Universitat Oberta de Catalunya

uoc.edu

Adaptación de una pyme a la futura normativa RGPD (EU RGPD)

Marcos Tarazona Ros
Seguridad de las Tecnologías de la Información y de las Comunicaciones
Máster Universitario

Marco Antonio Lozano Merino

Junio 2018

© Marcos Tarazona Ros
Reservados todos los derechos. Está prohibido la reproducción total o parcial de esta obra por cualquier medio o procedimiento, comprendidos la impresión, la reprografía, el microfilme, el tratamiento informático o cualquier otro sistema, así como la distribución de ejemplares mediante alquiler y préstamo, sin la autorización escrita del autor o de los límites que autorice la Ley de Propiedad Intelectual.

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Adaptación de una pyme a la futura normativa RGPD (EU RGPD)*
Nombre del autor:	*Marcos Tarazona Ros*
Nombre del consultor/a:	*Marco Antonio Lozano Merino*
Fecha de entrega (mm/aaaa):	06/2018
Titulación::	*Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones*
Área del Trabajo Final:	*Aspectos legales de la seguridad informática*
Idioma del trabajo:	*Castellano*
Palabras clave	*-Adaptación pyme RGPD* *-Normativa RGPD* *-Reglamento EU Protección Datos*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados y conclusiones del trabajo.*

Este trabajo final de Master explica la necesidad de cumplir con la nueva normativa europea RGPD para garantizar la privacidad y seguridad a la hora de tratar los datos personales dentro de una organización. En este caso, se realizará la adaptación en una pyme ficticia a la que llamaremos “Automotive X” y cuyo negocio se centra en la producción de piezas de vehículos.

Para empezar con este proyecto, se realizará una descripción del negocio y sus procesos. Seguidamente se identificará el tratamiento de los datos personales que realiza la empresa, así como también el flujo que estos siguen y los activos que se ven implicados en su tratamiento.

Una vez conocida esta información, se realizará un análisis de riesgos para poder evaluar cuál sería el impacto en el negocio y de este modo poder establecer controles de seguridad para eliminar o mitigar estos riesgos.

De igual modo, para garantizar la mejora continua y asegurar que la organización conoce su estado de madurez en cuanto a aspectos de seguridad de la información, se realizará un GAP análisis de la ISO 27001:2013 y contemplaremos algunas recomendaciones de seguridad de esta.

Finalmente, se aplicarán las acciones pertinentes para lograr la adaptación de los procesos de negocio de modo que se garantice la protección de los datos personales y su tratamiento legítimo.

Abstract (in English, 250 words or less):

This final Master's work explains the need to comply with the new European GDPR regulations to guarantee privacy and security when dealing with personal data within an organization. In this case, the adaptation will be made in a fictitious SME to which we will call "Automotive X" and whose business is focused on the production of vehicle parts.

To begin with this project, a description of the business and their processes will be made. Then an identification of the personal data handled by the company will be done, as well as the flow they follow and the assets that are involved in their treatment.

Once this information is known, a risk analysis will be carried out in order to evaluate the impact on the business and in this way establish security controls to eliminate or mitigate these risks.

Similarly, to ensure continuous improvement and ensure that the organization knows their state of maturity in terms of information security aspects, a GAP analysis of ISO 27001:2013 will be carried out and some safety recommendations of this will be contemplated.

Finally, the pertinent actions will be applied to achieve the adaptation of business processes in order to guarantee the protection of personal data and their legitimate treatment.

Índice

Introducción 1
Contexto y justificación del Trabajo 1
Objetivos del Trabajo 1
Enfoque y método seguido 1
Planificación del Trabajo 2
Breve descripción de los otros capítulos de la memoria 3
1. Introducción a la normativa RGPD 4
1.1. ¿Cuál es su objetivo? 4
1.2. ¿Qué novedades trae con respecto a la LOPD? 4
1.3. ¿A qué tipo de sanciones se pueden enfrentar las empresas? 5
1.4. ¿Qué tipo de datos personales requieren mayor protección? 7
1.5. ¿Cuáles son los Actores y Roles que conforman el reglamento? 8
2. Descripción del negocio 10
2.1. Tratamiento de los datos personales 15
2.2. Identificación de activos relacionados con el tratamiento de los datos 18
3. Análisis de riesgos 19
3.1. Calculo del nivel de riesgo 22
3.2. Establecer un nivel de riesgo aceptable 23
4. DPIA – Evaluación de impacto RGPD 24
5. Certificaciones de utilidad: ISO 27001 26
5.1. Introducción a la ISO 27001 26
5.2. Documentos obligatorios del estándar ISO 27001 27
5.3. ISO 27001 con respecto al RGPD 30
6. Gap análisis ISO 27001:2013 31
6.1. ¿Qué es el Gap Análisis? 31
6.2. Modelo de Niveles de madurez 31
6.3. Plantilla de Controles ISO 27001:2013 33
7. Adecuación del negocio a la norma RGPD 34
7.1. Actividades de tratamiento de datos y cláusulas informativas 34
7.2. Asignación del DPO 38
7.3. Realización de Inventario de Activos y asignación de propietario. 39
7.4. Realización de Análisis de Riesgos. 39
7.5. Análisis de la EIPD para los tratamientos de la empresa. 41
7.6. Realización de políticas de seguridad. 45
7.7. Procedimiento de reporte de brecha de seguridad de datos 48
7.8. Medidas de seguridad tecnológicas 50
7.9. Medidas para la captación de imágenes con cámaras 51
7.10. Auditorías para justificar el cumplimiento del RGPD 52
8. Conclusiones 53
9. Glosario 54
10. Bibliografía 57
11. Anexos 59
11.1. Anexo 1 – Diccionario de Acrónimos 59
11.2. Anexo 2 – Plantilla GAP ISO 27001 60
11.3. Anexo 3 – Herramientas de Utilidad 64
11.4. Anexo 4 – Listado de Cumplimiento del RGPD 69

Lista de figuras

Ilustración 1 Sanciones Leves LOPD - RGPD 6
Ilustración 2 Sanciones Graves o Muy Graves LOPD - RGPD 6
Ilustración 3 Inventario de Activos 18
Ilustración 4 Parámetros para medir la Probabilidad 20
Ilustración 5 Parámetros para medir el Impacto 20
Ilustración 6 Tabla valores cualitativos 21
Ilustración 7 Parámetros para medir el Nivel de Riesgo 21
Ilustración 8 Calculo del nivel de riesgo 22
Ilustración 9 Nivel de riesgo Aceptable 23
Ilustración 10 Niveles de riesgo superiores al aceptable 23
Ilustración 11 Ciclo de vida DPIA 25
Ilustración 12 Incremento Certificaciones ISO 27001 26
Ilustración 13 Top 10 Países europeos con certificaciones ISO 27001 27
Ilustración 14 Modelo de niveles de madurez 31
Ilustración 15 Gráfico Resultados Análisis GAP 33
Ilustración 16 Controles ISO 27001:2013 40
Ilustración 17 Política de Seguridad - Historial de modificaciones 45
Ilustración 18 Fases Auditoria ISO 19011 52
Ilustración 19 Plantilla Controles ISO 27001:2013 63
Ilustración 20 GlobalSUITE Gestor Documental 65
Ilustración 21 GlobalSUITE Análisis de Riesgos 65
Ilustración 22 GlobalSUITE Comunicación de Eventos 65
Ilustración 23 One Trust Cuestionario DPIA 66
Ilustración 24 One Trust Configuración de Riesgos 67
Ilustración 25 One Trust Flujo de Datos 67
Ilustración 26 One Trust Mantenimiento de Aplicaciones 67
Ilustración 27 Pilar Inventario de Activos 68
Ilustración 28 Pilar Análisis de Riesgos 68
Ilustración 29 Guía para el cumplimiento del RGPD 73

Introducción

Contexto y justificación del Trabajo

En mayo de 2018 será obligatorio el cumplimiento del nuevo reglamento general para la protección de datos en la Unión Europea.

Las sanciones por el incumplimiento de esta normativa pueden alcanzar cifras de hasta 20 millones de euros o el 4% del volumen total de facturación de la empresa, lo que sea mayor. Por esta razón, todas las empresas que en sus procesos de negocio traten con datos personales, deberán adaptarse.

Nos encontramos ante una empresa del sector de la automoción que llamaremos “Automotive X”, que desconoce la normativa, cuáles son los pasos a seguir y las sanciones que pueden acarrear su incumplimiento.

En este trabajo contemplaremos los aspectos esenciales y analizaremos los procesos del negocio relacionados con el tratamiento de los datos personales y que afectan a la empresa Automotive X. Finalmente, realizaremos las acciones necesarias para garantizar la privacidad y seguridad en el tratamiento de estos datos en cumplimiento con la normativa RGPD.

Objetivos del Trabajo

El objetivo de este trabajo es contemplar todos los procesos del negocio y aspectos esenciales que requieren del cumplimiento de la nueva normativa RGPD en esta organización.

Una vez se hayan identificado, se realizarán las acciones necesarias para la adaptación de la empresa y que de esta forma se asegure la protección de los datos personales y su tratamiento legítimo, a efecto de garantizar la privacidad de las personas físicas.

Enfoque y método seguido

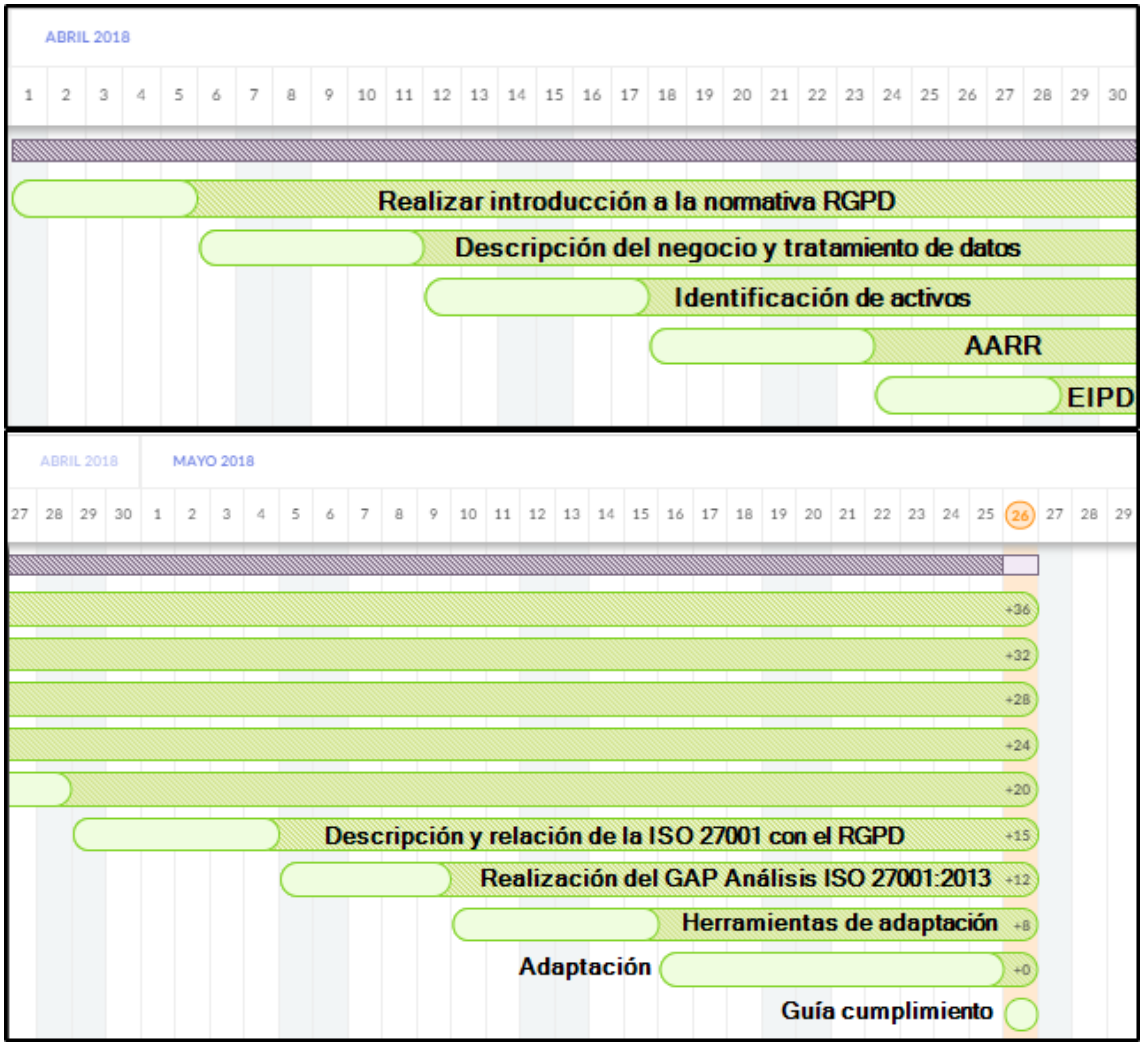
Para llevar a cabo este trabajo, es necesario conocer algunos aspectos básicos de la normativa RGPD. Por esta razón, nombraremos las principales novedades que trae y las sanciones que conlleva su incumplimiento.

El siguiente paso será conocer el negocio, es decir, identificaremos los procesos relacionados con el tratamiento de los datos personales, departamentos implicados, el flujo que realizan los datos, los activos que tratan con estos y designaremos a los actores encargados de adecuar a la compañía a la nueva normativa.

Llegados a este punto, podremos realizar el análisis de riesgos, GAP análisis, y en función de los resultados obtenidos, implantar controles de seguridad para tratar de mitigar o eliminar los riesgos y optimizar el nivel de seguridad que tiene la organización para la garantizar la seguridad y la protección del tratamiento de sus datos personales.

Planificación del Trabajo

Tareas	Fecha Inicio - Fin
Realizar introducción a la normativa RGPD	01/04/2018 a 05/04/2018
Descripción del negocio y tratamiento de datos personales	06/04/2018 a 11/04/2018
Identificación de activos relacionados con el tratamiento de datos	12/04/2018 a 17/04/2018
Realización del Análisis de Riesgos	18/04/2018 a 23/04/2018
Evaluación de necesidad de la EIPD	24/04/2018 a 28/04/2018
Descripción y relación de la ISO 27001 con el RGPD	29/04/2018 a 04/05/2018
Realización del GAP Análisis ISO 27001:2013	05/05/2018 a 09/05/2018
Descripción de herramientas útiles para la adaptación	10/05/2018 a 15/05/2018
Acciones para la adaptación del negocio a la norma RGPD	16/05/2018 a 25/05/2018
Rellenar Guía listado cumplimiento RGPD	26/05/2018



Breve descripción de los otros capítulos de la memoria

En el primer capítulo se explicará en que consiste la normativa RGPD para ponernos en contexto y conocer cuál es el objetivo del trabajo. Se nombrarán los requisitos que deben cumplir las organizaciones y se hablará de las sanciones que puede acarrear la empresa si no cumple con la norma.

En el segundo capítulo se hará una breve introducción del negocio e identificaremos los procesos relacionados con el tratamiento de los datos personales, departamentos implicados y los activos relacionados con su tratamiento de cara a la adecuación de la compañía a la nueva normativa.

En el tercer capítulo se realizará el análisis de riesgos a partir de los activos del negocio. Una vez hecho esto, posteriormente se indicarán los controles de seguridad para tratar de mitigar o eliminar los riesgos y de este modo tratar de optimizar el nivel de seguridad que tiene la organización para la protección de sus datos personales.

En el cuarto capítulo se hablará del DPIA análisis. Veremos en lo que consiste y lo aplicaremos a la pyme en concreto que vamos a adaptar.

En el quinto capítulo se hablará de la ISO 27001, puesto que es una certificación que resulta útil para la aplicación de algunas medidas de seguridad que se requieren para adaptar la organización a la nueva normativa RGPD.

En el sexto capítulo se hablará del GAP análisis utilizando la plantilla de la ISO 27001:2013, que permitirá evaluar los principales riesgos y necesidades en esta materia, sirviendo como hoja de ruta y plan de acción para futuras medidas a tomar, así como para el registro e inventario de las actividades de tratamiento.

Finalmente, puesto que ya hemos analizado y evaluado los riesgos, identificado el flujo de los datos y contemplado los procesos relacionados con el tratamiento de los datos personales de la organización, en este último capítulo se describirán las medidas realizadas para tratar de poner en marcha la adecuación de la compañía a la nueva normativa RGPD.

1. Introducción a la normativa RGPD

1.1. ¿Cuál es su objetivo?

El nuevo reglamento europeo de protección de datos entró en vigor el 25 de mayo de 2016 y será de obligatorio cumplimiento el 25 de mayo de 2018.

Existe actualmente un borrador de la normativa que reemplazará la actual ley LOPD en vigor desde el año 1995 y que se había quedado obsoleta debido al gran avance de las nuevas tecnologías y de la información. Esta normativa se alineará con el borrador.

Por otro lado, el nuevo reglamento tiene la misión de regular en toda la unión europea el tratamiento, recogida y procesamiento de datos personales para las empresas. De este modo, se reducen las cargas administrativas y se facilita la aplicación de esta por parte de las empresas pertenecientes a la unión europea.

Así mismo, el RGPD obliga a las empresas a reforzar los niveles de seguridad en la gestión de la información.

Otro aspecto importante que venía siendo necesario y se echaba en falta en la LOPD es una mayor protección de los datos personales de los ciudadanos. Por esta razón, otro de los objetivos es el de ampliar los derechos de los usuarios y aumentar las obligaciones de las organizaciones.

1.2. ¿Qué novedades trae con respecto a la LOPD?

Como todo nuevo reglamento, el RGPD trata de adaptarse a las necesidades que nos genera la nueva era digital e incluye una serie de requisitos para las empresas que ayudan a regular el tratamiento de datos personales y la libre circulación de estos en defensa de las personas físicas.

A continuación, se citan algunas de las principales novedades que trae:

- **Derechos de los ciudadanos**: Los ciudadanos se verán cubiertos por el derecho al olvido y por el derecho a la portabilidad de los datos de un usuario de un sistema de tratamiento electrónico a otro.

- **Creación de la figura del DPO**: El DPO o Delegado de Protección de Datos, a modo resumen, se encargará de supervisar el cumplimiento dispuesto en el Reglamento e informar y asesorar al responsable del tratamiento acerca de la evaluación de impacto relativa a la protección de datos.

- **Realización de Análisis de Riesgos y Evaluaciones de Impacto**: Las organizaciones deberán de realizar un análisis de riesgos y una posterior evaluación del impacto que supondría verse afectados por estos riesgos en lo relativo a la protección de sus datos personales.

- **Registro documental de las operaciones de tratamiento**: Tanto los responsables del tratamiento como los encargados, estarán obligados a realizar un registro documental de las operaciones realizadas para el tratamiento de los datos.

- **Nueva recomendación de información al interesado**: Para facilitar la comprensión de la información al ciudadano, se prevé implantar un sistema de iconos normalizado.

- **Incremento significativo en la cuantía de las sanciones**: Existen sanciones cuya cuantía se ha incrementado alcanzando multas de hasta 20 millones de euros.

- **Aplicación del concepto "Ventanilla Única"**: Este punto establece que las empresas multinacionales tendrán como interlocutor a una sola entidad de control nacional, la del establecimiento principal de la organización. Se aplicará el mismo concepto a los ciudadanos.

- **Establecimiento de obligaciones para nuevas categorías de datos**: Los datos genéticos y biométricos formarán parte ahora del grupo de datos de especial protección.

- **Nuevos principios en relación a las obligaciones de información**: Las empresas se verán obligadas a facilitar el entendimiento de sus avisos legales a los usuarios y sus políticas de privacidad serán más simples para ayudar a su comprensión.

1.3. ¿A qué tipo de sanciones se pueden enfrentar las empresas?

Tal y como se ha comentado antes, las sanciones por el incumplimiento de la normativa son mucho más rigurosas y la cuantía se ve enormemente incrementada. Las empresas tendrán 72 horas desde el momento de la detección del problema para notificar a la Agencia Española de Protección de datos.

Con la anterior ley de protección de datos LOPD, las sanciones leves podían ser desde los 900€ hasta los 40.000€. En cambio, con el nuevo reglamento RGPD, las sanciones leves alcanzan cifras de hasta 10.000.000€ o incluso el 2% del volumen de negocio anual global del ejercicio financiero anterior.

Algunos ejemplos de sanciones que vienen incluidas en esta categoría:

- No designación del DPO.
- No notificación de brechas de seguridad.
- No realización de la evaluación de impacto.
- No disposición del registro de actividades de tratamiento.
- No aplicación de medidas técnicas y organizativas por defecto.
- No consentimientos menores.

Ilustración 1 Sanciones Leves LOPD - RGPD

En cuanto a las sanciones graves y muy graves, la diferencia también viene siendo muy disparatada. Las sanciones de este tipo en la LOPD, oscilan entre los 40.001€ y los 600.000€. En cambio, para el nuevo RGPD, existen sanciones de hasta 20.000.000€ o el 4% del volumen de negocio anual global del ejercicio financiero anterior.

Algunos ejemplos de sanciones que vienen incluidas en esta categoría:

- No cumplir con los principios del RGPD.
- No cumplir con la resolución de la Autoridad de Control.
- No cumplir con requisitos de transferencia internacional de datos.
- No cumplir con los derechos de los interesados.

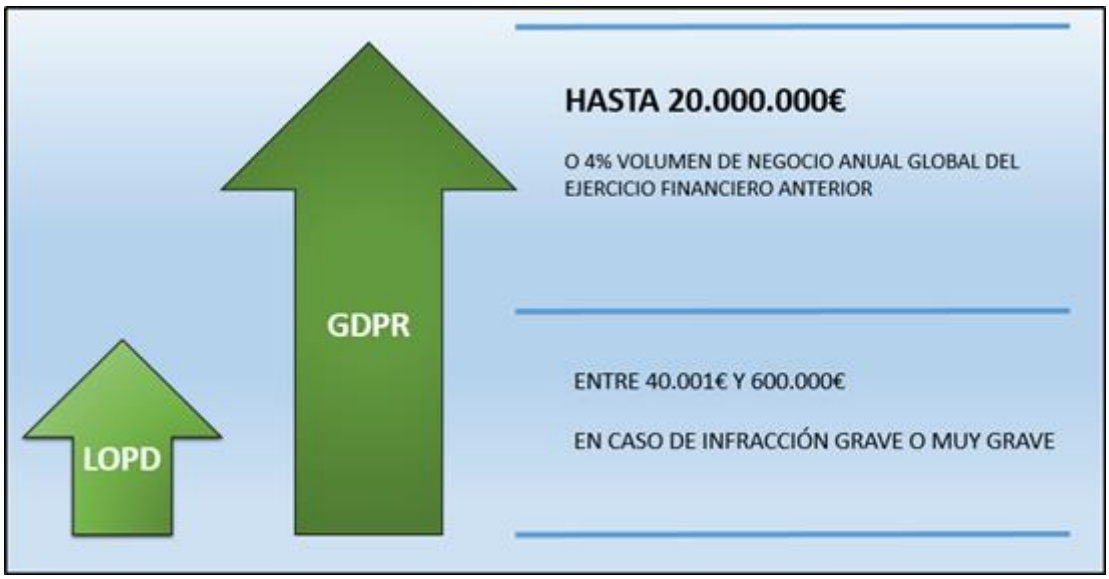


Ilustración 2 Sanciones Graves o Muy Graves LOPD - RGPD

1.4. ¿Qué tipo de datos personales requieren mayor protección?

En primer lugar, vamos a explicar lo que sería un dato personal según la ley.

Los datos personales hacen referencia a todo aquello que contiene información que identifique de forma directa o indirecta a una persona física a través de su nombre, apellido, número de teléfono, localización, etc.

Existen un tipo de datos personales que precisan de una especial protección y a los que llamaremos datos sensibles. Estos datos son todos aquellos que pueden revelar información de:

- Origen racial o étnico.
- Creencias religiosas o filosóficas.
- Opiniones políticas.
- Afiliación sindical.
- Datos genéticos.
- Datos biométricos que identifiquen a un individuo de forma exclusiva.
- Datos relativos a la salud o la vida sexual y/u orientación sexual.

El RGPD ha establecido la prohibición por defecto del tratamiento de estas categorías de datos, existiendo algunas excepciones que especificaremos a continuación.

- El interesado haya dado su consentimiento explícito para fines específicos (excepto si está prohibido por la legislación vigente).
- Es necesario para proteger los intereses vitales del interesado, cuando esté incapacitado para dar su consentimiento.
- El tratamiento lo realiza legítimamente una organización sin ánimo de lucro con finalidad política, filosófica, religiosa o sindical con relación a sus fines.
- El interesado ha hecho manifiestamente públicos sus datos.

O cuando el tratamiento esté fundamentado en la legislación vigente:

- Bajo la responsabilidad de personas sujetas a la obligación del secreto profesional.
- Para fines de asistencia sanitaria o social, medicina preventiva o laboral o diagnóstico médico incluida la evaluación de la capacidad laboral del trabajador.
- Para procedimientos judiciales.
- Es necesario para cumplir la legislación laboral, o la de seguridad o protección social o la de convenios colectivos.
- Es necesario por razones de interés público en el ámbito de la salud pública o la asistencia sanitaria.
- Es necesario para fines de archivo en interés público en investigaciones científicas, históricas o estadísticas.

1.5. ¿Cuáles son los Actores y Roles que conforman el reglamento?

Este nuevo reglamento incluye una serie de actores y roles cuyo conocimiento será necesario por parte de las organizaciones para poder realizar su desempeño y proceder con la adaptación a la normativa de manera correcta.

A continuación, se listan las principales figuras y roles que forman parte del reglamento y que según el tamaño de la organización y dependiendo de la categoría de los datos que trata, se contemplarán o no:

- **Data Protection Authority**: Se trata de la autoridad estatal de control independiente encargada de velar por el cumplimiento de la normativa sobre protección de datos.

  Su misión es garantizar el derecho a la protección de datos de carácter personal de los ciudadanos.

  En el territorio español, la encargada es la Agencia Española de Protección de Datos (AEPD).

- **Data Subject**: Se trata de cualquier ciudadano residente en la unión europea y cuyos datos personales trata de proteger y velar la nueva normativa.

- **Data Protection Officer (DPO)**: Esta figura es la encargada de informar y asesorar al responsable o al encargado del tratamiento.

  Tiene la función de supervisar el cumplimiento de lo dispuesto en el Reglamento y de supervisar las auditorías correspondientes.

  Además, tiene el papel de informar y ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos.

  Los casos en los que esta figura es absolutamente necesaria en una organización son:

  a) En organizaciones privadas que realicen tratamientos de categorías especiales de datos.
  b) En organizaciones privadas dedicadas a la elaboración de perfiles de personas físicas.
  c) En organizaciones privadas cuya actividad principal consista en el tratamiento de datos a gran escala.
  d) En todas las Administraciones Públicas sin importar su tamaño o naturaleza.

  El DPO podrá ser interno o externo, persona física o persona jurídica especializada en esta materia. Se le exigirán una serie de funciones reguladas en el artículo 39 del RGPD.

Artículo 39 Funciones del delegado de protección de datos

1. El delegado de protección de datos tendrá como mínimo las siguientes funciones:

a) Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;

d) Cooperar con la autoridad de control; e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

2. El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

- **Data Processor**: Se trata del encargado del tratamiento real de la información en el día a día de la organización que recibirá la orden del responsable del tratamiento.

  Esta figura ahora tendrá mayor importancia, ya que se le exigirán garantías técnicas y organizativas, compromiso de confidencialidad, especificación de medidas de seguridad. además de un contrato vinculante del cual quede constancia por escrito o electrónicamente.

- **Data Controller**: Se trata del responsable del tratamiento de la información que decidirá sobre los fines y medios del tratamiento.

  Sobre este recaerá la responsabilidad activa. Por lo tanto, deberá aplicar las medidas técnicas y organizativas apropiadas a fin de poder garantizar y demostrar que el tratamiento es conforme con el presente Reglamento.

2. Descripción del negocio

La empresa ficticia en la cual se va a realizar la adaptación la llamaremos “Automotive X”, puesto que supondremos que se trata de una PYME perteneciente al sector de la automoción y cuya tarea es fabricar piezas de vehículos para otra compañía.

A continuación, se expone el caso particular que vamos a considerar en este trabajo y que nos servirá para identificar posteriormente cuáles son los activos que guardan una relación con el tratamiento de los datos personales:

Empresa del sector automovilístico, formada por 100 empleados (cuyo comité ejecutivo lo conforman 7 personas), de los cuales 5 son técnicos y pertenecen al departamento de TI, otros 5 pertenecen a RRHH, otros 5 a Finanzas, otros 15 se dedican al mantenimiento de las instalaciones, otros 10 pertenecen al departamento de Calidad y el resto son operarios que trabajan en la línea de producción, ya sea como carretilleros o en la línea de montaje.

La empresa posee un pequeño centro de procesamiento de datos principal ubicado en las oficinas de la organización y otro CPD secundario que replica a este primario en otras oficinas cercanas. El CPD principal cuenta con 3 potentes servidores físicos, los cuales se utilizan para la virtualización de servidores (VMWare).

Para el entorno productivo existen 4 servidores Windows Server 2012 R2 virtualizados dedicados exclusivamente al Software de producción (2 servidores para el aplicativo y otros 2 para la BBDD). En este caso la base de datos forma un clúster SQL Server 2014 que almacena la trazabilidad de la producción.

También cuenta con 4 servidores Windows Server 2012 R2 más, dedicados al Software ERP de la planta (2 servidores para el aplicativo y otros 2 para la BBDD). La base de datos forma un clúster de SQL Server 2014 que almacena datos del cliente, proveedores y facturas del negocio.

Para el entorno de oficinas existen 2 servidores virtualizados Windows Server 2012 R2 que forman el Controlador de Dominio, para la autenticación de usuarios, que gestionan los archivos, copias de seguridad y las impresoras del negocio. La aplicación que gestiona las copias de seguridad está instalada en uno de ellos.

También cuentan con otro servidor virtualizado con Windows Server 2012 R2 que tiene instalada una aplicación de Recursos Humanos para llevar un control de la entrada y salida de los empleados y sus vacaciones. La Base de datos en este caso es un MySQL con información personal de los empleados.

Dentro del mismo CPD encontramos una librería de discos MSA para gestionar el almacenamiento de datos de los servidores, una unidad de cinta para las copias de seguridad y un Core switch que gestiona las comunicaciones entre los diversos dispositivos de redes ubicados por la planta.

Por otro lado, la organización tiene repartidos en puntos diversos *switches* y *Access points* para lograr una buena cobertura de las comunicaciones de los dispositivos. Además, tiene un *firewall* para proteger el acceso a la red interna.

En cuanto a las oficinas, todos los empleados que trabajan en ellas tienen un ordenador portátil con Windows 10 64bits y un Smartphone de empresa.

En el entorno de producción, los empleados trabajan con ordenadores táctiles que llevan Windows 10 y llevan instalado el cliente de la aplicación de producción.

En cuanto al hospedaje de la página web de la organización, se subcontrata a una empresa que ofrece servicios de hosting. Así mismo, el servicio de limpieza y de vigilancia también son subcontratados a otras empresas que ofrecen el correspondiente servicio.

Para el mantenimiento de los servidores y demás dispositivos críticos, también tiene subcontratado este servicio con su correspondiente SLA a otra compañía.

El servicio de las líneas de teléfono móvil y ADSL se contrata a una compañía de telefonía nacional.

A continuación, se listan los departamentos implicados en el funcionamiento del negocio y si se da el caso, la relación con el tratamiento de datos personales que realizan. Además, se incluyen las preguntas que nos tendremos que plantear a la hora de realizar la adecuación.

- **Mantenimiento:** Entre sus principales funciones, se encargan del mantenimiento de las máquinas y las instalaciones de la planta. Su objetivo es lograr la máxima disponibilidad del servicio y preservar la calidad del servicio evitando el deterioro prematuro de la infraestructura.

- **Logística y Operaciones:** Entre sus principales funciones, se encargan de la logística del negocio, petición de materiales, logística interna y externa de la empresa y fabricación del producto. Su objetivo es lograr la máxima disponibilidad del servicio, fabricar las piezas que solicita el cliente y garantizar la entrega del producto final a este.

- **Finanzas**: El departamento de finanzas se encargará de administrar los recursos financieros y presupuestarios del negocio, velando por su correcta utilización para el logro de los objetivos de la empresa.

  En este departamento nos haremos las siguientes preguntas:

  a) ¿Se han comprobado los procesos para garantizan que los identificadores digitales son seguros?

  b) ¿Se han analizado las multas que puede conllevar el incumplimiento del nuevo reglamento y se ha tenido en cuenta un plan de riesgo?

- **Recursos Humanos**: Entre sus principales funciones, se encargan de seleccionar, contratar, formar y emplear al personal de la organización.

  Por este motivo, este departamento es uno de los que más tratan con los datos personales de las personas físicas, ya que también reciben los currículums de personas ajenas a la empresa y tratan con los datos personales de los empleados para inscribirles en cursos, realizar las nóminas, etc.

  En este departamento nos haremos las siguientes preguntas:

  a) ¿Qué datos personales y sensibles se recogen?

  b) ¿Se almacena la información de futuros y actuales empleados?

  c) ¿Los trabajadores son conscientes de cómo son procesados sus datos personales y conocen lo que significa dar su consentimiento?

  d) ¿Las políticas, formularios y formaciones son acordes al RGPD?

- **Tecnologías de la Información**: Se trata del departamento encargado de administrar y gestionar los sistemas de la organización.

  Entre estas tareas se encargan de desarrollar, administrar y dar soporte a las redes, sistemas, equipos y servidores de la empresa.

  Los miembros de este departamento serán los custodios de la información y deberán velar por la protección de estos.

  En este departamento nos haremos las siguientes preguntas:

  a) ¿Los sistemas de información tienen que incluir una nueva categoría para el uso de datos personales?

  b) ¿Cuándo una persona física requiera encontrar un dato suyo seremos capaces de encontrarlo y a su vez borrarlo?

  c) ¿Los datos se encuentran debidamente protegidos?

  d) ¿En caso de haber una brecha de seguridad seremos capaces de identificarla y evaluar si ha tenido impacto en los datos personales almacenados?

- **Comité Ejecutivo**: El comité ejecutivo está formado por el gerente de la empresa, el manager de TI, Recursos Humanos, Finanzas, Logística y Operaciones, Mantenimiento y el supervisor de seguridad.

  Cada uno de ellos se encarga de gestionar y regular las tareas de su departamento para lograr el correcto funcionamiento del negocio.

Por otro lado, estarían los proveedores y el cliente.

- **Proveedores de materia prima:** Existe un contrato con un par de empresas que se encargan de suministrar la materia prima para la fabricación de las piezas de vehículos.

  En este caso nos haremos las siguientes preguntas:

  ¿Los contratos con las consecuentes empresas que prestan el servicio incluye las nuevas cláusulas contractuales en cumplimiento con el RGPD?

- **Proveedor de Servicios de Limpieza:** Existe una empresa contratada que se encarga de realizar la limpieza de las oficinas, comedores y servicios de la compañía.

  En este caso nos haremos las siguientes preguntas:

  ¿El contrato con la empresa que le presta el servicio incluye las nuevas cláusulas contractuales en cumplimiento con el RGPD?

- **Proveedor de Servicio de Mantenimiento Servidores y dispositivos:** Existe una empresa contratada que se encarga de realizar el mantenimiento de los servidores y demás dispositivos de comunicaciones tales como switches, Access points, etc...

  En caso de averías son los encargados de dar el soporte y reemplazar los dispositivos afectados dentro de los SLA definidos.

  En este caso nos haremos las siguientes preguntas:

  ¿El contrato con la empresa que le presta el servicio incluye las nuevas cláusulas contractuales en cumplimiento con el RGPD?

- **Proveedor de Servicio de Telefonía y ADSL:** Existe un contrato con una empresa de Telefonía que presta el servicio de líneas de teléfonos y ADSL para el negocio.

  En caso de averías con las líneas y dispositivos, son los encargados de dar el soporte y reemplazar o reparar los dispositivos afectados dentro de los SLA definidos.

  En este caso nos haremos las siguientes preguntas:

  ¿El contrato con la empresa que le presta el servicio incluye las nuevas cláusulas contractuales en cumplimiento con el RGPD?

- **Proveedor de Servicio Hosting:** Existe un contrato con una empresa que brinda el servicio de alojamiento de la web del negocio.

  En este caso nos haremos las siguientes preguntas:

  ¿El contrato con la empresa que le presta el servicio incluye las nuevas cláusulas contractuales en cumplimiento con el RGPD?

- **Proveedor de Servicios de vigilancia y seguridad:** Existe una empresa de seguridad que presta el servicio de vigilancia del negocio. De este modo se garantiza el acceso a las instalaciones de la empresa únicamente por parte de personal autorizado.

  En este caso nos haremos las siguientes preguntas:

  a) ¿El contrato con la empresa que le presta el servicio incluye las nuevas cláusulas contractuales en cumplimiento con el RGPD?

  b) ¿Los registros de entrada y salida de los empleados y visitas están debidamente guardados?

  c) ¿Los empleados son conocedores de la existencia de estos registros?

  d) ¿Existe alguna cámara de seguridad que no ha sido notificada su instalación?

- **Cliente fabricante de coches:** El cliente del negocio es una compañía que se encarga del montaje final del coche a partir de las piezas que nuestra empresa le suministra y vende.

  En este caso nos haremos las siguientes preguntas:

  ¿El cliente ha expresado de forma libre y explícita el consentimiento de que se traten sus datos personales?

2.1. Tratamiento de los datos personales

La empresa Automotive X realiza diferentes tratamientos de datos personales dependiendo del departamento y contexto. Según la normativa RGPD, si la empresa tiene más de 250 empleados o trata con datos sensibles, será necesario llevar un registro interno de estos tratamientos.

En este caso, puesto que se trata de una PYME que no supera los 250 empleados y además no trata con datos sensibles, no sería necesario hacer el registro del tratamiento de actividades. De todos modos, para documentarlo, a continuación, se muestran las actividades de tratamiento:

Tratamiento: Empleados

Finalidad del tratamiento: Gestión de la relación laboral con los empleados.

Descripción de las categorías de empleados y de las categorías de datos personales:

Empleados: Personas que trabajan para el responsable del tratamiento.

Categorías de datos personales: Los necesarios para el mantenimiento de la relación comercial. Gestionar la nómina, formación.

De identificación: nombre, apellidos, número de Seguridad Social, dirección postal, teléfonos, e-mail.

Características personales: estado civil, fecha y lugar de nacimiento, edad, sexo, nacionalidad y porcentaje de minusvalía.

Datos académicos.

Datos profesionales.

Datos bancarios, para la domiciliación del pago de las nóminas.

Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales: No se contempla.

Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos: Los previstos por la legislación fiscal y laboral respecto a la prescripción de responsabilidades.

Tratamiento: Clientes

Finalidad del tratamiento: Gestión de la relación profesional con los clientes.

Descripción de las categorías de clientes y de las categorías de datos personales:

Clientes: Personas que establecen una relación comercial con la empresa.

Categorías de datos personales: Los necesarios para que fluya una correcta relación comercial y laboral.

De identificación: nombre, apellidos, dirección postal, teléfonos, e-mail.

Datos bancarios, para la el pago y transferencias bancarias.

Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales: No se contempla.

Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos: Los previstos por la legislación fiscal y laboral respecto a la prescripción de responsabilidades.

Tratamiento: Proveedores

Finalidad del tratamiento: Gestión de la relación profesional con los proveedores.

Descripción de las categorías de proveedores y de las categorías de datos personales:

Proveedores: Personas que establecen una relación comercial con la empresa.

Categorías de datos personales: Los necesarios para que fluya una correcta relación comercial y laboral.

De identificación: nombre, apellidos, dirección postal, teléfonos, e-mail.

Datos bancarios, para la el pago y transferencias bancarias.

Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales: No se contempla.

Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos: Los previstos por la legislación fiscal y laboral respecto a la prescripción de responsabilidades.

Tratamiento: Candidatos

Finalidad del tratamiento: Gestión de la relación con los candidatos a un empleo en la empresa.

Descripción de las categorías de candidatos y de las categorías de datos personales:

Candidatos: Personas que desean trabajar para el responsable del tratamiento.

Categorías de datos personales: Los necesarios para gestionar los currículums de posibles futuros empleados

De identificación: nombre, apellidos, dirección postal, teléfonos, e-mail

Características personales: estado civil, fecha y lugar de nacimiento, edad, sexo, nacionalidad y otros excluyendo datos de raza, salud o afiliación sindical.

Datos académicos

Datos profesionales

Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales: No se contempla

Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos: Un año desde la presentación de la candidatura

Tratamiento: Vigilancia

Puesto que en este caso el servicio de vigilancia está “tercerizado”, será la propia empresa que presta ese servicio la que se encargue de realizar el tratamiento de los datos. Que en este caso sería el siguiente:

Finalidad del tratamiento: Seguridad de las personas y bienes.

Descripción de las categorías de interesados y de las categorías de datos personales:

Interesados: Personas que accedan o intenten acceder a las instalaciones.

Categorías de datos personales: De identificación: nombre, apellidos, DNI.

Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales: No se contempla.

Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos: Un mes desde su registro.

2.2. Identificación de activos relacionados con el tratamiento de los datos

Identificar los activos del negocio relacionados con el tratamiento de los datos personales es una tarea que nos ayudará a controlar cuales son los que tendremos que proteger y empezar a regular para el cumplimiento del RGPD.

Según la descripción del caso particular, a continuación, se listan los activos:

Activos	Tipo	Propietario	Ubicación Física	Crítico
CPD Principal	Infraestructura	Manager IT	Oficina	Sí
CPD Secundario	Infraestructura	Manager IT	Oficina externa	No
Servidores físicos VMWare	Hardware	Manager IT	CPD Principal	Sí
Máquinas Virtuales Windows Server 2012 R2	Software	Manager IT	CPD Principal	Sí
Software del ERP	Software	Manager IT	Servidores	Sí
BBDD del ERP	Datos	Manager IT	Servidores	Sí
Software de Producción	Software	Manager IT	Servidores	Sí
BBDD Software de Producción	Datos	Manager IT	Servidores	Sí
Software de RRHH	Software	Manager IT	Servidores	Sí
BBDD Software de RRHH	Datos	Manager IT	Servidores	Sí
Core Switch	Hardware	Manager IT	CPD Principal	Sí
Firewall	Hardware	Manager IT	CPD Principal	Sí
Switches	Hardware	Manager IT	Línea de Producción	No
Puntos de Acceso Wifi	Hardware	Manager IT	Línea de Producción	No
Unidad de cintas LTO	Hardware	Manager IT	CPD Principal	No
Librería de discos MSA	Hardware	Manager IT	CPD Principal	No
Portátiles Oficinas	Hardware	Manager IT	Oficina	No
Ordenadores Producción	Hardware	Manager IT	Línea de Producción	Sí
Smartphone	Hardware	Manager IT	Oficina	No
Sistemas Operativos Windows 10	Software	Manager IT	Portátil	Sí
Sistemas Operativos Windows Server 2012 R2	Software	Manager IT	Servidores	Sí
Medios de almacenamiento externo	Hardware	Manager IT	Empresa externa	No
Página web	Servicio	Manager IT	Empresa externa	No
Correo electrónico	Servicio	Manager IT	Empresa externa	No
Servicio de vigilancia	Servicio	Manager Seguridad	Oficina	No
Servicio de telefonía y ADSL	Servicio	Manager IT	Oficina	No
Servicio Mantenimiento Servidores e Infraestructura	Servicio	Manager IT	Empresa externa	Sí
Servicio de Hosting	Servicio	Manager IT	Empresa externa	No
Licencias SQL Server 2014	Software	Manager IT	Servidores	Sí
Licencias Windows 10	Software	Manager IT	Portátil	Sí

Ilustración 3 Inventario de Activos

3. Análisis de riesgos

El análisis de riesgos nos va a permitir conocer los riesgos a los que está expuesta la organización. Además, nos permite calcular la probabilidad que hay para que se produzca un incidente de seguridad para cada uno de los riesgos encontrados.

Teniendo en cuenta esto, seremos capaces de conocer lo que podemos perder en caso de ocurrir cada uno de estos riesgos y por lo tanto priorizaremos las medidas de seguridad y controles en algunos casos antes que en otros.

A continuación, se describirán de forma sencilla las principales tareas del análisis de riesgos, incluyendo algunas recomendaciones de cómo llevarlo a cabo. En nuestro caso particular, se han seleccionado un conjunto de fases que incluye el Instituto Nacional de Ciberseguridad en su método.

Fase 1 Definición del alcance

Antes de llevar a cabo el análisis de riesgos, debemos de establecer el alcance del estudio. Por ejemplo, podemos determinar que el análisis de riesgos abarque la totalidad del negocio dónde se han seleccionado las áreas donde mejorar la seguridad. También podemos definir un alcance reducido sobre los procesos que nos interesen. En nuestro caso particular, podremos enfocar los riesgos a los servicios y sistemas relacionados con el tratamiento de datos personales dentro de la organización.

Fase 2 Identificación de los activos

Una vez definido el alcance, debemos de identificar todos los activos que estén implicados en el tratamiento de los datos personales de la organización. Podemos mantener un inventario de activos sencillo tal y como se ha realizado en el capítulo 2.2 de la memoria.

Fase 3 Identificar las amenazas

Habiendo identificado los principales activos, el siguiente paso es identificar cuáles son las amenazas a las que estos están expuestos. Teniendo en cuenta que el conjunto de las amenazas puede ser amplio y diverso, si nuestra intención es evaluar el impacto en los datos personales que trata la organización, nos centraremos únicamente en plantearnos este tipo de riesgos.

Fase 4 Identificar vulnerabilidades y salvaguardas

Esta fase consiste en estudiar las características de nuestros activos para identificar cuáles son sus puntos débiles o vulnerabilidades. Por ejemplo, en nuestro caso particular un equipo sin los puertos USB bloqueados puede ser vulnerable a un robo de los datos.

Por otro lado, habrá que analizar y documentar las medidas de seguridad ya implantadas en la organización para tenerlas en cuenta a la hora de estimar el impacto y la probabilidad.

Fase 5 Evaluar el riesgo

Antes de poder evaluar el riesgo, debemos definir los parámetros o criterios que se van a utilizar para medir la probabilidad y el impacto.

En nuestro caso particular lo vamos a definir del siguiente modo:

Tabla para estimar la Probabilidad	
Valor	**Descripción**
Rara (0)	La probabilidad de que una amenaza se materialice es nula.
Improbable (0,25)	La probabilidad de que una amenaza se materialice es baja.
Moderada (0,5)	La probabilidad de que una amenaza se materialice es probable.
Probable (0,75)	La probabilidad de que una amenaza se materialice es bastante probable.
Muy Probable (1)	La probabilidad de que una amenaza se materialice es muy probable.

Ilustración 4 Parámetros para medir la Probabilidad

Tabla para estimar el Impacto	
Valor	**Descripción**
Insignificante (1)	El daño derivado de la materialización de la amenaza no tiene consecuencias para la organización.
Bajo (2)	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio (3)	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Grande (4)	El daño derivado de la materialización de la amenaza tiene consecuencias graves para la organización.
Catastrófica (5)	El daño derivado de la materialización de la amenaza tiene consecuencias muy graves para la organización.

Ilustración 5 Parámetros para medir el Impacto

Cuando vayamos a estimar la probabilidad y el impacto debemos de tener en cuenta las vulnerabilidades y salvaguardas existentes. *Por ejemplo,* la caída del servidor principal podría tener un impacto alto para el negocio. Sin embargo, si existe una solución de alta disponibilidad (*Ej*. Clúster de servidores), podemos considerar que el impacto será medio ya que estas medidas de seguridad reducirán el impacto.

Si por el contrario hemos identificado vulnerabilidades asociadas al activo, aplicaremos una penalización a la hora de estimar el impacto. *Por ejemplo*, si los equipos no están actualizados, incrementaremos el impacto de amenazas como posibles ataques de virus.

A la hora de calcular el riesgo, podremos utilizar tanto criterios cuantitativos como cualitativos. A continuación, se mostrarán ambos ejemplos.

Criterios cuantitativos: calcularemos el nivel de riesgo multiplicando los factores probabilidad e impacto.

Criterios cualitativos: haremos uso de la matriz de riesgo.

	IMPACTO					
PROBABILIDAD		Insignificante	Bajo	Medio	Grande	Catastrófico
	Rara	Bajo	Bajo	Moderado	Moderado	Moderado
	Improbable	Bajo	Bajo	Moderado	Moderado	Alto
	Moderada	Bajo	Moderado	Moderado	Alto	Alto
	Probable	Moderado	Moderado	Alto	Alto	Extremo
	Muy Probable	Moderado	Moderado	Alto	Extremo	Extremo

Ilustración 6 Tabla valores cualitativos

Tabla para estimar el Nivel de riesgo	
Valor	**Descripción**
Bajo (<= 1,25)	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio (1,25 > y <= 2,5)	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto (2,5 > y <= 3,75)	El daño derivado de la materialización de la amenaza tiene consecuencias graves para la organización.
Extremo (3,75 > y <= 5)	El daño derivado de la materialización de la amenaza tiene consecuencias catastróficas para la organización.

Ilustración 7 Parámetros para medir el Nivel de Riesgo

Fase 6 Tratar el riesgo

Una vez calculado el riesgo, debemos de tratar aquellos que superen el límite que hayamos definido. Por ejemplo, trataremos aquellos que sean superiores al nivel Moderado, puesto que hemos hecho un análisis en términos cualitativos.

A la hora de tratar el riesgo existen cuatro estrategias principales:

- Transferir el riesgo a un tercero.
- Eliminar el riesgo.
- Asumir el riesgo, siempre justificadamente.
- Implantar medidas para mitigarlo.

3.1. Calculo del nivel de riesgo

A continuación, se aplica la asignación de los parámetros a cada una de las siguientes amenazas que afectan a todos y cada uno de los activos.

De este modo, utilizando el análisis cualitativo obtenemos el nivel de riesgo.

Activos	Amenaza	Probabilidad	Impacto	Riesgo
CPD Principal	Incendio	Improbable	Grande	Moderado
CPD Secundario	Daños por agua	Improbable	Bajo	Bajo
Servidores físicos VMWare	Ataque aprovechando firmware desactualizado	Probable	Medio	Alto
Máquinas Virtuales Windows Server 2012 R2	Corrupción de la información	Probable	Grande	Alto
Software del ERP	Destrucción de información	Improbable	Medio	Moderado
BBDD del ERP	Alteración de información	Improbable	Medio	Moderado
Software de Producción	Caída del sistema por sobrecarga	Probable	Grande	Alto
BBDD Software de Producción	Fallo debido a errores de mantenimiento	Moderada	Medio	Moderado
Software de RRHH	Denegación de servicio	Probable	Bajo	Moderado
BBDD Software de RRHH	Interceptación de información (escucha)	Moderada	Medio	Moderado
Core Switch	Condiciones inadecuadas de temperatura o humedad	Moderada	Catastrófica	Alto
Firewall	Ataque aprovechando errores de configuración	Moderada	Grande	Alto
Switches	Ataque aprovechando vulnerabilidad de seguridad.	Moderada	Grande	Alto
Puntos de Acceso Wifi	Interceptación de información	Improbable	Grande	Moderado
Unidad de cintas LTO	Degradación de soportes de almacenamiento	Moderada	Medio	Moderado
Librería de discos MSA	Avería del dispositivo por falta de mantenimiento	Probable	Grande	Alto
Portátiles Oficinas	Robo	Probable	Grande	Alto
Ordenadores Producción	Errores de los usuarios por falta de formación	Probable	Bajo	Moderado
Smartphone	Acceso no autorizado por descuido	Moderada	Medio	Moderado
Sistemas Operativos Windows 10	Ataque por antivirus sin actualizar	Moderada	Medio	Moderado
Sistemas Operativos Windows Server 2012 R2	Ataque perpetrado por estar desactualizado	Probable	Grande	Alto
Medios de almacenamiento externo	Robo	Probable	Grande	Alto
Página web	Interrupción de los servicios	Moderada	Bajo	Moderado
Correo electrónico	Introducción de falsa información	Muy Probable	Medio	Alto
Servicio de vigilancia	Abuso de privilegios de acceso	Moderada	Bajo	Moderado
Servicio de telefonía y ADSL	Interrupción de los servicios	Improbable	Medio	Moderado
Servicio Mantenimiento Servidores e Infraestructura	Indisponibilidad del personal	Improbable	Medio	Moderado
Servicio de Hosting	Desastres naturales	Improbable	Bajo	Bajo
Licencias SQL Server 2014	Difusión de software dañino	Improbable	Medio	Moderado
Licencias Windows 10	Licencias caducadas	Moderada	Medio	Moderado

Ilustración 8 Calculo del nivel de riesgo

3.2. Establecer un nivel de riesgo aceptable

Una vez conocidos y clasificados los niveles de riesgo para cada amenaza, podemos establecer un límite para el nivel de riesgo que nos permita tomar las decisiones a la hora de implantar controles.

En este caso, el nivel de riesgo aceptable es el que asume la organización sin tomar acciones contra él, siempre y cuando el riesgo medio no afecte a un proceso crítico. Por ejemplo, en nuestro caso asumiremos el nivel aceptable a partir del nivel de riesgo Medio, y todo aquel que lo supere será tratado mediante controles que ayuden a reducirlo hasta un nivel aceptable.

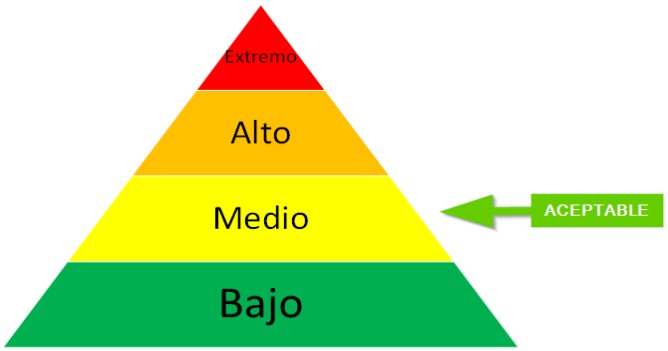


Ilustración 9 Nivel de riesgo Aceptable

Activos	Amenaza	Riesgo
Servidores físicos VMWare	Ataque aprovechando firmware desactualizado	Alto
Máquinas Virtuales Windows Server 2012 R2	Corrupción de la información	Alto
Software de Producción	Caída del sistema por sobrecarga	Alto
Core Switch	Condiciones inadecuadas de temperatura o humedad	Alto
Firewall	Ataque aprovechando errores de configuración	Alto
Switches	Ataque aprovechando vulnerabilidad de seguridad.	Alto
Librería de discos MSA	Avería del dispositivo por falta de mantenimiento	Alto
Portátiles Oficinas	Robo	Alto
Sistemas Operativos Windows Server 2012 R2	Ataque perpetrado por estar desactualizado	Alto
Medios de almacenamiento externo	Robo	Alto
Correo electrónico	Introducción de falsa información por pishing	Alto

Ilustración 10 Niveles de riesgo superiores al aceptable

Estas serían las amenazas a las cuáles deberíamos de poner controles hasta reducirlas a un nivel de riesgo aceptable para que no supongan ningún peligro para la organización según el criterio que hemos establecido. Hay que tener en cuenta que estos riesgos solo tratarán de reducirse siempre y cuando sea rentable económicamente para la organización.

4. DPIA – Evaluación de impacto RGPD

Un DPIA o Evaluación de Impacto de Privacidad es un proceso que ayuda a las empresas a identificar y minimizar los riesgos de privacidad en los nuevos proyectos o políticas.

Esta evaluación es realizada por la organización para auditar sus propios procesos a modo de conocer como estos afectan o pueden comprometer a la privacidad de las personas cuyos datos personales contiene, procesa o recopila.

Puesto que los DPIA son una medida para mantener segura la información privada dentro de la organización, se debe realizar esta evaluación siempre que la empresa tenga información personal de los empleados proveedores o clientes.

El nuevo reglamento establece que no siempre es necesario realizar una evaluación de impacto, aunque es recomendable que a la hora de establecer un nuevo tratamiento siempre se analicen los posibles riesgos que puede entrañar el mismo.

Los casos en los que se considera obligatoria son:

- Alto riesgo: Cuando el tratamiento va a suponer un alto riesgo para los derechos y libertades de las personas físicas.

- Evaluación sistemática: Cuando se evalúen aspectos personales de personas físicas basadas en un tratamiento automatizado por ejemplo en la elaboración de perfiles.

- Tratamiento a gran escala de datos especialmente protegidos: Cuando se realice un tratamiento a gran escala con datos especialmente protegidos incluidos en el artículo 9 y 10, apartado 1 del RGPD.

- Uso de tecnologías invasivas: Cuando se vayan a utilizar tecnologías que se consideran especialmente invasivas con la privacidad, por ejemplo: videovigilancia, biometría, geolocalizaciones técnicas genéticas, etc.

El resultado final de una evaluación de impacto no deja de ser un informe que recoge las características del tratamiento evaluado y las decisiones tomadas para mitigar sus riesgos.

En el artículo 35.7 del RGPD se concreta cuál debe ser el contenido mínimo de evaluación o las cuestiones que se deben analizar como mínimo para considerar que se ha hecho una evaluación de manera adecuada.

Las cuestiones en concreto serían:

- Descripción del tratamiento y finalidades: Se debe llevar a cabo un análisis del proyecto, obteniendo el detalle de las categorías de datos que se tratan, los usuarios, flujos de información y las tecnologías utilizadas.

- Evaluación de la proporcionalidad y necesidad del tratamiento: Se debe comprobar si la operación de tratamiento se puede obtener por otros medios, por ejemplo, utilizando menos medios u otros datos.

- Evaluación de los riesgos: Se tiene que llevar a cabo un análisis sobre los posibles riesgos para la protección de datos de los afectados y valoración de la probabilidad y el impacto de su materialización.

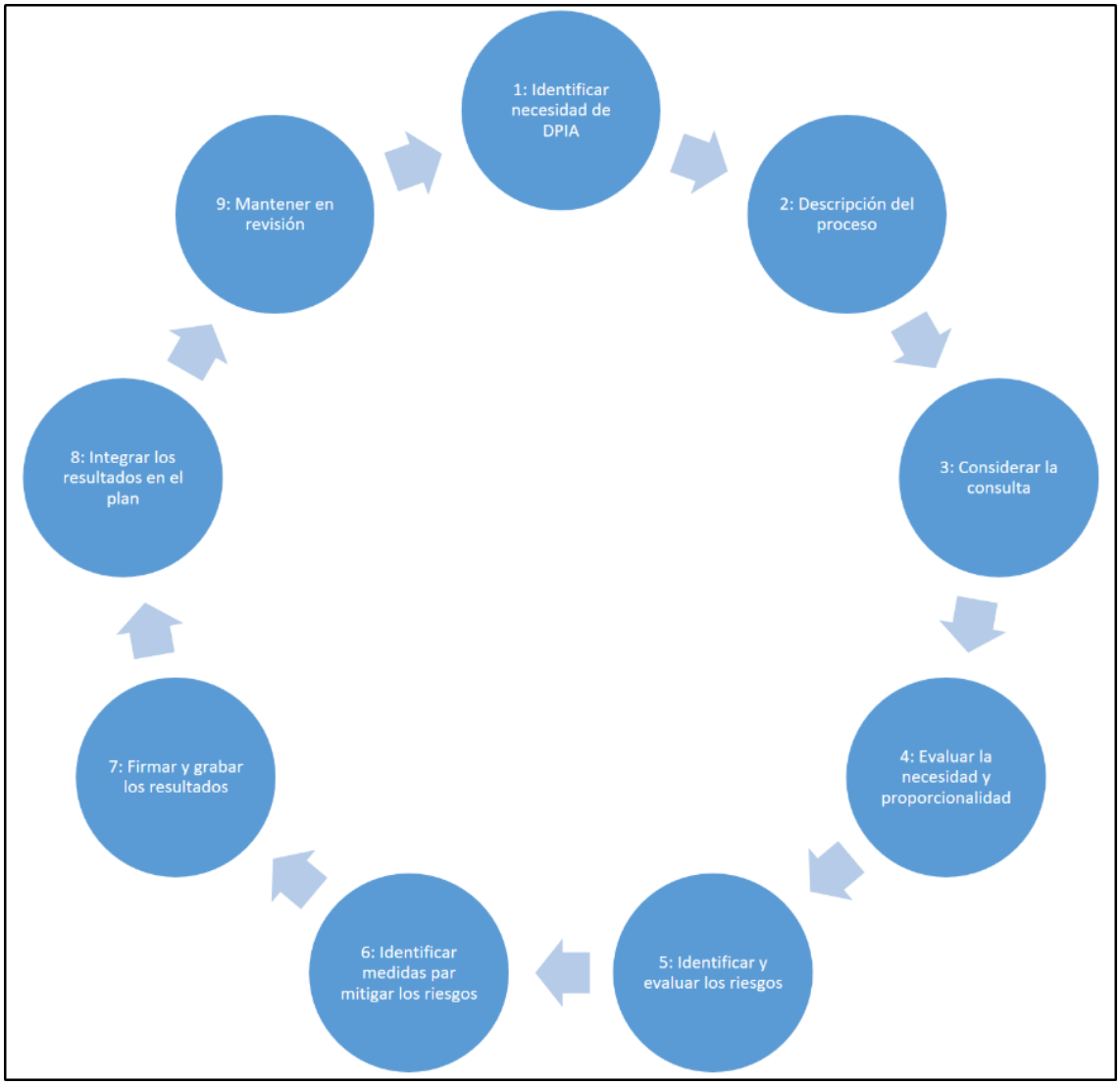


Ilustración 11 Ciclo de vida DPIA

5. Certificaciones de utilidad: ISO 27001

5.1. Introducción a la ISO 27001

El RGPD, a diferencia del Reglamento de la LOPD, introduce el concepto de "Seguridad Activa" que evita, como hasta ahora, señalar un catálogo de medidas de seguridad concretas, dejando la elección de éstas al Responsable y al Encargado en base al riesgo evaluado respecto a los tratamientos de datos personales. La norma ISO 27001:2013, junto a sus 114 controles, pueden ser una ayuda relevante para el cumplimiento del RGPD.

La ISO/IEC 27001 es un estándar para la Seguridad de los Sistemas de Información publicado como estándar internacional en octubre de 2005 por la International Organization for Standarization (ISO). Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI).

Los Sistemas de Gestión de Seguridad de la Información son el medio conocido más eficaz para tratar de minimizar los riesgos tras identificar y valorar los activos y sus amenazas. De este modo, se adoptan controles y procedimientos más coherentes con la estrategia de negocio.

La implementación de norma ISO 27001 tiene como resultados:

- Ahorrar costes por la reducción de incidentes.
- Proteger la reputación de la empresa.
- Permitir la detección prematura de brechas de seguridad.
- Cumplir con los requisitos legislativos.
- Identificar los principales riesgos en materia de seguridad informática.
- Proporcionar el marco más adecuado para la gestión de la seguridad.

Por otro lado, si comprobamos el número de certificaciones ISO 27001 totales en el mundo que recoge la ISO en un estudio realizado en 2016, podemos ver un crecimiento del 21% con respecto al año 2015, lo que implica un aumento de 5754 certificaciones durante ese año.

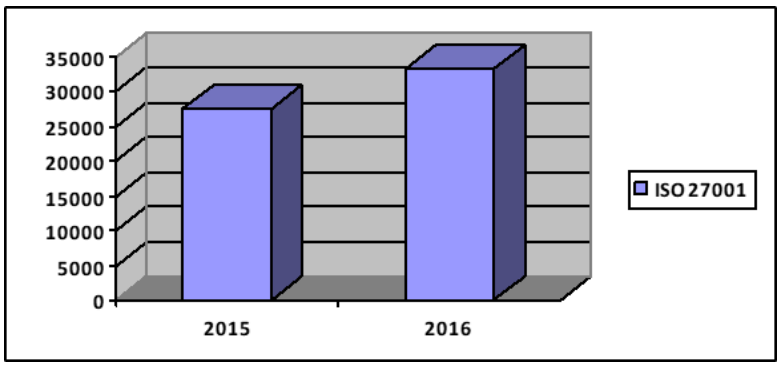


Ilustración 12 Incremento Certificaciones ISO 27001

Los datos obtenidos por la ISO sitúan a España entre el top 10 de países europeos con mayor número de certificaciones ISO 27001.

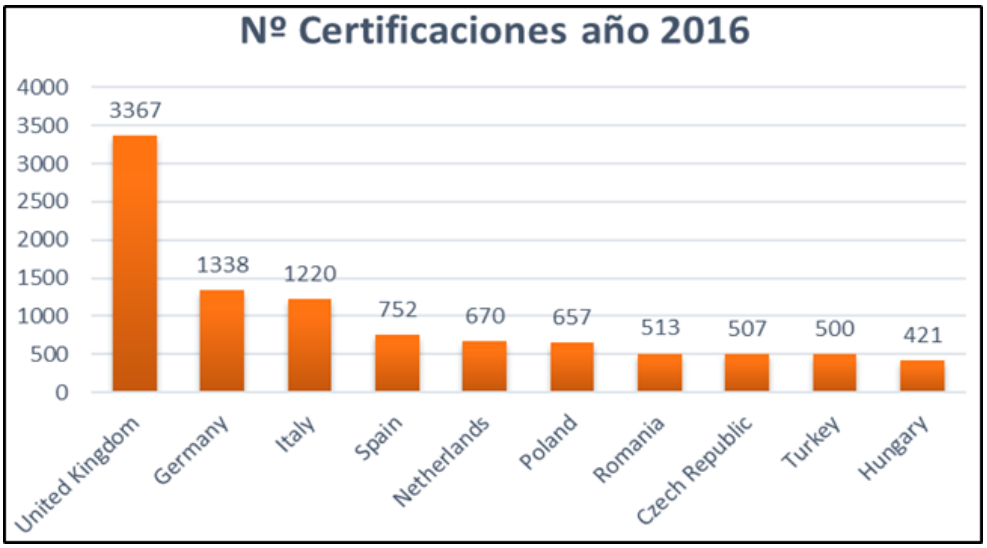


Ilustración 13 Top 10 Países europeos con certificaciones ISO 27001

5.2. Documentos obligatorios del estándar ISO 27001

El estándar ISO 27001 establece una serie de documentos obligatorios que se referencian como “información documentada”. Estos se listan a continuación:

- El alcance del sistema de gestión de seguridad de la información (cláusula 4.3): Este documento es generalmente corto y en él viene reflejado el alcance del SGSI.

- Política de seguridad de la información y objetivos (cláusulas 5.2 y 6.2): Este documento por lo general tiende a ser breve y detalla el objetivo del SGSI. Los objetivos pueden ir unificados en la política de seguridad.

- Metodologías de evaluación y tratamiento de riesgos (cláusula 6.1.2): La metodología de evaluación y tratamiento del riesgo suele ser un documento de 4 páginas aproximadamente y debe ser redactado antes que se realice la evaluación y el tratamiento de estos.

- Declaración de aplicabilidad (cláusula 6.1.3 d): se registran las medidas de seguridad que se van a aplicar, como se implementarán y su estado actual. Podemos considerar ese documento como el que describe el perfil de seguridad de la empresa.

- Plan de tratamiento de riesgo (cláusula 6.1.3 e y 6.2): El plan de tratamiento de riesgos es básicamente un plan de acción sobre cómo implementar los controles definidos en el análisis de riesgos.

- Informe sobre evaluación de riesgos (cláusula 8.2): El informe de evaluación y tratamiento de riesgos debe ser redactado contemplando los resultados de evaluación y tratamiento de estos.

- Definición de roles y responsabilidades de seguridad (cláusulas A.7.1.2 y A.13.2.4): En este documento se describen estas funciones y responsabilidades en todas las políticas y procedimientos de la forma más precisa posible. Las funciones y responsabilidades de seguridad para terceros se definen a través de contratos.

- Inventario de activos (cláusula A.8.1.1): Se deben tener todos los activos inventariados, ya que en la evaluación de riesgos se tienen que contemplar.

- Uso aceptable de los activos (cláusula A.8.1.3): Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de esta.

- Política de control de acceso (cláusula A.9.1.1): Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.
- Procedimientos de operación para gestión de TI (cláusula A.12.1.1): Se deberían documentar los procedimientos operativos y dejar a disposición de todos los usuarios que los necesiten.

- Principios de ingeniería de sistemas seguros (cláusula A.14.2.5): Se deberían establecer, documentar, mantener y aplicar los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información.

- Política de seguridad para proveedores (cláusula A.15.1.1): Se deberían acordar y documentar adecuadamente los requisitos de seguridad de la información requeridos por los activos de la organización con el objetivo de mitigar los riesgos asociados al acceso por parte de proveedores y terceras personas.

- Procedimiento para gestión de incidentes (cláusula A.16.1.5): Se debería responder ante los incidentes de seguridad de la información en atención a los procedimientos documentados.

- Procedimientos de Continuidad de negocio (cláusula A.17.1.2): La organización debería establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas.

- Requerimientos legales, regulatorios y contractuales (cláusula A.18.1.1): Se deberían identificar, documentar y mantener al día de manera explícita para cada sistema de información y para la organización todos los requisitos estatutarios, normativos y contractuales legislativos junto al enfoque de la organización para cumplir con estos requisitos.

- Registros de formación, habilidades, experiencia y calificaciones (cláusula 7.2): Se debería definir las responsabilidades de la Dirección para garantizar que la seguridad se aplica en todos los puestos de trabajo de las personas de la organización. Se debería establecer un proceso disciplinario normal para gestionar las brechas en seguridad.

- Seguimiento y resultados de medición (cláusula 9.1): Para describir cómo se miden los controles, se realizará a través de políticas y procedimientos que definan a cada control. Esta descripción puede ser realizada al final de cada documento, y cada descripción tiene que definir los tipos de ICD (indicadores clave de desempeño) que es necesario medir para cada control o grupo de controles.

  Una vez que se establece este método de control, se debe realizar la medición en función de dicho método. Es importante reportar los resultados de esta medición de forma regular a las personas que están a cargo de la evaluación.

- Programa de auditoria interna (cláusula 9.2): El programa de auditoría interna no es más que un plan anual para realizar las auditorías, para las empresas más pequeñas, puede tratarse solamente de una auditoría, mientras que para las organizaciones más grandes puede ser muchas más. Este programa debe definir quién realizará las auditorías, los métodos que se utilizarán, los criterios que se aplicarán, etc.

- Resultados de auditorías internas (cláusula 9.2): Un auditor interno debe generar un informe de auditoría, que incluye los resultados de la auditoría (observaciones y medidas correctivas).

  Este informe debe ser confeccionado dentro de un par de días tras realizar la auditoría interna. En algunos casos, el auditor interno tendrá que verificar que todas las medidas correctivas se aplicaron según lo esperado.

- Resultados de la Revisión por Dirección (cláusula 9.3): Estos registros se presentan, normalmente, bajo la forma de actas de reunión y deben incluir todo el material tratado durante la reunión de la dirección, como también todas las decisiones que se tomaron.

- Resultados de acciones correctivas (cláusula 10.1): Generalmente, estos son incluidos en los formularios para medidas correctivas (FMC). Las medidas correctivas no son más que listas de actividades a realizar con responsabilidades, tareas y plazos bien definidos.

- Registros de las actividades de usuario, excepciones y eventos de seguridad (cláusulas A.12.4.1 y A.12.4.3): Habitualmente se llevan de primero en formato digital, generados en forma automática o semiautomática como registros de diversas TI y de otros sistemas, y en segundo lugar en papel, donde cada registro se hace manualmente.

5.3. ISO 27001 con respecto al RGPD

Las empresas plantean cuestiones como:

Si mi empresa implementa la ISO 27001, ¿Cumplirá con los requisitos del RGPD – Reglamento General de Protección de Datos? Entonces, ¿La ISO 27001 abarca todos los requisitos del RGPD? La respuesta es sí, pero con matices.

La ISO 27001 abarca la gran mayoría de los controles previstos en los requisitos del GPDR, pero algunos procedimientos deben especificarse (por ejemplo, el procedimiento para la situación de pérdida o divulgación indebida de datos personales debe especificarse con una ventana temporal de 72 horas).

La ISO 27001, como norma del sistema de gestión de seguridad de la información, debe garantizar que se incluyan todos los requisitos, ya sean de clientes o reglamentarios, y que se traten todos los riesgos asociados. Por ello, se incluyen las particularidades del RGPD y se tratan los riesgos de pérdida de datos personales.

El nuevo reglamento del RGPD atribuye más responsabilidades a los subcontratados que procesen o traten datos en nombre de una empresa cliente.

La implementación de un sistema de gestión de seguridad de la información en una de estas empresas asegura que todos los controles para mitigar los riesgos relacionados con la confidencialidad, la integridad y la disponibilidad se implementan y se mantengan funcionando.

La certificación del sistema de gestión de seguridad de la información por la ISO 27001, constituye la mejor prueba de capacidad de garantizar el cumplimiento del RGPD que una empresa puede proporcionar.

El artículo 42 del RGPD especifica que:

“Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados.” [3]

El RGPD recomienda el uso de esquemas de certificación como la ISO 27001(empresas privadas) y el ENS (Esquema Nacional de Seguridad para empresas públicas) como una forma de proporcionar la garantía necesaria de que la organización es efectivamente capaz de gestionar sus riesgos de seguridad de la información.

6. Gap análisis ISO 27001:2013

6.1. ¿Qué es el Gap Análisis?

El Gap análisis aplicado sobre la norma ISO 27001:2013 evalúa el sistema de seguridad de la información del negocio y nos permite conocer el nivel de cumplimiento de la norma e identificar en que puntos debemos emplear las medidas correctivas oportunas. Este análisis surge de la necesidad de poder medir y evaluar la mejora continua y conocer cuál es el nivel de madurez actual del negocio en este aspecto.

La metodología seguida para realizar este análisis enfrenta los controles implantados actualmente en el negocio contra los controles necesarios y no existentes en relación con la norma ISO/IEC 27001, que desarrolla una serie de controles para la Gestión de la Seguridad de la Información.

El objetivo de este análisis es la verificación de la implantación de los controles establecidos en la Norma. Como resultado de este, se proponen una serie de recomendaciones necesarias para garantizar la mejora en la seguridad de la información, así como para priorizar la asignación de recursos en las áreas que se encuentren con mayor criticidad.

6.2. Modelo de Niveles de madurez

Los niveles de madurez consisten en un conjunto predefinido de áreas de proceso. Estos se miden por el alcance de los objetivos genéricos y específicos que se aplican a cada conjunto de áreas de proceso.

En este caso el nivel de madurez que emplearemos para la valoración de los controles es el definido por COBIT y basado en el CMM. De este modo los resultados del GAP Análisis se clasificarán según estos niveles.

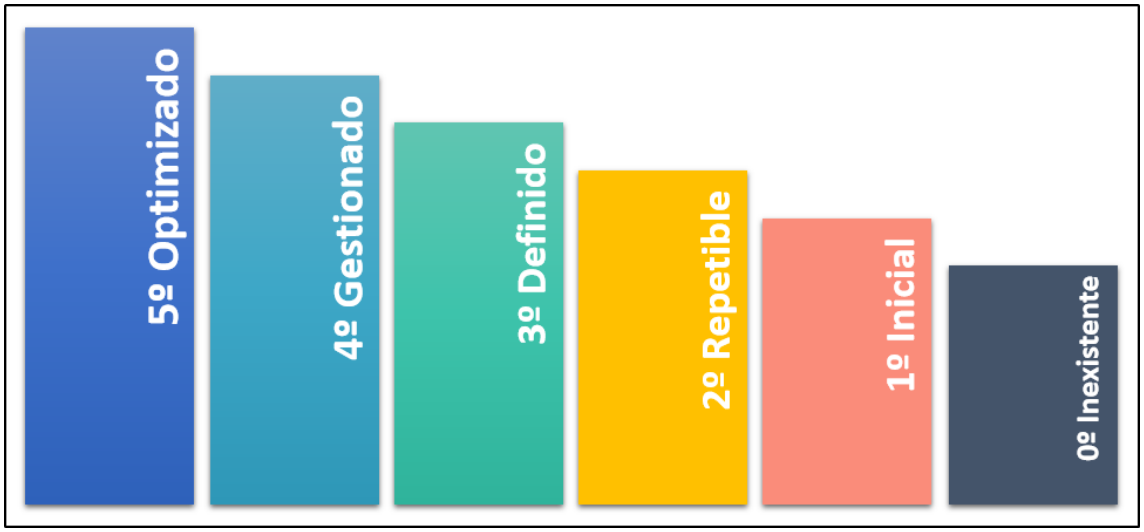


Ilustración 14 Modelo de niveles de madurez

- **Nivel de Madurez 0º Inexistente**: En este nivel de madurez hay ausencia total de los procesos reconocibles.

  La organización no es consciente o desconoce que debe gestionar la seguridad en esta área o proceso.

- **Nivel de Madurez 1º Inicial**: En este nivel de madurez no existen procesos estándar, aunque sí que hay planteamientos que se emplean adecuadamente en función de cada situación.

  Existen evidencias de que la organización ha reconocido que debe contemplar la seguridad, pero los procesos involucrados no se gestionan.

- **Nivel de Madurez 2º Repetible**: Los procesos han ido evolucionando hasta realizar el seguimiento de procedimientos similares a la hora de realizar una misma tarea. En cambio, no hay comunicación sobre el procedimiento ni formación estándar y las responsabilidades caen sobre el propio individuo.

  La sobreconfianza en el conocimiento de estos procedimientos puede derivar en la producción de errores.

- **Nivel de Madurez 3º Definido**: La organización asegura que se aplican los controles, se planifican, documentan, ejecutan, monitorizan y controlan.

  Se permite a los usuarios guiarse a partir de los procedimientos creados y es probable que no haya desviaciones respecto a los mismos.

- **Nivel de Madurez 4º Gestionado**: Los procesos están en mejora continua y proporcionan mejores prácticas. Se usan herramientas automatizadas para llevarlo a cabo.

  Se puede monitorizar y medir el cumplimiento con los procedimientos y tomar medidas en el momento en que los procesos no funcionen de manera efectiva.

- **Nivel de Madurez 5º Optimizado**: Los procesos han sido revisados hasta el nivel de mejores prácticas a partir de una mejora continua.

  Las tecnologías de la información se utilizan de manera integrada para automatizar los flujos de trabajo hasta el punto de proporcionar herramientas para mejorar la calidad y eficiencia.

6.3. Plantilla de Controles ISO 27001:2013

A continuación, se rellena la plantilla con los controles que ofrece la ISO 27001 para poder calcular posteriormente cual es el estado actual del negocio y de este modo definir la ruta que queremos tomar.

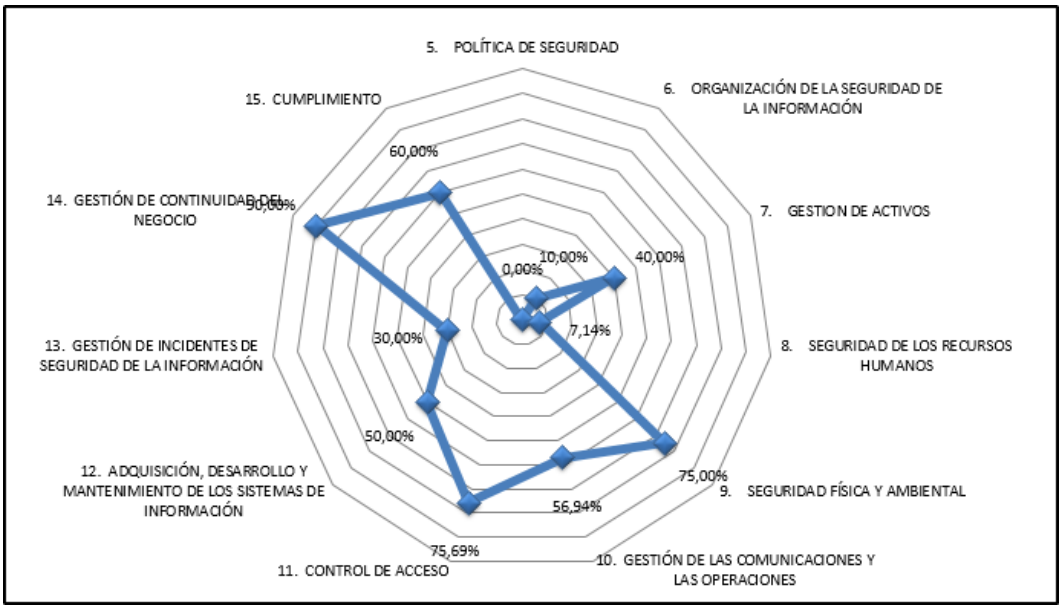


Ilustración 15 Gráfico Resultados Análisis GAP

Una vez obtenido el gráfico resultante del análisis GAP podemos observar la situación actual en la que se encuentra la empresa Automotive X.

A nivel general, la media obtenida por los controles daría un nivel de madurez de la institución del 51%, lo que a escala significaría que está en un nivel 3 Definido. Esto indica que los procesos y los controles se documentan y se comunican, pero no se han establecido mecanismos de monitoreo para una detección de desviaciones efectiva.

En base al resultado obtenido, podemos observar que los puntos en los que la organización flaquea y habría que optar por reforzar esos controles son los referentes a:

- Políticas de seguridad 0%
- Organización de la seguridad de la información 10%
- Gestión de activos 40%
- Seguridad de los recursos humanos 7,14%
- Gestión de incidentes de seguridad de la información 30%

Este resultado puede resultar orientativo en la correspondiente fase de adaptación del negocio al RGPD para implementar soluciones y obtener resultados más favorables de cara al cumplimiento de la normativa.

7. Adecuación del negocio a la norma RGPD

En el siguiente apartado veremos las acciones realizadas para la adecuación del negocio a la normativa RGPD.

7.1. Actividades de tratamiento de datos y cláusulas informativas

La desaparición de la obligación de registrar los ficheros o tratamientos en las Autoridades de Control es una de las novedades que ha introducido el RGPD. Sin embargo, exige llevar un registro interno de las actividades de tratamiento para organizaciones que se encuentren en los siguientes casos:

- Que empleen a más de 250 personas.
- Que realicen tratamientos de forma no ocasional.
- Que realicen tratamientos que puedan entrañar riesgos para las los derechos y libertades de las personas.
- Que realicen tratamientos de las categorías especiales de datos personales indicadas anteriormente.

Dentro de una organización que realiza tratamientos de bajo riesgo, es decir, que no se realizan tratamientos masivos ni con datos especialmente protegidos como es nuestro caso, la propia AEPD ofrece una herramienta llamada **Facilita.**

Se trata de una forma rápida y fácil para que las pymes sin apenas conocimientos puedan elaborar la documentación adecuada a los tratamientos de su negocio.

La herramienta en si consiste en cumplimentar un formulario sobre los tratamientos de datos que la empresa realiza y al finalizar genera un documento acorde a las respuestas indicadas.

Este documento contiene las cláusulas informativas que se deben incluir en los formularios de solicitud de información, el documento a anexar en cada uno de los contratos de prestación de servicios, el registro de actividades de tratamiento y un anexo con recomendaciones sobre medidas de seguridad.

Registro de las actividades de tratamiento de datos personales

En el capítulo 2.1 de la memoria se ha realizado el registro interno relativo a las actividades de tratamiento de datos personales obtenido por la herramienta **Facilita**.

Es importante tener en cuenta cualquier nuevo tratamiento de datos que se pueda empezar a realizar en la organización. Esto se puede incluir en las auditorías internas para asegurar que ningún tratamiento se escape y tenga un responsable asignado.

Clausulas Informativas para el tratamiento de los datos personales

Cuando un candidato a un puesto de trabajo en la empresa rellena un formulario para solicitar información de la vacante disponible o entregue su CV en papel, hay que añadir una cláusula informativa para que el candidato sea conocedor del tratamiento que se va a realizar sobre sus datos personales.

Para cumplir con esta parte de la normativa, añadiremos el siguiente texto a todos los formularios que así lo requieran:

"En nombre de la empresa_____tratamos la información que nos facilita con el fin de mantenerle informado de las distintas vacantes a un puesto de trabajo que se produzcan en nuestra organización. Los datos proporcionados se conservarán hasta la adjudicación de un puesto de trabajo o hasta que usted ejerza su derecho de cancelación por tanto tiene derecho a acceder a sus datos personales, rectificar los datos inexactos o solicitar su supresión cuando los datos ya no sean necesarios. Los datos no se cederán a terceros." [14]

En el caso de que los candidatos aporten su CV en un papel, sin formulario, se les pedirá que firmen un formulario en el que figure la información citada antes.

Cláusulas contractuales

De la misma manera, en los contratos con las empresas que prestan servicios a la organización, se deberán incluir las siguientes cláusulas contractuales:

1. Objeto del encargo del tratamiento

Mediante las presentes cláusulas se habilita a _____, como encargado del tratamiento, para tratar por cuenta de _____, en calidad de responsable del tratamiento, los datos de carácter personal necesarios para prestar el servicio que en adelante se especifican.

El tratamiento consistirá en _____.

2. Identificación de la información afectada

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, la entidad _____ como responsable del tratamiento, pone a disposición de la entidad _____ la información disponible en los equipos informáticos que dan soporte a los tratamientos de datos realizados por el responsable.

3. Duración

El presente acuerdo tiene una duración de _____, renovable.
Una vez finalice el presente contrato, el encargado del tratamiento debe devolver al responsable los datos personales, y suprimir cualquier copia que mantenga en su poder. No obstante, podrá mantener bloqueados los datos para atender posibles responsabilidades administrativas o jurisdiccionales.

4. Obligaciones del encargado del tratamiento

El encargado del tratamiento y todo su personal se obliga a:

- ✓ Utilizar los datos personales a los que tenga acceso sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

- ✓ Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento.

  Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos, el encargado informará inmediatamente al responsable.

- ✓ No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles.

- ✓ Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice el contrato.

- ✓ Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

- ✓ Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

- ✓ Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

- ✓ Notificación de violaciones de la seguridad de los datos

  El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida y a través de la dirección de correo electrónico que le indique el responsable, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

  Se facilitará, como mínimo, la información siguiente:

  a. Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

b. Datos de la persona de contacto para obtener más información.

c. Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales. Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

   Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

- ✓ Poner disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.

- ✓ Auxiliar al responsable de tratamiento a implantar las medidas de seguridad necesarias para:

  a. Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

  b. Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

  c. Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.

- ✓ Destino de los datos

  El responsable del tratamiento no conservará datos de carácter personal relativos a los tratamientos del encargado salvo que sea estrictamente necesario para la prestación del servicio, y solo durante el tiempo estrictamente necesario para su prestación.

5. Obligaciones del responsable del tratamiento

Corresponde al responsable del tratamiento:

a. Facilitar al encargado el acceso a los equipos a fin de prestar el servicio contratado.
b. Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado.

c. Supervisar el tratamiento.

7.2. Asignación del DPO

Tal y como hemos visto anteriormente, la figura del DPO es uno de los elementos claves del RGPD, ya que es la encargada de supervisar que la normativa se cumple dentro de la organización.

En nuestro caso particular, al tratarse de una pyme que no realiza un tratamiento de datos a gran escala, ni trata con datos personales sensibles, no sería necesario que esta figura estuviera presente en la organización.

A pesar de esto, para garantizar el cumplimiento de la normativa y para tener una figura visible dentro de la organización a la que poder consultarle temas relacionados con el RGPD, desde el comité de dirección se ha decidido asignar este rol al manager de seguridad.

Actualmente no existe un título certificado obligatorio para ejercer este puesto de trabajo, aunque dado que la demanda de esta figura se va a ver incrementada, se recomienda obtener una titulación validada por la AEPD que acredite que esta persona está capacitada para desempeñar las funciones de DPO.

A partir de este momento, el DPO dentro de la organización se encargará de:

1. Informar y asesorar al responsable/encargado del tratamiento de datos y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben según el Reglamento.

2. Supervisar el cumplimiento del Reglamento, y otras disposiciones de protección de datos.

3. Asesorar en los casos de evaluaciones de impacto y supervisar su aplicación.

4. Cooperar con la autoridad de control y actuar como punto de contacto para cuestiones relativas al tratamiento, incluida la consulta previa.

5. Prestar la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

6. Rendir cuentas directamente al más alto nivel jerárquico del responsable/encargado.

7. Atender a los interesados para cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos.

8. Mantener la confidencialidad en lo que respecta al desempeño de sus funciones.

7.3. Realización de Inventario de Activos y asignación de propietario.

Para poder controlar cuales son los riesgos que pueden afectar a los datos personales de la organización, hay que realizar previamente un inventario de todos los activos relacionados con el tratamiento de los datos personales, puesto que en base a estos podremos medir cuáles son más críticos que otros.

Para realizar este inventario, podemos utilizar cualquier plantilla gratuita que nos permita conocer el nombre del activo, un identificador, el propietario o responsable, el tipo, la ubicación y su criticidad, por ejemplo.

En nuestro caso, esto se ha realizado en el capítulo 2.2 de la memoria, donde hemos añadido todos los dispositivos e infraestructura que van a ser claves para el tratamiento de los datos personales de la organización.

Una vez hecho esto, podemos continuar con el análisis de riesgos para ver cómo afectarán estos a los datos personales que tratamos.

7.4. Realización de Análisis de Riesgos.

Tal y como se ha visto, este es el siguiente paso después de haber hecho el inventario de activos. Ahora ya podemos valorar y medir las amenazas que pueden afectar a los activos, y en base a esto a los datos personales que trata la organización.

En el capítulo 3 de la memoria se ha realizado el correspondiente análisis de riesgos para los activos inventariados por la organización. Aunque antes de esto, se han asignado los parámetros para estimar las probabilidades de que se materialicen los riesgos, el impacto que tendría en la organización y finalmente en función de estos se ha calculado una fórmula para que podamos medir el nivel de riesgo final.

El siguiente paso ha sido el de decidir cuál es el nivel de riesgo aceptable por la organización, es decir, que en caso de que se materialice la amenaza, la organización no tomará ninguna medida correctiva para tratar de erradicarlo o mitigarlo.

Esto puede ser debido a que es muy poco probable que se dé el caso, porque la organización considera que no supone ningún impacto considerable o porque ese dispositivo no tiene un valor alto para el negocio.

En cambio, para todos los puntos que superan el nivel aceptable, la organización va a tener que implementar una serie de controles para tratar de mitigar o erradicar estos riesgos. En este caso, la ISO 27001 ofrece una serie de controles y soluciones para aplicar.

Es posible que en algunos casos la cantidad de dinero a emplear para eliminar un riesgo suponga una inversión desorbitada para la organización y por lo tanto se tengan que conformar con tratar de reducirlo para que sea rentable.

A continuación, en función de los riesgos que no han sido considerados como aceptables en el capítulo 3.3 de la memoria, definiremos una serie de controles para tratar de mitigarlos o reducirlos.

Activos	Amenaza	Nivel Riesgo	Tratamiento	Control Seguridad ISO 27001	Fecha Límite	Responsable
Servidores físicos VMWare	Ataque aprovechando firmware desactualizado	Alto	Eliminar	A.12.6.1	1 mes	Manager IT
Detalles	Implantar una política para comprobar las actualizaciones disponibles.					
Máquinas Virtuales Windows Server 2012 R2	Corrupción de la información	Alto	Implantar	A.12.3.1	3 mes	Manager IT
Detalles	Crear snapshoots puntuales para evitar la pérdida de información.					
Software de Producción	Caída del sistema por sobrecarga	Alto	Implantar	A.12.1.3	15 días	Manager IT
Detalles	Implantar un sistema de monitorización para comprobar los recursos de que disponen los sistemas.					
Librería de discos MSA	Avería del dispositivo por falta de mantenimiento	Alto	Implantar	A.12.1.3	1 mes	Manager IT
Detalles	Implantar sistema de monitorización que avise en caso de que funcionamiento no sea el adecuado.					
Core Switch	Condiciones inadecuadas de temperatura o humedad	Alto	Implantar	A.11.1.4	7 días	Manager IT
Detalles	Se implantará un sistema de refrigeración adecuado para bajar la temperatura del ambiente.					
Firewall	Ataque aprovechando errores de configuración	Alto	Implantar	A.12.1.1	7 días	Manager IT
Detalles	Se implementará un procedimiento de operación para evitar malas configuraciones.					
Switches	Ataque aprovechando vulnerabilidad de seguridad.	Alto	Implantar	A.12.6.1	7 días	Manager IT
Detalles	Se implanta un sistema de monitorización de vulnerabilidades en los equipos de la red.					
Portátiles Oficinas	Robo	Alto	Reducir	A.6.2.2	45 días	Manager IT
Detalles	Se desarrollan unas medidas de seguridad de apoyo a proteger la información accedida en ubicaciones destinadas al teletrabajo.					
Sistemas Operativos Windows Server 2012 R2	Ataque perpetrado por estar desactualizado	Alto	Eliminar	12.6.1	15 días	Manager IT
Detalles	Se implanta un sistema de monitorización de vulnerabilidades en los equipos de la red.					
Medios de almacenamiento externo	Robo	Alto	Eliminar	10.1.1	30 días	Manager IT
Detalles	Se implanta una política de cifrado de medios de almacenamiento externo.					
Correo electrónico	Introducción de falsa información por pishing	Alto	Reducir	7.2.2	25 días	Manager RRHH
Detalles	Se realizará una campaña de concienciación y educación ante robos de claves por pishing					

Ilustración 16 Controles ISO 27001:2013

7.5. Análisis de la EIPD para los tratamientos de la empresa.

Según recoge la Guía para una Evaluación de Impacto en la Protección de Datos Personales de la AEPD, antes de adentrarse en la realización de un EIPD, es fundamental llevar a cabo una reflexión previa sobre las situaciones que aconsejarían su realización. A continuación, se muestran los casos:

- Cuando se enriquezca la información existente sobre las personas mediante la recogida de nuevas categorías de datos o se usen las existentes con nuevas finalidades o en formas que antes no se usaban.

- Cuando se lleve a cabo un tratamiento significativo no incidental de datos de menores o dirigido especialmente a tratar datos de estos.

- Cuando se vaya a llevar a cabo un tratamiento destinado a evaluar o predecir aspectos personales relevantes de los afectados, su comportamiento, su encuadramiento en perfiles, etc.

- Cuando se traten grandes volúmenes de datos personales a través de tecnologías como la de datos masivos (Big data), internet de las cosas (Internet of Things).

- Cuando se vayan a utilizar tecnologías que se consideran especialmente invasivas con la privacidad como la videovigilancia a gran escala.

- Cuando el tratamiento afecte a un número elevado de personas o, alternativa o adicionalmente, se produzca la acumulación de gran cantidad de datos respecto de los interesados.

- Cuando se cedan o comuniquen los datos personales a terceros y, en particular, siempre que se pongan en marcha nuevas iniciativas que supongan compartir datos personales con terceros que antes no tenían acceso a ellos.

- Cuando se vayan a transferir los datos a países que no forman parte del Espacio Económico Europeo (EEE).

- Cuando se vayan a utilizar formas de contactar con las personas afectadas que se podrían considerar especialmente intrusivas.

- Cuando se vayan a utilizar datos personales no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica.

- Cuando la recogida tenga como finalidad el tratamiento sistemático y masivo de datos especialmente protegidos.

Como hemos visto, en nuestro caso particular no existe ningún tratamiento de datos personales sensibles, aunque a pesar de esto, siempre que la organización realice un nuevo tratamiento de datos personales realizaremos el análisis de la necesidad para comprobar si hace falta una EIPD.

Como guía podemos realizar los pasos que mostraremos a continuación, para garantizar que cumplimos con el reglamento general de protección de datos.

- Paso 1: Valorar si hay que realizar la evaluación de impacto.

  Existe una plantilla en forma de cuestionario de la AEPD para analizar si la iniciativa realizada por el área implica tratamientos de datos de carácter sensible.

- Paso 2: Conocer en detalle las características del tratamiento de datos personales que se va a llevar a cabo.

  Existe una plantilla de la AEPD que recoge toda la información que permite identificar amenazas y valoración de los riesgos a los que están expuestos los datos de carácter personal afectados.

- Paso 3: Evaluar la necesidad del tratamiento y la proporcionalidad.

- Paso 4: Conocer la opinión de los interesados, es decir, que opinan del tratamiento que se va a hacer de sus datos personales.

- Paso 5: Gestión del riesgo: estimación y tratamiento de los riesgos implicados al tratamiento.

  Existe una plantilla de la AEPD para documentar el análisis básico de riesgos.

- Paso 6: Consulta a la Autoridad Estatal si existe un alto riesgo.

- Paso 7: Documentar y mantener un registro de las evaluaciones de impacto realizadas.

  Existe una plantilla de la AEPD para documentar el registro de actividades de tratamiento tanto para el Responsable como para el Encargado de este.

- Paso 8: Publicar de manera interna o externa la evaluación de impacto.

- Paso 9: Implementar el tratamiento de datos según la evaluación de impacto y supervisar-lo.

- Paso 10: Monitorizar el tratamiento y revisar la evaluación de impacto.

Puesto que en nuestro caso particular los tratamientos que realiza la organización no forman parte de las situaciones por las que se aconsejaría realizar una Evaluación de Impacto, lo que haremos es realizar el análisis para evaluar si realmente es necesario hacerlo.

A continuación, rellenaremos el cuestionario que ofrece la AEPD:

Indicar la siguiente información general sobre el tratamiento:

Tipología de Datos	SI/NO
¿Se van a tratar (1) datos personales (2)? (SI/NO)	
(1) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción	Sí
(2) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona	Sí
Continuar sólo en caso de contestar afirmativamente a la pregunta anterior:	

Finalidades del tratamiento	DETALLE	SI/NO
Marque SI/NO (donde aplique) en función de si el tratamiento responde a las siguientes posibles finalidades:		
¿La recogida de los datos tiene como finalidad el tratamiento a gran escala (3)? Por favor, detalle los puntos indicados a continuación para poder analizar si se trata de un tratamiento a gran escala:		
▪ *El número de sujetos afectados (es decir, cuantos interesados van a ser objeto de este tratamiento)*	☒ *de 0 a 10.000* ☐ *de 10.000 a 100.000* ☐ *+ de 100.000*	
▪ *Las categorías de datos tratados. (Datos especialmente protegidos, Datos de carácter identificativo, Características personales, Circunstancias sociales ,Datos académicos y profesionales, Detalles del empleo, Información comercial, Datos económicos, financieros y de seguro,Transacciones de bienes y servicios). Indicar cuántas de estas categorías aplicarían.*	☐ *1* ☐ *2* ☐ *3* ☐ *4* ☐ *5* ☐ *6* ☐ *7* ☒ *8* ☐ *9*	
▪ *La duración del tratamiento (instantáneo (I), días (D), semanas (S), meses (M),...)*	☐ *instantaneo* ☐ *días* ☐ *semanas* ☒ *meses*	
▪ *La extensión geográfica del tratamiento (Tratamiento a nivel regional (R), nacional (N) o internacional (I))*	☒ *regional* ☐ *nacional* ☐ *internacional*	
¿La recogida de los datos tiene como finalidad la monitorización o evaluación sistemática y exhaustiva de aspectos personales? (tratamiento para monitorizar, observar y/o controlar a los interesados, a través del cual, se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc. de personas identificadas o identificables?)		No
Por ejemplo, uso de registro de actividad sobre clientes para detectar patrones de usuarios susceptibles de contratar un producto, perfiles comerciales, scoring, etc.		

Finalidades del tratamiento (Continuación)	DETALLE	SI/NO
¿La recogida de los datos tiene como finalidad el tratamiento de datos especialmente protegidos (4)?		
(4) Datos identificativos de personas identificadas o identificables asociadas a: ▪ *Ideología o opiniones políticas* ▪ *Afiliación sindical* ▪ *Religión o opiniones religiosas* ▪ *Creencias o creencias filosóficas* ▪ *Origen étnico o racial* ▪ *Datos relativos a salud* ▪ *Vida sexual u orientación sexual* ▪ *Datos de violencia de género y malos tratos* ▪ *Datos biométricos* ▪ *Datos genéticos que proporcionan una información única sobre la fisiología o la salud del identificado obtenidas del análisis de una muestra biológica* ▪ *Datos solicitados para fines policiales sin consentimiento de las personas afectadas* ▪ *Datos relativos a condenas y delitos penales"*		No
¿El tratamiento involucra contacto con los interesados de manera que, dicho contacto, pueda resultar intrusivo (5) o se prevee el uso de tecnologías que se pueden percibir como especialmente intrusivas en la privacidad (6)?		No
(5) A modo de ejemplo, las llamadas telefónicas podrían considerarse intrusivas		
(6) A modo de ejemplo, la vigilancia electrónica, la minería de datos, la biometría, las técnicas genéticas, la geolocalización, Big Data o la utilización de etiquetas de radiofrecuencia o RFID10 (especialmente, si forman parte de la llamada internet de las cosas) o cualesquiera otras que puedan desarrollarse en el futuro"		

¿La finalidad del tratamiento implica el uso específico de datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad (p.e.: menores de 14 años, ancianos, personas con riesgo de exclusión social, empleados, …)?	No
¿Se van a tratar datos personales para elaborar perfiles, categorizar/segmentar, hacer ratings/scoring o para la toma de decisiones (7)?	No
(7) A modo de ejemplo, la segmentación de clientes en base a sus datos personales con el objetivo de realizar comunicaciones comerciales	
¿El tratamiento de los datos implica una toma de decisiones automatizada sin que haya ninguna persona que intervenga en la decisión o valore los resultados (8)?	No
(8) A modo de ejemplo, autorizar o denegar un tipo de producto a un cliente mediante un algoritmo automatizado sin que ningún gestor valore el resultado para confirmar las decisiones	
¿Se enriquece la información de los interesados mediante la recogida de nuevas categorías de datos o se usen las exitentes con nuevas finalidades que antes no se contemplaban, en particular, si estas finalidades son más intrusivas o inesperadas para los afectados (9), o incluso pueda llegar a bloquear el disfrute de algún servicio?	No
(9) A modo de ejemplo, el uso de la información contenida en ficheros externos como ASNEF o CIRBE	
¿El tratamiento implica que un elevado número de personas (más allá de las necesarias para llevar a cabo el mismo) tenga acceso a los datos personales tratados? Por ejemplo, un departamento que no participe en el tratamiento.	No
¿Se van a tratar datos relativos a la observación de zonas de acceso público? (por favor, tenga en cuenta que las zonas de acceso público únicamente estarán situadas en la via publica, excluyendo los lugares de trabajo (p.e.: oficinas comerciales))	No
Para llevar a cabo este tratamiento, ¿se combinan conjuntos de datos utilizados por otros responsables de tratamiento cuya finalidad diste en exceso de las expectativas del interesado (10)?	No
(10) A modo de ejemplo, utilizar el resultado de un tratamiento de análisis de datos de un cliente para realizarle ofertas comerciales en base a dichos resultados	
¿Se utilizan datos de carácter personal no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica.?	No

Tecnologías empleadas para el tratamiento	DETALLE	SI/NO
Marque SI/NO en función de si dichas tecnologías se usan para soportar las finalidades del tratamiento:		
¿Se prevé el uso de tecnologías que se pueden percibir como inmaduras, de reciente creación o salida al mercado, cuyo alcance no puede ser previsto por el interesado de forma clara o razonable e implique elevado riesgo para el acceso no autorizado (11)?		No
(11) A modo de ejemplo, la combinación de tecnologías ya existentes, como el uso de dispositivos inteligentes de nueva creación y reconocimiento facial para aumentar la seguridad del acceso físico a las instalaciones, se considera una tecnología inmadura		

Cesiones de datos y transferencias internacionales de datos	DETALLE	SI/NO
Marque SI/NO:		
¿Se realizan cesiones de datos a otras entidades, ya sean del mismo grupo o proveedores externos al mismo? (en caso afirmativo detallar cuáles)		No
¿Se realizan transferencias internacionales de datos a países fuera de la Unión Europea y que no cuenten con medidas de protección de datos de carácter personal similares a las establecidas por la Autoridad de Control (12)? (en caso afirmativo detallar cuáles)		No
(12) A modo de referencia, el siguiente listado contiene los países considerados seguros para las transferencias de datos: ▪ Andorra ▪ Argentina ▪ Canadá (Sector privado) ▪ Suiza ▪ Islas Feroe ▪ Guernsey ▪ Israel ▪ Isla de Man ▪ Jersey ▪ Nueva Zelanda ▪ Uruguay		

Percepción de la existencia un riesgo elevado por parte del responsable de la actividad de tratamiento	JUSTIFICACIÓN	SI/NO
Marque SI/NO:		
¿Es este tratamiento similar a otro para el que haya sido necesario realizar un EIPD (13)?		No
(13) En caso afirmativo, se pueden utilizar las conclusiones del EIPD ya realizado para dicho tratamiento		
¿Este tratamiento puede conllevar una pérdida o alteración de la información?		No
¿Se utilizada documentación en papel para tratar datos personales?, en tal caso, indicar las medidas aplicadas:		Sí
▪ Se guarda bajo llave		Sí
▪ Se destruye de forma confidencial		Sí
▪ Se guarda con un registro de accesos		No
▪ Otros		

7.6. Realización de políticas de seguridad.

El objetivo de realizar políticas de seguridad es proporcionan orientación y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normativa pertinentes.

Este es un aspecto que la organización de nuestro caso particular no tenía definido y es necesario para que la gerencia esté alineada y comprometida con la adaptación y a la normativa RGPD.

A continuación, se expone un ejemplo de una posible política de seguridad en las tecnologías de la información que podemos aplicar a nuestro caso.

En primer lugar, podemos empezar por incluir un historial de modificaciones, para documentar todas las revisiones y cambios realizados en dicha política.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción del cambio
dd.mm.aaaa	0.1	EUGDPRAcademy	Descripción básica del documento

Ilustración 17 Política de Seguridad - Historial de modificaciones

A continuación, podemos definir el objetivo del documento, alcance y usuarios de la organización que están implicados. En este caso, el objetivo sería definir las reglas para el uso de los sistemas y activos de información.

Podemos incluir también algún documento de referencia que hayamos utilizado para definir la política. En este caso, la ISO 27001 sería bastante útil.

Seguidamente, podemos empezar a definir las reglas básicas de seguridad que contendrá nuestra política.

- **Uso aceptable**: Los activos de información únicamente pueden ser utilizados para satisfacer las necesidades de negocio y cualquier otro uso personal puede ser motivo de despido.

- **Responsabilidad sobre los activos**: Cada usuario es responsable del activo que tiene asignado en el inventario. En caso de que el activo abandone las instalaciones de trabajo, el usuario deberá de asumir el coste de cualquier daño o desperfecto que le sea ocasionado.

- **Revisión Anual de la Seguridad en las TIC**: De manera anual se realizarán auditorías externas para evaluar las debilidades en seguridad.

- **Instalación indebida de Software**: Cualquier Software que se instale en el equipo y no esté relacionado con alguna de las tareas propias que realiza el usuario en su trabajo, podrá ocasionar el despido de este.

- **Uso de activos fuera de las instalaciones**: Los dispositivos móviles como portátiles, dispositivos de almacenamiento externo o documentos que contengan información del negocio, no pueden ser retirados de las instalaciones sin un consentimiento previo por escrito.

- **Devolución de activos al finalizar el contrato**: Al finalizar el contrato laboral, los empleados están obligados a devolver los activos asignados y firmar un documento tipo *check list* de alta/baja.

- **Uso responsable de Internet**: El acceso a Internet se deberá realizar de manera responsable y eludiendo el acceso a páginas con contenido ilícito, pornográfico y de incitación al odio de una raza o etnia.

- **Descarga de contenido con fines extra laborales**: La descarga de contenidos que no estén dentro de las funciones laborales del usuario o la reproducción en *streaming* de música o video está totalmente prohibida y puede ser motivo de despido.

- **Responsabilidad sobre la clave de usuario**: El usuario no debe de revelar las claves a otras personas incluyendo gerencia y administradores del sistema. Tampoco deberá de dejar la clave anotada ni en papel ni en forma digital.

- **Escritorio de trabajo limpio**: El escritorio de trabajo en el sistema operativo se gestionará por parte de los administradores del sistema y no se podrá modificar ni el fondo ni los iconos. Cualquier cambio en este será reseteado en cada reinicio del equipo.

- **Acceso autorizado a las instalaciones**: El acceso a las instalaciones del negocio se realizará únicamente por personal que trabaje en la planta. Cualquier visita deberá de ser registrada y siempre llevará algún acompañante de la propia organización.

- **Mecanismos de seguridad en las comunicaciones:** Las redes deben de estar segregadas en función de los grupos de servicios, usuarios y sistemas de información.

- **Copias de seguridad automáticas**: Diariamente se realizarán copias de seguridad de los ficheros y bases de datos de la organización automáticos de forma que en cualquier momento se pueda restaurar un fichero o base de datos del día anterior.

- **Seguridad en los correos**: Todos los archivos que se envíen a través del correo electrónico y contengan información relativa al negocio deberán estar protegidos con claves.

- **Mecanismos contra los fallos eléctricos**: Todos los equipos informáticos situados en el centro de cómputo y los que tengan un valor importante para la organización deberán de estar respaldados ante un posible fallo eléctrico. Esta medida se puede implementar mediante un generador de luz a gasolina o con SAIs que aseguren la vida del dispositivo hasta que podamos apagarlo manualmente o vuelva la luz.

- **Documentación de procesos**: Todos los procesos de trabajo estarán documentados y procedimentados y se revisarán una vez al año para asegurar que están actualizados.

- **Planes de contingencia**: Se establecerá un plan de contingencia para cada proceso crítico del negocio. Esto incluirá las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio.

- **Revisión anual de infraestructura**: Para garantizar el perfecto estado de la infraestructura, de manera anual se hará una revisión de cableado y dispositivos.

- **Apagado controlado de dispositivos**: Para garantizar el correcto funcionamiento de los dispositivos de la línea de producción, al finalizar la semana se apagarán y se revisarán para comprobar si funcionan correctamente.

- **Mantenimiento red wifi de visitas**: La red wifi asignada para las visitas irá cambiando de clave cada semana por motivos de seguridad y para mejorar el rendimiento, teniendo un mínimo número de conexiones.

- **Monitorización de tráfico de red**: La red de la empresa estará continuamente monitorizada para controlas se ha picos de descargas o si se accede a páginas no permitidas.

- **Categorización de ficheros**: Para identificar el nivel de confidencialidad de los archivos y carpetas almacenados, se categorizarán con los niveles alto, medio y bajo.

- **Estandarización de hardware**: Los equipos informáticos tales como impresoras, portátiles, sobremesa y dispositivos de red, se estandarizarán y solo podrá haber los siguientes modelos según el tipo de dispositivo:

    - Impresoras: HP Modelo Laserjet 600.
    - Portátiles: HP EliteBook 840 G4
    - Sobremesa: HP EliteDesk 800 G3 SFF
    - Switches: Cisco Catalyst 2960-48TC-S
    - Access Points: Cisco Aironet 702i Standalone

Finalmente, se incluirá la fecha de validez del documento y la firma del propietario.

7.7. Procedimiento de reporte de brecha de seguridad de datos

El RGPD define las violaciones de seguridad de los datos utilizando el término conocido como “brechas de seguridad”.

Este término abarca todo percance que origine la destrucción, pérdida o modificación accidental o ilícita de datos personales cedidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Algunos incidentes como la pérdida de un dispositivo móvil, el acceso no autorizado a las bases de datos de una organización (incluso por su propio personal) o el borrado accidental de algunos registros, son consideradas violaciones de seguridad a la luz del RGPD y deben ser tratadas como el Reglamento indica.

En el artículo 33 del RGPD se establece que cualquier Responsable del tratamiento deberá notificar a la Autoridad de protección de datos competente, sin dilación indebida y de ser posible, a más tardar 72 horas después de que se haya tenido constancia, de la violación de la seguridad de los datos, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.

Además, el Reglamento especifica el contenido mínimo que debe albergar la notificación:

- La naturaleza de la violación.
- Las categorías de datos y de interesados afectados.
- Medidas adoptadas por el responsable para solventar la brecha.
- Las medidas aplicadas para paliar los efectos de la brecha.

Pero no solo será suficiente con notificar la brecha de seguridad, pues el Reglamento prevé obligaciones adicionales, en particular será necesario documentar todas las violaciones de seguridad, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas y además en los casos en que sea probable que la violación de seguridad entrañe alto riesgo para los derechos o libertades de los interesados también se deberá notificar a dichos interesados (artículo 34).

El incumplimiento de la obligación de notificar las violaciones de seguridad por parte del responsable del tratamiento se considera como infracción grave y puede ser sancionada con multas administrativas de 10 millones de euros como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, eligiendo la de mayor cuantía.

La notificación se realizará por medios electrónicos a través de la sede electrónica de la Agencia Española de Protección de Datos en la dirección: https://sedeagpd.gob.es

En nuestro caso particular, el procedimiento establecido para la notificación de brechas de seguridad debe considerar lo siguiente:

1. Constatar cuándo se ha tenido conocimiento de la brecha de seguridad, registrando y documentando todas las actuaciones que se lleven a cabo.

   La propia Agencia Española de Protección de Datos interpreta que "la mera sospecha de que ha existido una quiebra o la constatación de que ha sucedido algún tipo de incidente sin que se conozcan mínimamente sus circunstancias no debería dar lugar, todavía, a la notificación" [15].

2. Una vez constatado que efectivamente se ha producido una brecha de seguridad en nuestra organización, habrá que establecer los criterios que nos indiquen el alcance de la brecha de seguridad, ya que es necesario valorar el impacto de la brecha. Es decir, ¿qué características tiene la brecha?, ¿qué tipo de datos o categorías de datos se han visto afectados?, ¿tiene consecuencias para los interesados?

3. Aplicar aquellas medidas técnicas u organizativas apropiadas al tipo de brecha de seguridad ante el que nos encontremos, en especial medidas correctoras que garanticen que no hay posibilidad de que se pueda materializar en un daño de alto alcance.

4. Tras tener claro los puntos anteriores, nuestro plan tiene que tener unos plazos de actuación para la notificación.

   Debemos plantearnos si es posible realizar la notificación dentro de esas 72 horas. En los casos en los que el problema sea muy complejo, se contemplará la posibilidad de notificarlo con posterioridad al plazo señalado, pero deberá justificarse los motivos de la dilación.

5. Finalmente habrá que reflexionar sobre si es necesario notificar a los interesados, puesto que no es obligatorio en todos los casos y realizar una comunicación a todos los afectados además de ser muy laborioso puede afectar a nuestra reputación.

El encargado de notificarlas será el Responsable de Seguridad, o si no contamos en nuestra entidad con esa figura, la responsabilidad recaerá en el representante del Responsable del Tratamiento.

En este caso será el Delegado de Protección de Datos el encargado de la notificación.

7.8. Medidas de seguridad tecnológicas

Cifrado de dispositivos móviles

El cifrado de los dispositivos de almacenamiento nos va a resultar útil puesto que garantiza la confidencialidad y la integridad, reduce el riesgo de acarrear sanciones por incumplimiento y además evita que tengamos que informar a los usuarios en caso de una brecha de seguridad.

Por esta razón, se han cifrado todos los dispositivos móviles tales como portátiles mediante la herramienta *Bitlocker* de Windows. De este modo cada usuario puede gestionar su clave de recuperación a través del directorio activo de Windows.

Sistema de detección de vulnerabilidades

Las medidas de seguridad serán revisadas de forma periódica, la revisión podrá realizarse por mecanismos automáticos (software o programas informáticos) o de forma manual. El simple hecho de no contar con las últimas actualizaciones del antivirus o del sistema operativo, ya suponen una posible vulnerabilidad para que se materialice una amenaza.

Por esta razón, se ha instalado la herramienta Nessus en un equipo para que realice un escáner continuo en búsqueda de vulnerabilidades de red, así como el S.O de las máquinas.

Sistema de caducidad de contraseñas por GPO

Las contraseñas de los usuarios del dominio se regularán por GPO. De este modo se establecerá un tiempo de caducidad de esta de 1 mes. Además, los requisitos de complejidad requerirán de al menos 10 caracteres de longitud, en los cuales haya una letra mayúscula, una letra minúscula y un carácter especial.

Gestión de Privilegios para el acceso a carpetas del sistema

Dentro del Directorio Activo de Windows, los usuarios que pertenecen a un determinado departamento, forman parte de un grupo que tiene los permisos de lectura/escritura a determinadas carpetas de acuerdo a las necesidades de este.

Cuando un usuario abandona el departamento y cambia a otro, se retira del grupo al que pertenece y se agrega si es necesario al del otro departamento de forma que impedimos el acceso no autorizado a las carpetas.

Sistema de revisión de equipos sin antivirus

Se generará un informa semanal para controlar si existen dispositivos en el dominio que no tienen el antivirus corporativo instalado o en su defecto tienen una versión anterior o actualización por instalar.

De este modo se podrán prever ciberataques.

7.9. Medidas para la captación de imágenes con cámaras

Actualmente la empresa no tiene ningún tipo de servicio de videovigilancia contratado con la empresa de seguridad, pero posiblemente para aplicar mejores controles de acceso a las instalaciones se instalen cámaras en los accesos.

En este caso deberíamos de hacer una EIPD y además tendremos en cuenta las siguientes medidas para garantizar los derechos de los empleados:

- **UBICACIÓN DE LAS CÁMARAS**: Las cámaras se han instalado a modo de evitar la captación de imágenes en zonas destinadas al descanso de los trabajadores.

- **UBICACIÓN DE MONITORES**: Los monitores donde se visualizan las imágenes de las cámaras se ubicarán dentro de la garita de seguridad, dónde el acceso sea restringido de forma que no sean accesibles a terceros.

- **CONSERVACIÓN DE IMÁGENES**: Las imágenes se almacenarán durante el plazo máximo de un mes, con excepción de las imágenes que sean aportadas a los tribunales y las fuerzas y cuerpos de seguridad.

- **DEBER DE INFORMACIÓN**: Se informará acerca de la existencia de las cámaras y grabación de imágenes mediante un distintivo informativo donde mediante un pictograma y un texto se detalle el responsable ante el cual los interesados podrán ejercer su derecho de acceso**.**

- **CONTROL LABORAL**: Cuando las cámaras vayan a ser utilizadas con la finalidad de control laboral según lo previsto en el artículo 20.3 del Estatuto de los Trabajadores, se informará al trabajador o a sus representantes acerca de las medidas de control establecidas por el empresario con indicación expresa de la finalidad de control laboral de las imágenes captadas por las cámaras.

- **DERECHO DE ACCESO A LAS IMÁGENES**: Para dar cumplimiento al derecho de acceso de los interesados se solicitará una fotografía reciente y el Documento Nacional de Identidad del interesado, así como el detalle de la fecha y hora a la que se refiere el derecho de acceso. No se facilitará al interesado acceso directo a las imágenes de las cámaras en las que se muestren imágenes de terceros. En caso de no ser posible la visualización de las imágenes por el interesado sin mostrar imágenes de terceros, se facilitará un documento al interesado en el que se confirme o niegue la existencia de imágenes del interesado.

7.10. Auditorías para justificar el cumplimiento del RGPD

El nuevo reglamento no exige en ningún artículo el deber de auditar a las organizaciones, por lo que únicamente se centra en que las empresas garanticen sus resultados de protección de manera adecuada a la naturaleza del tratamiento.

En nuestro caso particular, se realizarán auditorías internas y externas para evaluar la situación de la empresa en cuanto a seguridad de la información. De este modo, podremos descubrir posibles debilidades que terminen afectando de un modo u otro a los datos personales de los sujetos que tratamos. Esto nos va a permitir demostrar que la organización está implicada en la protección de los datos personales que trata y sabremos si está adecuada al RGPD.

A la hora de establecer los programas de auditoria, podemos basarnos en la ISO 19011: Directrices para la Auditoría de los Sistemas de Gestión, ya que, al fin y al cabo, para que haya una buena gestión deberemos de implantar un Sistema de Gestión de la Seguridad.

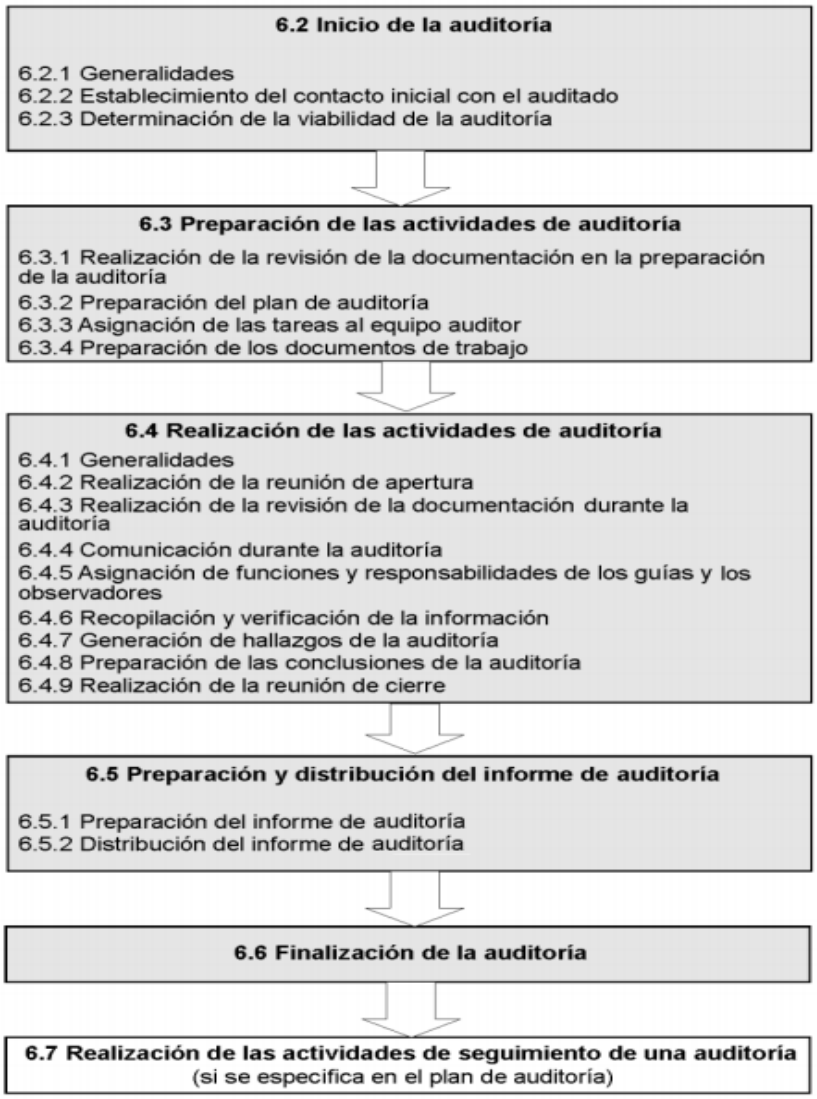


Ilustración 18 Fases Auditoria ISO 19011

8. Conclusiones

El nuevo Reglamento General de Protección de Datos es una forma de garantizar que las empresas aseguran que el tratamiento de datos personales que realizan es seguro y que se respeta la privacidad de las personas.

Podemos decir que este surge de la necesidad de unificar en una única ley las leyes de protección de datos personales de los Estados miembros de la Unión Europea obligando a las empresas a tener un mayor control de los datos y transparencia.

Además, la actual norma vigente de protección de datos es del año 1995 y puesto que la tecnología en estos últimos 20 años ha evolucionado a un nivel muy elevado, ya era necesario actualizar la normativa en vigor.

Se puede decir que todas las empresas que hagan tratamientos de datos personales están obligadas a cumplir con la nueva normativa, aunque dependiendo del tipo de datos que traten y la forma, se deberán tomar acciones más exhaustivas o menos.

En el caso particular que hemos hablado durante el trabajo, al tratarse de una Pyme que no trata con datos personales sensibles, ha permitido realizar un cumplimiento más extenso de la normativa, ya que muchas de las metodologías seguidas como el GAP análisis, el análisis de riesgos y las medidas técnicas o políticas de seguridad establecidas se podrían aplicar también a negocios que traten datos personales sensibles.

Por otro lado, la Agencia Española de Protección de Datos ofrece algunas herramientas muy útiles como Facilita para las Pymes o las Guías para el análisis de riesgos y el listado de cumplimiento, que nos ha ayudado bastante a llegar al objetivo del trabajo de adecuar la pyme a la futura normativa.

Asimismo, existen los gestores documentales, las herramientas Pilar, GlobalSuite o OneTrust para todo lo relativo al inventario de activos, análisis de riesgos, realización de EIPD, etc. Así que podemos concluir que de un modo u otro siempre existen herramientas para facilitar las tareas de adaptación y que no resulten tan costosas las tareas para la adecuación.

Como valoración personal al trabajo realizado, considero que me ha ayudado a adquirir conocimientos esenciales sobre el RGPD que antes desconocía y que estoy aplicando en mi actual empleo para ayudar a adaptarnos a la nueva normativa.

9. Glosario

1. **Ámbito territorial**: El ámbito territorial del RGPD incluye el Área Económica Europea (AEE – todos los 28 países miembros UE), Islandia, Liechtenstein, y Noruega, y no incluye a Suiza.

2. **Autoridad de Control**: se trata de las autoridades nacionales para la protección de datos que tienen como tarea la protección de la privacidad y datos personales. Cada estado miembro debe designar una entidad APD para implementar y hacer cumplir las leyes locales de protección de datos, y ofrecer asesorías al respecto. Las APDs tienen poderes significativos para hacer cumplir las leyes, incluyendo la potestad de aplicar multas substanciales.

3. **Consentimiento del interesado**: atribuiremos como consentimiento del interesado a toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

4. **Datos Biométricos**: se considerarán datos biométricos a los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

5. **Datos Genéticos**: se considerarán datos genéticos a los datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

6. **Datos Personales**: se considerarán datos personales a toda la información sobre una persona física identificada o identificable.

7. **Datos personales sensibles**: El RGPD se refiere a los datos personales sensibles como una “categorías especiales de datos personales”. La categoría especial de datos incluye origen racial o étnico, opiniones políticas, puntos de vista religiosos o filosóficos, membresía sindical, orientación sexual, y datos de salud, genéticos y biométricos procesados para identificar unívocamente a un individuo. Los datos personales correspondientes a los arrestos y crímenes cometidos no se incluyen, pero se deben aplicar medidas de seguridad similares al ser procesados.

8. **Datos Relativos a la Salud**: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

9. **Destinatario**: se considerará destinatario a la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento.

10. **Encargado del tratamiento o Encargado**: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

11. **Elaboración de perfiles**: se considerará elaboración de perfiles a toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

12. **Fichero**: se considerará fichero a todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

13. **Interesado**: El interesado es una persona física. Ejemplos de un interesado pueden ser un individuo, un cliente, un empleado, una persona contacto, etc.

14. **Limitación del tratamiento**: se trata del marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.

15. **Persona Física Identificable**: se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

16. **Responsabilidad proactiva**: La responsabilidad proactiva es la capacidad de demostrar el cumplimiento con el RGPD. El Reglamento explícitamente establece que es responsabilidad de la organización. Para demostrar cumplimiento, las medidas técnicas y organizacionales apropiadas deben estar implementadas. Las mejores prácticas, tales como evaluaciones de impacto de privacidad y privacidad por diseño ahora son legalmente requeridas bajo ciertas circunstancias.

17. **Seudonimización**: se considerará seudonimización al tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

18. **Tercero**: se considerará tercero a la persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

19. **Transferencia**: La transferencia de los datos personales a países fuera del AEE o a organizaciones internacionales está sujeta a restricciones. Tal como se establece en la Directiva de Protección de Datos, los datos no necesitan ser transportados físicamente para que se haga la transferencia. Visualizar los datos alojados en otra ubicación es considerado transferencia para los propósitos del RGPD.

20. **Tratamiento**: se considerará tratamiento a cualquier operación realizada sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

21. **Responsable del tratamiento o Responsable**: será la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros

22. **Violación de la seguridad de los datos personales**: se considerará como toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

10. Bibliografía

- Videos de Interés:

    1. Charla informativa Subdirector general RGPD
       Link: https://www.youtube.com/watch?v=z-csYfA7sJc
       Consultado: 09/04/2018

    2. Charla sobre el RGPD por Base10 y VERITAS
       Link: https://www.youtube.com/watch?v=5pvUmr4PTyw
       Consultado: 09/04/2018

- Páginas Web:

    3. Reglamento General de Protección de Datos
       Link: http://rgpd.es/
       Consultado: 09/04/2018

    4. Agencia Española de Protección de Datos
       Link:
       https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf
       Consultado: 09/04/2018

    5. ISO 27000
       Link: http://iso27000.es/iso27002.html
       Consultado: 27/04/2018

    6. Blog CIBERSEGURIDAD
       Link:
       https://ciberseguridad.blog/documentos-y-registros-iso-27001-2013/
       Consultado:27/04/218

    7. CMMI Maturity Levels
       Link: http://www.tutorialspoint.com/cmmi/cmmi-maturity-levels.htm
       Consultado: 29/04/2018

    8. Centro Criptológico Nacional
       Link: https://www.ccn-cert.cni.es/publico/herramientas/Pilar-5.4.8/web/help/html/niveles_de_madurez.html
       Consultado: 29/04/2018

9. Gydeline Blog
Link: https://www.gydeline.com/dpia
Consultado: 03/05/2018

10. Instituto Nacional de Ciberseguridad
Link: https://www.incibe.es/protege-tu-empresa/rgpd-para-pymes
Consultado: 18/05/2018

11. Agencia Vasca de Protección de Datos
Link:
http://www.avpd.euskadi.eus/contenidos/informacion/20161118/es_def/adjuntos/AVPD-Adecuacion_PYMES_a_RGPD_en_8pasos-v.1-es.pdf
Consultado: 18/05/2018

12. Agencia Española de Protección de Datos - Guía Práctica de Análisis de riesgos en los tratamientos de datos personales sujetos al RGPD
Link:
https://www.google.es/search?q=guia+practica+de+analisis+de+riesgos+en+los+tratamientos+de+datos+personales+sujetos+al+rgpd&oq=guia+practica+de+analisis&aqs=chrome.1.69i57j0l5.7474j0j4&sourceid=chrome&ie=UTF-8
Consultado: 23/04/2018

13. Agencia Española de Protección de Datos - Guía Listado de Cumplimiento Normativo del RGPD
Link: https://www.aepd.es/media/guias/guia-listado-de-cumplimiento-del-rgpd.pdf
Consultado: 25/05/2018

14. Agencia Española de Protección de Datos – Herramienta Facilita
Link: https://www.servicios.agpd.es
Consultado: 20/04/2018

15. Agencia Española de Protección de Datos – FAQS
Link:
https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/detallePreguntaFAQ.jsf?idPregunta=FAQ%2F00026
Consultado: 24/05/2018

11. Anexos

11.1. Anexo 1 – Diccionario de Acrónimos

1. **AEE**: Área Económica Europea
2. **AGPD**: Agencia Española de Protección de Datos
3. **APD**: Agencia de Protección de Datos
4. **BBDD**: Bases de datos
5. **CMM**: Capability Maturity Model
6. **COBIT**: Control Objectives for Information Systems and related Technology
7. **CPD**: Centro de procesamiento de datos
8. **DPIA**: Data Protection Impact Assesment
9. **DPO**: Data Protection Officer
10. **EIPD**: Evaluación de Impacto en la Protección de Datos
11. **ERP**: Enterprise resource planning
12. **FMC**: Formularios de medidas correctivas
13. **GDPR**: General Data Protection Regulation
14. **ICD**: Indicadores claves de desempeño
15. **ISO**: International Organization for Standardization
16. **LOPD**: Ley Orgánica de Protección de Datos
17. **PIA**: Privacy Impact Assessment
18. **PYME**: Pequeña y mediana empresa
19. **RGPD**: Reglamento General de Protección de Datos
20. **SGSI**: Sistema de gestión de la seguridad de la información
21. **SLA**: Service level agreement

11.2. Anexo 2 – Plantilla GAP ISO 27001

Gestión de Seguridad de la Información

Cuestionario Análisis de Brechas- Norma ISO 27001

Control	Si	Parcial	No	Observaciones	GDPR	Prioridad 1 - 2 - 3
5. POLÍTICA DE SEGURIDAD						
5.1. Política de seguridad de la información						
5.1.1. Documentar política de Seguridad de la Información			x	No se dispone de política de seguridad. Falta adaptarla la planta y firma por gerente.	SI	1
5.1.2. Revisión de la política de Seguridad de la Información			x	No se revisa, dado que no está elaborada.	SI	1
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN						
6.1. Organización Interna						
6.1.1. Compromiso de la gerencia con la seguridad de la información			x	Haría falta una firma de la política, asegurando así un compromiso.	SI	1
6.1.2. Coordinación de la Seguridad de la Información			x	Faltaría definir roles (solo está definido el DPO).	SI	1
6.1.3. Definición de las responsabilidades de Seguridad de la Información			x	Faltaría definir roles.	SI	1
6.1.4. Procesos de autorización para el uso de la infraestructura de información		X		Faltaría terminar de definirlo.	SI	1
6.1.5. Acuerdos de confidencialidad		x		Pendiente de implantación con proveedores y empleados antiguos.	SI	1
6.1.6. Contacto con autoridades			x	Incluir en plan de contingencia: agencia de protección de datos	SI	1
6.1.7. Contacto con grupos de interés			x	Crear documento con las entidades que se mantiene contacto.	SI	1
6.1.8. Revisión Independiente de la Seguridad de la Información					NO	2
6.2. Entidades externas						
6.2.1. Identificación de riesgos asociados a terceras partes			x	Controlar cumplimiento de los proveedores. Pendiente de realizar.	SI	1
6.2.2. Enfoque de la seguridad al interactuar con clientes			x	Requerimientos de terceros que se conectan a nuestra red interna. Crear procedimiento (on going).	SI	1
6.2.3. Enfoque de la seguridad en acuerdos con terceras partes			x	Pendiente definir estándar y asegurar que los diferentes proveedores lo cumplan.	SI	1
7. GESTION DE ACTIVOS						
7.1. Responsabilidad de los activos						
7.1.1. Inventario de activos		x		Consultar posibilidad trasladar la información de Excel a la plataforma PILAR.	SI	1
7.1.2. Propiedad de activos	x			Cada activo esta asociado un owner.	SI	1
7.1.3. Uso adecuado de activos		x		Faltaría terminar de definir un documento estandar.	SI	1
7.2. Clasificación de la Información						
7.2.1. Guía para la clasificación			x		SI	1
7.2.2. Identificación y manejo de la información			x		SI	1
8. SEGURIDAD DE LOS RECURSOS HUMANOS						
8.1. Previo al empleo						
8.1.1. Funciones y Roles de seguridad			x	Resp datos, Encarg datos, DPO, Personal IT, Empresas proveedoras.	SI	1
8.1.2. Selección y verificación de candidatos					NO	3
8.1.3. Términos y condiciones de empleo			x	Solicitar a proveedores documento de cumplimiento.	SI	1
8.2. Durante el empleo						
8.2.1. Responsabilidades de la gerencia			x	Difusión de la política de seguridad a nivel interno y externo.	SI	1
8.2.2. Concientización, educación y entrenamiento en la seguridad de la información.			x	Curso de formación, evidencias escritas de comunicación.	SI	1
8.2.3. Proceso disciplinario					NO	2
8.3. Finalización o cambio de empleo						
8.3.1. Finalización de responsabilidades			x	Clausulas de confidencialidad, hay que recordarlas a la finalización del contrato.	SI	1
8.3.2. Devolución de activos			x	Será necesario definir un formulario que indique todos los activos que tiene un trabajador.	SI	1
8.3.3. Retiro de los permisos de acceso		x		Faltaría definirlo más a fondo y contemplar todas las opciones (usuarios antiguos, etc.).	SI	1

9. SEGURIDAD FÍSICA Y AMBIENTAL						
9.1. Áreas seguras						
9.1.1. Controles de seguridad física		x		Se debería plantear disponer de más seguridad en departamentos como RRHH.	SI	1
9.1.2. Controles físicos de entrada	x				SI	1
9.1.3. Seguridad en oficinas, cuartos y edificios					NO	2
9.1.4. Protección contra amenazas externas y ambientales	x			Plan de emergencia / evacuación y simulacros.	SI	1
9.1.5. Trabajo en áreas seguras					NO	2
9.1.6. Áreas de acceso pública, carga y entrega					NO	2
9.2. Seguridad de los equipos						
9.2.1. Ubicación y protección de equipamiento	x			SAI y accesos no autorizados.	SI	1
9.2.2. Suministros de soporte	x			Equipos críticos conectados al SAI.	SI	1
9.2.3. Seguridad en el cableado					NO	3
9.2.4. Mantenimiento de equipos		x		Pendiente revisión anual de SAIs.	SI	1
9.2.5. Seguridad de los equipos fuera de las instalaciones					NO	2
9.2.6. Desecho y/o "reutilización" seguro de los equipos	x			Formateo de equipo según procedimiento corparativo.	SI	1
9.2.7. Retiro de propiedad			x	Debería haber un formulario para sacar equipos/información de la planta.	SI	1
10.1. Responsabilidad y procedimientos operacionales						
10.1.1. Procedimientos operacionales documentados					NO	3
10.1.2. Administración de cambios					NO	3
10.1.3. Segregación de funciones					NO	3
10.1.4. Separación de ambientes ("facilities")					NO	3
10.2. Gestión de servicios por terceras partes						
10.2.1. Entrega de servicios			x	Solicitar cumplimiento a terceros.	SI	1
10.2.2. Monitoreo y revisión de los servicios de terceros			x	Solicitar cumplimiento a terceros.	SI	1
10.2.3. Administración de cambios en los servicios de terceros			x	Solicitar cumplimiento a terceros.	SI	1
10.3. Planificación y aceptación del sistema						
10.3.1. Gestión de la Capacidad					NO	2
10.3.2. Aceptación de sistemas					NO	3
10.4. Protección contra código móvil y malicioso						
10.4.1. Controles contra software malicioso		x		Antivirus. Faltarían Procedimientos de buen uso y campañas de concienciación.	SI	1
10.4.2. Controles contra código móvil					NO	2
10.5. Back-up						
10.5.1. Copia de respaldo de información		x		Realizar una checklist mensual para testear el correcto funcionamiento.	SI	1
10.6. Gestión de seguridad en la red						
10.6.1. Controles de red					NO	2
10.6.2. Seguridad de servicios de red					NO	2
10.7. Gestión de soportes						
10.7.1. Gestión de los medios removibles					NO	2
10.7.2. Eliminación de medios		x		Existe práctica, pero NO procedimiento elaborado.	SI	1
10.7.3. Procedimientos para el manejo de información		x		Los procedimientos existen pero no hay comunicación suficiente.	SI	1
10.7.4. Seguridad de la documentación de los sistemas		x		Existen permisos por directorio activo.	SI	1
10.8. Intercambio de información						
10.8.1. Políticas y procedimientos de intercambio de información					NO	3
10.8.2. Acuerdos de intercambio		x		Acuerdos de uso de información confidencial en función del grado de sensibilidad.	SI	1
10.8.3. Medios físicos en tránsito					NO	3
10.8.4. Mensajería electrónica	x			Existen herramientas corporativas. OFICE365.	SI	1
10.8.5. Sistemas de información de negocio		x		Crear los PIA (Privacy impact assessment) antes de firmar los contratos con los proveedores.	SI	1

10.9. Servicios de comercio electrónico						
10.9.1. Comercio electrónico	x			No aplica		
10.9.2. Transacciones en línea	x			No aplica		
10.9.3. Información de acceso publico	x			No aplica		
10.10. Monitoreo						
10.10.1.Registro de eventos					NO	3
10.10.2.Monitoreo del uso de los sistemas					NO	3
10.10.3.Protección de la información de registros					NO	3
10.10.4.Registros del administrador y operador					NO	3
10.10.5.Registro de fallas					NO	
10.10.6.Sincronización de relojes					NO	3
11. CONTROL DE ACCESO						
11.1. Requerimientos de negocio para el control del acceso						
11.1.1. Política de control de acceso		x		No hay un control de la totalidad de aplicaciones.	SI	1
11.2. Gestión de accesos de usuarios						
11.2.1. Registro de usuarios		x		Faltaría definir un documento.	SI	1
11.2.2. Gestión de privilegios			x	Con cambios de dpto no se restringen accesos anteriores. Es necesario implementar un control.	SI	1
11.2.3. Gestión de contraseñas de usuarios	x			Se ha definido un procedimiento para la creación de contraseñas seguras y el cambio de estas.	SI	1
11.2.4. Revisión de los derechos de acceso de los usuarios			x	No se actualiza ni se revisa.	SI	1
11.3. Responsabilidades de usuario						
11.3.1. Uso de contraseñas		x		No se ha definido del todo	SI	1
11.3.2. Equipos de usuarios desatendidos	x			Política por GPO (políticas de grupo), cada 5 min se bloquea el ordenador.	SI	1
11.3.3. Política de escritorio y pantalla limpia					NO	2
11.4. Control de acceso a redes						
11.4.1. Política para el uso de servicios de red	x			Políticas de directorio activo.	SI	1
11.4.2. Autenticación del usuario para conexiones externas	x			Se crea un usuario con restricciones para los proveedores.	SI	1
11.4.3. Identificación de equipos en las redes	x			Sí, para entornos de testeo.	SI	1
12.2.1. Validación de los datos de entrada					NO	3
12.2.2. Control del procesamiento interno					NO	3
12.2.3. Integridad de mensajes					NO	3
12.2.4. Validación de datos de salida					NO	3
12.3. Controles criptográficos						
12.3.1. Política en el uso de controles de encriptación			x	No se ha implementado política alguna al respecto.	SI	1
12.3.2. Administración de claves			x	No se cifran los documentos de claves.	SI	1
12.4. Seguridad de los archivos del sistema						
12.4.1. Control del software operacional					NO	3
12.4.2. Protección de los datos de prueba del sistema					NO	3
12.4.3. Control de acceso al código fuente de programas					NO	3
12.5. Seguridad en el desarrollo y soporte de procesos						
12.5.1. Procedimiento de control de cambios					NO	3
12.5.2. Revisión técnica de aplicaciones después de cambios al sistema operativo					NO	3
12.5.3. Restricciones en los cambios a los paquetes de software					NO	3
12.5.4. Fuga de información					NO	3
12.5.5. Desarrollo de software en outsourcing					NO	3
12.6. Gestión de vulnerabilidades técnicas						
12.6.1. Control de debilidades técnicas de seguridad			x	No se ha definido	SI	1

13. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN						
13.1. Informes de los eventos de seguridad de la información y vulnerabilidades						
13.1.1. Reporte de eventos de seguridad de la información			x		SI	1
13.1.2. Reporte de debilidades de seguridad			x		SI	1
13.2. Gestión de incidentes y mejoras de seguridad de la información						
13.2.1. Responsabilidades y procedimientos		x			SI	1
13.2.2. Aprender de los incidentes de seguridad de la información			x	Investigar los incidentes más relevantes.	SI	1
13.2.3. Recolección de evidencia			x	Investigar los incidentes más relevantes.	SI	1
14. GESTIÓN DE CONTINUIDAD DEL NEGOCIO						
14.1. Gestión de los aspectos de seguridad de la continuidad del negocio						
14.1.1. Inclusión de la información de seguridad en el proceso de administración de la continuidad del negocio	x			Plan de contingencia.	SI	1
14.1.2. Continuidad del negocio y evaluación de riesgos	x			Plan de contingencia.	SI	1
14.1.3. Desarrollo e implementación de planes de continuidad incluyendo seguridad de la información	x			Plan de contingencia.		
14.1.4. Modelo para la planeación de la continuidad del negocio	x			Definido por Gerencia.	SI	1
14.1.5. Prueba, mantenimiento y re-evaluación de los planes de continuidad del negocio		x		Falta evidenciar mediante informe.	SI	1
15. CUMPLIMIENTO						
15.1. Cumplimiento de los requerimientos legales						
15.1.1. Identificación de la legislación aplicable		x			SI	1
15.1.2. Derechos de propiedad intelectual (IPR)					NO	3
15.1.3. Protección de los registros de la organización		x		Será necesario hacer una revisión general y actualizar los contratos antiguos.	SI	1
15.1.4. Protección y privacidad de la información personal		x		On going.	SI	1
15.1.5. Prevención del mal uso de la infraestructura para el procesamiento de información	x			Sí, se ha enviado una circular al respecto.	SI	1
15.1.6. Regulación de controles criptográficos					NO	3
15.2. Cumplimiento de las políticas y estándares de seguridad y cumplimiento técnico						
15.2.1. Cumplimiento de políticas y estándares de seguridad		x		On going.	SI	1
15.2.2. Verificación del cumplimiento técnico					NO	2
15.3. Consideraciones de auditoria de sistemas de información						
15.3.1. Controles de auditoría de los sistemas de información					NO	3
15.3.2. Protección de herramientas de auditoria de los sistemas de información					NO	3

Ilustración 19 Plantilla Controles ISO 27001:2013

11.3. Anexo 3 – Herramientas de Utilidad

Existen diversas herramientas software que facilitan la mayor parte de las tareas implicadas en llevar a cabo la adaptación del RGPD, ya que facilitan su implantación, gestión y mantenimiento de forma sencilla y ágil.

Las principales ventajas que ofrecen estas herramientas son la agilidad para gestionar e implementar las tareas de adaptación al RGPD y además proporcionan un mantenimiento automatizado, ya que podemos realizar la programación para llevar a cabo las auditorias y reuniones según su necesidad.

Todo esto sin utilizar papeles, ya que todo queda registrado en la plataforma y además algunas disponen de un gestor documental para gestionar toda la información inherente a la normativa RGPD con total trazabilidad de las acciones realizadas.

A continuación, se nombran e incluyen capturas de algunas de las más conocidas obtenidas de sus versiones demo.

GlobalSUITE – Data Protection (GDPR)

GlobalSUITE – Data Protection (GDPR) es un software concebido para servir de ayuda en la implantación, gestión y mantenimiento del Reglamento General de Protección de Datos a través de un proceso sencillo, ágil, automatizado y trazable.

Las principales características que incluye junto con algunas capturas son:

- Asistente para el análisis de impacto (PIA).
- Asistente para el análisis de riesgos asociados.
- Gestión y definición de tratamientos de datos.
- Gestión de controles implantados.
- Control de cesiones de datos, proveedores y encargos de tratamiento.
- Cláusulas legales predefinidas.
- Gestor Documental.
- Cuadro de mando de indicadores.
- Cuadro de control de cumplimiento.

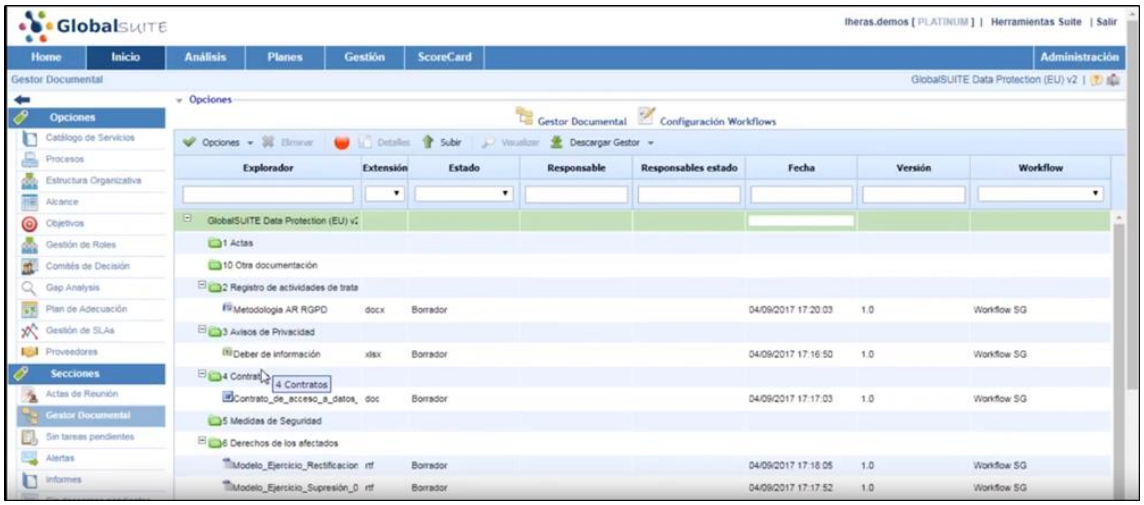


Ilustración 20 GlobalSUITE Gestor Documental

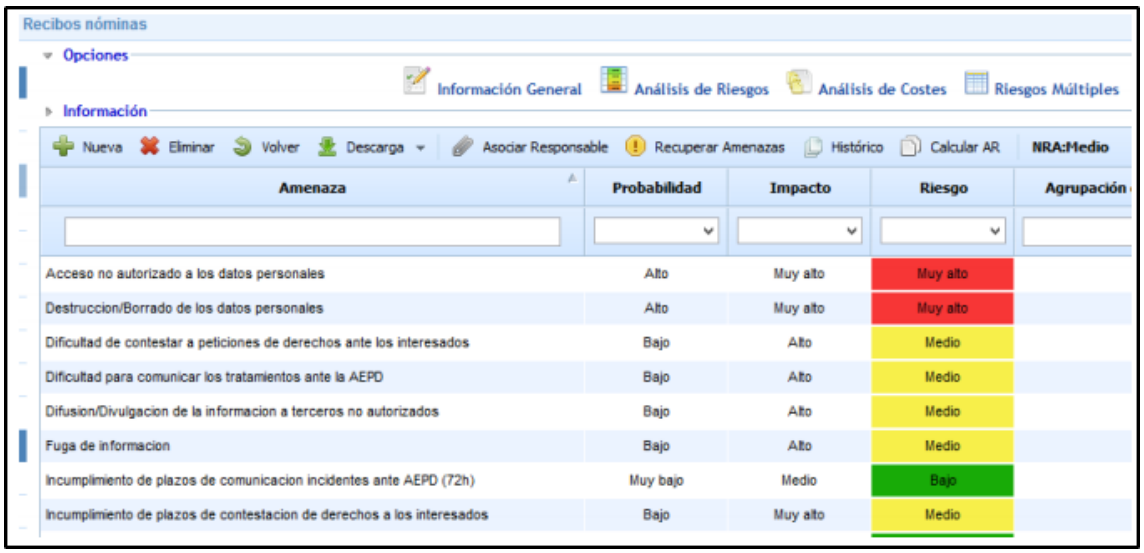


Ilustración 21 GlobalSUITE Análisis de Riesgos

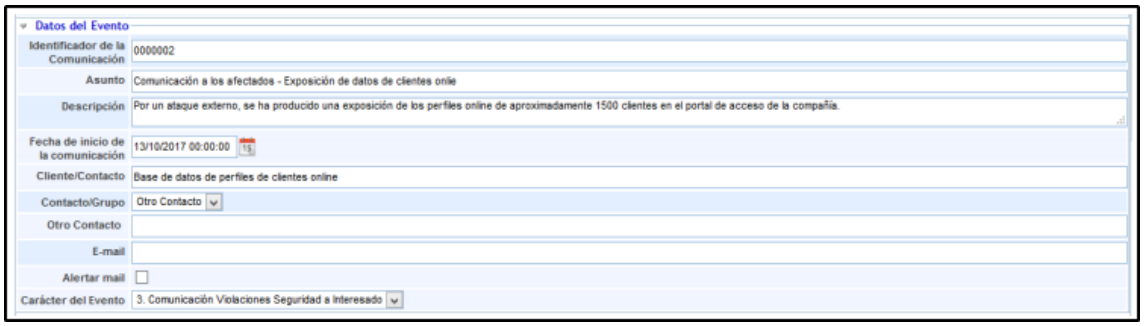


Ilustración 22 GlobalSUITE Comunicación de Eventos

One Trust

One Trust es un software integral para la gestión de privacidad empresarial orientado a operar el cumplimiento del RGPD y la privacidad por diseño.

Se trata de un software utilizado por más de 1500 organizaciones para cumplir con las normas relativas a la privacidad de datos a través de diversas jurisdicciones, incluido el RGPD de la UE.

Las principales características que incluye junto con algunas capturas son:

- Herramienta de preparación y cumplimiento de responsabilidades.
- Automatización de evaluaciones de impacto (PIA y DPIA).
- Automatización de registros de tratamientos de datos.
- Consentimiento de cookies y escaneo de sitios web.
- Portal de solicitudes de acceso de interesados.
- Gestión de consentimientos.
- Gestión de riesgos de proveedores.
- Gestión de incidentes y violaciones de la seguridad.

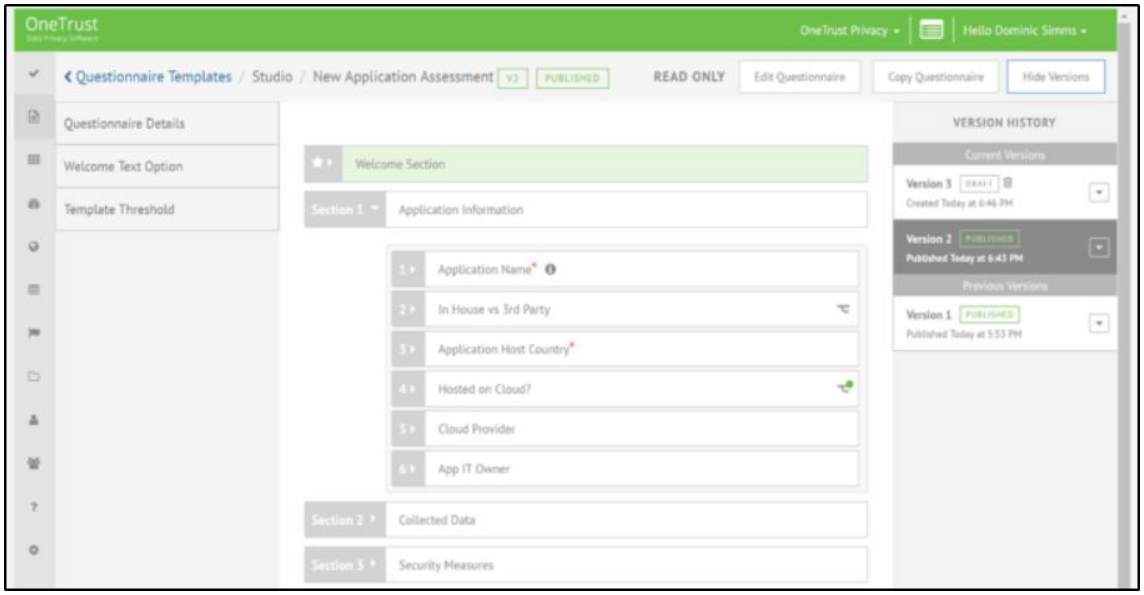


Ilustración 23 One Trust Cuestionario DPIA

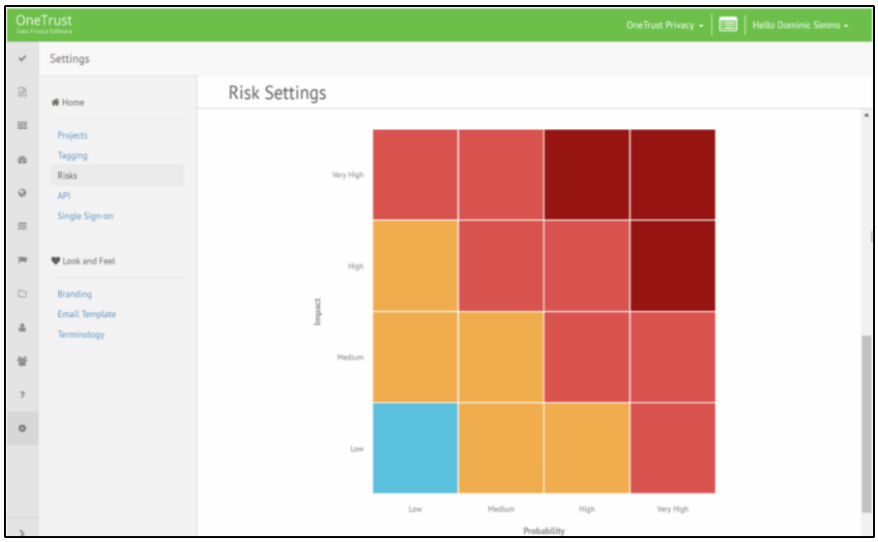


Ilustración 24 One Trust Configuración de Riesgos

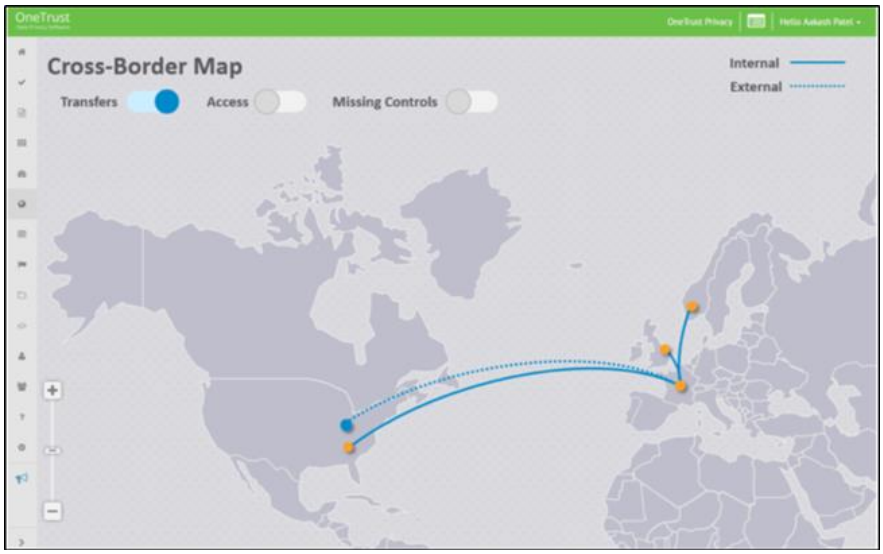


Ilustración 25 One Trust Flujo de Datos

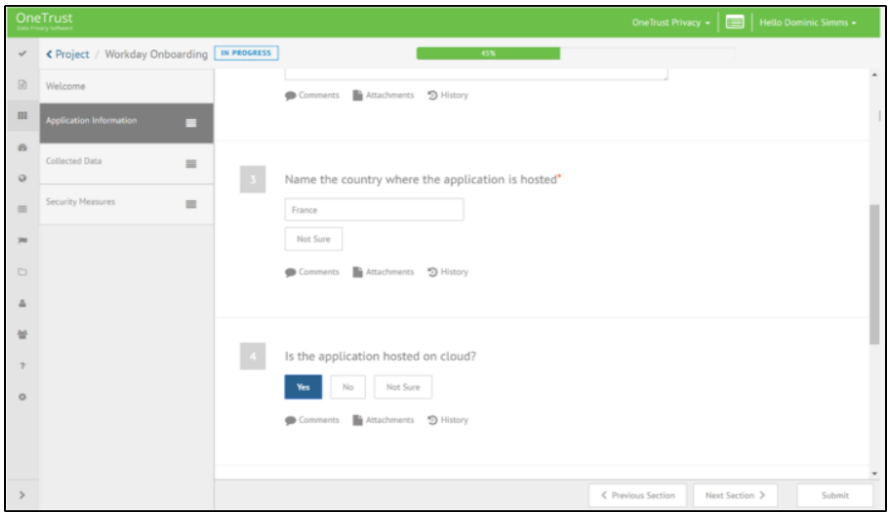


Ilustración 26 One Trust Mantenimiento de Aplicaciones

Pilar / Magerit

Pilar de Magerit se trata de un software orientado al análisis y gestión de riesgos de los sistemas de información siguiendo la metodología de Magerit.

Se analizan los riesgos en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

Para el tratamiento de estos riesgos se proponen: salvaguardas, normas de seguridad y procedimientos de seguridad analizándose el riesgo residual a lo largo de las diversas etapas de tratamiento.

Se analiza el efecto de las interrupciones de servicio teniendo en cuenta la duración de la interrupción.

Para el tratamiento del riesgo se proponen: salvaguardas, elementos de respaldo y planes de recuperación de desastres.

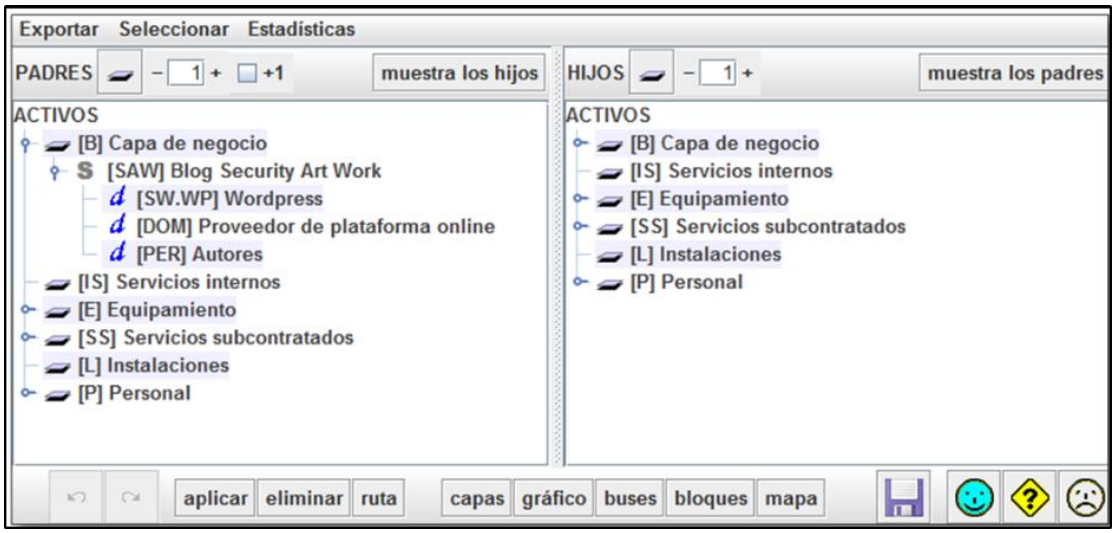


Ilustración 27 Pilar Inventario de Activos

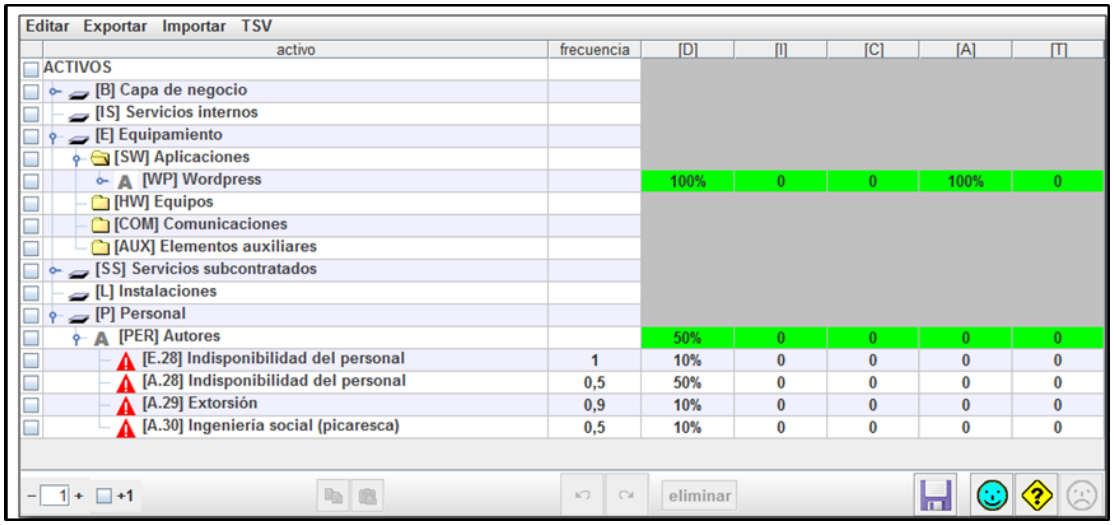


Ilustración 28 Pilar Análisis de Riesgos

11.4. Anexo 4 – Listado de Cumplimiento del RGPD

LISTADO DE CUMPLIMIENTO DEL RGPD	CUMPLE SI/NO
PRINCIPIOS RELATIVOS AL TRATAMIENTO	
Se recogen los datos personales con fines determinados	SI
Se recogen los datos personales con fines explícitos	SI
Se recogen los datos personales con fines legítimos	SI
Se tratan ulteriormente de manera incompatible con otros fines	
Los datos personales se mantienen exactos	SI
Se mantienen actualizados	SI
Se rectifican los datos personales inexactos respecto de la finalidad	
Se suprimen los datos personales inexactos respecto de la finalidad	
Se mantienen durante más tiempo del necesario respecto de la finalidad	
Se tratan con fines de archivo en interés público	
Se tratan con fines de investigación científica	
Se tratan con fines históricos	
Los datos personales se tratan con fines estadísticos	
Se han implantado medidas de seguridad para proteger la integridad y confidencialidad de los datos	SI
Se han implantado medidas de seguridad contra el tratamiento no autorizado o ilícito de los datos	SI
Se han implantado medidas de seguridad para evitar su pérdida, destrucción o daño accidental	SI
Se mantiene la trazabilidad de los fines del tratamiento	SI
LICITUD DEL TRATAMIENTO	
Se tiene consentimiento para cada finalidad del tratamiento	SI
El tratamiento es necesario para ejecutar un contrato o precontrato	SI
Existe obligación legal	SI
El tratamiento es necesario para proteger intereses vitales	SI
El tratamiento es necesario para el cumplimiento de interés público	
El tratamiento es necesario para satisfacer intereses legítimos	SI
CONDICIONES PARA EL CONSENTIMIENTO	
Se puede demostrar que el afectado dio su consentimiento para el tratamiento	SI
Se puede demostrar que el tratamiento se realiza como resultado del cumplimiento de una obligación legal	SI
Se solicita el consentimiento de forma clara e independiente de los demás asuntos	SI
Se solicita el consentimiento de forma inteligible y de fácil acceso	SI
Se solicita usando lenguaje claro y sencillo	SI
Se informa con carácter previo a recabar el consentimiento	SI
Se permite retirar el consentimiento con la misma facilidad que se recaba	SI
Se ofrecen medios para retirar el consentimiento en cualquier momento	SI
Se recaba el libre consentimiento	SI
Para prestar un servicio se solicitan sólo los datos necesarios	SI
Para ejecutar un contrato se solicitan sólo los datos necesarios	SI

DERECHOS DEL INTERESADO. TRANSPARENCIA DE LA INFORMACIÓN	
Se toman medidas para facilitar al interesado toda la información relativa al tratamiento	SI
La información se facilita de forma concisa, transparente e inteligible	SI
La información se facilita en lenguaje claro y sencillo	SI
Se facilita por escrito o por otros medios, incluidos los electrónicos	SI
Se facilita verbalmente, previa acreditación de su identidad	SI
Se facilita al interesado el ejercicio de sus derechos	SI
Se atienden las peticiones del ejercicio de derechos aunque el tratamiento no requiera identificación salvo que no se pueda identificar al interesado	SI
Se informa al interesado en el plazo de un mes desde la recepción de su solitud	SI
Se informa ante el ejercicio de derechos complejos o ante muchas solicitudes en el plazo máximo de tres meses desde la recepción de la solicitud	
Se informa en el plazo de un mes de la prórroga de tres meses indicando el motivo de la dilación	
Se permite a los interesados el ejercicio de derechos por medios electrónicos	
Se informa por medios electrónicos cuando se recibe la solicitud por esos medios salvo que solicite que se realice por otro medio	SI
Se informa de las razones de la no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales, en el plazo de un mes desde la recepción de la solicitud cuando no se da curso a la solicitud	
Se facilita gratuitamente el ejercicio de derechos	SI
Se solicita información para acreditar la identidad de la persona física que ejerce sus derechos	SI
Cuando la información que se facilita utiliza iconos normalizados, el formato electrónico es legible mecánicamente	

DERECHOS DEL INTERESADO. DERECHO DE ACCESO	
Se informa respecto a los fines del tratamiento	SI
Se informa de las categorías de datos personales que se tratan	SI
Se informa de los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales	SI
Se informa del plazo previsto de conservación de los datos personales	SI
Se informa de los criterios utilizados para determinar el plazo de conservación	SI
Se informa del derecho a solicitar la rectificación o supresión de sus datos	SI
Se informa del derecho a solicitar la limitación del tratamiento de los datos	SI
Se informa del derecho a solicitar la oposición al tratamiento	
Se informa del derecho a presentar una reclamación ante una autoridad de control	SI
Se proporciona información sobre el origen de los datos cuando no recogen del propio interesado	
Se facilita copia de los datos personales objeto de tratamiento cuando el interesado lo solicita	SI
Se facilita la información en formato electrónico de uso común si lo solicita por medios electrónicos salvo que se facilite otro medio	SI

DERECHOS DEL INTERESADO. DERECHO DE SUPRESIÓN («EL DERECHO AL OLVIDO»)	
Se suprimen los datos cuando no son necesarios en relación con los fines para los que fueron recogidos	SI
Se suprimen los datos cuando se retira el consentimiento en que se basa el tratamiento	SI
Se suprimen los datos cuando se opone al tratamiento	SI
Se suprimen los datos cuando han sido tratados ilícitamente	SI
Se suprimen los datos cuando lo exige una obligación legal	SI
Se suprimen los datos cuando se obtienen en relación con la oferta de servicios de la sociedad de la información	SI

RESPONSABILIDAD DEL RESPONSABLE DEL TRATAMIENTO	
Se tiene en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento para garantizar y poder demostrar que el tratamiento es conforme con el RGPD	SI
Se tienen en cuenta los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas	SI
Se aplican medidas técnicas y organizativas apropiadas	SI
Las medidas se revisan y actualizan cuando es necesario	SI
Se han confeccionado políticas de protección de datos	SI
Se aplican las políticas de protección de datos	SI
PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO	
Se analizan las medidas técnicas y organizativas apropiadas antes de determinar los medios de tratamiento	SI
Durante el diseño del tratamiento se tienen en cuenta las medidas técnicas y organizativas apropiadas para cumplir con el RGPD	SI
Durante el tratamiento se aplican las medidas que han sido determinadas	SI
Durante el tratamiento se comprueba la efectividad de las medidas aplicadas	SI
Se aplican medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo se tratan datos necesarios para cada uno de los fines	SI
Se aplican medidas técnicas y organizativas teniendo en cuenta la cantidad de datos personales recogidos, la extensión del tratamiento, el plazo de conservación y la accesibilidad	SI
Las medidas garantizan que, por defecto, los datos no son accesibles a un número indeterminado de personas físicas, sin la intervención de personal	SI
ENCARGADO DEL TRATAMIENTO	
Se eligen los que ofrecen garantías suficientes conforme con los requisitos del RGPD y garantizando la protección de los derechos del interesado	SI
El encargado del tratamiento no recurre a otro encargado sin la autorización previa por escrito	SI
El tratamiento por el encargado se rige por un contrato u otro acto jurídico vinculante con arreglo a las normas de Derecho	
El contrato establece el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados así como las obligaciones y derechos del responsable	SI
El contrato establece que se tratan los datos personales únicamente siguiendo instrucciones documentadas del responsable	SI
El contrato garantiza que las personas autorizadas para tratar datos personales se han comprometido a respetar la confidencialidad o están sujetas a una obligación de confidencialidad de naturaleza estatutaria	SI
El contrato establece que se tomarán las medidas de seguridad necesarias	SI
El contrato establece que se respetarán las condiciones indicadas para recurrir a otro encargado del tratamiento	SI
El contrato establece que el encargado asistirá para que se pueda responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados	SI
El contrato establece que se suprimirán o devolverán los datos personales una vez finalice la prestación de los servicios, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales	SI
El contrato establece que pondrá a disposición toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas, así como para permitir y contribuir a la realización de auditorías e inspecciones, por parte del responsable o de otro auditor autorizado por el responsable	SI
El contrato establece que si el encargado del tratamiento recurre a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se imponen a este otro encargado las mismas obligaciones de protección de datos que las estipuladas en el contrato, mediante contrato u otro acto jurídico establecido con arreglo a Derecho	SI
El contrato consta por escrito	SI
Sólo se accede a los datos siguiendo instrucciones del responsable	SI

REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO	
Se lleva un registro de las actividades de tratamiento	SI
El registro recoge el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos	SI
El registro recoge los fines del tratamiento	SI
Recoge una descripción de las categorías de interesados y de las categorías de datos personales	SI
Recoge las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales	SI
Recogen las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional	
Incluye los plazos previstos para la supresión de las categorías de datos	SI
Incluye una descripción general de las medidas técnicas y organizativas apropiadas al riesgo de los tratamientos	SI
SEGURIDAD DEL TRATAMIENTO	
Para determinar las medidas a aplicar se tiene en cuenta el estado de la técnica, costes de aplicación, y la naturaleza, alcance, contexto y fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas	SI
Se aplican las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo	SI
Se han incluido medidas para asegurar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento	SI
Medidas para asegurar la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico	SI
Existe un proceso de verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento	SI
Se han tenido en cuenta los riesgos que presenta el tratamiento como consecuencia de su destrucción, pérdida o alteración accidental o ilícita que son transmitidos, conservados o tratados, o la comunicación o acceso no autorizados a dichos datos para evaluar el nivel de seguridad aplicado	SI
Se han tomado medidas para garantizar que las personas autorizadas a acceder a datos sólo los tratan siguiendo instrucciones	SI
NOTIFICACIÓN DE BRECHAS DE LA SEGURIDAD DE LOS DATOS PERSONALES A LA AUTORIDAD DE CONTROL	
Se ha establecido un procedimiento para identificar y gestionar las brechas de seguridad	SI
Existe un procedimiento para que los encargados del tratamiento notifiquen las brechas al responsable en el momento en que tengan conocimiento de ellas	SI
Existe un procedimiento para notificar a la autoridad de control en el plazo de 72 horas	SI
Existe un procedimiento para documentar los motivos por los que no se puede notificar en el plazo de 72 horas	SI
Existe un procedimiento para facilitar la información de manera gradual cuando no es posible facilitarla simultáneamente	SI
Se documenta cualquier brecha de seguridad de los datos personales	SI
En la documentación se incluyen los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas	SI
Se ha comprobado que el procedimiento de notificación funciona	SI
COMUNICACIÓN DE UNA BRECHA AL INTERESADO	
Existe un procedimiento para comunicar la brecha sin dilación indebida cuando sea probable que entrañe un alto riesgo para los derechos y libertades	SI
La comunicación al interesado, se lleva a cabo en un lenguaje claro y sencillo, describe la naturaleza de la brecha	SI

EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS	
Se recaba el asesoramiento del DPD	
Se realiza EIPD antes del tratamiento cuando es probable que entrañe un alto riesgo para los derechos y libertades de las personas	
Se realiza una EIPD antes en tratamientos a gran escala de categorías especiales de datos o relativos a condenas e infracciones penales	
Se realiza una EIPD antes de tratamiento que suponen una observación sistemática a gran escala de una zona de acceso público	
Se realiza una EIPD en operaciones de tratamiento incluidas en la lista publicada por la autoridad de control	
La EIPD incluye una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, y cuando procede el interés legítimo perseguido	
Incluye una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad	SI
La EIPD incluye una evaluación de los riesgos para los derechos y libertades	SI
Incluye medidas previstas para demostrar la conformidad con el RGPD, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas	
Incluye las medidas previstas para afrontar los riesgos, garantías y mecanismos para garantizar la protección de datos	
Se reexaminan las EIPD siempre que es necesario y cuando exista un cambio de los riesgos que representen las operaciones de tratamiento	SI
Se consulta a la autoridad de control antes de proceder al tratamiento cuando una EIPD muestre que el mismo entrañaría un alto riesgo si no se toman medidas para mitigarlo	
Se informa de las responsabilidades respectivas de los implicados en el tratamiento en la consulta a la autoridad de control	
Se informa de los fines y medios del tratamiento previsto en la consulta	
Se informa de las medidas y garantías establecidas para proteger los derechos y libertades en la consulta	
Se facilitan los datos de contacto del delegado de protección de datos	
Se incluye la evaluación de impacto	
Cuando se consulta se facilita cualquier información adicional que solicite la autoridad de control	
DELEGADO DE PROTECCIÓN DE DATOS	
Se ha designado un DPD por requerimiento legal	
Se ha designado un DPD atendiendo a sus cualidades de profesionalidad, conocimientos y competencias en la materia	SI
Se han publicado los datos de contacto del DPD y se ha comunicado a la autoridad de control	SI
Se garantiza que el DPD participa de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales	SI
Se da respaldo en el desempeño sus funciones	SI
Se le facilitan los recursos necesarios para el desempeño de sus funciones, el acceso a los datos personales y a las operaciones de tratamiento	SI
Se le facilitan los recursos necesarios para mantener sus conocimientos	SI
Se garantiza que el DPD no recibe ninguna instrucción en lo que respecta al desempeño de sus funciones	SI
No se puede destituir ni sancionar al DPD por desempeñar sus funciones	SI
El DPD rinde cuentas directamente al más alto nivel jerárquico	SI
El DPD atiende las solicitudes de los interesados	SI
El DPD está obligado a mantener la confidencialidad en el desempeño de sus funciones	SI
Si el DPD desempeña otras funciones, se garantiza que no dan lugar a conflicto de intereses	SI
Las funciones del DPD son informar, asesorar y formar al personal de las obligaciones que les incumben	SI

Ilustración 29 Guía para el cumplimiento del RGPD