, además de exigir que el ordenador esté actualizado, se puede dar acceso a los recursos imprescindibles y de bajo riesgo.

5-Se deben monitorizar los accesos a la red corporativa desde el exterior. Se debe informar previamente si esta información es usada para verificar que se cumplen las obligaciones laborales. Los mecanismos de monitorización deben respetar lo establecido en los artículos 87, 88 y 90 de la LOPDGDD. La configuración de los equipos que se usan para acceder remotamente a los recursos de debe revisar y debe estar actualizada.

6-Se debe evaluar si merece la pena exponer los datos a ciertos riesgos cuando se hace teletrabajo. Los dispositivos utilizados para el teletrabajo deben ser auditados.

El personal que lleve a cabo el teletrabajo debe seguir las prácticas indicadas en la guía:

1-Se deben seguir las políticas de protección especificadas en la guía para situaciones de movilidad segura.

2-El dispositivo usado para el teletrabajo debe cumplir una serie de requisitos: tener una contraseña segura y diferente al que usa el empleado en otras cuentas o redes sociales, no se debe descargar software que la organización no haya permitido, evitar conectarse a redes que pueden no ser seguras, no utilizarlo con fines personales, el equipo debe estar actualizado, así como su antivirus, estar seguro de que los correos recibidos son de una fuente segura y evitar descargar ficheros adjuntos que estos contengan, desactivar las conexiones que vayan a ser utilizadas y al finalizar la jornada desconectarse y apagar el equipo. Si el equipo que se usa para el teletrabajo es personal se debe evitar usarlo de forma simultánea para trabajar y para llevar a cabo actividades personales.

3-Se deben tomar precauciones para proteger la información que se está manejando: evitar los documentos en papel ya que no se pueden desechar con total seguridad, bloquear el dispositivo cuando no estemos y no dejar a la vista información, proteger la pantalla de miradas de terceros y evitar que las conversaciones puedan ser escuchadas bien con el uso de auriculares o yendo a un espacio libre de gente.

4-La información debe ser guardada en almacenamientos compartidos o nubes, autorizados por la organización en lugar de localmente. Se debe respetar la política de

copias de seguridad que la empresa y eliminar periódicamente la información residual que pueda quedar en el dispositivo.

3.3. Datos biométricos para el control de acceso

Los datos biométricos permiten identificar de forma inequívoca a un individuo mediante sus características físicas, fisiológicas o conductuales. Estos datos se almacenan en forma de plantilla o patrón biométrico. Una plantilla biométrica describe una característica humana como el rostro o una huella dactilar y esta es tratada por una máquina con un propósito, que en nuestro caso será el registro de jornada y el control de acceso.

Lo primero a tener en cuenta y que se menciona en repetidas ocasiones en esta guía (24) es el artículo 9 del Reglamento UE 2016/679. Este artículo hace referencia al tratamiento de categorías especiales de datos personales. Está prohibido tratar datos personales que hagan referencia a la etnia, opiniones políticas, religión, afiliación sindical, datos genéticos, datos biométricos y datos relacionados con la salud. Hay algunas circunstancias en las cuales estos datos pueden ser tratados: si el interesado ha dado su consentimiento, si el tratamiento es necesario para cumplir con obligaciones y derechos en el ámbito laboral, para proteger los intereses de una persona física, los datos personales se han hecho públicos, son necesarios en el ámbito judicial, se necesitan para el interés público o en el ámbito de la medicina.

Nos interesan los datos biométricos a la hora de realizar el registro de jornada y controlar el acceso al recinto de trabajo. En ambos casos el tratamiento de datos personales está sujeto al RGPD, además de otras consideraciones por el hecho de ser un tipo de dato especial. Los datos biométricos son un tipo de datos especiales ya que a través de ellos se pueden inferir datos médicos o que indiquen la etnia del individuo. Se podría pensar que las fotografías pudieran ser un tipo especial de dato personal, pero no lo son ya que no son un método infalible para identificar a una persona.

Registro de jornada

El registro de jornada deberá incluir un horario concreto de inicio y finalización de la jornada. Estos registros serán preservados por la empresa durante cuatro años y podrán ser consultados por los trabajadores, sus representantes legales y los inspectores de trabajo. Este registro tiene como objetivo que se cumpla con la jornada laboral establecida protegiendo así, tanto a trabajadores como a las empresas.

Control de acceso con fines laborales

La empresa podrá utilizar sistemas de vigilancia para verificar que el trabajador cumpla con sus obligaciones laborales.

Control de acceso con otras finalidades

También se puede querer controlar el acceso de terceros como usuarios o clientes al recinto de la empresa.

El artículo 5 de la RGPD nos habla de la minimización de datos, es decir, que los datos que se traten deben ser los adecuados, necesarios y limitados para lograr el objetivo del tratamiento. Cuando se utilicen datos biométricos para el control de presencia se han de tratar esto aplicando el principio de minimización. El mercado actual ofrece, en muchos casos, productos que recaban más información de la debida y vulneran el principio de minimización. Por lo tanto, al implementar uno de estos sistemas se debe hacer una

evaluación objetiva para determinar si se recogen datos excesivos para el objetivo del tratamiento.

Cuando realizamos un tratamiento de datos para registrar la jornada se realizan una serie de operaciones: se identifica al empleado, se recogen sus datos, se almacenan, se identifica y autentica a la persona, se registra el tiempo y también se puede obtener su localización.

La identificación electrónica es el proceso de utilizar datos de identificación para identificar a una persona en particular dentro de un grupo. La autenticación es un proceso que permite probar que la identidad de esta persona es cierta.

Cuando implementamos un sistema biométrico, la primera vez que se recogen datos es con el alta o registro del nuevo empleado y es crucial que se haga de forma correcta, ya que con estos datos se identificará el resto de las veces al individuo. El resto de las veces que se realice el control se compararán los datos recogidos con los que se encuentran en la base de datos y fueron recogidos la primera vez. Si se quieren usar estos datos para otros fines se debe tener en cuenta la normativa de protección de datos.

El encargado del tratamiento debe justificar por qué se tienen que utilizar sistemas de control de presencia biométricos y no se pueden utilizar otros medios como tarjetas o certificados que eviten el tratamiento de datos biométricos. Se ha de evaluar objetivamente si la única forma (si es la forma idónea) de llevar a cabo los objetivos se puede conseguir mediante datos biométricos. Además, se debe informar a los interesados de los riesgos de dicho tratamiento.

El empleado está obligado a facilitar sus datos para el registro de jornada y control de acceso, pero no tiene la obligación de que se haga con sus datos biométricos. El interesado debe dar su consentimiento libremente para que se puedan tratar sus datos biométricos, sin embargo, al haber un desequilibrio de poder entre el empleador y el empleado este consentimiento puede estar viciado y ser más bien una obligación ante la posibilidad de algún tipo de castigo. Para que pueda considerarse que se ha dado el consentimiento libremente se debe ofrecer otra alternativa al empleado. Esto puede provocar que los trabajadores escogen la alternativa que evite que se traten sus datos biométricos y que por lo tanto este tratamiento no sea necesario y al no cumplir este requisito no se pueda llevar a cabo.

Entre otros requisitos para implantar un sistema biométrico se deberá superar una Evaluación de Impacto para la Protección de Datos (EIPD) que también cumpla con los principios de idoneidad, necesidad y proporcionalidad.

3.4. Otras guías de la AEPD

Anteriormente hemos analizado y resumido un par de guías relativas al teletrabajo y al control de acceso mediante datos biométricos, pero, cabe decir que en la web de la AEPD podemos encontrar muchas más guías. Por ejemplo, hay guías sobre cumplimiento, categorías especiales de datos, educación y menores, buenas prácticas, entre otras.

Aparte de las herramientas mencionadas anteriormente y las guías podemos encontrar más material[9] que puede ser de utilidad como informes jurídicos, medidas provisionales que se han tomado contra entidades que incumplían la normativa, resoluciones y un

[9] Guías de protección de datos: https://www.aepd.es/guias-y-herramientas/guias

largo etcétera. Todos estos materiales pueden ayudar y complementar a la hora de cumplir con la normativa.

3.5. Modelos de contrato

Para ayudar al cumplimiento de la normativa de protección de datos hemos buscado una serie de modelos de contrato[10] que se pueden utilizar o bien tomar como base para realizar los contratos.

- Modelo de consentimiento para el tratamiento de datos[11]. Este documento debe incluir datos de contacto del responsable, el delegado de protección de datos, si lo hay, información sobre cómo ejercer los derechos A.R.C.O, los fines del tratamiento etc.
- Modelo de consentimiento para el tratamiento de datos de categoría especial con el fin de llevar un registro de jornada y controlar los accesos.
- Un acuerdo de teletrabajo que incluye las directrices a seguir para llevar a cabo el teletrabajo con seguridad.

3.6. Seguridad en el CPD

Otro aspecto a tener en cuenta a la hora de preservar la seguridad de nuestra base de datos es proteger el lugar donde estos se almacenan, los centros de procesamiento de datos o CPD.

Un centro de datos es el lugar donde se guardan los recursos de la organización y se procesa la información. Es una instalación robusta que debe dar servicio a las necesidades de la empresa de forma ininterrumpida. Cuando los empleados realicen teletrabajo se conectarán a estos servidores mediante VPN para acceder a los recursos de la empresa. También, cuando se trabaje desde la propia empresa los empleados accederán a la información de estos servidores. Nos centraremos en analizar los aspectos que afectan a la seguridad de los datos que estos almacenan.

Uno de los atributos de confiabilidad de un CPD es la seguridad-confidencialidad, que consiste en que solo accedan al CPD las personas autorizadas. Para garantizar esta seguridad implementaremos sistemas de control de acceso. Tendremos un historial donde se registrarán todas las entradas, implementaremos un nivel alto de seguridad y además tendremos sistemas de videovigilancia, entre los que se encuentran cámaras de seguridad, en concreto, un CCTV o circuito cerrado de televisión.

Para implementar la seguridad nos fijaremos en una norma, la TIA 942 (25), que es un estándar publicado por la TIA (Telecomunications Industry Association). Esta norma es una guía que describe cómo diseñar y construir un CPD. Esta norma clasifica los CPD según el nivel[12] de seguridad con el que han sido diseñados. En esta norma nos encontramos niveles con requerimientos técnicos que deberemos implementar.

[10] En el anexo podremos encontrar los modelos.

[12] En las imágenes extraídas de la norma TIA se usa la palabra TIER, que nosotros podríamos traducir como nivel o clasificación por niveles. Las abreviaturas y conceptos en inglés de las tablas se explican en un anexo.

	TIER 1	TIER 2	TIER 3	TIER 4
Security				
System CPU UPS capacity	na	Building	Building	Building + Battery (8 hour min)
Data Gathering Panels (Field Panels) UPS Capacity	na	Building + Battery (4 hour min)	Building + Battery (8 hour min)	Building + Battery (24 hour min)
Field Device UPS Capacity	na	Building + Battery (4 hour min)	Building + Battery (8 hour min)	Building + Battery (24 hour min)
Security staffing per shift	na	1 per 3,000 sq m / 30,000 sq ft (2 minimum)	1 per 2,000 sq m / 20,000 sq ft (3 minimum)	1 per 2,000 sq m / 20,000 sq ft (3 minimum)
Security Access Control/Monitoring at:				
Generators	industrial grade lock	intrusion detection	intrusion detection	intrusion detection
UPS, Telephone & MEP Rooms	industrial grade lock	intrusion detection	card access	card access
Fiber Vaults	industrial grade lock	intrusion detection	intrusion detection	card access
Emergency Exit Doors	industrial grade lock	monitor	delay egress per code	delay egress per code
Accessible Exterior Windows/opening	off site monitoring	intrusion detection	intrusion detection	intrusion detection
Security Operations Center	na	na	card access	card access
Network Operations Center	na	na	card access	card access
Security Equipment Rooms	na	intrusion detection	card access	card access
Doors into Computer Rooms	industrial grade lock	intrusion detection	card or biometric access for ingress and egress	card or biometric access for ingress and egress
Perimeter building doors	off site monitoring	intrusion detection	card access if entrance	card access if entrance
Door from Lobby to Floor	industrial grade lock	card access	Single person interlock, portal or other hardware designed to prevent piggybacking or pass back of access credential, preferably with biometrics.	single person interlock, portal or other hardware designed to prevent piggybacking or pass back of access credential, preferably with biometrics.
Bullet resistant walls, windows & doors				
Security Counter in Lobby	na	na	Level 3 (min)	Level 3 (min)
Security Counter in Shipping and Receiving	na	na	na	Level 3 (min)

Figura 17: Requisitos niveles de seguridad. Fuente: (25)

En la tabla anterior se nos muestran los requisitos de seguridad que tiene cada nivel. En los niveles 3 y 4, en el apartado Door from Lobby to Floor (Puerta del vestíbulo a la planta) entre otras cosas, recomienda, preferiblemente, implementar el control mediante acceso biométrico. Esta puede ser una razón de peso para implementar el tratamiento de datos biométricos, ya que sería una manera de justificar los principios de idoneidad, necesidad y proporcionalidad.

	TIER 1	TIER 2	TIER 3	TIER 4
CCTV Monitoring				
Building perimeter and parking	no requirement	no requirement	yes	yes
Generators	na	na	yes	yes
Access Controlled Doors	no requirement	yes	Yes	Yes
Computer Room Floors	no requirement	no requirement	Yes	Yes
UPS, Telephone & MEP Rooms	no requirement	no requirement	Yes	Yes
CCTV				
CCTV Recording of all activity on all cameras	no requirement	no requirement	Yes; digital	Yes; digital
Recording rate (frames per second)	na	na	20 frames/secs (min)	20 frames/secs (min)
Structural				
Seismic zone -any zone acceptable although it may dictate more costly support mechanisms	no restriction	no restriction	no restriction	no restriction
Facility designed to seismic zone requirements	no restriction	no restriction	no restriction	In Seismic Zone 0, 1, 2 to Zone 3 requirements. In Seismic Zone 3 & 4 to Zone 4 requirements
Site Specific Response Spectra - Degree of local Seismic accelerations	no	no	with Operation Status after 10% in 50 year event	with Operation Status after 5% in 100 year event
Importance factor - assists to ensure greater than code design	I=1	I=1.5	I=1.5	I=1.5
Telecommunications equipment racks/cabinets anchored to base or supported at top and base	no	Base only	Fully braced	Fully braced
Deflection limitation on telecommunications equipment within limits acceptable by the electrical attachments	no	no	yes	yes
Bracing of electrical conduits runs and cable trays	per code	per code w/ Importance	per code w/ Importance	per code w/ Importance
Bracing of mechanical system major duct runs	per code	per code w/ Importance	per code w/ Importance	per code w/ Importance
Floor loading capacity superimposed live load	7.2 kPa (150 lbf/sq ft).	8.4 kPa (175 lbf/sq ft)	12 kPa (250 lbf/sq ft)	12 kPa (250 lbf/sq ft)
Floor hanging capacity for ancillary loads suspended from below	1.2 kPa (25 lbf/sq ft)	1.2 kPa (25 lbf/sq ft)	2.4 kPa (50 lbf/sq ft)	2.4 kPa (50 lbf/sq ft)

	TIER 1	TIER 2	TIER 3	TIER 4
Concrete Slab Thickness at ground	127 mm (5 in)	127 mm (5 in)	127 mm (5 in)	127 mm (5 in)
Concrete topping over flutes for elevated floors affects size of anchor which can be installed	102 mm (4 in)	102 mm (4 in)	102 mm (4 in)	102 mm (4 in)
Building LFRS (Shearwall/Braced Frame/Moment Frame) indicates displacement of structure	Steel/Conc MF	Conc. Shearwall / Steel BF	Conc. Shearwall / Steel BF	Conc. Shearwall / Steel BF
Building Energy Dissipation - Passive Dampers/Base Isolation (energy absorption)	none	none	Passive Dampers	Passive Dampers/Base Isolation
Battery/UPS floor vs. building composition. Concrete floors more difficult to upgrade for intense loads. Steel framing with metal deck and fill much more easily upgraded.	PT concrete	CIP Mild Concrete	Steel Deck & Fill	Steel Deck & Fill
Steel Deck & Fill/ PT concrete/ CIP Mild - PT slabs much more difficult to install anchors	PT concrete	CIP Mild Concrete	Steel Deck & Fill	Steel Deck & Fill

Figura 18: Niveles de CCTV. Fuente: (25)

Un Circuito cerrado de Televisión o CCTV consiste en varios equipos interconectados mediante los cuales se puede visualizar y registrar en video lo que sucede en un determinado lugar. En la tabla anterior tenemos las especificaciones que deben tener estos sistemas para cumplir con cada nivel. Para este trabajo lo relevante es tener en cuenta que artículos de las leyes de datos se deben tener en cuenta para implementar este tipo de sistemas.

La implementación de estos niveles de seguridad es necesaria en caso de que queramos conseguir un certificado de seguridad. El Uptime Institute (26) es una organización que se dedica a asesorar a otras empresas en lo relativo a diseño de infraestructuras, como puede ser un CPD. Esta organización define los niveles que han sido recogidos en la norma TIA 492. En caso de cumplir con los requisitos de cada nivel esta organización nos daría un certificado. Por último, cabe destacar que, también se deben cumplir otros niveles relativos a copias de seguridad, cableado, refrigeración, entre otros, para obtener una de estas certificaciones.

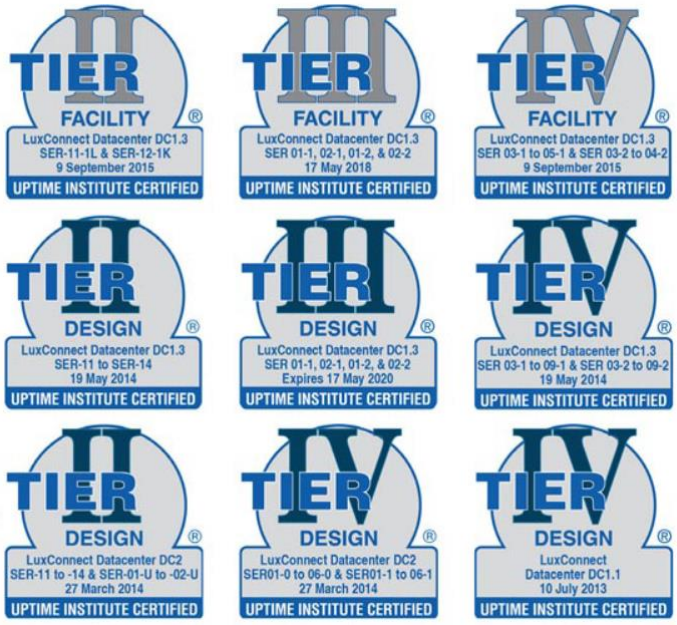


Figura 19: Certificados de nivel. Fuente: (26)

3.7. Protección de bases de datos

En los apartados anteriores nos hemos centrado en la protección de los datos desde una perspectiva legal, refiriéndonos a las normas de protección de datos y desde una perspectiva física haciendo referencia dónde están guardados, pero no debemos olvidar que los datos están ordenados en bases de datos y debemos tener muy en cuenta este aspecto. Según el RGPD debemos adoptar una serie de medias técnicas y organizativas para proteger los datos, ahora analizaremos qué medidas tomar para proteger debidamente nuestra base de datos.

La seguridad de las bases de datos se puede definir como el conjunto de herramientas y medidas tomadas para proteger la confidencialidad, integridad y disponibilidad de la BD. A la hora de proteger una base de datos debemos tener en cuenta que hay que proteger la base de datos en sí, el SGBD, las aplicaciones asociadas a la BD, el servidor físico y el virtual, además del hardware que la contiene y la infraestructura utilizada para acceder a la BD.

En el contexto de la seguridad de bases de datos nos encontramos con la regla de Anderson, que dice que cuanta más seguridad tenga una base de datos más difícil será

de utilizar y por el contrario cuanto más accesible y fácil de usar sea la seguridad estará más comprometida.

El hecho de que se produzca una violación en la seguridad de una base de datos puede acarrear los siguientes problemas:
-La propiedad intelectual se ve comprometida
-Se daña la reputación de la empresa
-Afecta a los procesos y el buen funcionamiento de la empresa
-Multas o sanciones impuestas por los organismos de protección de datos
-Indemnizaciones a los afectados

¿Cuáles son las amenazas más habituales a las BBDD?
-Empleados que dañen algún componente de la BD
-Empleados que cometen errores y no aplican debidamente las medidas de seguridad
-Usuarios externos que acceden a las instalaciones obteniendo las credenciales de algún empleado por medios ilícitos, como phishing.
-Vulnerabilidades en el software que pueden ser aprovechadas por hackers
-Ataques por inyección SQL/NoSQL
-Desbordamiento del almacenamiento
-Ataques a la copia de seguridad
-Ataques de denegación de servicio

¿Qué medidas podemos adoptar para proteger nuestra base de datos?

-Seguridad física. En el apartado anterior ya hemos expuesto cómo podemos proteger el centro de procesamiento de datos o CPD.
-Controlar el número de usuarios que tienen acceso a la BD y los permisos que se otorgan a los usuarios.
-Los dispositivos físicos que se conecten a la BD también deben estar asegurados.
-Los datos deben estar cifrados.
-Mantener el software de gestión de datos actualizado.
-Asegurarse de que las aplicaciones que accedan a la BD sean seguras.
-Las copias de seguridad deben estar guardadas a buen recaudo y seguras.
-Auditar de forma periódica la BD y los elementos que tiene a su alrededor.

También podemos establecer controles y políticas para acceder a la BD. Tenemos 3 tipos de controles:
-Administrativo. Controla la instalación, las actualizaciones y gestiona la configuración de la BD.
-Preventivo. Controla el acceso, el cifrado y el enmascaramiento.
-Detección. Supervisa la actividad de la BD y detecta si hay actividad sospechosa.

A la hora de crear nuestra guía para proteger bases de datos tendremos en cuenta las amenazas y las medidas a adoptar para evitar problemas.

4. Guía de control interno

4.1. La auditoría y sus fases

Finalmente, también recabaremos información sobre cómo llevar a cabo una auditoría. Buscaremos en webs de organismos oficiales para ver qué pasos se recomiendan y que directrices seguir.

ISACA (27)

ISACA o Asociación de Control y Auditoría de Sistemas de Información es una asociación independiente de auditores de TI y profesionales que trabajan en las áreas de gobierno TI. Esta organización tiene como fin establecer unos estándares para el gobierno, control y seguridad de los sistemas de información. Ofrece herramientas y cursos para profesionales. En su página web encontramos una serie de publicaciones que indican cómo llevar a cabo una auditoría:

1. Determinar el tema de la auditoría. En nuestro caso será una base de datos. Una base de datos es una colección estructurada de datos que representa una realidad, la realidad que representa será nuestra organización y sus clientes. También deberemos tener en cuenta las tecnologías de vigilancia (CCTV). Deberemos diferenciar entre datos de empleados y datos de clientes.
2. Establecer el objetivo u objetivos de la auditoría. Para establecer los objetivos es recomendable hacerlo teniendo en cuenta los riesgos. También tendremos en cuenta que se cumpla con la legislación, es decir, con las ya mencionadas anteriormente LOPDGDD y RGPD.
3. Establecer el alcance de la auditoría. Una vez definidos los objetivos el proceso de determinar el alcance de esta, es decir, qué servidores, qué bases de datos y qué otros agentes relacionados con el tratamiento de datos deberemos auditar.
4. Planificar previamente la auditoría. Una vez conocemos las actividades y áreas en las cuales se ubica la organización a auditar deberemos evaluar los riesgos.
5. Determinar los procedimientos de la auditoría y los pasos a seguir.

ISO 19011 (28)

También analizaremos un poco que nos dice la norma ISO 19011 sobre las auditorías. Esta norma nos describe una serie de etapas:

1. Realizar una reunión con los empleados, departamentos o personas a las que se va a auditar. Se les informará de cómo se llevará a cabo la auditoría.
2. Durante toda la auditoría se informará periódicamente de los progresos y se contestarán las preguntas de los auditados.
3. Recopilar y verificar la información de la auditoría.
4. Generación de hallazgos. Recopilaremos la información encontrada como incumplimientos de leyes y también se resaltarán las cosas buenas.
5. Conclusiones de la auditoría. Se realizará un informe con los resultados de la auditoría ya sean irregularidades o puntos fuertes.

Auditoría informática y aplicación a un caso en una empresa real, es el título de un TFG (29) en el cual nos apoyaremos para la realización de nuestra auditoría interna.

Una auditoría interna es aquella realizada por la propia empresa, se debe hacer como si se tratase de una auditoría real para comprobar si se podría superar una auditoría externa. La auditoría que nosotros haremos estará enfocada a la protección de datos. En el TFG se mencionan algunas pautas a seguir a la hora de hacer una auditoría interna:

-El personal encargado de realizar la auditoría rendirá cuentas ante la dirección de la empresa, nunca ante el departamento de TI.

-El personal que realice la auditoría debe tener conocimientos en informática, por lo tanto, es posible que el que realice la auditoría pertenezca al departamento de informática. Es fundamental que la auditoría sea lo más objetiva posible.

-Como se ha mencionado anteriormente la objetividad es crucial y esta se puede ver comprometida si el auditor y los auditados tienen algún tipo de relación. Puede ser recomendable contratar a un externo para que realice la auditoría.

-El auditor debe centrarse en hacer la auditoría y no podrá hacer otras tareas de forma simultánea.

-Al pertenecer el auditor a la empresa este tiene un gran conocimiento sobre ella y puede detectar deficiencias que un auditor externo no podría.

¿Cuáles son las fases de una auditoría?

En nuestro caso nos quedaremos con las fases que más nos interesen para nuestro trabajo.

Fase I - Alcance y objetivos

Alcance
El alcance de una auditoría son los límites y profundización de esta, se tienen en cuenta las áreas a auditar o las sedes y se define qué materias se auditarán.

Objetivos
Se establecerán unos objetivos, al tratarse de una auditoría de protección de datos el principal objetivo será cumplir con la normativa de protección de datos. A su vez este objetivo principal se dividirá en una serie de objetivos, por ejemplo, protección del CPD, teletrabajo, entre otros.

Fase V - Actividades de la auditoría informática

En esta fase, entre otras cosas, determinaremos las herramientas que utilizaremos para recopilar los datos de la auditoría. En nuestro caso, será un libro de Excel con checklist que generará un informe con las conclusiones obtenidas.

El CCN o Centro Criptológico Nacional (30) se creó para dar respuesta a los incidentes de ciberseguridad. Su misión es mejorar la ciberseguridad a nivel español. En su página web encontramos una Guía para auditar las TIC (31) y preservar así su seguridad. Las pautas descritas en la guía se deberán adaptar a cada organización.

¿Cómo se debe hacer una auditoría?

1. Debemos identificar los siguientes puntos:
    - el alcance y los objetivos de la auditoría. Estos deben estar claramente definidos, documentados y se deben consensuar con los directivos cuya organización se audite. Se debe tener claro qué elementos se van a auditar, en nuestro caso y como hemos mencionado anteriormente será la BD, las aplicaciones que acceden a ella y su entorno.
    - los recursos que tenemos para realizar la auditoría. Debemos tener claro cuántos auditores forman el equipo y de qué equipamiento se dispone.
    - comunicación con los responsables de la organización que han solicitado la auditoría
    - se ha hecho una planificación preliminar para determinar qué se hará en la auditoría
    - se establece un plan con las actividades, revisiones y pruebas

- se presentan los resultados
- se evalúan los resultados en relación a los objetivos y el alcalde definidos
- se presenta el informe a los solicitantes de la auditoría

2. Se debe registrar todo el proceso de la auditoría incluyendo el desarrollo de las tareas y las actividades realizadas.

Como conclusión de analizar las distintas fuentes que detallan como realizar una auditoría podemos sacar las siguientes conclusiones. Se debe establecer el alcance y objetivos de la auditoría, los recursos disponibles, se debe tener claro quién es el equipo auditor, se deben aclarar los detalles de la auditoría con los responsables de la organización, a quiénes daremos cuenta de los resultados, se deberá documentar todo el proceso y las limitaciones de la auditoría. Finalmente, deberemos crear un informe en el que conste toda la información, los resultados y conclusiones de la auditoría.

4.2. Análisis de riesgos

Cómo hemos visto en el apartado de fases de la auditoría es recomendable que los objetivos se establezcan desde el punto de vista de los riesgos. Por este motivo haremos un análisis de riesgos. Las herramientas vistas en el apartado del estado del arte no nos sirven para este caso. Estas herramientas tienen como objetivo analizar si merece la pena tratar ciertos tipos de datos sensibles como pueden ser datos biométricos. Nosotros nos centraremos en analizar los riesgos que tienen que ver con el incumplimiento de las leyes de protección de datos y las consecuencias de estos incumplimientos.

4.2.1. Riesgos económicos

En este apartado recopilaremos los tipos de sanciones en función de los artículos que sean violados. Estas sanciones económicas se pagan a la AEPD. Para que la organización que incumple con la ley pueda ser sancionada se deberá denunciar la situación a la AEPD. La LOPDGDD distingue entre infracciones leves, graves y muy graves, mientras que el RGPD distingue entre graves y muy graves.

Uno de los principales riesgos y que buscamos evitar con esta guía es el incumplimiento de la LOPDGDD[13] y el RGPD[14]. En este aspecto hay 3 artículos de la LOPDGDD que nos indican las distintas sanciones económicas que hay por incumplir algún artículo. El artículo 74 nos habla de las infracciones leves, el artículo 73 de las infracciones graves y el artículo 72 de las infracciones muy graves. Ofrecemos a continuación una tabla resumen:

Tipo de infracción	Artículos LOPDGDD	Artículos RGPD	Cuantía de la sanción	Estas sanciones prescriben…
Leves Art. 74 LOPDGDD	13 y 14, 3, 34,	15 a 22, 19, 26, 28, 30, 33, 34, 36, 37	Igual o inferior a 40.000€	al año

[13] Consultar la LOPDGDD: BOE-A-2018-16673 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Graves Art. 73 LOPDGDD	72, 28, 34	8, 25, 32, 27, Capítulo IV, 28, 30, 33, 34, 36, 37	Entre 40.001€ y 300.000€	a los dos años
Muy graves Art. 72 LOPDGDD	10, 27, 12, 5, 32	5, 6, 7, 9, 10, 13 y 14, 58	Superior a 300.000€	a los tres años

Tabla 1: Infracciones LOPDGDD. Fuente: elaboración propia

Si nos vamos al RGPD[15], en el artículo 83, en los apartados 4, 5 y 6 encontramos la cuantía de las sanciones impuestas por este reglamento.

Artículo 83.4.
- Artículos 8, 11, 25 a 39, 42 y 43. Obligaciones del responsable y el encargado
- Artículos 42 y 43. Obligaciones de los organismos de certificación
- Artículo 41.4. Obligaciones de la autoridad de control

Las infracciones de los artículos citados anteriormente se sancionarán con 10.000.000€ o el 2% del volumen de negocio total anual, adaptándose por la de mayor cuantía.

Artículo 83.5
- Artículos 5, 6, 7 y 9. Principios básicos del tratamiento de datos
- Artículos 12 a 22. Derechos de los interesados
- Artículos 44 a 49. Transferencias de datos internacionales
- Capítulo IX. Obligaciones del Derecho de los estados miembros
- Artículo 58.1 y 58.2. Limitación del tratamiento y facilitar acceso al tratamiento

Las infracciones de los artículos citados anteriormente se sancionarán con 20.000.000€ o el 4% del volumen de negocio total anual, adaptándose por la de mayor cuantía.

Para la creación de nuestra guía obviáremos aquellas sanciones dirigidas a entidades certificadoras y autoridades de control, puesto que nuestra organización no es ninguna de estas.

A modo de resumen podemos ver la siguiente tabla:

Tipo de infracción	Artículo(s)	Cuantía sanción
Grave	8,11, 25 a 39, 42 y 43	máximo de 10.000.000€ o 2% del volumen total
Muy grave	5, 6, 7 y 9 12 a 22	máximo de 20.000.000€ o 4% del volumen total

[15] Consultar el RGPD: 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).

	44 a 49 Capítulo IX 58.1 y 58.2	

Tabla 2: Infracciones RGPD. Fuente: elaboración propia

Encontramos también otros artículos a tener en cuenta:

Artículo 70. En este artículo se nos dice qué figuras están sujetas al régimen sancionador. Tenemos a los responsables, los encargados, representantes de los responsables o encargados del tratamiento establecidos en territorio europeo. Al delegado de protección de datos no se le aplican estas sanciones.

Artículo 75. Nos habla de la interrupción de la prescripción de una infracción. La prescripción de una infracción se interrumpirá cuando se inicie el proceso sancionador y se reiniciará cuando el expediente sancionador esté paralizado más de 6 seis meses por causas no imputables al presunto infractor.

Artículo 76. Nos dice qué factores se deben tener en cuenta a la hora de determinar el tipo de sanción:

- La infracción se produce de forma reiterada.
- Los beneficios obtenidos gracias a la infracción.
- La relación de la actividad del infractor con la realización del tratamiento de datos.
- La conducta del afectado ha podido provocar la infracción.
- Afecta a los derechos de menores.
- Tener un delegado de protección de datos, aun cuando no sea necesario.
- Proceso de fusión por absorción posterior a la infracción.
- El responsable o el encargado se someten a un proceso de resolución de conflictos de forma voluntaria para resolver disputas.

Si la autoridad competente es la AEPD, la sanción es mayor a un millón de euros y el infractor es una persona jurídica se publicará en el BOE la siguiente información: la identidad del autor, la infracción cometida y el importe de la sanción. Si la autoridad competente es autonómica se seguirá su normativa.

Según el artículo 83.2 del RGPD hay otras circunstancias a tener en cuenta:

- Intencionalidad o negligencia
- Medidas tomadas para reducir los daños y perjuicios
- Naturaleza, gravedad y duración de la infracción
- Grado de responsabilidad de los implicados teniendo en cuenta las medidas técnicas y organizativas adoptadas
- Infracciones anteriores
- Cooperación con la autoridad de control
- Categorías de datos afectadas
- Forma en la cual la autoridad de control supo sobre la infracción
- Adhesión a los códigos de conducta
- Incumplimiento de medidas tomadas previamente contra el responsable o encargado del tratamiento

4.2.2. Medidas técnicas y organizativas

Las medidas técnicas y organizativas (32) son las medidas de seguridad que se adoptan con el fin de prevenir brechas de seguridad en los datos. En el RGPD no se específica exactamente qué medidas adoptar, a continuación, listaremos algunas:

Medidas técnicas
-Uso de VPN, firewall, servidores Proxy, antivirus etc.
-Mantener los sistemas actualizados
-Protección del correo electrónico con filtros anti-spam y anti-phishing
-Copias de seguridad
-Cifrar los datos
-Llevar a cabo una seudonimización de los datos
-Controles de acceso y obligar a establecer contraseñas seguras, p.e: 8 dígitos, mayúsculas y minúsculas, algún número y algún carácter especial.

Medidas organizativas
-Formar y concienciar a los empleados en materia de seguridad
-Designar un DPD
-Políticas de destrucción de documentos
-Inventariar los dispositivos
-Registro de actividades del tratamiento
-Políticas de uso de dispositivos corporativos

4.2.3. Riesgos socioeconómicos y de imagen de la organización

Puede suceder que la organización sufra un robo de información. Esto puede provocar desconfianza entre los clientes, lo que puede hacer que dejen de requerir los servicios de la empresa y hablar mal de ella, lo que puede espantar a futuros clientes. Por esto es conveniente salvaguardar los datos siguiendo todas las medidas de seguridad que sean necesarias. Debemos proteger nuestro CPD tanto físicamente como su parte lógica. Para proteger la información de la empresa lo mejor es adoptar una actitud proactiva y evitar que estos sean robados, sufran daños y sean tratados de forma correcta, nuestra guía nos ayudará a lograr esto.

4.2.4. Encuesta sobre protección de datos

La AEPD junto con la CEPYME lanzaron una encuesta (33) a las pymes para conocer su situación respecto al tratamiento de datos. Para realizar este análisis se parte de los datos que gestionan las empresas y que están supeditados a la normativa de protección de datos.

¿Cuáles son los tipos de datos que más gestionan las empresas?
Los recursos que las organizaciones gestionan en mayor frecuencia son los datos de los clientes, los de los proveedores y los de los empleados, seguidos de las cámaras de videovigilancia. A continuación, vemos la gráfica.

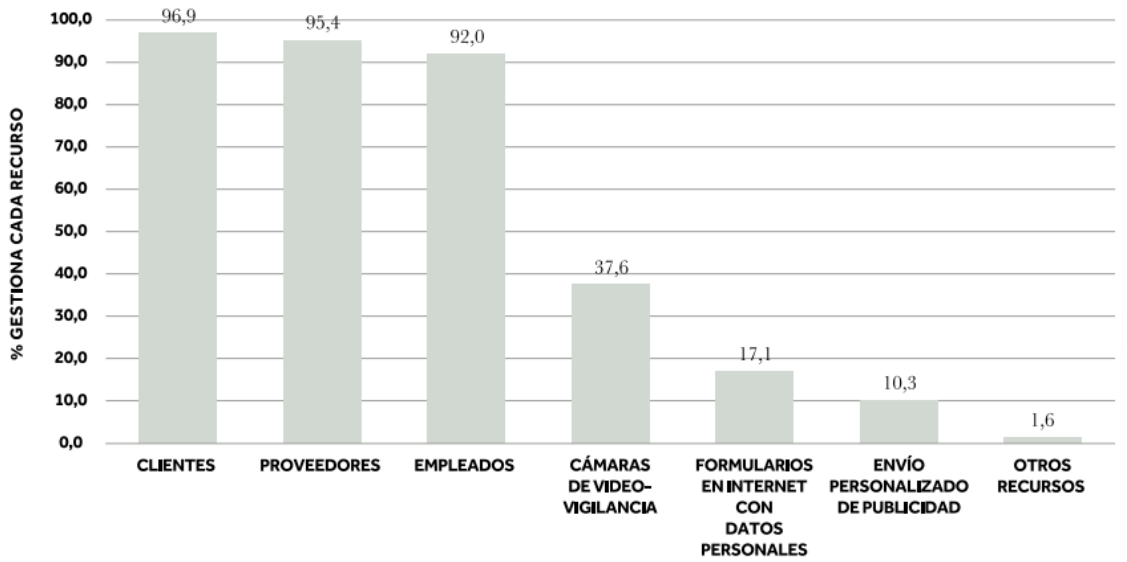


Figura 20: Diagrama de barras datos tratados por las empresas. Fuente: (33)

¿Cómo actúan las pymes en relación a la protección de datos?
El 80% de las pymes tiene un servicio de asesoramiento en materia de protección de datos o piensa contratarlo en poco tiempo, ha notificado sus ficheros a la AEPD y tiene elaborado el documento de seguridad.
El 69% de las pymes incluye cláusulas informativas en los formularios
El 58% de las pymes incluye cláusulas de protección de datos en los contratos.
El 39% de las pymes ha previsto o atendido solicitudes de ejercicio de los derechos de las personas.
El 24% de las pymes utiliza la página web de la AEPD.

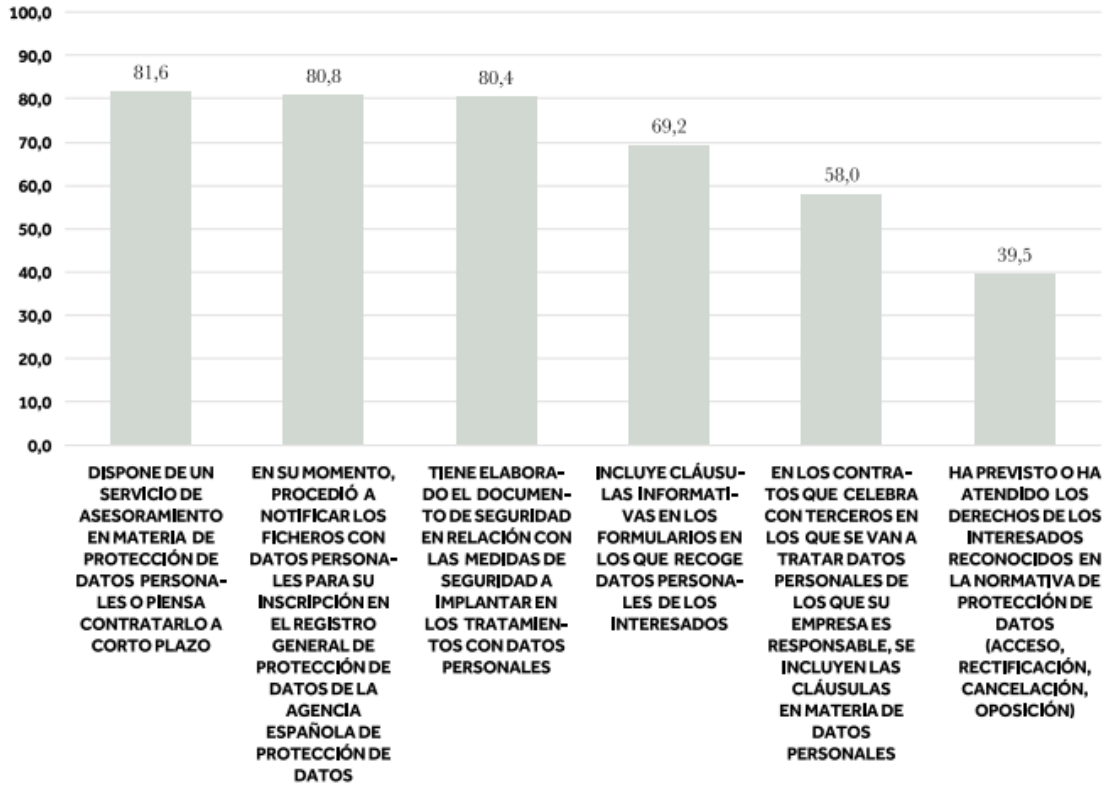


Figura 21: Diagrama de barras actuación frente a la normativa de protección de datos. Fuente: (33)

¿Cuánto saben las empresas sobre la normativa de protección de datos?

El 63% de las pymes tiene conocimiento del RPGD.
El 60% de las pymes conoce la obligación de elaborar el registro de actividades del tratamiento.
El 59% de las pymes sabe de las nuevas obligaciones del responsable del tratamiento.
El 47% de las pymes sabe sobre las guías de la AEPD.

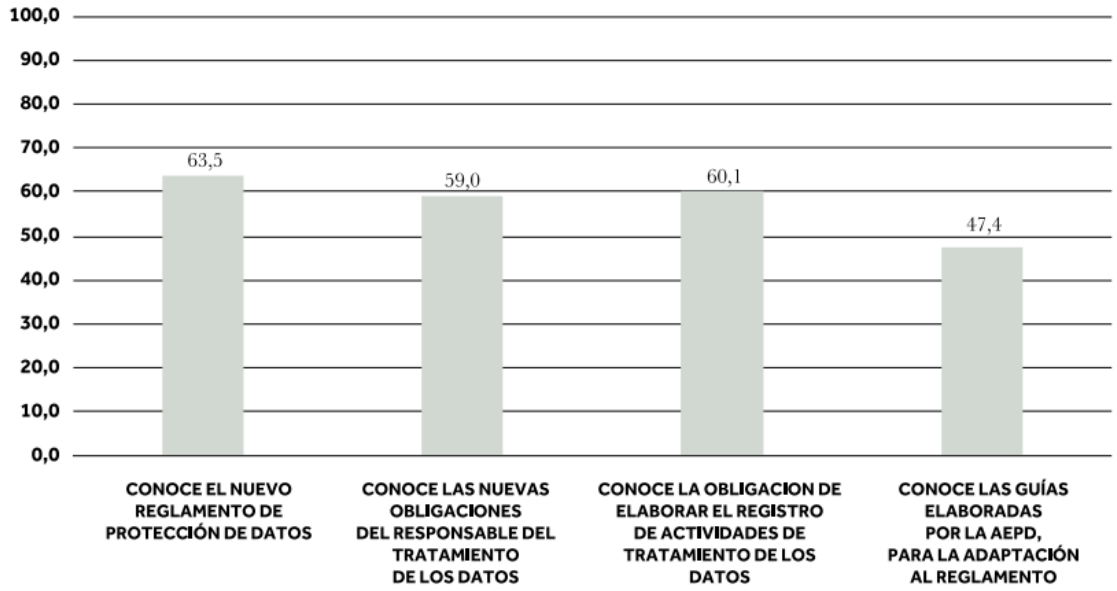


Figura 22: Diagrama de barras conocimientos de las pymes. Fuente: (33)

¿Cómo perciben las pymes la protección de datos?

El 80% de las pymes tienen un concepto positivo de la normativa de protección de datos. Las pymes tienen un concepto negativo de la normativa de protección de datos debido a que deben invertir demasiados recursos para el cumplimiento de este reglamento, lo que entorpece el desarrollo de sus actividades. Para paliar esto la AEPD tiene multitud de recursos a disposición de estas empresas, sin embargo, las pymes señalan que los consideran densos, poco claros y que no se adaptan a ellas.

Casi el 90% de las pymes considera que el Reglamento es mejor que la normativa anterior.

¿Cuál es la visión de las pymes sobre la gestión de los datos?

El 90% está de acuerdo con que "los datos deben ser protegidos siempre, es algo que nos afecta a todos"
El 62% está en desacuerdo con que "los datos personales no tienen valor para mi negocio"
El 47% está en desacuerdo con que "la protección de datos no justifica los costes", el 28% está a favor de esta afirmación y el 25% es neutral.

A partir de estos datos podemos inferir las debilidades o problemas que las empresas tienen en cuanto a la protección de datos.

¿Cuál es la actitud futura de las pymes ante la protección de datos?
El 85% están dispuestas a contratar un servicio de asesoramiento
El 79% están dispuestas a informarse mejor del Reglamento.
El 60% intentará gestionar las obligaciones ellas mismas y con ayuda de las herramientas que proporciona la AEPD.

Las conclusiones que podemos sacar de esto son que la mayor parte de las pymes están de acuerdo con la normativa de protección de datos, sin embargo, los costes de cumplir con la normativa provocan rechazo a esta. En general, estas tampoco son conscientes de las guías y herramientas que facilita la AEPD y en mayor medida prefieren contratar a un tercero para que les asesore sobre esto. Respecto al futuro, parece haber una actitud positiva respecto a estar informado sobre la protección de datos y cumplir la normativa. Otro dato interesante y que es de relevancia a la hora de crear nuestra guía es que solo el 39% atiende las solicitudes de ejercicio de los derechos.

4.3. Introducción a modelado de procesos

Para crear nuestra guía de desarrollo interno utilizaremos la notación BPMN (34) para modelar el proceso de una auditoría y sus distintas etapas. Para ello antes investigaremos y comentaremos un poco esta metodología.

El modelado de procesos o también conocido como BPMN por sus siglas en inglés (Business Process Management Notation) es una notación que permite modelar procesos y sirve para cualquier organización. Una de las grandes ventajas de esta metodología es su simpleza, ya que puede ser entendida por cualquiera y es fácil de aprender. En nuestro caso utilizaremos esta notación para modelar el proceso de la auditoría y sus pasos.

Pasaremos a introducir los símbolos BPMN necesarios para entender la guía.

- Eventos. Los eventos representan algo que ocurre en el sistema y provoca la activación de actividades. Un evento puede iniciar un proceso, provocarse durante el proceso o terminarlo.

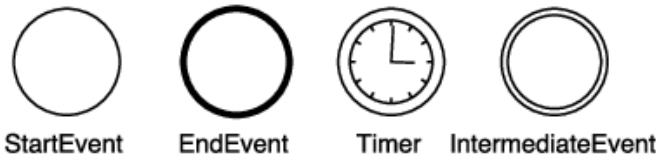


Figura 23: Eventos. Fuente: (35)

- Actividades. Las actividades representan los pasos de un proceso. Son la unidad básica de trabajo. También debemos mencionar un tipo de actividad llamada subproceso que consiste en una actividad que se puede descomponer en una serie de actividades.

Figura 24: Actividades. Fuente: (35)

- Puertas. Sirven para guiar el flujo de secuencia del proceso. Por ejemplo, si en un proceso hay actividades que se realizan de forma paralela, actividades que se

realizan en función de si se cumple una condición, si se deben cumplir una serie de condiciones para continuar el proceso o si se debe producir cierto evento para continuar.

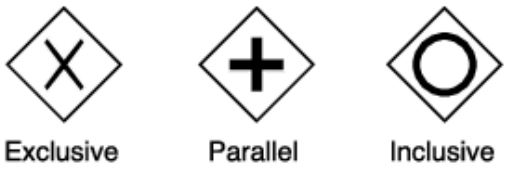


Figura 25: Puertas lógicas. Fuente: (35)

- Conectores. Conectan al resto de objetos de modelado. Representan el flujo del proceso y son flechas. Las flechas continuas representan el flujo de secuencia de las actividades y las discontinuas el intercambio de mensajes entre los participantes de la actividad.

Sequence Flow

Figura 26: Flujo de un proceso. Fuente: (35)

4.4. Identificación y análisis de las soluciones posibles

Solución 1
Utilizar el análisis anterior de las principales leyes que rigen la protección de datos para crear un libro de Excel. Con esta opción partiríamos de 0 sin tener en cuenta ninguna de las herramientas o documentos que nos facilitan los distintos organismos de protección de datos. Desarrollaríamos esta idea utilizando el BPMN y checklist en Excel.

Solución 2
Nos apoyaríamos en algunos documentos que facilitan algunas de estas agencias, como el documento del CNIL para registrar las actividades del tratamiento, pero un poco adaptado. Además, de incorporar parte de este documento se agregarían, como en la solución 1 una serie de checklist y diagramas BPMN, todo esto en un documento Excel.

Solución 3
Crearíamos un software parecido al que tiene algunas de estas organizaciones, pero añadiendo otras funcionalidades que creemos que son necesarias para un análisis completo de protección de datos.

4.5. Solución propuesta

En este caso optaremos por la solución que consta de un documento Excel al que se le agregaran partes ya hechas por algunas agencias y añadiremos otras cosas como modelado BPMN y checklist. Haremos hincapié en aquellos temas en los que más flojean las empresas españolas según la encuesta vista anteriormente. Evitaremos desarrollar software para que nuestra herramienta pueda ser utilizada independientemente del sistema operativo que se tenga. Al utilizar un documento de formato enriquecido este puede ser abierto mediante el programa Excel u otro software gratuito como podría ser Libre Office.

5. Diseño de la solución propuesta

Con la información expuesta anteriormente podemos empezar a confeccionar nuestra guía teniendo en cuenta las necesidades y debilidades de las organizaciones. Centraremos nuestra guía en el teletrabajo, el control de acceso mediante datos biométricos y los puntos en los que más fallan las empresas en materia de protección de datos. Según el estudio que hemos visto anteriormente y las noticias que hemos analizado una de las infracciones más comunes es que no se atienden las peticiones para ejercer los derechos fundamentales que se recogen en el RGPD de los artículos 15 a 22, a la hora de recoger el consentimiento no se informa debidamente de la normativa y al parecer también hay desconocimiento a la hora de tratar datos de categoría especial. Otro gran problema que tienen las empresas son los costes de llevar a cabo el cumplimiento de la normativa, motivo por el cual estamos desarrollando una herramienta gratuita que en la medida de lo posible proteja los datos y evite infracciones.

Para dar solución a todos estos problemas nuestra guía hará énfasis en los siguientes temas: fomentar que se atiendan las solicitudes para ejercer los derechos, informar sobre cómo se debe recoger el consentimiento y los datos que deben tener los formularios y contratos, cómo llevar a cabo el teletrabajo, que a día de hoy y desde la pandemia está al alza, el control de acceso mediante biometría, el cual a pesar de sus riesgos puede ser beneficioso tanto para la empresa como para el trabajador y tendremos en cuenta la realización del registro de las actividades del tratamiento, el cual es muy beneficioso para la organización cuando tenga que dar cuenta del tratamiento de datos que lleve a cabo.

5.1. Arquitectura del sistema

La herramienta desarrollada se compone de un libro en formato xlsx, también conocido como hoja de cálculo. Este libro cuenta con 11 hojas:

- Las dos primeras hojas contienen el diagrama BPMN, el cual actuará como interfaz principal de nuestra solución y que nos guiará en las distintas actividades que contiene la auditoría.

- La hoja llamada AlcyObj contiene 2 tablas en las cuales deberemos rellenar con datos sobre la auditoría, los objetivos y el alcance de esta.

- La siguiente hoja contiene información sobre el análisis de riesgos.

- Las siguientes hojas se deben cumplimentar con información sobre el tratamiento de datos y nos dan directrices sobre el cumplimiento de la normativa , comenzando por información sobre el delegado de protección de datos, siguiendo por el cumplimiento de las partes más críticas de la LOPDGDD y el RGPD, luego se toca el tema del teletrabajo y cómo llevar este a cabo de forma segura, los datos biométricos para el control de acceso, cómo proteger el CPD debidamente y finalmente, pero no menos importante, se deberá rellenar el registro de actividades del tratamiento.

- La última hoja contendrá los resultados de la auditoría.

5.2. Diseño detallado de la solución

La primera hoja del documento constará de la portada de la guía, en la cuál se nos dará contexto sobre la protección de bases de datos y sobre la motivación de la guía.

Figura 27: Portada de la guía. Fuente: elaboración propia

Al final de esta página encontramos dos enlaces, uno para las guías de la AEPD y otra para las herramientas que ofrece la AEPD. A la derecha encontramos el botón continuar que nos llevará a la interfaz principal de la guía.

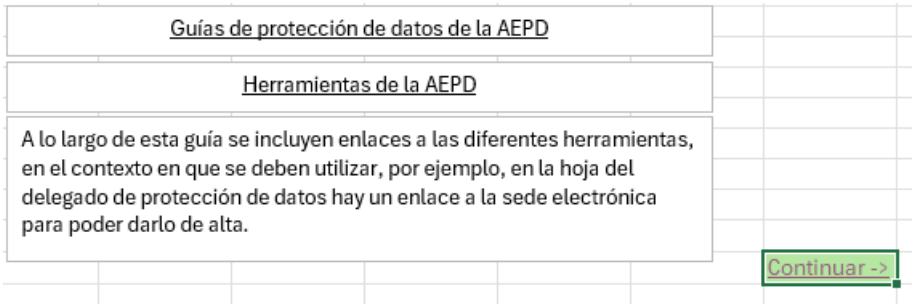


Figura 28: Portada 2ª parte. Fuente: elaboración propia.

La segunda hoja del documento y la que consideraremos como interfaz principal consta de un diagrama en notación BPMN que detalla los pasos a seguir. Al pulsar sobre cada una de las actividades nos llevará a otra hoja que deberemos rellenar con la información pertinente. A continuación, comentaremos el proceso que detalla el diagrama.

5.2.1. Diagrama BPMN

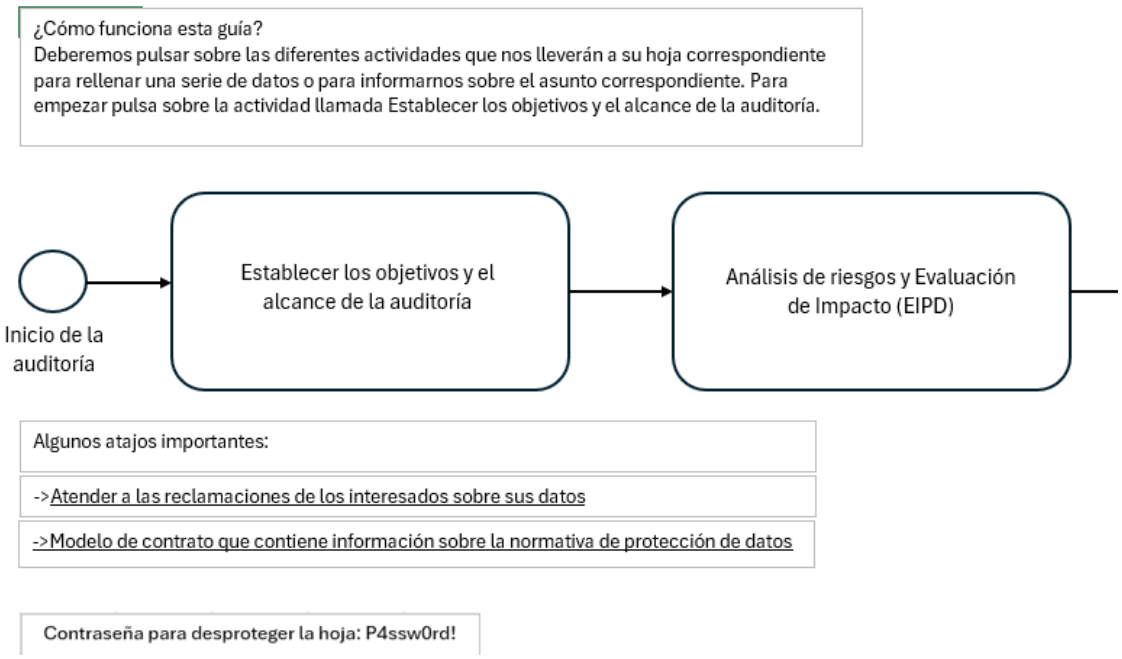


Figura 29: Primera parte del diagrama. Fuente: elaboración propia

El diagrama comienza con un evento de inicio que marca el principio de la auditoría. La fecha indica el por donde continua el flujo, que en este caso nos lleva a una actividad. Al pulsar sobre la actividad llamada Establecer los objetivos y el alcance de la auditoría nos llevará a una hoja para introducir los datos correspondientes. Una vez finalizada esta actividad pasaremos al análisis de riesgos y evaluación de impacto. También podemos ver una breve explicación de como empezar a usar la guía y algunos atajos a funciones especialmente importantes.

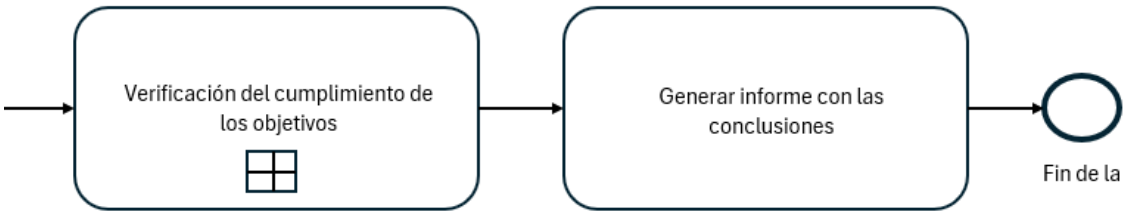


Figura 30: Segunda parte del diagrama. Fuente: elaboración propia

Una vez realizado el análisis de riesgo y la evaluación de podremos pasar al subproceso Verificación del cumplimiento de los objetivos, este subproceso está compuesto por una serie de actividades que detallaremos más adelante. La última actividad consiste en la generación de un informe con los resultados de la auditoría, tras la cual pasamos al evento de fin, con el que acaba la auditoría.

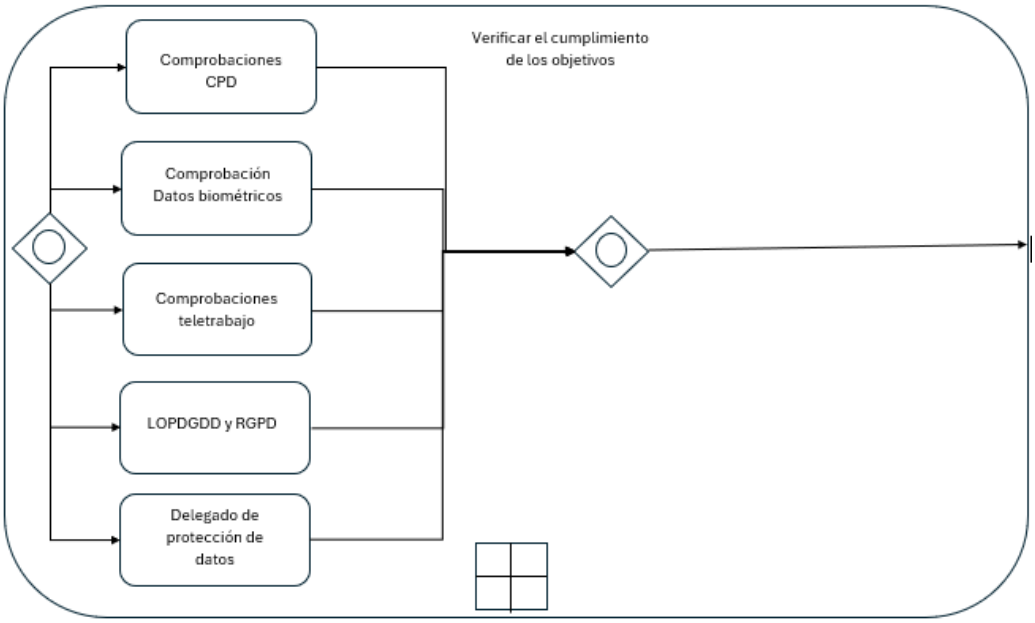


Figura 31: Subproceso Verificación del cumplimiento de los objetivos. Fuente: elaboración propia

El subproceso Verificación del cumplimiento de los objetivos está compuesto por cuatro actividades, las cuales se deberán cumplir para pasar a través de la puerta lógica y continuar con el proceso.

Para evitar que la portada o la interfaz principal sea modificada por error del usuario podemos bloquear las hojas. La contraseña que protege estas hojas figurará en ellas para que si el usuario quiere modificar el proceso para adaptarlo a su organización pueda.

Contraseña para desproteger la hoja: P4ssw0rd!

Figura 32: Contraseña protección de hojas. Fuente: elaboración propia

5.2.2. Establecer los objetivos y el alcance de la auditoría

En esta primera hoja deberemos introducir datos sobre la organización, comenzando por el nombre de esta. Después deberemos rellenar una tabla con el objetivo principal de la auditoría y los objetivos secundarios.

Nombre de la organización:	

	Detalles
Objetivo principal	Cumplimiento de la LOPDGDD y RGPD
Objetivo secundario 1	Protección del CPD
Objetivo secundario 2	Teletrabajo
Objetivo secundario 3	Categorías especiales de datos
Objetivo secundario 4	
Objetivo secundario 5	
Objetivo secundario 6	
Objetivo secundario 5	

Figura 33: Objetivos de la auditoría. Fuente: elaboración propia

A continuación, nos encontraremos con una segunda tabla que se deberá completar con los datos del alcance de la auditoría. Los datos que hemos considerado más relevantes a la hora de establecer el alcance de la auditoría han sido los departamentos auditados, duración de la auditoría, datos de quién realiza la auditoría, limitaciones de la auditoría y expectativas de los interesados.

Alcance	Detalles
Departamentos auditados	
Duración de la auditoría	
Datos del auditor	
Limitaciones de la auditoría	
Expectativas de los interesados	

Figura 34: Alcance de la auditoría. Fuente: elaboración propia

Si nos fijamos en las imágenes anteriores, algunas celdas tienen un triángulo rojo en la parte derecha, esto significa que tienen una nota. Al colocar el cursor sobre una de estas celdas se nos abrirá un cuadro que nos ayudará a completar la tabla. Por ejemplo, si nos colocamos sobre duración de la auditoría se nos mostrará la información de la siguiente figura:

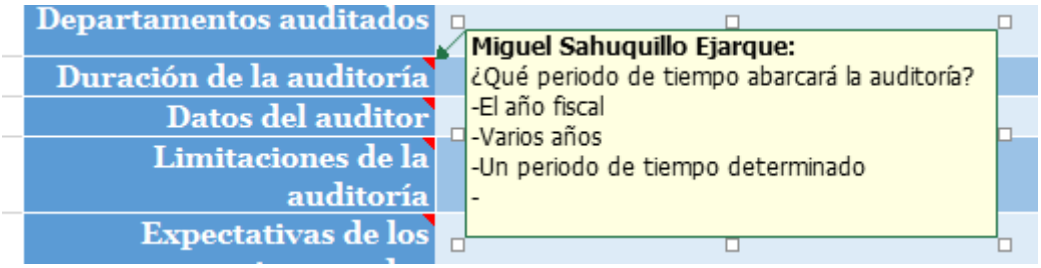


Figura 35: Notas explicativas. Fuente: elaboración propia

5.2.3. Análisis de riesgos y Evaluación de impacto

En esta hoja encontraremos una tabla que podremos completar con los posibles riesgos a los que se enfrente la empresa y asignar una puntuación a cada uno de estos.

También se facilita información sobre los tipos de sanciones por infringir la normativa de protección de datos y qué motivos pueden agravar estas sanciones.

LOPDGDD

Sanciones	Importe	Artículos LOPDGDD	Artículos RGPD
Leves	40.000€ o menos	72, 73, 3, 34	13 y 14, 15 a 22, 19, 26, 28, 30, 33, 34, 36 , 37
Graves	40.001€ - 300.000€	72, 28, 34	8, 25, 32, 27, Capítulo IV, 28, 30, 33, 34 36, 37
Muy graves	superior a 300.000€	10, 27, 12, 5, 32	5, 6, 7, 9, 10, 13 y 14, 15 a 22, 44 a 49 58.2

RGPD

Sanciones	Importe	Artículos
Graves	máx (10.000.000€ o 2% volumen total del negocio)	8, 11, 25 a 39, 42 y 43
Muy graves	máx (20.000.000€ o 4% volumen total del negocio)	5, 6, 7 y 9; 12 a 22; 44 a 49; Capítulo IX y 58.1 y 58.2

Figura 36: Tablas sanciones. Fuente: elaboración propia

¿Qué determina la gravedad de una sanción?

Para establecer el grado de la sanción, es decir, si es leve, grave o muy grave la LOPDGDD y el RGPD lo establecen en dos artículos, el artículo 76 y el artículo 83.2 respectivamente. Los detallamos a continuación:

Si la infracción se produce de forma reiterada.
Los beneficios obentidos de cometer la fracción.
Si la actividad del infractor está relacionada con el tratamiento de datos.
Si afecta a menores.
Si la infracción ha sido en parte por culpa del interesado.
Si se dispone de un delegado de protección de datos, aunque no sea obligatorio.
Si el responsable o el encargado se someten, con carácter voluntario, a resolver conflictos sin llegar a procesos judiciales.
Si ha habido un proceso de fusión por absorción posterior a la infracción.

Si ha habido intencionalidad o negligencia.
Si se han tomado medidas para reducir los daños y prejuicios.
La naturaleza, gravedad y duración de la infracción.
El grado de responsabilidad de los implicados teniendo en cuenta las medidas técnicas y organizativas adoptadas.
Si han habido infracciones anteriores.
Si se ha cooperado con la autoridad de control.
Las categorias de datos afectadas.
Si se ha informado a la autoridad de control sobre la infracción.
Si se han seguido los codigos de conducta.
Si se incumplen medidas tomadas previamente contra el responsable o el encargado del tratamiento.

Figura 37: Gravedad de las sanciones. Fuente: elaboración propia

Para acabar se informa de que previo al tratamiento se debe realizar un análisis de riesgos o una evaluación de impacto, dependiendo del riesgo que supongan los datos tratados para los derechos y libertades de las personas. En este TFG no abarcaremos este tema, remitiremos a un trabajo de un compañero que realizó una Guía de evaluación de impacto. Como alternativa a este trabajo también se puede recurrir al DPD para que nos asesore sobre este tema o utilizar la herramienta que nos proporciona la AEPD para la evaluación de impacto.

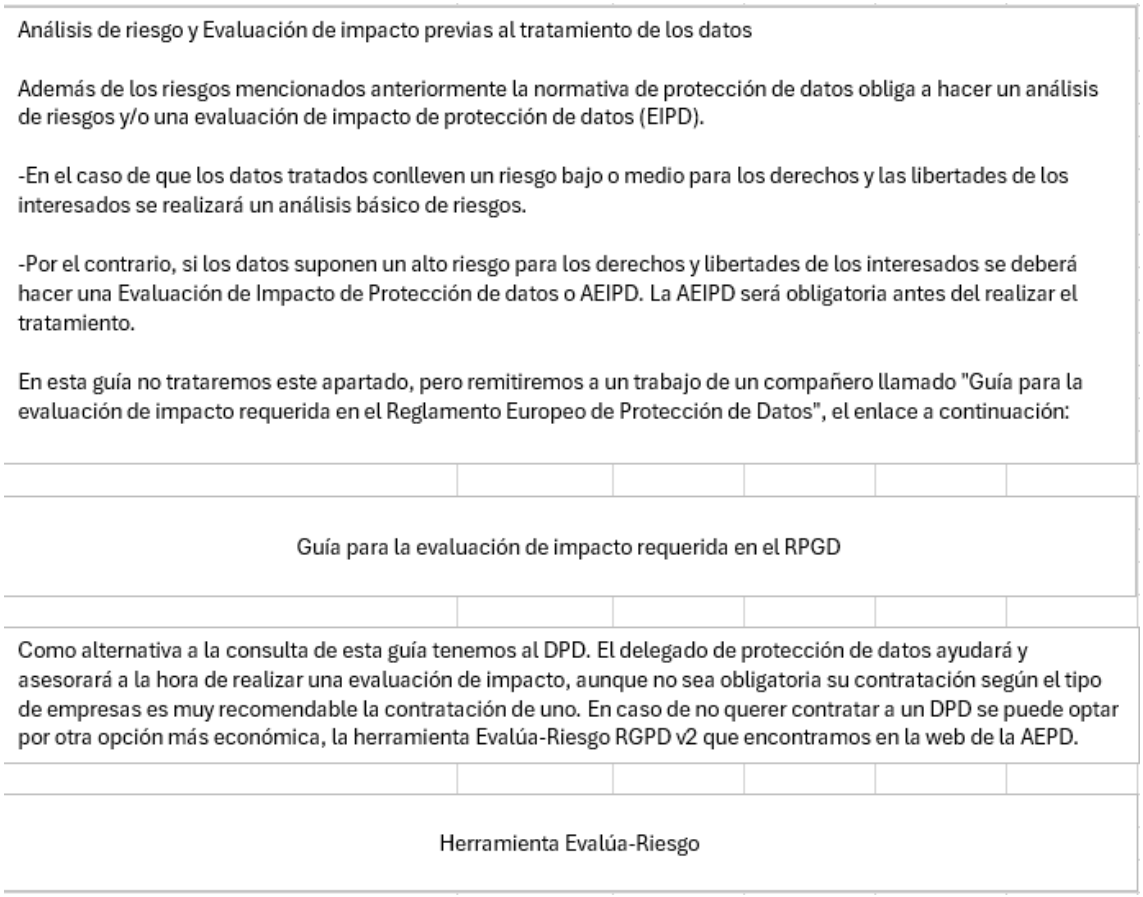


Figura 38: Análisis de riesgo y EIPD previa al tratamiento. Fuente: elaboración propia

5.2.4. Delegado de protección de datos (DPD)

En esta hoja se explica la figura del delegado de protección de datos. Para empezar, se explica en qué casos es necesario contratar a uno de estos. Si completamos el campo con Sí el motivo o tipo de entidad por la que tenemos que contratar un delegado de protección de datos se verá reflejada en la hoja de las conclusiones.

¿ En que casos es obligatorio tener un DPD? Si tu empresa trata datos personales de forma masiva o los datos que trata pueden afectar gravemente a los derechos y libertades de las personas será necesario un DPD. Además, hay ciertas entidades que también están obligadas a tenerlo, a continuación, indica que si tu empresa es una de estas entidades.

Tipo de entidad	¿Es tu empresa una de estas entidades? Sí/No
Colegios profesionales y sus consejos	
Centros docentes	
Empresas de telecomunicaciones cuando traten datos de forma habitual y a gran escala	
Prestadores de servicios de la sociedad de la información que elaboren perfiles de usuarios	
Entidades financieras	
Aseguradoras	
Empresas de inversión	
Distribuidores de energía eléctrica y gas	
Entidades que evalúan la solvencia	
Entidades dedicadas al envío de publicidad que creen perfiles o hagan un tratamiento basado en las preferencias de los interesados	
Centros sanitarios	
Entidades que emiten informes comerciales	
Empresas privadas de seguridad	
Federaciones deportivas cuando traten datos de menores	
Operadores que se dediquen a actividades de juegos a través de internet	

Figura 39: Casos en que se necesita un DPD. Fuente: elaboración propia

Seguido de esto se exponen las funciones que debe llevar a cabo el delegado de protección de datos y qué formación y conocimientos son necesarios para desempeñar este puesto.

¿Cuáles son las funciones de un delegado de protección de datos? -Informa y asesora al responsable y/o encargado en materia de protección de datos -Comprueba que se cumpla con la normativa -Ofrece asesoramiento sobre evaluaciones de impacto -Coopera con las autoridades de protección de datos -Atiende a las consultas de los interesados -Es en el enlace entre la autoridad de control y la empresa
¿Qué actitudes y conocimientos son necesarios para ser un delegado de protección de datos? -No es necesario ser jurista, pero sí tener conocimientos sobre Derecho -Experiencia en el ámbito de la protección de datos -Puede lleva a cabo las funciones mencionadas anteriormente.

Figura 40: Funciones y conocimientos del DPD. Fuente: elaboración propia

Para acabar se explica cómo dar de alta a un delegado de protección de datos.

¿Cómo designo un delegado de protección de datos? El responsable o el encargado de protección de datos deben comunicar a la AEPD el nombramiento del DPD y publicitar su existencia a través de medios electrónicos. Las empresas pueden registrar a su DPD a través del siguiente formulario:
Alta/Modificación Delegado de Protección de Datos

Figura 41: Designación DPD. Fuente: elaboración propia

5.2.5. LOPDGDD y RPGD

En esta hoja hemos dividido por bloques temáticos los principales aspectos de la LOPDGDD y el RGPD.

El primer bloque hace referencia a los principios básicos del tratamiento, se informa de a qué artículos se hace referencia y además se facilita un posible modelo de consentimiento para el tratamiento de datos personales. Además, en la columna estado introduciendo el número uno la tarea se dará por completada.

Progreso:			
0%			
Totales:	**9**		
Completadas:	**0**		
ESTADO	**TAREAS A COMPLETAR**	**ARTÍCULO(S) A LOS QUE SE REFIERE**	**ENLACES DE INTERÉS**
	Los datos deben ser exactos y en caso de que no lo sean deben ser actualizados a la mayor brevedad posible.	Art. 4 LOPDGDD Art. 5 RGPD	
	Si el responsable del tratamiento ha adoptado las medidas pertinentes para que los datos inexactos se rectifiquen o supriman y estos datos se han obtenido del afectado, de un intermediario, provienen de otro responsable o de un registro público, no se le podrá imputar.		
	Los implicados en el tratamiento de datos deben garantizar su confidencialidad, de forma complementaria se debe mantener el secreto profesional.	Art. 5 LOPDGDD Art. 5 RGPD	
	La obligación de mantener el deber de confidencialidad aun cuando el responsable o el encargado ya no estén a cargo del tratamiento o este haya finalizado.		
	Se obtiene el consentimiento para el tratamiento de datos de forma clara y libre y el interesado sabe para qué se usaran sus datos exactamente.	Art. 6 LOPDGDD Art. 4 RGPD	
	En caso de que el tratamiento tenga distintos fines, se deben indicar todos ellos de forma clara.		
	No se podrá condicionar la ejecución de un contrato a que el interesado consienta el tratamiento de sus datos para otras finalidades.		
	Cuando el responsable del tratamiento reciba los datos personales esta obligado a facilitar cierta información: los datos personales del responsable o el delegado de protección de datos, los fines del tratamiento, la posibilidad de ejercer los derechos básicos (acceso, supresión, rectificación etc.), los destinatarios de los datos y sus categorías, información sobre las transferencias internacionales, el plazo de conservación de los datos, el derecho a reclamar ante la autoridad de control y si hay decisiones automatizadas en el tratamiento de sus datos.	Art. 11 LOPDGDD	Ejemplo modelo de un contrato de consentimiento para el tratamiento de datos: Modelo consentimiento.docx
	Si los datos personales no son obtenidos directamente del interesado, además de la información anterior se incluirá la fuente de la que proceden sus datos y las categorías de datos que se tratan.		

Figura 42: Derechos básicos. Fuente: elaboración propia

En el segundo bloque temático se hace referencia a los derechos A.R.C.O y los pasos y requisitos a seguir para cumplir con estos.

	El interesado podrá solicitar la limitación del tratamiento en los siguientes supuestos:	Derecho a la limitación del tratamiento Art. 18 RGPD; Art. 16 LOPDGDD
	Se impugna la exactitud de los datos y estos deben ser verificados.	
	Si el tratamiento es ilícito.	
	Los datos ya no son necesarios para el tratamiento pero sí para reclamaciones.	
	Hay una oposición al tratamiento y se verifica si los motivos son legítimos.	
	Si se concede el derecho de limitación el interesado será informado antes de su aplicación y esta limitación deberá figurar en el sistema de información.	

Figura 43: Derecho de limitación. Fuente: elaboración propia

En el tercer bloque se enumeran derechos que afectan a los empleados de la empresa.

Derecho	Detalles
Geolocalización Art. 90 LOPDGDD	Antes de implantar sistemas de geolocalización para controlar a los empleados se deben valorar métodos menos intrusivos, teniendo en cuenta el principio de proporcionalidad.
	Se podrán tratar los datos de geolocalización de los trabajadores para funciones de control, siempre que se haga de forma legal y con límites.
	Se deberá informar previamente a los trabajdores de este tratamiento mediante una circular, cartel informativo o incluyendo una clausula en el acuerdo de teletrabajo.
	El documento informativo deberá incluir los derechos básiccos, qué dispositivo de geolocalización se usará, con qué fin, cuánto tiempo se almacenarán los datos y si terceros tendrán acceso a ellos.
Desconexión digital Art. 88 LOPDGDD	Los trabajadores tendrán derecho a la desconexión digital fuera del horario laboral .
	Los empleadores deben acordar con los trabajadores y/o sus representantes cómo se llevará a cabo la desconexión.
	Se debe tener especialmente en cuenta a los trabajadores que teletrabajan.
Intimidad y uso de dispositivos digitales en el ámbito laboral Art. 87 LOPDGDD	El empleador podrá acceder a los dispositivos para controlar el cumplimiento de las obligaciones laborales y comprobar la integridad del dipositivo.
	El empleador deberá establecer cómo usar los dispositivos, siempre respetando la intimidad del trabajador. Se elaborarán unos criterios junto con los trabajdores y/o sus representantes.
	Si los dispositivos pueden ser usados para fines privados se debe especificar su modo de uso e informar a los trabajadores de ellos. Por ejemplo, cuándo podrán ser usados con fines privados y podríamos establecer que en los descansos.

Figura 44: Derechos de los empleados. Fuente: elaboración propia

El cuarto bloque temático hace referencia a uno de los derechos de los clientes, el envío de publicidad.

Derecho	Detalles	Enlaces de interés
Exclusión publicitaria Art. 23 LOPDGDD	Si el interesado solicita que se le excluya de las comunicaciones de mercadotecnia, el responsable deberá informar de los sistemas de exclusión. Podemos facilitar a los interesados un enlace de la web de la AEPD donde se explican estas cuestiones.	Publicidad no deseada
	Para llevar a cabo comunicaciones de mercadotecnia se deberán consultar previamente los sistemas de exclusión publicitaria. En el caso de España deberemos consultar la lista Robinson. En el siguiente enlace las empresas podrán registrarse en su web oficial para llevar a cabo este cometido.	Registro empresas lista Robinson

Figura 45: Derecho a la exclusión publicitaria. Fuente: elaboración propia

El quinto bloque temático indica cómo se debe actuar ante una brecha de seguridad. Se enumeran los pasos a seguir y se facilitan un par de enlaces, el primer es uno que se puede ayudar al responsable en caso de que suceda una brecha y el segundo es la dirección de la sede electrónica para notificar brechas de seguridad.

Art. Relacionados	Pasos a seguir	Enlaces de interés
Art. 33 RGPD	Cuando suceda una brecha de seguridad se debe notificar a la autoridad de control, la AEPD.	
	El responsable deberá informar de la brecha en un plazo máximo de 72 horas desde que haya tenido constancia de ella, si se tarda más se deberá indicar el motivo de la tardanza.	
	Si la brecha de seguridad no supone un riesgo para los derechos y las libertades de los interesados no será necesario informar.	
	La notificación de la brecha de seguridad deberá incluir la siguiente información:	
	naturaleza de la violación de seguridad, categorías de datos afectadas, el número y categoría de afectados y el número de registros afectados.	
	el nombre y datos de contacto del delegado de protección de datos u otro método para informarse.	
	descripción de las consecuencias de la brecha de seguridad.	
	descripción de las medidas que el responsable ha adoptado para solucionar la brecha y medidas para mitigar las posibles consecuencias.	
	Si no es posible facilitar esta información de forma simultánea se facilitará según se tenga conocimiento de ella.	
	Si es el encargado quien detecta la brecha de seguridad deberá comunicarlo al responsable a la mayor brevedad posible.	
	En la web de la AEPD encontramos una herramienta que puede ayudar al responsable a determinar la gravedad de la situación.	Asesora Brecha
	Las notificaciones de brechas de datos se deben hacer vía electrónica, rellenando un formulario con los datos mencionados anteriormente. A continuación, facilitamos el enlace.	Notificar brecha de seguridad
Art. 34 RGPD	Si el responsable considera que el nivel de riesgo de la brecha de seguridad es muy alto deberá comunicarlo también a las personaas afectadas.	
	Se deberá poner en conocimiento de los interesados la misma información que hemos facilitado a la AEPD, además esta información estará expuesta de forma clara y sencilla.	
	No será necesario comunicar la brecha de seguridad a los interesados si:	
	el responsable ha adoptado medidas técnicas y organizativas que se han aplicado a los datos afectados y han hecho que estos sean ininteligibles para cualquier persona no autorizada.	
	el responsable ha tomado medidas para garantizar que la brecha de seguridad no suponga un alto riesgo para los derechos y libertades de los afectados.	
	si comunicar la brecha de seguridad a las personas afectadas supone un esfuerzo desmedido se optará por una vía pública para hacerlo, como puede ser el BOE o los noticiarios.	
	Si el responsable no ha comunicado la brecha de seguridad de los datos, la autoridad de control le puede exigir que lo haga o que adopte medidas para minimizar los daños.	

Figura 46: Brecha de seguridad. Fuente: elaboración propia

El sexto bloque indica qué cosas se deben tener en cuenta respecto a la videovigilancia tanto para empleados como para clientes. Podemos marcar las tareas completadas poniendo un uno en la columna de estado. También tenemos una tabla dónde introducir el nombre de los archivos de la grabación, su fecha de eliminación y si se han mantenido más tiempo el porqué.

Progreso:

0%

Totales: 12
Completadas: 0

ESTADO	TAREAS A COMPLETAR	ENLACES DE INTERÉS
	Los sistemas de vigilancia tienen como fin preservar la seguridad.	
	Se captan las imágenes imprescindibles de la vía pública para llevar a cabo la tarea mencionada anteriormente.	
	No se captan imágenes del interior de viviendas privadas.	
	Las imágenes serán eliminadas en el plazo máximo de un mes desde su captación.	Pincha aquí
	Si las imágenes muestran algún delito se deberán conservar y facilitar a la autoridad en un plazo de 62 horas. En estos casos no se aplicará la obligación de bloqueo.	Pincha aquí
	Se deberá colocar una señal en un lugar visible que, informe de la existencia del sistema de videovigilancia. Esta señal deberá indicar la identidad del responsable, un medio para contactar y una dirección web donde consultar sus derechos. Podemos encontrar una plantilla de la señal en la AEPD.	Señal Videovigilancia
	El responsable deberá estar atento a las peticiones que reciba para ejercer sus derechos y atenderlas.	
	Las empresas de seguridad privada que ofrezcan servicios de videovigilancia también están sujetas a estas leyes.	
	Las imágenes y sonidos obtenidos por las Fuerzas y Cuerpos de Seguridad, los órganos de centros penitenciarios y lo relacionado con el tráfico se regulará por esta ley cuando el tratamiento tenga fines de prevención, investigación, detección, enjuiciamientos penales y protección y prevención frente a amenazas a la salud pública. En el resto de casos estos datos se regiran por la 2016/680.	
	Los empleadores podrán tratar las imágenes para controlar los horarios de los trabajadores	
	Los dispositivos de vigilancia no pueden estar en lugares destinados al descanso de los trabajadores, vestuarios, aseos, comedores y similares.	
	La grabación de sonidos está sujeta a los mismos principios que la videovigilancia.	

Nombre archivo	Fecha de eliminación	Motivo de no eliminación

Figura 47: Videovigilancia. Fuente: elaboración propia

Finalmente, el último bloque trata sobre las transferencias de datos internacionales.

Casos de transferencias	Detalles	Enlace de interés
Decisión de adecuación Art. 45 RGPD	Se podrán realizar transferencias de datos a países que cuenten con garantías de protección de	
	Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay,	
Excepciones Art. 49 RGPD	Hay ciertas excepciones en que se pueden hacer transferencias de datos internacionales aunque no se garanticen los requisitos mínimos de protección de datos:	
	el interesado ha dado su consentimiento sabiendo los riesgos que conlleva	
	la transferencia es necesaria para la ejecución de un contrato entre el interesado y el responsable	
	es necesaria por razones de interés público	
	es necesaria para reclamaciones	
	para proteger intereses de terceros	
	la transferencia se hace desde un registro público	
	la transferencia se hace una sola vez y afecta a un número pequeño de interesados	
	es imprescindible para que el responsable lleve a cabo su trabajo y no atenta contra los derechos y libertades de terceros	
Otros casos	También es posible realizar transferencias internacionales si hay garantías adecuadas o normas vinculantes (BCR). Para obtener más información sobre este tema se puede visitar la web de la AEPD.	Transferencias de datos internacionales

Figura 48: Transferencias de datos internacionales. Fuente: elaboración propia

5.2.6. Biometría

En esta hoja se analizan en qué casos se levanta la prohibición del tratamiento de datos de categoría especial. Si en la columna de consentimiento se pone un uno se marcará con un check y la información se pondrá automáticamente en la hoja de las conclusiones.

Consentimiento	Se levanta la prohibición del tratamiento si...
	El interesado ha dado su consentimiento explícito para tratar este tipo de datos.
	El tratamiento es necesario para cumplir las obligaciones y ejercicio de los derechos del responsable o el interesado en el ámbito del Derecho laboral y la seguridad y la protección social.
	Es necesario para proteger los intereses del interesado si este no está capacitado física o jurídicamente para dar su consentimiento.
	Se tratan datos que el interesado ha hecho públicos.
	El tratamiento es necesario para fines judiciales.
	El tratamiento tiene razones de interés público.
	El tratamiento es necesario para medicina preventiva o laboral, evaluación de la capacidad laboral, diagnóstico médico, prestaciones sanitarias o gestión del sistema de asistencia sanitaria.
	El tratamiento es de interés para la salud pública.
	El tratamiento tiene fines de investigación científica, investigación histórica o fines estadísticos.
	El tratamiento lo realiza un organismo sin ánimo de lucro con finalidad política, religiosa o sindical, los datos que se tratan pertenecen a miembros o exmiembros de la organización o personas relacionadas y estos datos no se comuniquen fuera de la organización.

Figura 49: Excepciones prohibición del tratamiento. Fuente: elaboración propia

También exponemos que requisitos debemos cumplir para implementar el registro de jornada y el control de acceso mediante biometría.

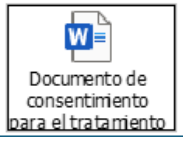
Tipo de uso	Detalles
Registro de jornada y control de acceso	Horario de inicio y finalización de jornada
	Los registros ser conservarán durante 4 años
	Los registros podrán ser consultados por trabajadores, sus representantes legales e inspectores de trabajo
	Evaluación previa de la tecnología que recoge los datos para que cumpla con el principio de minimización y recoja solo los datos necesarios
	El encargado debe justificar el uso de sistemas de control de presencia biométricos
	Se ofrecen otras alternativas a los empleados para cumplir con el registro de jornada y el control de acceso
	Modelo de consentimiento para el tratamiento de datos biométricos: 

Figura 50: Normas registro de jornada. Fuente: elaboración propia

5.2.7. CPD

En esta hoja se trata la protección del centro de procesamiento de datos o CPD. Para esto nos hemos basado en los requisitos que impone una norma, la TIA 942. Esta norma contempla la necesidad del uso de datos biométricos y la videovigilancia para proteger el CPD.

Se deberá rellenar una tabla respondiendo Sí o No para comprobar el nivel de seguridad del CPD con respecto los estándares de la norma TIA 942.

Requisito	Sí/No	Nivel alcanzado
¿ El CCTV monitoriza el perimetro del edificio y el parking?		
¿El CCTV monitoriza los generadores?		
¿El CCTV monitoriza las puertas de acceso?		
¿El CCTV monitoriza el acceso a las plantas con ordenadores?		
¿El CCTV monitoriza el sistema de alimentación, los teléfonos y la instalación eléctica?		
¿El CCTV graba de forma continua y graba todo el perimetro?		
¿El CCTV graba las imágenes a 20 fps (frames/segundo) o más?		
¿Se controla el acceso a los generadores mediante algún sistema de detección de intrusos?		
¿Se controla el acceso a los sistemas de alimenación, teléfonos e instalación eléctrica mediante tarjeta?		
¿Los compartimentos que tienen los cables de fibra óptica tienen control de acceso mediante tarjeta?		
¿Las salidas de emergencia tienen sistema de retardo de apertura de puertas?		
¿Las ventanas accesibles desde el exterior tienen detección de intrusos?		
¿El centro de operaciones de seguridad tiene control de acceso mediante tarjeta?		
¿El centro de operaciones de red tiene control de acceso mediante tarjeta?		
¿Las puertas de entrada a las salas de ordenadores tiene control de acceso mediante tarjeta o biometría?		
¿Las puertas de acceso al edificio requieren de tarjeta de acceso para entrar?		
¿La puerta del vestíbulo tiene bloqueo para que entre una persona cada vez, hay algún sistema que evite el piggybacking o se debe acceder por biometría?		

Figura 51: Requisitos TIA. Fuente: elaboración propia

Finalmente, se recordará que debemos tener en cuenta la normativa de protección de datos y se facilitarán 2 enlaces a otras hojas del documento.

Además de tener en cuenta lo que dicta la norma sobre la seguridad del CPD debemos tener encuenta la normativa de protección de datos. Es primordial que tengamos en cuenta el artículo 9 del RPGD, que dice como tratar categorías de datos especiales, en este caso biométricos y los artículos que hacen referencia a la videovigilancia.	
Biometría	Videovigilancia

Figura 52: Normativa de biometría y videovigilancia. Fuente: elaboración propia

5.2.8. Teletrabajo

Basándonos en una guía que encontramos en la AEPD hemos desarrollado una serie de tareas con las que poder desempeñar el teletrabajo con seguridad. Esta guía se puede dividir en dos partes, la primera, son las tareas que el responsable del tratamiento debe llevar a cabo, contiene también una serie de enlaces y documentos que serán de ayuda. Por último, también deberá rellenar dos tablas con información relativa al teletrabajo.

Totales:	16	
Completadas:	0	
ESTADO	**TAREAS A COMPLETAR**	**Enlaces de interés**
	Se garantiza el cumplimiento de la desconexión digital y no se contacta con el empleado fuera del horario laboral o lo establecido en el convenio que hayan acordado la empresa y los trabajadores.	Pincha aquí
	Establecer qué tipo de dispositivos se usarán.	Pincha aquí
	Establecer formas de acceso remoto permitidas.	Pincha aquí
	Creación de una guía funcional que informe a los empleados de los riesgos del teletrabajo, cómo protegerse y un punto de contacto por si sucede algo. Podemos encontrar más información sobre como hacer esta guía en esta misma hoja.	Pincha aquí
	Creación de un acuerdo en el que se recojan las directrices de la guía y que debe ser firmado por los empleados.	Acuerdo teletrabajo.docx
	Escoger soluciones de teletrabajo que sean ofrezcan seguridad.	Pincha aquí
	Si la empresa que nos ofrece las soluciones de teletrabajo accede a los datos será considerada encargada del tratamiento. Deberemos establecer un contrato con esta empresa, para más detalles sobre este acuerdo podemos consultar el enlace.	https://www.aepd.es/sites/default/files/2019-10/guia-directrices-contratos.pdf
	Restringuir el acceso a la información en función del rol de cada empleado, el nivel de acceso y el dispositivo que utilicen para acceder.	Pincha aquí
	Revisar periódicamente los servidores de acceso remoto, comprobando que están actualizados y debidamente configurados.	Pincha aquí
	Revisar que los equipos de teletrabajo estén actualizados, tengan deshabilitados los servicios que no vayan a usar, que no tengan privilegios de administrador, que tengan instalado el software autorizado por la organización, el antivirus está actualizado, tienen activadas solo las comunicaciones necesarias e incorporan mecanismos de cifrado.	Pincha aquí

Figura 53: Guía del responsable para el teletrabajo. Fuente: elaboración propia

	Si se utilizan dispositivos personales para el teletrabajo se deben incrementar más las medidas de seguridad y dar acceso a la información con menor nivel de riesgo.	
	Monitorizar los accesos a la red corporativa y actualizar la configuración de acceso de forma periódica.	
	Comunicar las brechas de seguridad.	Pincha aquí
	Si las actividades de monitorización se utilizan para verificar el cumplimiento de las obligaciones laborales se debe informar previamente a los empleados.	Se puede informar mediante una circular o en el acuerdo de teletrabajo.
	Valorar los riesgos que conlleva el teletrabajo para los datos tratados.	Pincha aquí
	Establecer procedimientos para auditar los dispositivos de teletrabajo de forma remota.	Pincha aquí

Figura 54: Guía del responsable para el teletrabajo 2ª parte. Fuente: elaboración propia

Información sobre el teletrabajo	Detalles
Forma(s) de acceso remoto	
Dispositivos de teletrabajo permitidos (ordenadores, tablets, smartphones etc.)	
Soluciones de teletrabajo	
Fecha última revisión servidores	
Fecha última revisión de los equipos de teletrabajo	
Fecha última auditoría de los equipos de teletrabajo	

Empleado	Nivel de acceso, puesto de trabajo, rol y dispostivo de teletrabajo	Bases de datos y elementos relacionados con estas a los que pueden acceder

Figura 55: Tablas de información para rellenar sobre teletrabajo. Fuente: elaboración propia

La segunda parte de la guía de teletrabajo consta de una serie de tareas que el empleado deberá realizar para asegurarse de que teletrabaja con seguridad. Como en las checklist anteriores poniendo un uno en la columna estado la tarea se dará por completada.

Progreso:	
0%	
Totales:	19
Completadas:	0

ESTADO	TAREAS A COMPLETAR
	Establecer una contraseña única y segura.
	Descargar únicamente software autorizado por la organización.
	Evitar conectarse a redes públicas o de baja seguridad.
	Utilizar el equipo de teletrabajo sólo con fines laborales.
	Si se utilizar equipo propio evitar utilizarlo de forma simultánea para trabajar y para uso personal.
	Mantener actualizado el equipo.
	Mantener el antivirus actualizado.
	Se revisa atentamente quien es el remitente de los correos.
	Evitar si es posible descargar ficheros adjuntos.
	Desactivar las conexiones que no sean necesarias (Bluetooth, NFC).
	Apagar el equipo al finalizar la jornada.
	Evitar los documentos en papel.
	Evitar que la pantalla del dispositivo sea vista por terceros y bloquear el dipositivo cuando no se use.
	No dejar información sensible a la vista, como una contraseña.
	Las reuniones deben llevarse a cabo en un espacio privado para evitar escuchas de terceros o utilizando cascos o auriculares.
	Se guarda la información en la nube o servicio de almacenamiento compartido indicado por la empresa.
	Eliminar periódicamente información residual del ordenador.
	Comprobar que se hace la copia de seguridad.
	Informar al responsable si se produce una brecha de seguridad para que tome medidas.

Figura 56: Guía de teletrabajo para el empleado. Fuente: elaboración propia

5.2.9. Registro de actividades del tratamiento

Para elaborar el registro de actividades del tratamiento hemos cogido el documento que nos facilitaba el CNIL en su página web oficial y lo hemos traducido a nuestro idioma, además de incluir las explicaciones pertinentes para que sea rellenado con facilidad.

5.2.10. Conclusiones de la auditoría

6. Tecnología utilizada

La tecnología usada para el desarrollo de este trabajo ha sido Excel. Durante el desarrollo del trabajo se han utilizado las siguientes funciones:

- Formato condicional. Para la creación de las checklist que se encuentran en el documento.
- Notas. Creación de notas, las cuales, al pulsar sobre la celda donde ha sido creada se abre un cuadro de texto con la información que hayamos puesto.

7. Desarrollo de la solución propuesta

La solución final es similar a la solución propuesta, pero se han añadido algunas cosas. Por ejemplo, se han añadido enlaces a las distintas herramientas que ofrece la AEPD y también se han añadido modelos de contratos para el tratamiento de datos.

Se ha hecho énfasis en los aspectos en los que más flaquean las pymes según el estudio mencionado anteriormente, además se ha comentado un par de guías para llevar a cabo el teletrabajo y para el control de acceso mediante datos biométricos.

8. Implantación y pruebas

Puesto que este TFG no se ha realizado con ninguna empresa no podemos poner a prueba su funcionamiento. En el anexo incluiremos algunos ejemplos de cómo utilizar la guía para cumplir con la normativa.

9. Conclusiones

Para garantizar la protección de las bases de datos se ha desarrollado una guía que contempla los distintos ámbitos de la protección de datos. Hemos comenzado por analizar las leyes a las cuáles las empresas están sujetas a la hora de realizar tratamientos de datos, estas son, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. También hemos ahondado en algunas guías y herramientas que ofrece la página web de la Agencia Española de Protección de Datos. Una vez que hemos buscado cómo proteger los datos nos centramos en cómo proteger el lugar donde se alojan los datos, las bases de datos. A la hora de realizar la auditoría de la base de datos no solo deberemos auditar la propia base de datos si no también el lugar físico dónde se encuentra, el centro de procesamiento de datos, también hay que tener en cuenta qué aplicaciones acceden a la base de datos, el sistema de gestión de bases de datos, el servidor virtual de la base de datos y la infraestructura utilizada para acceder a la base de datos. Así pues, teniendo en cuenta la información anteriormente recabada se ha procedido a la elaboración de una guía para auditar una base de datos. La guía contiene los aspectos más relevantes de la normativa de protección de datos y hace hincapié en las debilidades de las empresas a la hora de cumplir la normativa. Con esta guía se pretende que las empresas sean capaces de llevar a cabo una auditoría interna que les diga cómo de protegida está su base de datos y si serían capaces de superar una auténtica auditoría. Además, también se pretenden que las empresas pueden ahorrar recursos, por un lado, pueden evitar sanciones económicas por parte de los organismos de protección de datos e indemnizaciones a particulares, por otro lado, según el estudio muchas organizaciones sienten rechazo hacia la normativa de protección de datos, porque esta les obliga a invertir muchos recursos en su cumplimiento, lo que les impide crecer y dificulta sus actividades. Con esta guía se pretende acercar la protección de datos a las empresas de una forma amigable y sobre todo ahorrarles recursos.

10. Relación con los estudios

Durante todo el proceso de realización del trabajo se ha intentado relacionar este con algunas de las distintas asignaturas vistas en la carrera. Las detallamos a continuación:

- Deontología y profesionalismo. En esta asignatura se trata, entre otras cosas, las leyes que más nos atañen a los informáticos, dos de las más importantes son las leyes que rigen la protección de datos.

- Análisis de requisitos de negocio (ARN). En esta asignatura se enseña el modelado de procesos mediante notación BPMN. Una de las ventajas de esta notación es que es fácil de entender, por esto ha sido utilizada para hacer la interfaz principal de la guía.

- GCA. En esta asignatura se vio lo que eran los centros de procesamiento de datos y cómo proteger estos. Para proteger los CPD existe el estándar TIA 942 que ofrece una serie de directrices para diseñar y mantener protegidos los CPD. De todos los aspectos que contempla la TIA nosotros haremos hincapié en los relativos al control de acceso al CPD y la videovigilancia.

11. Trabajos futuros

- Transferencias internacionales de datos. Por falta de tiempo y porque no es el tema principal de este trabajo no se ha tratado en profundidad el tema de las transferencias internacionales de datos.

- Futuros cambios en la normativa de protección de datos. Debido a que la tecnología avanza a pasos agigantados las normativas de protección de datos deben ir adaptándose cada cierto tiempo.

- Protección de datos e IA. La IA está tomando una gran importancia en todos los ámbitos de nuestra vida. Quizá en un futuro se deba incluir explícitamente el uso de la inteligencia artificial en el tratamiento de datos, a pesar de que en la actual normativa ya se contempla el tratamiento de datos automatizados no estaría de más profundizar en este tema.

12. Glosario

BPMN: Business Process Model and Notation o en español Modelado y notación de procesos de negocio.
CPD: Centro de Procesamiento de Datos.

RGDP: Reglamento General de Protección de Datos, también conocido como Reglamento UE 2016/679.
AEPD: Agencia Española de Protección de Datos.
LOPDGDD: Ley Orgánica de Protección de Datos y garantía de los derechos digitales.

13. Bibliografía

1. Llopis Ferriol, Jesús. *Creación de una guía para la aplicación del nivel básico, medio y alto del Reglamento de Protección de Datos para microempresas*. [En línea]. Trabajo de fin de grado: UPV, 2016. [consulta: 3 de junio de 2024.]. Disponible en: https://riunet.upv.es/bitstream/handle/10251/68612/LLOPIS%20-%20Creaci%c3%b3n%20de%20una%20gu%c3%ada%20para%20la%20aplicaci%c3%b3n%20del%20nivel%20b%c3%a1sico%2c%20medio%20y%20alto%20del%20Reglamento%20de....pdf?sequence=1&isAllowed=y.

2. Villacorta Rivera, Mónica Jazmin. *Autocheking sobre una auditoría de SI RGPD*. [En línea]. Trabajo de fin de grado: UPV, 2022. [consulta: 3 de junio de 2024.]. Disponible en: https://riunet.upv.es/bitstream/handle/10251/185819/Villacorta%20-%20Autocheking%20sobre%20una%20auditoria%20de%20SI%20Reglamento%20General%20de%20Proteccion%20de%20Datos.pdf?sequence=1&isAllowed=y.

3. Mompó Alberola, Josep. *Guía Interactiva para el cumplimiento de normas de Protección de Datos en el entorno laboral*. [En línea]. Trabajo de fin de grado: UPV, 2020. [consulta: 4 de junio de 2024.]. Disponible en: https://riunet.upv.es/bitstream/handle/10251/152190/Momp%c3%b3%20-%20Gu%c3%ada%20interactiva%20para%20el%20cumplimiento%20de%20las%20normas%20de%20protecci%c3%b3n%20de%20datos%20en%20el%20entorno%20....pdf?sequence=1&isAllowed=y.

4. Grupo Atico34. Grupo Atico34. [En línea] [fecha de consulta: 4 de juio de 2024.]. Disponible en: https://protecciondatos-lopd.com/empresas/documento-seguridad/.

5. Mullor Berenger, Marta. *Guía sobre protección de datos e implantación de la LOPDGDD en centros sanitarios*. [En línea]. Trabajo de fin de grado: UPV, 2023. [consulta: 4 de junio de 2024.]. Disponible en: https://riunet.upv.es/bitstream/handle/10251/190960/Mullor%20-%20Guia%20sobre%20proteccion%20de%20datos%20e%20implantacion%20de%20la%20LOPDGDD%20en%20centros%20sanitarios.pdf?sequence=1&isAllowed=y.

6. Rodríguez Ferrer, Marc. *Guía para la evaluación de impacto requerida en el Reglamento Europeo de Protección de Datos*. [En línea]. Trabajo de fin de grado: UPV, 2020. [consulta: 1 de junio de 2024.]. Disponible en: https://riunet.upv.es/bitstream/handle/10251/151243/Rodr%c3%adguez%20-

%20Gu%c3%ada%20para%20la%20evaluaci%c3%b3n%20de%20impacto%20requerida%20en%20el%20Reglamento%20Europeo%20de%20Protecci%c3%b3n%20d....pdf?sequence=1&isAllowed=y.

7. *Agencia Española de Protección de Datos*. [En línea] [consulta: 2024 de febrero de 20.]. Disponible en: https://www.aepd.es/guias-y-herramientas/herramientas.

8. *Autoridad Catalana de Protección de Datos*. [En línea] [consulta: 16 de marzo de 2024.]. Disponible en: https://apdcat.gencat.cat/es/documentacio/programari/.

9. *Commission Nationale de l'Informatique et des Libertés*. [En línea] [consulta: 16 de marzo de 2024.]. Disponible en: https://www.cnil.fr/en/gdpr-toolkit/record-processing-activities.

10. *Comité Europeo de Protección de Datos*. [En línea] [consulta: 17 de marzo de 2024.]. Disponible en: https://www.edpb.europa.eu/news/news/2024/edpb-launches-website-auditing-tool_en.

11. *Commission Nationale pour la protection des données*. [En línea] [consulta: 20 de febrero de 2024.]. Disponible en: https://cnpd.public.lu/en/professionnels/outils-conformite/projet-alto.html.

12. *Microsoft*. [En línea] [consulta: 10 de febrero de 2024.]. Disponible en: https://www.microsoft.com/es-mx/security/business/security-101/what-is-data-protection?msockid=2b193e361d2863e825362a4d1c0362a9.

13. BÉLGICA. 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). Diario Oficial de la Unión Europea, 4 de mayo de 2016, número 119, 88 páginas.

14. *Oracle*. [En línea] [consulta: 25 de febrero de 2024.]. Disponible en: https://www.oracle.com/mx/database/what-is-database/.

15. ESPAÑA. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos personales y Garantía de los derechos digitales. Boletín Oficial del Estado, 6 de diciembre de 2018, número 16673, 70 páginas.

16. *Agencia Española de Protección de. Agencia Española de Protección de Datos*. [En línea] [consulta: 1 de junio de 2024.]. Disponible en: https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/designacion-delegado-proteccion-datos.

17. *Agencia Española de Protección de Datos*. [En línea] [consulta: 29 de mayo de 2024.]. Disponible en: https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/brechas-de-datos-personales-notificacion.

18. *Agencia Española de Protección de Datos*. [En línea] [consulta: 28 de mayo de 2024.]. Disponible en: https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/garantias-para-las-transferencias-de.

19. *Vistazo*. [En linea] [consulta: 25 de mayo de 2024]. Disponible en: https://techweez.com/2023/07/27/everything-about-worldcoin/.

20. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *CO-000297-2023-medida-provisional*. [En línea].Marzo de 2024. [consulta: 29 de mayo de 2024.]. Disponible en: https://www.aepd.es/documento/co-000297-2023-medida-provisional.pdf.

21. *Noticias Jurídicas*. [En línea] [consulta: 25 de mayo de 2024.]. Disponible en: https://noticias.juridicas.com/actualidad/jurisprudencia/19093-indemnizan-a-un-trabajador-por-vulnerar-sus-derechos-a-la-desconexion-digital-y-a-la-proteccion-de-datos/.

22. LENCINA, Fernanda. Multa de 20.000 euros por pedir una copia del DNI de los padres de un menor. En: *The Huffingtonpost* [En linea]. 2024. [consulta: 1 de junio de 2024.]. Disponible en: https://noticiastrabajo.huffingtonpost.es/sociedad/multa-de-20000-euros-por-pedir-una-copia-del-dni-de-los-padres-de-un-menor/.

23. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo* [En línea]. Abril de 2020. [consulta: 6 de febrero de 2024.]. Disponible en: https://www.aepd.es/guias/nota-tecnica-proteger-datos-teletrabajo.pdf.

24. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía sobre tratamiento de control de presencia mediante sistemas biométricos* [En línea]. Noviembre de 2023. [consulta: 6 de febrero de 2024.]. Disponible en: https://www.aepd.es/guias/guia-control-presencia-biometrico.pdf.

25. TIA-942. *Telecommunications Infrastructure Standard for Data Centers*.

26. *Uptime Institute - Digital Infrastructure Authority* [En línea] [consulta: 2024 de febrero de 26.]. Disponible en: https://pt.uptimeinstitute.com/.

27. COOKE, Ian. Auditoría básica: Auditando la privacidad de los datos. En: ISACA Journal [en línea]. 2018. Vol. 3, n.º X, págs. 1.

28. *EALDE Business School* [En línea] [consulta: 25 de abril de 2024.]. Disponible en: https://www.ealde.es/fases-auditoria-iso-19011/.

29. Barrio Ibánez, Jorge. *Auditoría Informática y apliación a un caso en una empresa real* [En línea]. Trabajo de fin de grado: UC3M, 2014. [consulta: 15 de junio de 2024.] . Disponible en: https://e-archivo.uc3m.es/rest/api/core/bitstreams/3734daa1-2e66-48f6-a4c9-588523d9ef1a/content.

30. *CCN-CERT - Centro Criptológico Nacional - CNI - ES* [En línea] [consulta: 20 de junio de 2024.]. Disponible en: https://www.ccn-cert.cni.es/es/sobre-nosotros/centro-criptologico-nacional?format=html.

31. *CCN-CERT - CENTRO CRIPTOLÓGICO NACIONAL - CNI - ES. Guía de Seguridad de las TIC CCN-STIC 802* [En línea]. Abril de 2017. [consulta: 20 de junio de 2024.] https://www.ccn-cert.cni.es/es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/502-ccn-stic-802-auditoria-del-ens/file?format=html.

32. *Atico34* [En línea] [consulta: 14 de junio de 2024.]. Disponible en: https://protecciondatos-lopd.com/empresas/medidas-tecnicas-organizativas/#:~:text=En%20cuanto%20a%20las%20medidas%20organizativas%20en%20protecci%C3%B3n,Pol%C3%ADtica%20de%20uso%20de%20dispositivos%20corporativos.%20M%C3%A1s%20elementos.

33. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Encuesta sobre el grado de preparación de las empresas españolas ante el Reglamento General de Protección de datos*[En línea]. Julio de 2018 [consulta: 1 de junio de 2024.]. Disponible en: https://www.aepd.es/guias/estudio-proteccion-de-datos-aepd-cepyme.pdf.

34. HITPASS, Bernhard. *BPMN 2.0 Manual de Referencia y Guía Práctica*. s.l. : Camunda, 2011. ISBN 1546905782.

35. *EVBN*. [En línea] [consulta: 15 de marzo de 2024.]. Disponible en: https://evbn.org/understanding-bpmn-diagrams-and-symbols-1678090220/.

36. *Agencia Española de protección de datos*. [En línea] [consulta: 7 de junio de 2024.]. Disponible en: https://www.aepd.es/sites/default/files/2019-09/cartel-videovigilancia.pdf.

37. *Agencia Española de Protección de Datos* [En línea] [consulta: 10 de febrero de 2024.]. Disponible en: https://www.aepd.es/guias-y-herramientas/herramientas/facilita-rgpd.

38. *Ayudaley* [En línea] [consulta: 20 de mayo de 2024.]. Disponible en: https://ayudaleyprotecciondatos.es/modelos-plantillas/.

39. *Delegados de protección de datos* [En línea] [consulta: 23 de mayo de 2024.]. Disponible en: https://delegadosdeprotecciondedatos.com/.

40. SESST SOCIEDAD ESPAÑOLA DE SALUD Y SEGURIDAD EN EL TRABAJO. *Modelo orientativo acuerdo trabajo a distancia* [En línea]. Marzo de 2024. [consulta: 20 de mayo de 2024]. Disponible en: https://sesst.org/wp-content/uploads/2020/10/acuerdo_trabajo_distancia_rdl28_20.pdf .

41. *Infoteknico* [En línea] [consulta: 10 de junio de 2024.]. Disponible en: https://www.infoteknico.com/que-es-un-ups-y-como-funciona/.

42. *Mundo Posgrado* [En línea] [consulta: 10 de junio de 2024.]. Disponible en: https://www.mundoposgrado.com/que-son-las-instalaciones-mep-arquitectura/.

43. *Novalight* [En línea] [consulta: 10 de junio de 2024.]. Disponible en: https://www.novalight.com/blog/Handholes-the-Whole-Story#:~:text=Handholes%20are%20underground%20vaults%20that%20provide%20access%20to,pull%20boxes%2C%20splice%20boxes%2C%20underground%20enclosures%20or%20vaults..

44. *Locksmith Ledger* [En línea] [consulta: 10 de junio de 2024.]. Disponible en: https://www.locksmithledger.com/home/article/10951359/delayed-egress-what-where-why-and-how.

45. *Ciberseguridad* [En línea] [consulta: 10 de junio de 2024.]. Disponible en: https://ciberseguridad.com/amenzas/tailgating-piggybacking/.

46. *Pyv technology* [En línea] [consulta: 10 de junio de 2024.]. Disponible en: https://pyv.technology/es/blog/anti-passback/.

47. *Ekomodo* [En línea] [consulta: 10 de febrero de 2024.]. Disponible en: https://www.ekomodo.eus/blog/empresas-por-un-mundo-mejor/que-son-los-ods-y-por-que-son-tan-importantes/.

48. *Microsoft* [En línea] [consulta: 10 de febrero de 2024.]. Disponible en: https://www.microsoft.com/es-mx/security/business/security-101/what-is-data-protection?msockid=2b193e361d2863e825362a4d1c0362a9.

Anexo

Anexo 1: Señales de videovigilancia

Como se menciona en el apartado de LOPDGDD, en el artículo 22, que habla sobre la videovigilancia, nos informa sobre la información que debe tener una señal que informe sobre videovigilancia. Podemos ver una plantilla que la agencia de protección de datos facilita:

Figura 57: Plantila señal videovigilancia. Fuente: (36)

En el transcurso de la realización de este trabajo me he fijado más en este tipo de señales y he fotografiado algunas.

En el lugar dónde he realizado unas prácticas extracurriculares he fotografiado uno de los carteles que están repartidos por las inmediaciones de las Cortes Valencianas. Al ser esta una institución pública la señal cumple a la perfección con la normativa.

Figura 58: Señal de videovigilancia de las Cortes Valencianas. Fuente: elaboración propia

También puede fotografiar una señal perteneciente a un negocio particular, en concreto una joyería.

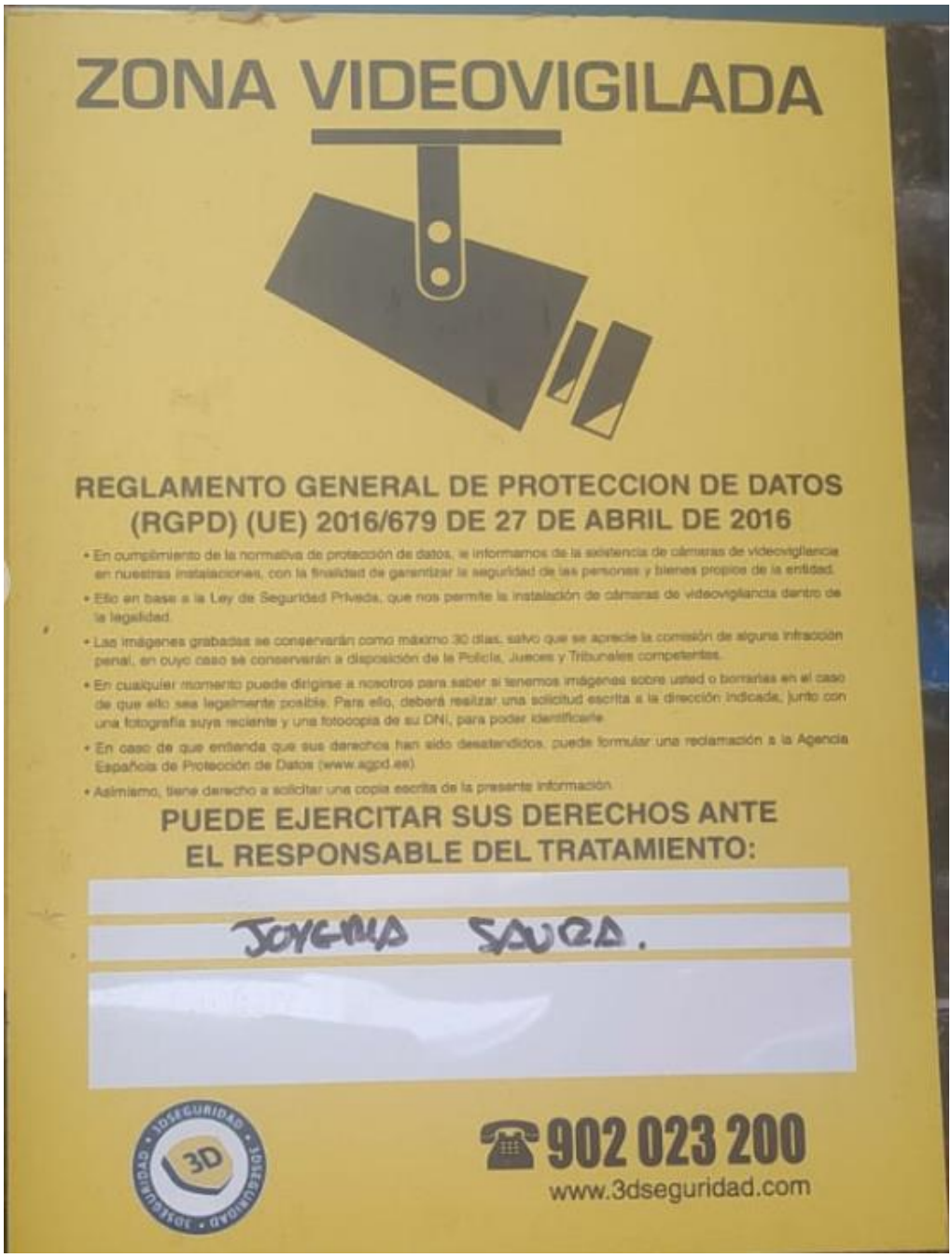


Figura 59: Señal de videovigilancia de una joyería. Fuente: elaboración propia

En esta señal se ha juntado el apartado del responsable y el apartado de ejercitar los derechos en uno solo. Lo que viene a decir es, que si quieres ejercer tus derechos de protección de datos debes entrar en el establecimiento. En la parte de arriba se informa del artículo 22 de la LOPDGDD, que habla sobre videovigilancia e indica como se puede solicitar el borrado de las grabaciones, por último, también informa de qué si su reclamación no es atendida se puede poner en contacto con la AEPD.

Anexo 2: Funcionamiento de las herramientas

¿Cómo funciona la herramienta facilita RPGD? Primero deberás seleccionar el sector de tu empresa, por ejemplo, sanidad, seguros, publicidad, entre otros. Nos encontraremos estas 3 pantallas:

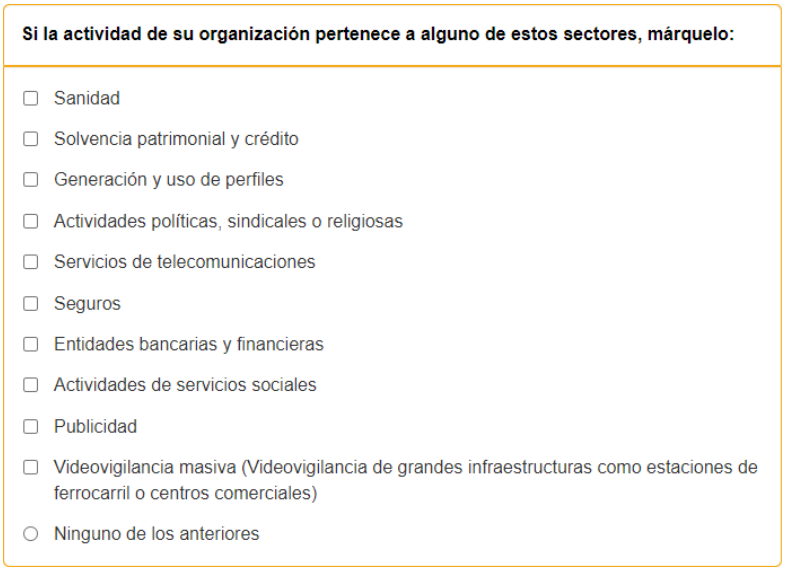


Figura 60: Pantalla 1 sectores. Fuente: (37)

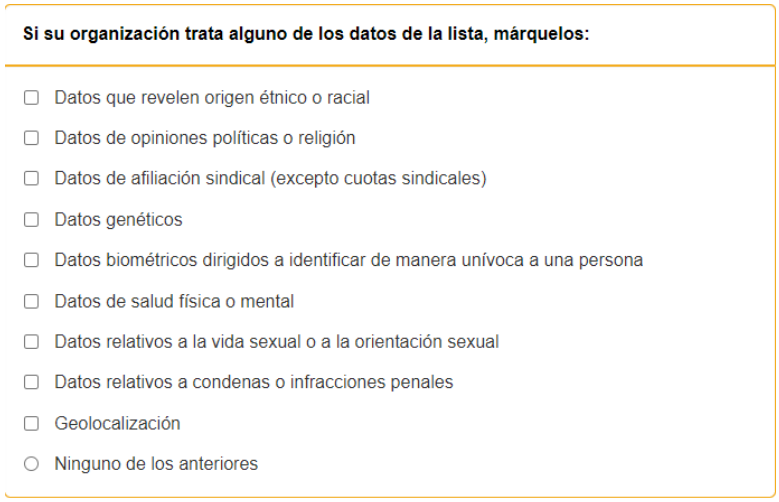


Figura 61: Pantalla 2 sectores. Fuente: (37)

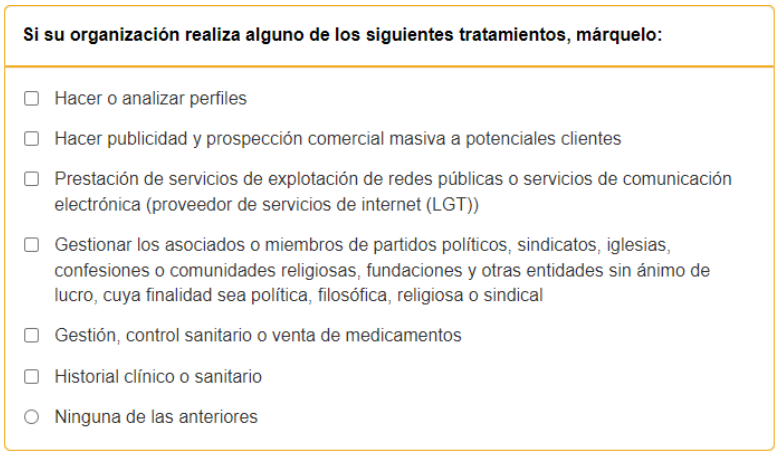


Figura 62: Pantalla 3 sector. Fuente: (37)

Si en las 3 pantallas hemos seleccionado la opción Ninguna de las anteriores significa que nuestra organización no trata datos sensibles y por lo tanto podemos utilizar esta herramienta sin problemas. A continuación, deberemos introducir los datos de la empresa como el nombre, dirección, correo electrónico etc.

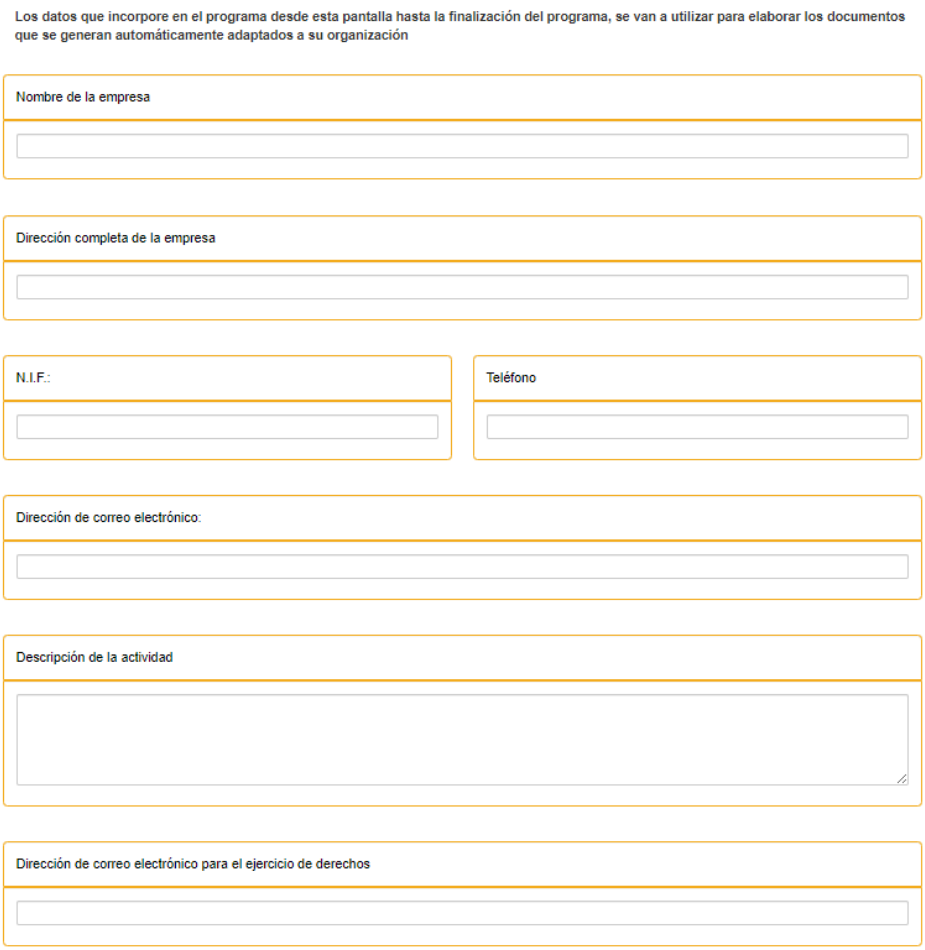


Figura 63: Formulario datos empresa. Fuente: (37)

En los siguientes formularios deberemos introducir información sobre nuestros clientes: el tipo de datos y para que se usan estos. También deberemos hacer esto con los datos de los empleados. Otros datos relevantes que se nos solicitarán son: los datos de la empresa que gestiona las nóminas, en caso de que esto lo haga una empresa externa, datos de los proveedores, indicar si tenemos cámaras de videovigilancia e indicar datos de otras empresas externas que nos presten sus servicios.

Una vez introducidos todos los datos la herramienta nos proporcionará un documento editable, formato Word, con instrucciones sobre cómo hacer el tratamiento de datos. Muy posiblemente este documento deba ser adaptado a las necesidades de la organización. Cabe decir que, los datos proporcionados sobre nuestra empresa serán eliminados al finalizar el proceso y la AEPD tendrá conocimiento de la información que hemos aportado.

RAT permite dar de alta las actividades del tratamiento, modificarlas, darlas de baja, consultarlas y permite exportar esta información a otros formatos como Word o Excel. Esta aplicación nos ofrece una serie de campos que deberemos rellenar, nos indica cuales son de carácter obligatorio y deben ser rellenados. Encontraremos una serie de pestañas con distintas informaciones, una para las bases jurídicas, otra relativa a las categorías de datos y las transferencias, entre otras. Cuando registremos una nueva actividad de tratamiento se nos abrirá esta ventana que contiene varias pestañas.

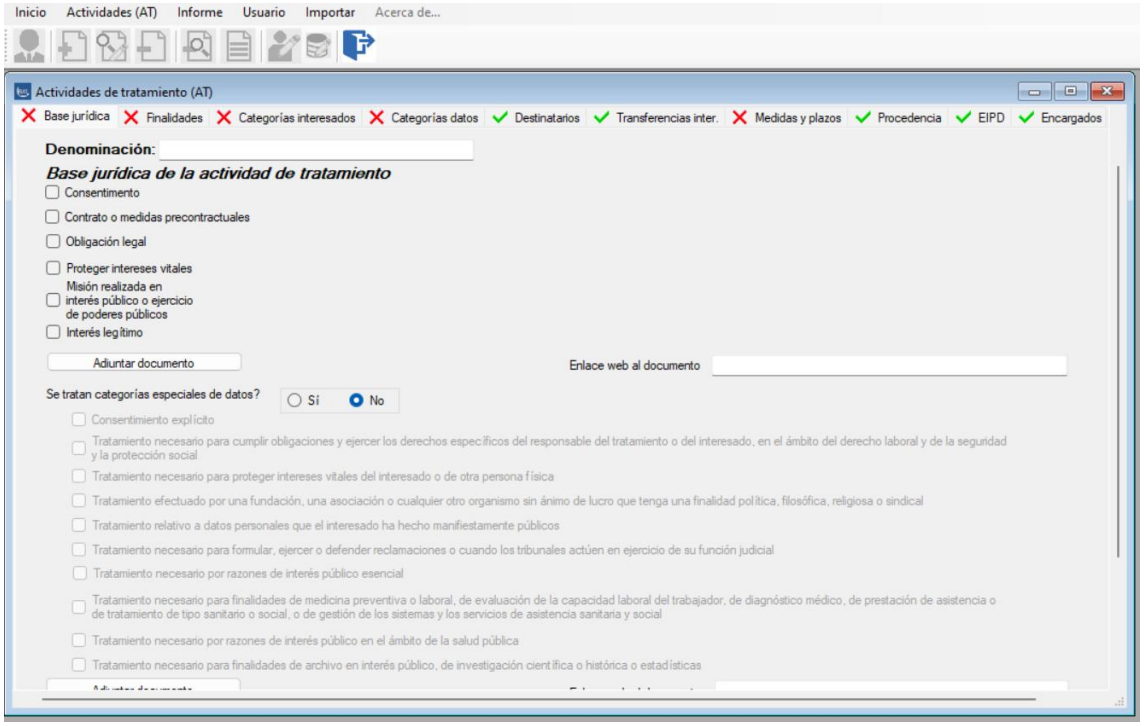


Figura 64: Registro actividades del tratamiento. Fuente: Herramienta RAT

Podemos también introducir los datos de aquellas figuras que participan en el tratamiento de datos.

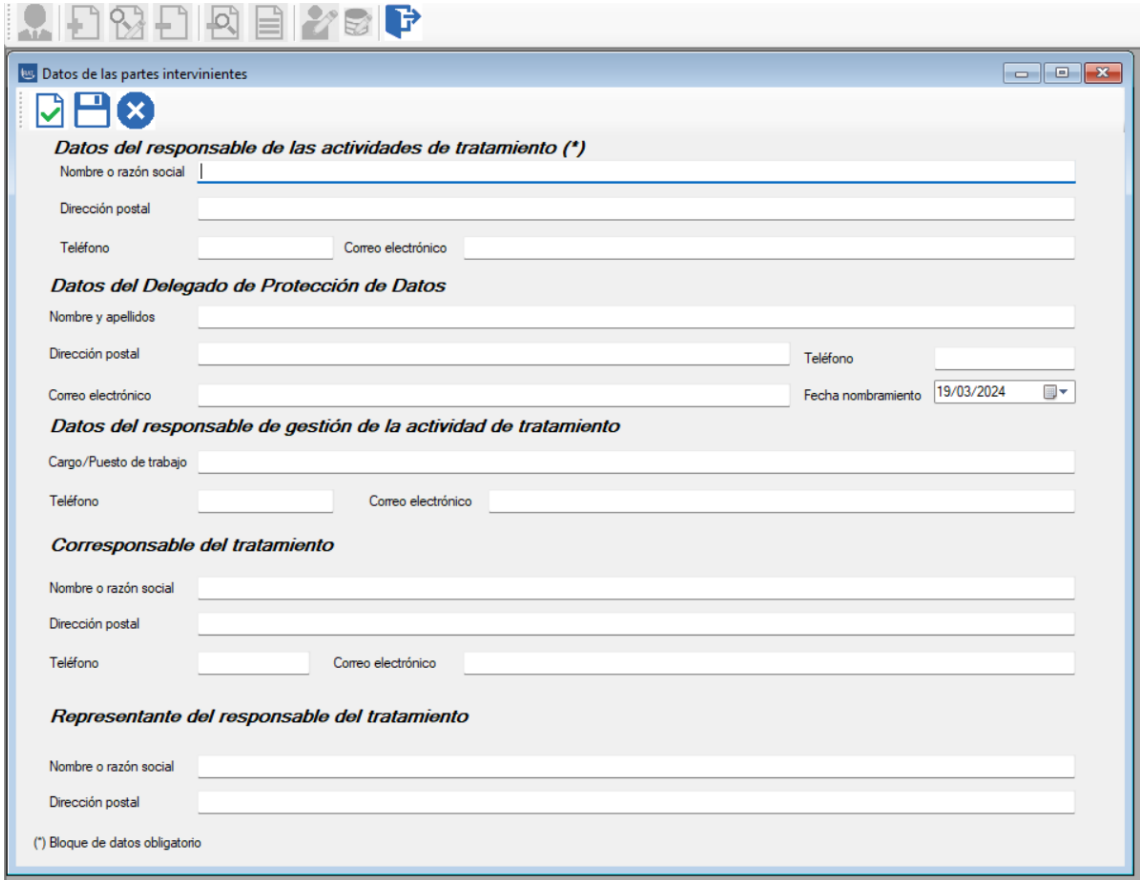


Figura 65: Registro de implicados en el tratamiento. Fuente: Herramienta RAT

Anexo 3: Ejemplo de funcionamiento de la guía

Ejemplo 1 – Auditoría general

Para mostrar el funcionamiento de la guía supondremos que somos una pyme que se dedica a la venta de muebles de madera llamada Pinosa, que tiene 100 trabajadores y 4 tiendas por toda España, además de sus oficinas centrales que están en Valencia. Esta empresa tiene los datos personales de sus empleados y quiere aumentar las medidas de seguridad de su centro de procesamiento de datos. Tiene también datos de sus clientes, los cuales usa para el envío de publicidad personalizada. Quieren curarse en salud y asegurarse de que sus bases de datos son seguras y no tendrán problemas legales.

En la primera página de la guía se encuentran con una breve explicación sobre las principales leyes de protección de datos y se recalcan las principales debilidades de las empresas en materia de protección de datos. Se incluyen enlaces a las leyes y a las guías y herramientas que ofrece la AEPD. Tras leer esta explicación le dan a continuar y pasan a la interfaz principal.

Una vez en la interfaz principal se pulsa sobre la primera actividad Establecer los objetivos y alcance de la auditoría.

Nombre de la organización:	Pinosa
	Detalles
Objetivo principal	Cumplir con la normativa de protección de datos
Objetivo secundario 1	Evitar sanciones económicas e indemnizaciones
Objetivo secundario 2	Evitar brechas de seguridad
Objetivo secundario 3	Proteger adecuadamente nuestras bases de datos
Objetivo secundario 4	
Objetivo secundario 5	
Objetivo secundario 6	
Objetivo secundario 5	
Alcance	Detalles
Bases de datos auditadas, SGBD, aplicaciones, servidor físico y virtual, etc.	Base de datos de clientes, base de datos de empleados, página web, centro de procesamiento de datos
Departamentos auditados	Toda la organización
Duración de la auditoría	3 meses
Datos del auditor(es)	Perico Navarro Pérez DNI:67684302Z
Limitaciones de la auditoría	El equipo auditor se compone de un único empleado externo que se ha contrado para esta labor
Expectativas de los interesados	Comprobar la segurirdad de la organización y el cumplimiento de la legislación

Figura 66: Objetivos y alcance de Pinosa. Fuente: elaboración propia

Una vez completadas las tablas se pasa a la siguiente actividad, Análisis de Riesgos y Evaluación de Impacto. En esta hoja podemos consultar las sanciones impuestas por la LOPDGDD y el RGPD por incumplir ciertos artículos y los agravantes de las sanciones. Se informa también que previo al tratamiento de datos se debe hacer un análisis de riesgo o una evaluación de impacto previas. Se facilitan varios enlaces para poder llevar a cabo la evaluación de impacto y el análisis de riesgos. Finalmente se informa de los riesgos específicos a los que están sometidas las bases de datos. Una vez informados se pasa al grueso de la guía.

La actividad Verificación del cumplimiento de los objetivos es un subproceso que se compone de las distintas comprobaciones que llevaremos a cabo.

Primero se informará sobre sobre la figura del delegado de protección de datos y en qué casos es necesario contratar uno.

Tipo de entidad	¿Es tu empresa una de estas entidades? Sí/No
Colegios profesionales y sus consejos	No
Centros docentes	No
Empresas de telecomunicaciones cuando traten datos de forma habitual y a gran escala	No
Prestadores de servicios de la sociedad de la información que elaboren perfiles de usuarios	No
Entidades financieras	No
Aseguradoras	No
Empresas de inversión	No
Distribuidores de energía eléctrica y gas	No
Entidades que evalúan la solvencia	No
Entidades dedicadas al envío de publicidad que creen perfiles o hagan un tratamiento basado en las preferencias de los interesados	Sí
Centros sanitarios	No
Entidades que emiten informes comerciales	No
Empresas privadas de seguridad	No
Federaciones deportivas cuando traten datos de menores	No
Operadores que se dediquen a actividades de juegos a través de internet	No

Figura 67: Necesidad DPD. Fuente: elaboración propia

Debido a los envíos de publicidad personalizados la empresa deberá contar con un delegado de protección de datos. En esta hoja contamos con un enlace a la sede electrónica dónde poder darlo de alta.

Lo siguiente es revisar directamente que se cumplen con las leyes. Se comenzaría por el primer bloque, el de los principios básicos del tratamiento.

Progreso:			
89%			
Totales:	9		
Completadas:	8		
ESTADO	TAREAS A COMPLETAR	ARTÍCULO(S) A LOS QUE SE REFIERE	ENLACES DE INTERÉS
✔	~~Los datos deben ser exactos y en caso de que no lo sean deben ser actualizados a la mayor brevedad posible.~~	Art. 4 LOPDGDD Art. 5 RGPD	
✔	~~Si el responsable del tratamiento ha adoptado las medidas pertinentes para que los datos inexactos se rectifiquen o supriman y estos datos se han obtenido del afectado, de un intermediario, provienen de otro responsable o de un registro público, no se le podrá imputar.~~		
✔	~~Los implicados en el tratamiento de datos deben garantizar su confidencialidad, de forma complementaria se debe mantener el secreto profesional.~~	Art. 5 LOPDGDD Art. 5 RGPD	
✔	~~La obligación de mantener el deber de confidencialidad aun cuando el responsable o el encargado ya no estén a cargo del tratamiento o este haya finalizado.~~		
✔	~~Se obtiene el consentimiento para el tratamiento de datos de forma clara y libre y el interesado sabe para qué se usaran sus datos exactamente.~~	Art. 6 LOPDGDD Art. 4 RGPD	
✔	~~En caso de que el tratamiento tenga distintos fines, se deben indicar todos ellos de forma clara.~~		
✔	~~No se podrá condicionar la ejecución de un contrato a que el interesado consienta el tratamiento de sus datos para otras finalidades.~~		
✔	~~Cuando el responsable del tratamiento reciba los datos personales esta obligado a facilitar cierta información: los datos personales del responsable o el delegado de protección de datos, los fines del tratamiento, la posibilidad de ejercer los derechos básicos (acceso, supresión, rectificación etc.), los destinatarios de los datos y sus categorías, información sobre las transferencias internacionales, el plazo de conservación de los datos, el derecho a reclamar ante la autoridad de control y si hay decisiones automatizadas en el tratamiento de sus datos.~~	Art. 11 LOPDGDD	Ejemplo modelo de un contrato de consentimiento para el tratamiento de datos: Modelo consentimiento.docx
	Si los datos personales no son obtenidos directamente del interesado, además de la información anterior se incluirá la fuente de la que proceden sus datos y las categorías de datos que se tratan.		

Figura 68: Tareas derechos básicos. Fuente: elaboración propia

En este caso se cumple con todo menos con el último punto, cosa que se deberá incluir en los resultados de la auditoría. Se verifica que se cumplan los derechos de los empleados, los de los clientes y se revisa qué hacer en caso de una brecha de seguridad. Puesto que la empresa solo opera en España no se llevará a cabo ninguna transferencia de datos. Finalmente se comprueba que se cumplen las tareas con respecto a la videovigilancia.

Progreso:		
100%		
Totales:	12	
Completadas:	12	
ESTADO	TAREAS A COMPLETAR	ENLACES DE INTERÉS
✔	~~Los sistemas de vigilancia tienen como fin preservar la seguridad.~~	
✔	~~Se captan las imágenes imprescindibles de la vía pública para llevar a cabo la tarea mencionada anteriormente.~~	
✔	~~No se captan imágenes del interior de viviendas privadas.~~	
✔	~~Las imágenes serán eliminadas en el plazo máximo de un mes desde su captación.~~	Pincha aquí
✔	~~Si las imágenes muestran algún delito se deberán conservar y facilitar a la autoridad en un plazo de 62 horas. En estos casos no se aplicará la obligación de bloqueo.~~	Pincha aquí
✔	~~Se deberá colocar una señal en un lugar visible que informe de la existencia del sistema de videovigilancia. Esta señal deberá indicar la identidad del responsable, un medio para contactar y una dirección web donde consultar sus derechos. Podemos encontrar una plantilla de la señal en la AEPD.~~	Señal Videovigilancia
✔	~~El responsable deberá estar atento a las peticiones que reciba para ejercer sus derechos y atenderlas.~~	
✔	~~Las empresas de seguridad privada que ofrezcan servicios de videovigilancia también están sujetas a estas leyes.~~	
✔	~~Las imágenes y sonidos obtenidos por las Fuerzas y Cuerpos de Seguridad, los órganos de centros penitenciarios y lo relacionado con el tráfico se regulará por esta ley cuando el tratamiento tenga fines de prevención, investigación, detección, enjuiciamientos penales y protección y prevención frente a amenazas a la salud pública. En el resto de casos estos datos se regiran por la 2016/600.~~	
✔	~~Los empleadores podrán tratar las imágenes para controlar los horarios de los trabajadores~~	
✔	~~Los dispositivos de vigilancia no pueden estar en lugares destinados al descanso de los trabajadores, vestuarios, aseos, comedores y similares.~~	
✔	~~La grabación de sonidos está sujeta a los mismos principios que la videovigilancia.~~	

Figura 69: Tareas videovigilancia. Fuente: elaboración propia

Se rellena la tabla con los datos de las grabaciones que se deben ir borrando.

Nombre archivo	Fecha de eliminación	Motivo de no eliminación
mesenerosemana12024.avi	2 de febrero de 2024	
mesenerosemana22024.avi	por determinar	posible indicio de delito

Figura 70: Tabla datos grabaciones. Fuente: elaboración propia

Como se quiere mejorar la protección del centro de procesamiento de datos se verificará si se cumple con los requisitos de la TIA 942.

Requisito	Sí/No
¿ El CCTV monitoriza el perimetro del edificio y el parking?	Sí
¿El CCTV monitoriza los generadores?	No
¿El CCTV monitoriza las puertas de acceso?	Sí
¿El CCTV monitoriza el acceso a las plantas con ordenadores?	Sí
¿El CCTV monitoriza el sistema de alimentación, los teléfonos y la instalación eléctica?	Sí
¿El CCTV graba de forma continua y graba todo el perimetro?	Sí
¿El CCTV graba las imágenes a 20 fps (frames/segundo) o más?	Sí
¿Se controla el acceso a los generadores mediante algún sistema de detección de intrus	No
¿Se controla el acceso a los sistemas de alimenación, teléfonos e instalación eléctrica mediante tarjeta?	Sí
¿Los compartimentos que tienen los cables de fibra óptica tienen control de acceso mediante tarjeta?	No
¿Las salidas de emergencia tienen sistema de retardo de apertura de puertas?	No
¿Las ventanas accesibles desde el exterior tienen detección de intrusos?	No
¿El centro de operaciones de seguridad tiene control de acceso mediante tarjeta?	No
¿El centro de operaciones de red tiene control de acceso mediante tarjeta?	No
¿Las puertas de entrada a las salas de ordenadores tiene control de acceso mediante tarjeta o biometría?	No
¿Las puertas de acceso al edificio requieren de tarjeta de acceso para entrar?	No
¿La puerta del vestíbulo tiene bloqueo para que entre una persona cada vez, hay algún sistema que evite el piggybacking o se debe acceder por biometría?	No

Figura 71: Requisitos TIA 942. Fuente: elaboración propia

Cómo se ve en la tabla anterior no hay control de acceso mediante biometría para acceder al CPD, lo siguiente será comprobar si podemos implementar este tipo de acceso y qué cosas debemos tener en cuenta para ello.

Consentimiento	Se levanta la prohibición del tratamiento si...
Sí	El interesado ha dado su consentimiento explícito para tratar este tipo de datos.
	El tratamiento es necesario para cumplir las obligaciones y ejercicio de los derechos del responsable o el interesado en el ámbito del Derecho laboral y la seguridad y la protección social.
	Es necesario para proteger los intereses del interesado si este no está capacitado física o jurídicamente para dar su consentimiento.
	Se tratan datos que el interesado ha hecho públicos.
	El tratamiento es necesario para fines judiciales.
	El tratamiento tiene razones de interés público.
	El tratamiento es necesario para medicina preventiva o laboral, evaluación de la capacidad laboral, diagnóstico médico, prestaciones sanitarias o gestión del sistema de asistencia sanitaria.
	El tratamiento es de interés para la salud pública.
	El tratamiento tiene fines de investigación científica, investigación histórica o fines estadísticos.
	El tratamiento lo realiza un organismo sin ánimo de lucro con finalidad política, religiosa o sindical, los datos que se tratan pertenecen a miembros o exmiembros de la organización o personas relacionadas y estos datos no se comuniquen fuera de la organización.

Figura 72: Motivos para tratamiento de datos de categoría especial. Fuente: elaboración propia

Según la tabla anterior se ha podido obtener el consentimiento para tratar los datos biométricos de los empleados para fines de control de acceso. Esto puede no bastar para tratar datos de categoría especial, se recomienda consultarlo en la web de la AEPD. Una la organización pueda implementar este tratamiento deberá revisar las condiciones para el control de acceso mediante biometría. También se encuentra a su disposición un modelo para obtener el consentimiento para tratar este tipo de datos.

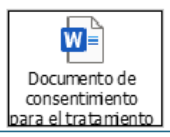
Tipo de uso	Detalles
Registro de jornada y control de acceso	Horario de inicio y finalización de jornada
	Los registros ser conservarán durante 4 años
	Los registros podrán ser consultados por trabajadores, sus representantes legales e inspectores de trabajo
	Evaluación previa de la tecnología que recoge los datos para que cumpla con el principio de minimización y recoja solo los datos necesarios
	El encargado debe justificar el uso de sistemas de control de presencia biométricos
	Se ofrecen otras alternativas a los empleados para cumplir con el registro de jornada y el control de acceso
	Modelo de consentimiento para el tratamiento de datos biométricos: 

Figura 73: Requirimientos control de acceso por biometría. Fuente: elaboración propia

Finalmente, puesto que tratan datos de categoría especial y se elaboran perfiles para el envío de publicidad personalizada se deberá rellenar el registro de actividades del tratamiento.

Datos de contacto del responsable del tratamiento	Apellidos:	Saéz Luján	Nombre:	Pepe	Dirección:	Calle Locomotora, P3	Dirección de correo:	
	Código postal:	46012	Ciudad:	Valencia	Número de teléfono:	695843855	pepesl@gmail.com	
Datos de contacto del representante	Apellidos:		Nombre:		Dirección:		Dirección de correo:	
	Código postal:		Ciudad:		Número de teléfono:			
Datos de contacto del delegado de protección de datos	Apellidos:	Villa Alcorcón	Nombre:	Juana	Organización (si el DPD es externo)	Asesoría Villar S.L.	Dirección:	Avenida Cortes Valencianas
	Código postal:	46017	Ciudad:	Valencia	Número de teléfono:	694354977	Dirección de correo:	juanavillar1997@gmail.com

Detalles del procesamiento				Finalidad(es) del tratamiento	¿Hay categorías especiales de datos?
Nombre de la actividad	Nº / REF	Fecha de creación del registro	Última actualización del registro		Sí/No
Publicidad personalizada	001	20/06/2024		Envío de publicidad personalizada a los clientes según sus compras anteriores	No
Biometría ctrl de acceso	002	18/06/2024		Control de acceso y registro de jornada	Sí

Figura 74: RAT. Fuente: elaboración propia

En la tabla anterior la empresa introduce los datos del DPD y el responsable. También se listan todas las actividades de tratamiento de datos que lleva a cabo la empresa. En este caso son la publicidad y el control de acceso mediante biometría.

Para cada actividad se deberán rellenar las siguientes tablas:

Fin(es) del tratamiento de datos	
Finalidad principal	Envío de publicidad personalizada en función de las compras anteriores
Finalidad secundaria 1	
Finalidad secundaria 2	
Finalidad secundaria 3	
Finalidad secundaria 4	
Finalidad secundaria 5	

Categorías de datos personales	Descripción	Periodo de conservación de los datos
Estado Civil, DNI, datos identificativos, imágenes...	DNI, nombre y apellidos	4 años
Vida personal como el estilo de vida o la situación familiar	Datos sobre la familia (hijos, casado o soltero etc.)	4 años
Información económica y financiera		
Datos de conexión como la IP		
Datos de localización	Lugar dónde está la vivienda familiar	4 años
Número de la seguridad social		

Figura 75: RAT. Fuente: elaboración propia

Categorías de interesados	Descripción	Detalles
Categoría 1	Clientes	
Categoría 2		
Destinatarios de los datos	**Tipo de destinatario**	**Detalles**
Destinatario 1	Departamento de marketing	
Destinatario 2		
Destinatario 3		
Destinatario 4		
Medidas técnicas y organizativas de seguridad	**Tipo de medida de seguridad**	**Detalles**
Medida de seguridad 1	Implementación de la TIA 942	Se implementan los principios de la TIA 942 para proteger los servidores que contiene los datos de los clientes
Medida de seguridad 2	Los datos esta cifrados	En el caso de que los datos fuesen robados no podrán ser descifrados
Medida de seguridad 3	Se controlan los accesos a la base de datos	Hay un historial de los accesos a la base datos, que incluye usuario y fecha

Figura 76: RAT. Fuente: elaboración propia

Para acabar en la última hoja deberá ser completada con las conclusiones y resultados de la auditoría.

Ejemplo 2 – Solicitud para ejercer el derecho de rectificación

La empresa Pinosa ha recibido una reclamación para ejercer su derecho de rectificación ya que, recientemente el Sr. Ejarque ha cambiado de domicilio y esto está ocasionando que sus pedidos se envíen a su domicilio anterior.

Puesto que una de las debilidades de las organizaciones es atender a los derechos de los interesados esta guía tiene un atajo que lleva directamente a la parte de la guía que explica cómo atender los derechos A.R.C.O.

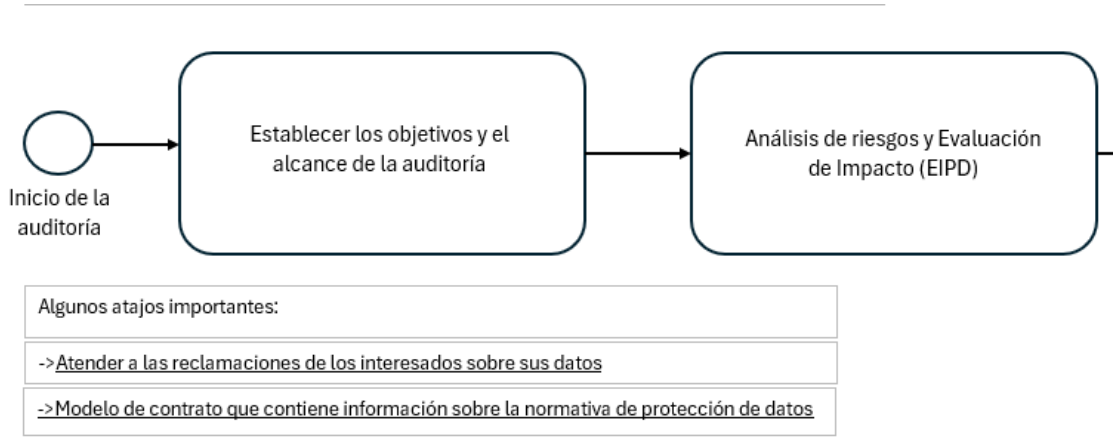


Figura 77: Atajo atender reclamaciones. Fuente: elaboración propia

Ya que en este caso los datos de los interesados no son correctos se deberán corregir a la mayor brevedad posible.

El interesado ha manifestado que ha cambiado de vivienda	El interesado tendrá derecho a la rectificación de sus datos personales cuando estos sean inexactos.	Derecho de rectificación Art. 16 RGPD Art. 14 LOPDGDD
	El interesado tendrá derecho a que se completen los datos personales que estén incompletos.	

Figura 78: Derecho de rectificación. Fuente: elaboración propia

Anexo 4: Modelos de contrato

Documento de consentimiento para el tratamiento de datos de categoría especial

De conformidad con lo dispuesto en el art. 9 del Reglamento (UE), de 27 de abril de 2016, o Reglamento General de Protección de datos (RGDP), en lo relativo al tratamiento de categorías especiales de datos, _____ con CIF nº: _____ y domicilio a efectos de notificaciones en: _____, le informa de que recabará el/los siguiente/s dato/s biométrico/s:

☐ Huella dactilar

☐ Análisis de retina

☐ Reconocimiento facial

para proceder a su tratamiento, en virtud de la relación de carácter laboral que vincula a ambas partes, y con la finalidad de:

☐ Llevar a cabo un control de presencia del empleado en el centro de trabajo.

☐ Realizar un control de identificación en los accesos al centro de trabajo.

Sus datos biométricos no serán transmitidos a terceros sin su consentimiento, salvo obligación legal, y serán conservados durante un período mínimo de cinco años, mientras usted no solicite su supresión.

Asimismo, se le informa de que le asisten los derechos de acceso, rectificación, supresión, oposición, limitación y portabilidad, pudiendo ejercitarlos mediante petición escrita a la dirección de _____, especificada en el primer párrafo.

En base a las consideraciones anteriormente descritas, _____ solicita su consentimiento expreso para el tratamiento de su huella dactilar, retina y/o reconocimiento facial, para la finalidad señalada previamente.

☐ Consiento EXPRESAMENTE el tratamiento de mi/s dato/s biométrico/s (huella dactilar y/o reconocimiento facial) por parte de _____, para la finalidad expresada en este documento.

Don / Doña: _____ DNI: _____

Figura 79: Modelo tratamiento de datos biométricos. Fuente: (38)

_____(1) es el **Responsable del tratamiento** de los datos personales del **Interesado/a** y le informa que estos datos serán tratados de conformidad con lo dispuesto en el Reglamento (UE) 2016/679 de 27 de abril (GDPR) y la Ley Orgánica 3/2018 de 5 de diciembre (LOPDGDD), por lo que se le facilita la siguiente información del tratamiento:

Fines del tratamiento:

Por consentimiento explícito del interesado: (2)

☐ _____

☐ _____(3)

Criterios de conservación de los datos: se conservarán durante no más tiempo del necesario para mantener el fin del tratamiento y cuando ya no sea necesario para tal fin, se suprimirán con medidas de seguridad adecuadas para garantizar la seudonimización de los datos o la destrucción total de los mismo o durante los años necesarios para cumplir con las obligaciones legales. (4)

Cesión de los datos: no se comunicarán los datos a terceros, salvo obligación legal o en los casos que sea imprescindible u obligación legal.

Derechos que asisten al Interesado:

- Derecho a retirar el consentimiento en cualquier momento.
- Derecho de acceso, rectificación, portabilidad y supresión de sus datos y a la limitación u oposición a su tratamiento.
- Derecho a presentar una reclamación ante la Autoridad de control (www.aepd.es) si considera que el tratamiento no se ajusta a la normativa vigente.
- Más información sobre sus derechos en: https://www. (5)

Datos de contacto para ejercer sus derechos:

_____(1) con direción en _____

_____de_____mail:_____

Para realizar el tratamiento de datos descrito, el Responsable del tratamiento necesita su consentimiento explícito o el de su representante legal. Con su firma, el Interesado/a consiente el tratamiento de sus datos en los términos expuestos.

En_____a,_____de_____de 20__

Nombre del interesado: _____

DNI:_____Edo: _____

Figura 80:Modelo consentimiento para el tratamiento de datos. Fuente: (39)

Este documento te servirá para recoger el consentimiento explícito de clientes, empleados, proveedores, candidatos, etc. a los que tomas sus datos personales para cualquier tratamiento que realices en tu actividad empresarial o profesional.

Deberás guardarlo por si en el futuro debes justificar el tratamiento realizado. En este documento deberás indicar claramente los fines del tratamiento que realizas:

- Relación comercial
- Relación laboral
- Envío de correspondencia comercial
- Etc.

En este documento se indicarán tantos fines como se vayan a tratar, es decir, un fin es la inclusión de los datos para emitir facturas como cliente y otro fin es el de mandarle correos electrónicos. Hay que indicar ambos fines y el cliente deberá aceptar el que quiera

La cesión de datos se da cuando, por ejemplo, envías la información a tu asesor fiscal.

Te recomiendo que tengas un protocolo por escrito para cuando un cliente te reclame los derechos que le asisten, de esta forma podrás contestarle de forma inmediata y respetando al máximo la normativa en protección de datos.

Según el RGPD, *"(32) El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal"* esta última (verbal) no es aconsejable.

Para rellenar el formulario:

(1) – nombre de la empresa que recoge los datos para tratarlos.
(2) – indicar para qué se van a utilizar los datos recogidos.
(3) – hay que indicar cada uno de los fines que se tratan.
(4) – tendrás que documentar cuanto tiempo mantendrás los datos en tu poder
(5) – puedes dirigir al interesado al apartado de "política de privacidad" de tu página web

Si tienes alguna duda puedes contactar con nosotros por teléfono, mail o a través de nuestra página web.

Figura 81: Modelo consentimiento para el tratamiento de datos 2ª parte. Fuente: (39)

MODELO ORIENTATIVO ACUERDO TRABAJO A DISTANCIA (teletrabajo)

RD-ley 28/2020, de 22 de septiembre

REUNIDOS

En _____, a _____ de _____ de _____

De una parte, D. _____, que interviene en nombre y representación de la empresa _____, en su calidad de _____.

De otra parte, D. _____, como persona trabajadora de la empresa _____.

Ambas partes reconociéndose capacidad legal suficiente para el otorgamiento del presente documento,

MANIFIESTAN

PRIMERO.- Que el objeto del presente documento es formalizar voluntariamente un acuerdo de trabajo a distancia en la modalidad de teletrabajo, de conformidad con lo establecido en el artículo 5.1 del Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia (BOE del 23-09-2020).

SEGUNDO.- El trabajo a distancia se llevará a cabo mediante el uso exclusivo o prevalente de medios y sistemas informáticos, telemáticos y de telecomunicación.

A tales efectos se establece el siguiente inventario de los medios, equipos y herramientas que exige el desarrollo del trabajo a distancia concertado, así como los consumibles y elementos muebles:

-

-

-

Figura 82:Modelo acuerdo teletrabajo. Fuente: (40)

La vida útil o periodo máximo para la renovación de estos se establece en un periodo temporal de:

-

La persona trabajadora deberá cumplir las condiciones e instrucciones de uso y conservación establecidas en la empresa en relación con los equipos o útiles informáticos, y tiene la obligación de cuidado de los equipos suministrados, y el uso adecuado y responsable del correo electrónico corporativo y no podrá recolectar o distribuir material ilegal a través de internet, ni darle ningún otro uso que no sea determinado por el contrato de trabajo.

La persona trabajadora se compromete a cuidar los elementos de trabajo, así como las herramientas que la empresa ponga a su disposición y a utilizarlas exclusivamente con los fines laborales que previamente se hayan fijado.

Finalizado la modalidad de trabajo a distancia en teletrabajo se deberá reintegrar los equipos informáticos que se le haya asignado.

TERCERO.- El lugar de trabajo a distancia elegido por la persona trabajadora para el desarrollo del trabajo a distancia esta ubicado en :

-

Cualquier cambio del lugar de trabajo deberá ser comunicado con carácter previo y con plazo temporal suficiente a la empresa, para poder dar cumplimiento a las obligaciones legales en materia de prevención de riesgos laborales.

A los efectos de la obligación empresarial de evaluación de riesgos y planificación preventiva, las visitas necesarias al domicilio del trabajador, requerirá, en cualquier caso, el permiso de la persona trabajadora, o de la persona titular del mismo.

La persona trabajadora debe cumplir las condiciones especiales sobre la prevención de riesgos laborales que se encuentren definidas en la evaluación de riesgos y en la planificación de la actividad preventiva.

CUARTO.- La duración de este acuerdo de modalidad de trabajo a distancia se establece en :

-

No obstante, la duración pactada, la empresa y la persona trabajadora podrán revertir el acuerdo de trabajo presencial a distancia en los siguientes supuestos:

-

-

Se establece un de plazo de preaviso de _____ para el ejercicio de las situaciones de reversibilidad.

Figura 83:Modelo acuerdo teletrabajo 2ª parte. Fuente: (40)

QUINTO.- El horario de trabajo de la persona trabajadora se desarrollará de:

-

Estableciéndose las siguientes reglas de disponibilidad: (optativo)

Se establece que el porcentaje y distribución entre trabajo presencial y trabajo a distancia, será el siguiente: (optativo) _____.

SEXTO.- Los gastos que pude tener la persona trabajadora por el hecho de prestar servicios a distancia, son los siguientes:

-

-

Estos gastos se cuantifican de la siguiente forma:

-

-

La compensación que abonará la empresa será por un importe:

-

El importe se abonará en los siguientes plazos temporales y forma siguientes:

-

SÉPTIMO.- La persona trabajadora queda adscrita al centro de trabajo de la empresa sito en _____, donde desarrollará la parte de la jornada de trabajo presencial en caso de existir la misma.

OCTAVO.- El procedimiento a seguir en el caso de producirse dificultades técnicas que impidan el normal desarrollo del trabajo a distancia, será el siguiente:

-

-

NOVENO.- Se establecen en materia de protección de datos y sobre seguridad de la información, las siguientes instrucciones:

Sólo los sistemas de comunicación aprobados por la empresa pueden ser usados para llevar a cabo sus actividades. Toda la información y equipos de la empresa deben mantenerse seguros en todo momento. Si la información se almacena

Figura 84:Modelo acuerdo teletrabajo 3ª parte. Fuente: (40)

temporalmente en su domicilio, debe estar bajo llave en lugar seguro o protegida adecuadamente por otros medios.

El acceso a los diferentes entornos y sistemas informáticos de la persona trabajadora será efectuado siempre y en todo momento bajo el control y la responsabilidad de la misma, siguiendo los procedimientos establecidos por la empresa que se hacen parte integral del presente acuerdo.

DÉCIMO.- La persona trabajadora se compromete a respetar la legislación en materia de protección de datos, las políticas de privacidad y de seguridad de la información que la empresa ha implementado, como también a:

- Utilizar los datos de carácter personal a los que tenga acceso único y exclusivamente para cumplir con sus obligaciones para con la empresa
- Cumplir con las medidas de seguridad que la empresa haya implementado para asegurar la confidencialidad, secreto e integridad de los datos de carácter personal a los que tenga acceso, así como no a no ceder en ningún caso a terceras personas los datos de carácter personal a los que tenga acceso, ni tan siquiera a efectos de su conservación.

UNDÉCIMO.- La empresa establece como medidas de vigilancia y control para verificar el cumplimiento por la persona trabajadora de sus obligaciones y deberes laborales, las siguientes:

-

-

DUODÉCIMO.- La persona trabajadora se compromete a guardar la máxima reserva y confidencialidad sobre las actividades laborales que desarrolle. Se considerará Información confidencial la información de propiedad de la empresa y la información que genere la persona trabajadora en virtud del contrato de trabajo. Comprometiéndose a no divulgar dicha Información confidencial, por ningún medio físico o electrónico, así como a no publicarla ni ponerla a disposición de terceros, a no ser que cuente con el consentimiento de la empresa

DECIMOTERCERO.- Se garantiza a la persona trabajadora el derecho a la desconexión digital fuera de su horario de trabajo en los términos establecidos en el artículo 88 de la Ley Orgánica 3/2018, de 5 de diciembre.

Figura 85:Modelo acuerdo teletrabajo 3ª parte. Fuente: (40)

Anexo 5: Conceptos TIA 942

UPS (41) son las siglas de Uninterrupted Power Supply, es español fuente de alimentación ininterrumpida. Se trata de un dispositivo que proporciona energía de forma inmediata cuando la fuente de alimentación principal falla.

MEP (42) son las siglas de Mechanical Electrical y Plumbing, una sala MEP es por tanto aquella en la que se encuentran los sistemas mecánicos, eléctricos y de fontanería de un edificio.

Fiber Vaults (43) son las estructuras que albergan los cables de fibra óptica y sus componentes.

Delay egress per code (44) es un sistema que retrasa la apertura de las salidas de emergencia para evitar problemas de seguridad.

Piggybacking (45) sucede cuando un empleado abre una puerta con sus credenciales y mantiene la puerta abierta para dejar pasar a un tercero. Para combatir esto tenemos el single person interlock, que solo permite pasar a una persona cada vez.

Pass back of access credential (46) es un problema de seguridad que se da cuando una persona deja su credencial a otra para que pueda acceder.

Anexo 6: Objetivos de Desarrollo Sostenible

Los ODS son una serie de objetivos fijados por las Naciones Unidas para poner fin a la pobreza, proteger el planeta, acabar con la discriminación, entre otros.

Grado de relación del trabajo con los Objetivos de Desarrollo Sostenible (ODS).

Objetivos de Desarrollo Sostenibles	**Alto**	**Medio**	**Bajo**	**No Proceede**
ODS 1. **Fin de la pobreza.**				**x**
ODS 2. **Hambre cero.**				**x**
ODS 3. **Salud y bienestar.**		**x**		
ODS 4. **Educación de calidad.**				**x**
ODS 5. **Igualdad de género.**	**x**			
ODS 6. **Agua limpia y saneamiento.**				**x**
ODS 7. **Energía asequible y no contaminante.**				**x**
ODS 8. **Trabajo decente y crecimiento económico.**	**x**			
ODS 9. **Industria, innovación e infraestructuras.**				**x**
ODS 10. **Reducción de las desigualdades**.	**x**			
ODS 11. **Ciudades y comunidades sostenibles**.				**x**
ODS 12. **Producción y consumo responsables.**				**x**
ODS 13. **Acción por el clima.**				**x**
ODS 14. **Vida submarina.**				**x**
ODS 15. **Vida de ecosistemas terrestres.**				**x**
ODS 16. **Paz, justicia e instituciones sólidas.**				**x**
ODS 17. **Alianzas para lograr objetivos.**				**x**

Pasaremos a analizar que ODS tienen relación con este trabajo:

3 - Salud y Bienestar. Uno de los puntos que trata esta guía es como tratar adecuadamente los datos referentes a la salud, los cuales son una categoría de datos especiales. Al aplicar los principios de minimización e idoneidad del tratamiento evitamos que estos datos sean tratados salvo que sean completamente necesarios y protegemos así a los empleados y su privacidad.

5 - Igualdad de Género. Al igual que con el ODS anterior el género de las personas en un tipo de datos especial y por lo tanto se debe tratar con sumo cuidado, cosa que se refleja en esta guía. Al tratar estos datos de forma cuidadosa estamos evitando que se produzca discriminación.

8 - Trabajo Decente y Crecimiento Económico. Al realizar un tratamiento de datos para llevar un registro de la jornada evitamos que las compañías obliguen a los empleados a realizar horas extra. Las administraciones públicas pueden usar los datos de registro de entrada y salida de los empleados para cerciorarse de que se trabajan las horas que corresponden. Esto contribuye a lograr empleos decentes para todos los trabajadores y evitar que sean explotados.

10 - Reducción de las desigualdades. Como hemos mencionado anteriormente uno de los temas que trata nuestra guía es la protección de categorías de datos especiales como pueden ser el género, la raza o la etnia. Al proteger este tipo de datos evitamos que pueda producir algún tipo de discriminación en el trabajo respecto a los salarios o al trato.

El resto de los ODS no tiene ninguna relación con este TFG puesto que no se trata ningún tema relacionado con el medio ambiente.