Universidad Zaragoza
1542

Trabajo Fin de Grado

Protección de datos:
Análisis de la web de Gabinete Jurídico Jiloca

Autor/es

Jesús M. Pascual Martín

Director/es

María Jesús Lapeña Marcos

Facultad de Economía y Empresa

2020/2021

ÍNDICE

ÍNDICE DE ILUSTRACIONES

1. Introducción

A día de hoy el intercambio de productos y servicios a través de internet, más conocido como e-commerce, se ha convertido en una herramienta imprescindible para las empresas de la gran mayoría de sectores. Esta forma de comercio nos ofrece la posibilidad de llegar a un gran volumen de potenciales clientes a través de nuestra página web, dando lugar a un nuevo escenario competitivo en el que pueden competir las empresas.

Dentro de esta actividad desarrollada dichas empresas incurren en el tratamiento de datos de sus clientes, los cuales, en muchas ocasiones son de carácter personal y hacen identificables a los mismos dando lugar de esta manera a que dichas empresas deban de adecuarse a la normativa que rige el tratamiento de este tipo de datos.

Es por ello que toda página web de empresa que opte a una cuota de mercado online deberá encontrarse adecuada al cumplimiento de la normativa de protección de datos, siendo el incumplimiento de la misma penalizable con cuantiosas multas por las consecuencias que una filtración de dichos datos podría acarrear.

En este trabajo nos centraremos en este aspecto de adecuación a la normativa vigente de protección de datos para asegurar la calidad y seguridad del sitio web de Gabinete Jurídico Jiloca.

1.1 Planteamiento del problema y trascendencia

En el mundo del comercio electrónico, a menudo debemos introducir datos personales que nos hacen en la mayoría de ocasiones dudar sobre si continuar la compra o no. Esto es así porque no sabemos qué tratamiento ni fines seguirán los mismos. Sabemos que son necesarios, pero no si los utilizarán con fines comerciales o incluso si venderán esos datos a otras compañías sin enterarnos.

Ahí comienza el problema del usuario con la protección de datos: inseguridad, desinformación y falta de comprensión.

Si abordamos el tema desde la posición de la empresa, vemos que muchas personas contratan la creación de una página web o incluso la hacen ellos mismos, sin saber de seguridad. Esto supone un gran riesgo para la persona responsable de la empresa, que puede estar infringiendo la normativa y acabar pagando multas por su desinformación.

1.2 Justificación

Hace ya varios años que nos encontramos en una dinámica continuada de crecimiento de la compra online en todos los sectores, llegando a ser más relevante si cabe a raíz del impulso generado por el Covid-19. Como bien refleja el estudio anual del ecommerce realizado por Elogia, se ha producido un aumento en 2021 del nivel de penetración en España pasando de un 72% a un 76%.

La excelencia de un sitio web no solo ayudará a la empresa a encontrarse mejor posicionada en buscadores, sino que aspectos de gran relevancia como un cuidado sistema de protección datos que cumpla con la normativa pasarán a ser un factor de diferenciación para la empresa, el cual proporcionará fidelización y retención de clientes. Toda empresa que cumpla con la normativa vigente de protección de datos podrá garantizar a sus clientes que sus datos no corren ningún peligro otorgando a la misma una mayor relevancia, mejor imagen empresarial, o un aumento de la confianza de los clientes, entre otras cosas.

Debemos ser conscientes de la importancia de la seguridad informática, con el objetivo de evitar aquellas operaciones que no estén autorizadas en cuanto a información personal en sistemas o redes informáticas. El término de seguridad informática engloba distintas partes: cumplir las normas y leyes, asegurar la confidencialidad y privacidad de los usuarios, tener localizada la información íntegra y evitar los incidentes y las interrupciones de virus. Vigilando y cumpliendo todo ello, podremos decir que la página web es segura, lo que repercutirá de una forma muy positiva en la experiencia del usuario.

La protección de datos es un tema al que muchas personas no dan la importancia que merece, cometiendo a diario miles de errores que resultan ser ilegalidades en el marco normativo de la seguridad informática. Uno de los más comunes, es la aceptación de las cookies: los usuarios deberían aceptarlas proactivamente y pudiendo elegir siendo diferenciadas por su objetivo (analítica, rastreo…), algo que en multitud de webs no ocurre. Además, es muy complicado rechazarlas y en la mayoría de páginas no se especifica qué finalidad tienen. Otro de los errores, que hemos comentado en el planteamiento del problema, es la dificultad del lenguaje que se utiliza para la explicación de las normativas, haciendo que el usuario no pueda comprender lo que

está, o no, consintiendo. Algunas empresas conocidas por su mal uso de los datos son Sony, Target e incluso el Gobierno de EEUU.

En cuanto a la regulación de los datos en relación con el marketing, en mayo de 18 se comenzó a aplicar un conjunto de normas denominadas Reglamento General de Protección de Datos (RGPD), el cuál aseguran que ha sido el cambio más importante de los últimos 20 años. Tras dicha mejora, las empresas han tenido que adaptarse y que comenzar a llevar a cabo procesos nuevos: controles de privacidad, auditorías periódicas, vigilar filtraciones…

Todo esto, además de afectar a la confianza del usuario para el uso de nuestro sitio web, se traduce en pérdida económica de la empresa procedente de dos vertientes: menor actividad económica (compra de productos o contratación de servicios) y mayor pago de multas por incumplimiento de la normativa.

1.3 Objetivos

Este proyecto tiene como **objetivo general** mejorar la web de Gabinete Jurídico Jiloca SL; centrándonos en un aspecto principal, la protección de datos.

Los **objetivos específicos** del mismo serán en cuanto a protección de datos:

- Adecuar el sitio a la normativa vigente de protección de datos
- Comprobar que se cumplen el RGPD (Reglamento General de Protección de Datos) y la LOPD (Ley Orgánica de Protección de Datos).

En cuanto a protección de datos, toda web de empresa deberá estar al día del cumplimiento de las normativas vigentes, impuestas por la Unión Europea y a las particulares de su respectivo país para evitar las sanciones pertinentes, como es el Reglamento Europeo 2016/79 y la publicación de la Ley Orgánica 3/2018.

Este es un aspecto de gran importancia ya que la seguridad informática en materia de protección de datos, ha cobrado un gran protagonismo como principal valedor de la calidad y fiabilidad de las páginas web en internet.

1.4 Motivación

La principal motivación que me llevó a seleccionar esta temática de Trabajo de Fin de Grado es la posibilidad de aumentar mis conocimientos acerca de todo lo relacionado con protección de datos.

Esto es así ya que considero que a día de hoy con el aumento progresivo de la rigurosidad de la normativa, la cual imparte multas cuantiosas, toda empresa que se precie deberá contar con especialistas en la materia internos o externos que la aseguren una correcta adecuación a la normativa vigente, y es por ello que para mí como profesional me parece de un gran valor poseer y ampliar conocimientos sobre esta temática.

Y en un ámbito más personal decidí seleccionarla puesto que en mi caso particular, era la ocasión perfecta para primero, poder profundizar en un tema vinculado a la rama de la carrera que más me ha apasionado, la cual es la de marketing online; y segundo, aprovechar todos los conocimientos adquirido en las prácticas que desarrolle en una agencia de marketing, la cual contaba con especialistas en protección de datos y aplicar ahora esos conocimientos al negocio familiar, generando un doble valor para este trabajo más allá de la calificación académica.

1.5 Estructura

Comenzaremos especificando el marco teórico vigente en cuestión de protección de datos, que usaremos como base para conseguir que el sitio cumpla de forma eficaz con los requisitos que se estipulan en la normativa nacional actual vigente del RGPD. Posteriormente, en el apartado de aplicación a un caso práctico, pondremos en práctica lo estipulado en el marco teórico; desarrollando una guía de cumplimiento de todo lo relativo al ámbito de protección de datos para vislumbrar qué aspectos cumple y cuáles no, así como conocer las medidas que se podrían llevar a cabo para mejorar esta situación. Finalmente elaboraremos y redactaremos las conclusiones extraídas del análisis, las limitaciones con las que nos hemos encontrado y una serie de propuestas a seguir para mejorar el cumplimiento de la normativa por parte del sitio seleccionado.

2. Marco teórico

En este apartado vamos a encontrar en primera instancia multitud de definiciones de los conceptos relacionados con calidad de sitios web, particularizando en protección de datos, entendiendo y profundizando en sus implicaciones y sensibilizándonos de la

importancia que merece. Además, realizaremos una revisión del marco normativo: leyes, normas y guías, estándares o referentes internacionales en materia de protección de datos para obtener de esta manera una idea concreta de la situación legal actual.

2.1 Calidad

La **calidad de un sitio web** va a ser el concepto general que engloba el trabajo puesto que dentro de todos los conceptos que la conforman encontramos la protección de datos. Podemos definir la calidad de un sitio web como la capacidad de sitio para satisfacer las necesidades de los usuarios y propietarios del mismo.

La calidad es relevante para la empresa, ya que a mayor calidad de la web mejor experiencia para el usuario y por lo tanto, como hemos comentado previamente, mayor probabilidad de que contrate nuestros servicios y de fidelización del mismo.

Dicha capacidad se verá afectada por el nivel de optimización de una serie de características medibles, algunas de las más importantes las siguientes:

- **Ergonomía:** entendemos esta como la capacidad de adaptación del site a las necesidades de sus usuarios.
- **Navegación:** sistema de enlaces del sitio que conducen a páginas del mismo dominio si son internos y a páginas de otros dominios si esto enlaces son externos.
- **Estética o identidad corporativa:** en la cuál tienen gran importancia la elección logo, paleta de colores seleccionada, fuentes usadas en los textos,... En definitiva, una serie de aspectos que proporcionen una imagen corporativa clara y con sentido.
- **Seguridad y cumplimiento legal:** en este apartado entrarían todos aquellos aspectos relacionados con el cumplimiento de la normativa vigente así como la capacidad de la página de proteger y mantener a salvo toda la información que circula por la misma.
- **Protección de datos personales:** conjunto de sistemas de protección, prevención y tratamiento de datos que se llevan a cabo dentro de la propia web.
- **Contenidos:** imágenes vídeos, que refuercen la imagen corporativa y quede claro a qué se dedica la entidad.

- **Diseño responsive:** capacidad del site a adaptarse a diferentes formatos de pantalla en función del dispositivo del que accedamos al mismo.
- **Accesibilidad:** concepto amplio que engloba diferentes maneras a través de las cuales el site facilita su acceso a todo tipo de usuarios en función de las características o carencias particulares de estos.
- **Usabilidad:** esta será la manera a través de la cual la página facilita su uso e interacción a los visitantes de la misma de una forma segura, sencilla, intuitiva y cómoda.
- **Posicionamiento:** conjunto de técnicas de SEO (Search Engine Optimization) que permiten al site situarse mejor en cuanto a los resultados de búsqueda para determinadas clave para llegar antes que la competencia a un público objetivo.
- **Vulnerabilidades:** nivel de defensa de la web ante usuarios maliciosos que pretendan sustraer, modificar o acceder a contenidos de carácter privado del site.
- **Tiempos de descarga:** velocidad del site para descargar o mostrar los contenidos de una de sus páginas en la ventana del navegador a sus visitantes.

2.2 Protección de datos

Cuando nos referimos a **protección de datos** en el ámbito de páginas web hablamos de todas aquellas medidas pertinentes para asegurar que la empresa posea convencimiento de que su página web se ajusta y cumple correctamente con la normativa jurídica vigente, recogiendo las medidas técnicas y organizativas necesarias para garantizar protección, confidencialidad, integridad y disponibilidad de los datos de su página web.

En muchas ocasiones los datos personales son cedidos a empresas o entidades para el tratamiento de los mismos, situaciones en las que estas organizaciones deberán de cumplir y aferrarse a una serie de obligaciones de la normativa vigente para realizar esta actividad de forma legal respetando unos derechos, a continuación vamos a comentar la normativa actual que regula estos aspectos en nuestro país.

Entendemos como **dato personal** cualquier información que permita identificar o hacer identificable a una persona física, correo, una dirección ip, una matrícula de coche, datos de geo localización, etc. y como **tratamiento de datos** cualquier operación que se realice con datos personales: modificar, almacenar, destruir, etc. dicho tratamiento

deberá de realizarse de forma justa, legal y transparente. Siendo estos datos personales obtenidos para finalidades específicas, explícitas y legítimas. Este se realizará de manera transparente, con información más completa y sencilla. Además, el consentimiento para poder tratar los datos de carácter personal ha de ser inequívoco, libre y revocable.

Respecto a los cargos que deberán tomar parte en el proceso de gestión de datos a continuación comentamos **quiénes son los responsables** de dicha información y que funciones cubren:

- **Responsable** es aquel que decide que datos se tratan y como se tratan, en un ecomerce por ejemplo el titular de la web ósea aquel el que oferta los bienes o servicios.
- **Encargado** es aquella persona física, jurídica o entidad pública que lo que hace es tratar los datos por cuenta del responsable, una gestoría, el proveedor de hosting, proveedores de mail marketing como mail chimp, en un ecommerce las empresas de transporte,... deberemos tener suscrito un contrato de encargado de tratamiento conforme al artículo 28 del reglamento y ahí se establecen las obligaciones de ese encargado en medidas de seguridad, cumplir las indicaciones, etc.

La protección de datos cobrará por tanto un papel fundamental en la constitución y correcto funcionamiento de cualquier página web ya que esta se encuentra totalmente vinculada con la seguridad de la información y el correcto tratamiento de datos en la misma, el cual deberá de realizarse acorde con la normativa vigente.

2.3 Organismo Regulador

Respecto al **organismo regulador** que se ocupa de esto en nuestro país nos encontramos con la Agencia Española de Protección de Datos, siendo esta la autoridad estatal que garantizará y tutelará el cumplimiento de la legislación de protección de datos y controlará su aplicación. Esta publicó el 25 de mayo de 2018 los nuevos derechos que tendrá cada ciudadano, los cuales vienen a completar los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) que son: derecho a conocer, derecho a solicitar al responsable, derecho a rectificar tus datos personales, derecho a suprimir tus datos personales y derecho a la oposición al tratamiento de tus datos.

Los derechos ARCO son aquellos que ya se encontraban reconocidos en la LOPD (Ley Orgánica de Protección de Datos) el derecho al olvido, el derecho a la portabilidad de los datos y el derecho a la limitación de tratamiento. Y como bien comentábamos estos son reforzados por el RGPD para proporcionar a los ciudadanos una protección homogénea a la del resto de países de la UE.

En cuanto a la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal LOPD, esta es el principio jurídico ley donde se establecen las órdenes y prohibiciones de este carácter junto con el Real Decreto 1720/2007 desarrollado a partir de esta en el cual se desarrolla la parte técnica de esta normativa. Esta ley es la normativa previa que regulaba estos aspectos antes del establecimiento del reglamento europeo, que ha pasado a relegarla a la LOPD a cubrir aquellos puntos de la normativa que el establecido RGPD no llega a cubrir. Fundamentalmente estas abogarán por garantizar y proteger el tratamiento de datos personales de las personas físicas cuando el tratamiento se realice dentro del territorio español, cuando el responsable del tratamiento se encuentre en territorio no español pero le sea aplicable la legislación española por norma de derecho internacional público o cuando no se encuentre en territorio de la UE pero use medios para el tratamiento situados en el territorio español.

Como bien comentábamos dentro de nuestro país la normativa se encuentra sujeta a al mandato por pertenencia a la Unión Europea, siendo por ello de aplicación el **RGPD,** el cual es una serie de reglas ordenadas por la autoridad competente para la ejecución de una ley que completan la LOPD y la relegan a cubrir aquellos aspectos de la normativa que este reglamento no llega a abarcar. Este RGPD fue aprobado el 27 de abril de 2016 al cual se dio un plazo para su plena adaptación hasta el 25 mayo de 2018 comenzando a ser aplicable en todos los estados miembros, el 27 abril se aprobó un real **decreto ley** más breve que una ley orgánica para poder ir trabajando en temas procedimentales que se dejaban a los estados miembros, reemplazando de esta forma a la directiva anterior 95/46/CE.

Este RGPD sigue una serie de principios de aplicación homogénea en todos los estados miembros los cuales son fundamentalmente: un incremento del volumen de las sanciones, una ampliación del ámbito de aplicación, la necesidad de un consentimiento explícito, la existencia de un DPD (Delegado de Protección de Datos), la existencia de privacidad de principio a fin, un aumento de los derechos, el registro de actividades, una responsabilidad proactiva y un enfoque distinto del riesgo.

El fin último de este RGPD será reforzar y garantizar el mismo nivel de protección de datos personales en todos los estados miembros de la unión europea. Dado que el objetivo de este reglamento es dar a los residentes de la unión europea el control de sus propios datos, este regulará la forma en que las personas y empresas recopilan, procesan, almacenan y eliminan datos personales de los residentes de cualquiera de los estados de la unión europea, por tanto su aplicación definitiva no tendrá implicación solo para las empresas europeas, sino que también tendrá implicaciones para toda aquella empresa que almacene y procese datos de residentes en la unión europea.

Existen diferencias entre la normativa nacional y la europea, uno de los **cambios más importantes** que introduce este reglamento es la necesidad de que las empresas demuestren la legitimidad de la recopilación y el procesamiento de datos personales. Este reglamento establece 6 formas diferentes para que las empresas cumplan con el artículo 6, y una de ellas es obtener el consentimiento de los propietarios de los datos para poder procesarlos.

Muchos de los cambios que introduce el nuevo reglamento a los que se deberán adaptar todas las empresas son de gran alcance, lo que significa que por un lado las empresas deberán comprender por qué y para qué necesitan recopilar y procesar datos personales, y por otro deberán conocer las implicaciones legales y técnicas que tendrá el hecho de tener que adaptar o modificar los procedimientos que ya tengan establecidos para almacenar y procesar datos personales.

Uno de los aspectos particulares a comentar será que el consentimiento deberá de recabarse de forma libre, inequívoca, específica e informada mediante una clara acción afirmativa. Se deberá informar al interesado de forma clara, transparente e inteligible, sin ocultar información al usuario e informándole a cerca de todos sus derechos.

Cabe resaltar que no siempre es preciso el consentimiento para tratar datos como son los casos de ejecución de contratos, obligaciones legales, situaciones en las que exista un interés público o en situaciones con intereses vitales. Es decir en una situación de interés legítimo.

Toda empresa se encontrará sujeta al RGPD cuando desarrolle una actividad profesional en la cual se traten datos. En un ámbito doméstico o personal fuera de actividad comercial, profesional o empresarial no se aplicará.

El RDPD proporciona a las empresas los manuales pertinentes para que estas puedan adecuarse a la normativa de forma sencilla, con guías a seguir y cumplimentar aclarando aspectos en las mismas como la gestión del riesgo y evaluación de impacto en tratamientos de datos personales, facilidades para la notificación de brechas de seguridad, vías para la resolución de malentendidos relacionados con el anonimato, etc. Facilitando de esta manera la labor a las empresas.

2.4 Medidas y controles para la seguridad de los datos

Los organismos reguladores que hemos comentado previamente como la AEPD que son los ocupados de establecer y asegurar el cumplimiento de la normativa, hacen referencias a las formas de proteger dicha información mediante medidas de seguridad, por ello es relevante a continuación comentar al respecto de la seguridad de nuestra página web, las diferentes formas en que podemos proteger la información tratada en función de las medidas utilizadas, a continuación comentaremos las más relevantes.
Podemos considerar la **seguridad informática** como la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinadas a conseguir un sistema de información seguro y confiable.

En términos de sistemas informáticos, hablamos más bien de fiabilidad del mismo que de seguridad ya que no podemos garantizar la seguridad de este al 100%.

Existen diversas ramas para adaptar este tipo de seguridad en función de que pretendamos proteger específicamente. Podemos realizar dos grandes clasificaciones entre **seguridad lógica**, aquella que protege digitalmente la información de manera directa; y **seguridad física,** aquella que protege la información de forma física, es decir a través de instrumentos y herramientas tangibles equipos, instalaciones,...)

Algunos métodos para preservar la seguridad lógica pueden ser:

- Establecer controles de acceso mediante nombre de usuario y contraseña
- Cifrado de datos para asegurar que únicamente emisor y receptor tengan acceso a esos datos
- Establecimiento de antivirus
- Cortafuegos protegiendo la integridad de la información
- Firmas digitales para identificar la responsabilidad de un mensaje

- Certificados digitales, etc.

En cuanto a la seguridad física algunos métodos de protección podrían ser:

- Dispositivos físicos de protección como pararrayos, extintores, alarmas frente a intrusiones, detectores de humo, asegurar los sistemas de abastecimiento de energía...
- Guardias jurados para controlar el acceso de las personas a las instalaciones
- Copias de seguridad resguardadas en lugar seguro distinto al que se encuentren los sistemas, etc.

En función del momento en que se ponen en marcha dichas medidas podemos clasificar entre **seguridad activa** y **seguridad pasiva**.

La seguridad activa son aquellas medidas que aplicamos con el objetivo de reducir los riesgos existentes de forma previa a que estos hayan sucedido, como es el caso del uso de antivirus, encriptación, evitar lecturas no autorizadas de mensajes,.. ; y la seguridad pasiva son aquellas que un vez producido el incidente de seguridad se reduzca todo lo posible la repercusión del mismo y facilite así la recuperación del sistema, como es el caso de disponer de copias de seguridad, estipular control de accesos, uso de sistemas de alimentación ininterrumpida,...

La **ciberseguridad** es un término bastante general que engloba el conjunto de medidas, métodos, herramientas y procedimientos que utilizamos para proteger nuestra información dentro de los dispositivos que utilizamos (ordenadores, móviles, tablets,...) Esta no engloba una serie de medidas específicas, sino que se deberá adaptar a las necesidades particulares de cada usuario.

Dentro de dichos datos que maneja la empresa deberemos de realizar una **clasificación de la información según el nivel de criticidad** de la misma, en función del nivel del impacto que tendría una filtración de esta.

El estándar ISO/IEC 27001 indica que cada organización debe establecer los criterios que mejor se adapten a sus circunstancias particulares y encontramos como dentro de la nueva normativa se realiza una explicación de los tipos de información pero más breve que la que existía previamente.

Por lo tanto, se deberán establecer inequívocamente los criterios de clasificación para que sean tenidos en cuenta por todos los responsables afectados. Además, deberán estar

alineados con las medidas de seguridad que se llevarán a cabo para proteger la información. Se deberá de clasificar la información en base a la confidencialidad de la misma y el impacto para la empresa en caso de pérdida o robo:

Confidencial. Aplica a toda información de gran relevancia para el futuro de la empresa como los proyectos futuros que se llevarán a cabo.

Restringido. Accesible únicamente para determinado personal de la organización y sin la cual no pueden desempeñar su trabajo.

Uso interno. Accesible para todo el personal de la empresa exclusivamente.

Público. Información de dominio público como la publicada en la página web.

En cuanto al proceso de evaluación del riesgo que se propone de llevar a cabo encontramos que hay que realizar las siguientes tareas:

- Identificar los factores de riesgo o amenazas para los derechos y libertades.
- Analizar los mismos en cuanto a su impacto y probabilidad para poder llevar a cabo la evaluación del nivel de riesgo inherente que se deriva de cada uno de los factores de riesgo.
- Evaluar el nivel global del riesgo del tratamiento para los derechos y libertades del tratamiento

Podemos definir un factor de riesgo o amenaza como una causa potencial de la que se puede derivar un perjuicio para los derechos y libertades de las personas físicas.

El **riesgo inherente** es el resultante de evaluar el nivel de riesgo previamente a la implantación de medidas y garantías para reducir el riesgo derivado de cada uno de los factores de riesgo. Por su parte el **riesgo residual** es el resultante de evaluar el nivel de riesgo resultante después de tomar las medidas y garantías orientadas a reducir el riesgo

Nuestro objetivo será que ese riesgo residual se reduzca a un nivel aceptable.

Deberemos identificar esos factores de riesgo, lo cual consiste en detectar la fuente que puede propiciar un evento capaz de ocasionar impacto en los derechos y libertades de los interesados.

En la tarea de identificar fuentes de riesgo, el responsable o encargado no tiene que comenzar desde cero, sino que el RGPD y su normativa de desarrollo ya han identificado fuentes específicas de riesgo.

Esta metodología es orientativa, y no es la única posible, existiendo un amplio margen de libertad para que la entidad pueda elegir la más adecuada a sus características y necesidades.

El objetivo de tratar los riesgos es disminuir su nivel de exposición con medidas de control que permitan reducir la probabilidad y/o impacto de que estos se materialicen. El riesgo inherente se puede tratar con el objetivo de reducir o mitigar el mismo, en función de la medida que se adopte, hasta situar el riesgo residual en un nivel que se considere razonable.

Como propuesta, para determinar el nivel de un riesgo específico en función de su impacto y probabilidad se puede establecer el siguiente mapa de calor:

Ilustración 1. Tabla probabilidades de riesgo 1

Probabilidad	Muy alta	Medio	Alto	Muy alto	Muy alto
	Alta	Bajo	Alto	Muy alto	Muy alto
	Baja	Bajo	Medio	Alto	Muy alto
	Improbable	Bajo	Bajo	Medio	Muy alto
		Muy limitado	Limitado	Significativo	Muy significativo
		Impacto			

Tabla 14 Matriz Probabilidad x Impacto para determinar el nivel de riesgo

Fuente: https://www.aepd.es/es

Podremos tener en cuenta las siguientes consideraciones:

Ilustración 2. Tabla de probabilidades de riesgo 2

Nivel de Impacto	Descripción	Derechos fundamentales
Muy significativo	Afecta al ejercicio de derechos fundamentales y libertades públicas establecidos en la Constitución[89], y sus consecuencias son irreversibles. y/o Las consecuencias están relacionadas con categorías especiales de datos o relativos a infracciones penales, y es irreversible. y/o Causa un daño social significativo, como la discriminación, y es irreversible y/o Afecta a interesados en situación de especial vulnerabilidad, en particular niños, y de forma irreversible. y/o Causa perdidas morales o materiales significativas e irreversibles.	Igualdad No discriminación Vida Integridad física Libertad religiosa Libertad personal Intimidad personal y familiar Propia imagen Expresión Información Cátedra Reunión Asociación Libre acceso a cargos y funciones públicas en condiciones de igualdad
Significativo	Los casos anteriores cuando los efectos son reversibles. y/o Pérdida de control del interesado sobre sus datos personales, cuando la extensión de los datos sea alta con relación a las categorías de datos o al número de sujetos.	

Fuente: https://www.aepd.es/es

Ilustración 3. Tabla probabilidades riesgo 3

	y/o Se produce o puede producirse usurpación de la identidad de los interesados y/o Pueden producirse pérdidas financieras significativas a los interesados y/o Pérdida de confidencialidad de datos sujetos al deber de secreto profesional o vulneración del deber de confidencialidad y/o Existe un perjuicio social para los interesados o determinados colectivos de interesados	Tutela judicial efectiva Legalidad penal Educación Libertad de sindicación Derecho de petición
Limitado	Pérdida muy limitada del control de algún dato personal y a interesados puntuales, que no sea categoría especial o relativos a infracciones o condenas penales de carácter irreversible y/o Pérdidas financieras insignificantes e irreversibles y/o Perdida de confidencialidad de datos sujetos al secreto profesional pero que no sean categorías especiales o sobre infracción penales	
Muy limitado	En el caso anterior, cuando todos los efectos son reversibles	

Tabla 15 Criterios para determinar el nivel de impacto

Fuente: https://www.aepd.es/es

2.5 Estándares de Seguridad Informática

Respecto a los **estándares de seguridad informática** vigentes a los cuales se deberán aferrar las empresas nos encontramos con las normas de ISO (Internacional Organization for Standardization), esta es una norma que permite el manejo seguro de la información confidencial, apoyando a las pequeñas, medianas y grandes empresas a mantener sus activos de forma segura, lo que viene a significar que esta vela por la seguridad de la información. Dentro de todo el abanico de seguridad informática le incumbirá la protección de datos en uno de sus apartados.

En nuestro caso específico será de aplicación la ISO 27001, esta defiende un sistema de gestión de la información basado en un enfoque en base a procesos apoyándose en un ciclo de mejora continua (Planificar - Hacer – Verificar - Actuar). El contenido de la misma son 10 cláusulas homogéneas a las últimas normas publicadas por la ISO las cuales son: objeto, referencias, términos y definiciones, contexto de la organización, tipo de liderazgo, planificación, apoyo operación y finalmente evaluación y mejora.

Es posible obtener el certificado ISO 27001 para nuestra organización, sin embargo este no es un requisito que dicte la norma ya que se podrá ejercer la actividad sin poseerlo.

En cuanto la relación **de la ISO 27001 con el RGPD** esta encuentra reflejada en uno de sus apartados la gestión y protección de datos personales y el caso es que para muchas empresas la preparación de dicho RGPD puede tener su punto de partida en la ISO 27001 puesto que el primer paso para adecuarse a dicho RGPD será realizar una auditoría interna y evaluar los riesgos de los datos personales. Esta ha sido reconocida por algunas autoridades europeas por su capacidad de proporcionar pruebas del intento y esfuerzo de cumplir el RGPD.

La relación entre ambas normativas de la seguridad de la información radica en que los puntos de control de la ISO 27001 ayudan a los auditores a comunicar a la empresa donde radican los mayores riesgos y donde debe actuar y mejorar, asegurando prácticamente la totalidad de puntos que el RGPD me va a exigir ya que estos se encuentran alineados con la pro actividad en la protección de los datos.

2.6 Situación Internacional

Como ya sabemos, la Unión Europea ha trabajado mucho los últimos años en materia de protección de datos, y podemos afirmar que tiene leyes bastante estrictas. Pero no todos los países externos a la UE han hecho lo mismo.

La regulación de Estados Unidos es tan ambigua que en 2015 el Tribunal de Justicia de la UE declaró inválido el acuerdo *Safe Harbour*, que permitía la transferencia de datos personales de usuarios de Europa a EEUU. Años después, se aprobó el *Privacy Shield*, que muchos consideran que precisa ser revisado próximamente.

De hecho, la situación estadounidense de la protección de datos es tan arcaica que fue en 2020 cuando entró en vigor la primera ley de privacidad que permitía que los consumidores prohibieran a las empresas vender sus datos personales. Dicha ley fue denominada como la ley de Privacidad del Consumidor (CCPA) y se llevó a cabo en California.

La situación de otra de las grandes potencias mundiales, China, también es importante. El China’s National People’s Congress Standing Committee aprobó este verano la nueva Ley de Seguridad de Datos. Dicha ley restringe la recopilación de datos personales por parte de las empresas privadas, pero deja vía libre al gobierno, que podrá seguir recopilándolos. Esta ley se ha creado por la preocupación de los ciudadanos chinos debido a las filtraciones de datos.

Como podemos comprobar, los países más avanzados en cuanto a muchos aspectos en el panorama internacional, aún tienen mucho que mejorar en materia de protección de datos. En cambio, la UE ha hecho un gran esfuerzo en regular este campo.

2. Caso Práctico: Evaluación de la Protección de datos en la web de Gabinete Jurídico Jiloca

En este apartado abordaremos el caso práctico del análisis del sitio en cuestión a través de un cuestionario que hemos elaborado acorde a las características del sitio y siguiendo siempre los criterios establecidos por el RGPD, de esta manera conoceremos si nuestra web cumple con los requisitos pertinentes y con lo exigido por la AEPD.

Antes de comenzar el análisis, es necesario introducir el sitio web. https://abogadoregistro.es/ es la página web de Gabinete Jurídico Jiloca, un despacho de abogados del turolense pueblo de Calamocha. Son especialistas en varias áreas del derecho y se dirigen a personas físicas, autónomos, PYMES y administraciones públicas. Los servicios que ofrecen son: gestión de obligaciones fiscales, administración de fincas, protección de datos (derecho informático), gestión de procesos en el sector público y urbanismo y gestión de documentos del registro de la propiedad.

Dentro de la web encontramos los siguientes apartados:

Ilustración 4. Apartados de la web

Fuente: https://abogadoregistro.es/

En el apartado de *Inicio*, encontramos un resumen de la información más importante de la empresa: dónde se encuentran, cómo ponerse en contacto con ellos, los servicios que ofrecen y las ventajas de contratar sus servicios. En el apartado *Sobre Nosotros*, se explica quiénes son, su filosofía y las personas que conforman el equipo con sus respectivos estudios. A continuación, encontramos el desplegable de *Servicios*, donde ofrecen cada uno de ellos detalladamente. Tras ello, aparece el apartado de *Artículos* que es el blog donde se publican nuevos post que ayudan al posicionamiento de la web. Y finalmente el apartado de *Contacto* con toda la información necesaria para localizarles.

Primero hemos utilizado la herramienta **Facilita RGPD** la cual nos ayuda a clasificar a nuestra empresa en función de sus características y de su situación respecto del tipo de datos personales tratados, básicamente vamos a conocer si es necesario realizar un análisis de riesgos.

Ilustración 5. Captura web AEPD Herramienta Facilita

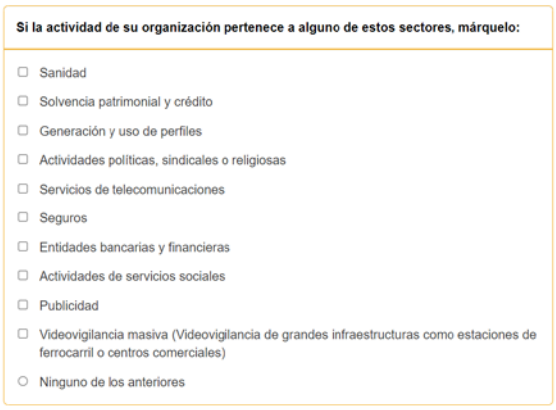
Fuente: https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd

En esta herramienta respondemos una serie de cuestiones acerca de qué tipos de datos trata nuestra empresa para poder clasificarla y saber si precisa de realizar un análisis de riesgos. En nuestro sitio únicamente son requeridos los datos de: nombre, teléfono y correo electrónico.

Ilustración 6. Captura Gabinete Jurídico Jiloca Datos contacto

Fuente: https://abogadoregistro.es/

Ilustración 7. Captura Herramienta Facilita AEPD cuestionario



Fuente: https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd

Siendo la resolución de la misma que no deberemos realizar un análisis de riesgos dado el carácter de los datos tratados, cabe destacar que dicho análisis de riesgo es aplicable a cualquier tratamiento, independientemente de su nivel de riesgo.

Los datos que incorpore en el programa desde esta pantalla hasta la finalización del programa, se van a utilizar para elaborar los documentos que se generan automáticamente adaptados a su organización

A continuación, podríamos acceder a la herramienta si fuera necesario llevar a cabo la evaluación de dichos riesgos. Esta es una de las muchas facilidades que el RGPD y la AEPD ponen a disposición de las empresas para facilitar su adecuación a la normativa.

Ilustración 8. Captura web AEPD Evaluación riesgo

Fuente: https://www.aepd.es/es/guias-y-herramientas/herramientas/evalua-riesgo-rgpd

Esta herramienta tiene como objeto servir de ayuda a responsables y encargados a identificar los factores de riesgo para los derechos y libertades de los interesados cuyos datos están presentes en el tratamiento.

A continuación desarrollamos la guía con la cual vamos a auditar/ evaluar el cumplimiento RGPD, para ello se ha elaborado un en el que se llevará a cabo la comprobación de que medidas se cumplen y cuáles no. Dicha guía ha sido creada teniendo como referencia otras guías de la AEPD, realizando sobre ellas un filtrado y selección de aquellas cuestiones que son de interés para la empresa que se va a auditar: Gabinete Jurídico Jiloca. Así, obtenemos como resultado final una forma de evaluación completa y personalizada, que nos va a permitir tan precisos como la protección de datos requiere. Este documento, y otros con sus mismas características, serán por tanto relevante para responsables, encargados y delegados de tratamiento de protección de datos.

Esta evaluación se estructura en grupos de afirmaciones en función de la temática de las mismas. Dichas preguntas cuestionan:

- Principios relativos al tratamiento
- Licitud del tratamiento.
- Condiciones para el consentimiento.
- Tratamiento de categorías especiales de datos.
- Tratamientos que no requieren identificación.
- Derechos del interesado:
    - Transparencia de la información.
    - Información a facilitar cuando los datos se obtienen del interesado.
    - Información a facilitar cuando los datos se obtienen del interesado.
    - Derecho de acceso.
    - Derecho de rectificación.
    - Derecho de supresión.
    - Derecho a la limitación del tratamiento.
    - Información al interesado ante rectificación, supresión o limitación en el tratamiento.
    - Derecho a la portabilidad de los datos.
    - Derecho de oposición.
    - Decisiones individuales automatizadas, incluida la elaboración de perfiles.
- Responsabilidad del responsable del tratamiento.
- Protección de datos desde el diseño y por defecto.

- Corresponsables del tratamiento.
- Encargado del tratamiento.
- Registro de las actividades de tratamiento.
- Seguridad del tratamiento.
- Notificación de brechas de la seguridad de los datos personales a la autoridad de control.
- Comunicación de una brecha al interesado.
- Evaluación de impacto relativa a la protección de datos.
- Delegado de protección de datos.

Marcaremos en cada apartado con V: si cumple y X: si no cumple los requisitos.

GUÍA PARA EL CUMPLIMIENTO DE LA PROTECCIÓN DE DATOS:

PRINCIPIOS RELATIVOS AL TRATAMIENTO	
Se recogen los datos personales con fines determinados	V
Se recogen los datos personales con fines explícitos	V
Se recogen los datos personales con fines legítimos	V
Se tratan ulteriormente de manera incompatible con otros fines	V
Los datos personales se mantienen exactos	V
Se mantienen actualizados	V
Se revisa anualmente la permanencia	V
Se rectifican los datos personales inexactos respecto de la finalidad	V
Se suprimen los datos personales inexactos respecto de la finalidad	V
Se mantienen durante más tiempo del necesario respecto de la finalidad	X
Se han implantado medidas de seguridad para proteger la integridad y confidencialidad de los datos	V
Se han implantado medidas de seguridad contra el tratamiento no autorizado o ilícito de los datos	V
Se han implantado medidas de seguridad para evitar su pérdida, destrucción o daño accidental	V
LICITUD DEL TRATAMIENTO	
Se tiene consentimiento para cada finalidad del tratamiento	V
El tratamiento es necesario para ejecutar un contrato o precontrato	V
Existe obligación legal	V
El tratamiento es necesario para el cumplimiento de interés público	V
El tratamiento es necesario para satisfacer intereses legítimos	V

CONDICIONES PARA EL CONSENTIMIENTO	
Se puede demostrar que el afectado dio su consentimiento para el tratamiento	V
Se puede demostrar que el tratamiento se realiza como resultado del cumplimiento de una obligación legal	V
Se solicita el consentimiento de forma clara e independiente de los demás asuntos	V
Se solicita el consentimiento de forma inteligible y de fácil acceso	V
Se solicita usando lenguaje claro y sencillo	V
Se informa con carácter previo a recabar el consentimiento	V
Se permite retirar el consentimiento con la misma facilidad que se recaba	V
Se ofrecen medios para retirar el consentimiento en cualquier momento	V
Se recaba el libre consentimiento	V
Para prestar un servicio se solicitan sólo los datos necesarios	V
Para ejecutar un contrato se solicitan sólo los datos necesarios	V
TRATAMIENTO DE CATEGORIAS ESPECIALES DE DATOS	
Se tratan los datos con consentimiento explícito y no existen normas de derecho que prohíban expresamente su tratamiento	V
Es necesario para proteger los intereses vitales de una persona y el interesado no está capacitado, física o jurídicamente, para dar su consentimiento	V
Se efectúa en el ámbito de actividades legítimas y con las debidas garantías y no se comunican a terceros sin consentimiento de los interesados	V
Se tratan datos que el interesado ha hecho manifiestamente públicos	X
Existe posibilidad de reclamaciones	V
Es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social	X
Derecho que establece medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional	V
Es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos en base a normas de derecho	X
Se realiza cumpliendo las condiciones con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud que establece la normativa nacional	V
TRATAMIENTOS QUE NO REQUIEREN IDENTIFICACIÓN	
Se mantiene información adicional con vistas a identificar al interesado cuando los fines no requieren esa identificación	X
Se puede demostrar que los datos anonimizados no permiten identificar a los	V

interesados	
Se informa al interesado y se recaba su consentimiento cuando se llega a su identificación	V
Se cancelan los datos cuando se llega a identificar al interesado	V
DERECHOS DEL INTERESADO. TRANSPARENCIA DE LA INFORMACIÓN	
Se toman medidas para facilitar al interesado toda la información relativa al tratamiento	V
La información se facilita de forma concisa, transparente e inteligible	V
La información se facilita en lenguaje claro y sencillo	V
Se facilita por escrito o por otros medios, incluidos los electrónicos	V
Se facilita verbalmente, previa acreditación de su identidad	V
Se facilita al interesado el ejercicio de sus derechos	V
Se atienden las peticiones del ejercicio de derechos aunque el tratamiento no requiera identificación salvo que no se pueda identificar al interesado	V
Se informa al interesado en el plazo de un mes desde la recepción de su solitud	V
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	V
Se informa en el plazo de un mes de la prórroga de tres meses indicando el motivo de la dilación	V
Se permite a los interesados el ejercicio de derechos por medios electrónicos	V
Se informa por medios electrónicos cuando se recibe la solicitud por esos medios salvo que solicite que se realice por otro medio	V
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	V
Se facilita gratuitamente el ejercicio de derechos	V
Se solicita información para acreditar la identidad de la persona física que ejerce sus derechos	V
Cuando la información que se facilita utiliza iconos normalizados, el formato electrónico es legible mecánicamente	V
DERECHOS DEL INTERESADO. INFORMACIÓN A FACILITAR CUANDO LOS DATOS SE OBTIENEN DEL INTERESADO	
Se facilita la identidad y los datos de contacto del responsable y, en su caso, del representante cuando se solicitan datos	V
Se facilitan los datos de contacto del delegado de protección de datos	V
Se facilitan los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento	V

Se facilita información sobre el interés legítimo	V
Se informa sobre los destinatarios o las categorías de destinatarios	V
Se informa del plazo de conservación de los datos personales o los criterios utilizados para determinarlo	V
Se informa sobre la existencia del derecho a solicitar el acceso, rectificación o supresión, la limitación del tratamiento, a oponerse y el derecho a la portabilidad	V
Si el tratamiento se basa en el consentimiento se informa de la existencia del derecho a retirarlo en cualquier momento	V
Se informa del derecho a presentar una reclamación ante una autoridad de control	V
Se informa de las cesiones basadas en requisitos legales o contractuales	V
Se informa de las cesiones basadas en un requisito necesario para suscribir un contrato	V
Se informa de la existencia de decisiones automatizas, elaboración de perfiles, sobre la lógica aplicada, la importancia y consecuencias previstas del tratamiento	V
Antes de realizar tratamientos de datos personales para una finalidad distinta de la que fueron recogidos, se informa al interesado y la información abarca esa otra finalidad y cualquier otra información pertinente	V
DERECHOS DEL INTERESADO. DERECHO DE ACCESO	
Se informa respecto a los fines del tratamiento	V
Se informa de las categorías de datos personales que se tratan	V
Se informa de los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales	V
Se informa del plazo previsto de conservación de los datos personales	V
Se informa de los criterios utilizados para determinar el plazo de conservación	V
Se informa del derecho a solicitar la rectificación o supresión de sus datos	V
Se informa del derecho a solicitar la limitación del tratamiento de los datos	V
Se informa del derecho a solicitar la oposición al tratamiento	V
Se informa del derecho a presentar una reclamación ante una autoridad de control	V
Se proporciona información sobre el origen de los datos cuando no recogen del propio interesado	V
Se facilita copia de los datos personales objeto de tratamiento cuando el interesado lo solicita	V
Se facilita la información en formato electrónico de uso común si lo solicita por medios electrónicos salvo que se facilite otro medio	V
DERECHOS DEL INTERESADO. DERECHO DE RECTIFICACIÓN	

Se rectifican los datos personales inexactos sin dilación indebida	V
Se completan los datos personales incompletos teniendo en cuenta los fines del tratamiento	V
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	V
Se suprimen los datos cuando se retira el consentimiento en que se basa el tratamiento	V
Se suprimen los datos cuando se opone al tratamiento	V
Se suprimen los datos cuando han sido tratados ilícitamente	V
Se suprimen los datos cuando lo exige una obligación legal	V
Se suprimen los datos cuando se obtienen en relación con la oferta de servicios de la sociedad de la información	V
DERECHOS DEL INTERESADO. DERECHO A LA LIMITACIÓN DEL TRATAMIENTO	
Se limita el tratamiento durante un plazo para verificar la exactitud de los datos, cuando el interesado impugna su exactitud	V
Se limita el tratamiento cuando es ilícito y el interesado se opone a la supresión de sus datos personales y solicita en su lugar la limitación de su uso	V
Se limita el tratamiento cuando no son necesarios para los fines pero el interesado los necesita para la formulación, el ejercicio o la defensa de reclamaciones	V
Se limita el tratamiento cuando el interesado se opone al tratamiento mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado	V
Se informa al interesado cuando se levanta la limitación del tratamiento	V
INFORMACIÓN AL INTERESADO ANTE RECTIFICACIÓN, SUPRESIÓN O LIMITACIÓN EN EL TRATAMIENTO	
Se comunican al interesado la rectificación, supresión o limitación en el tratamiento	V
DERECHOS DEL INTERESADO. DERECHO A LA PORTABILIDAD DE LOS DATOS	
Se facilitan los datos cuando el interesado lo solicita en un formato estructurado, de uso común y lectura mecánica	V
Se transmiten dichos datos a otro responsable si el tratamiento está basado en el consentimiento o en un contrato	V
Se transmiten dichos datos si el tratamiento se efectúe por medios automatizados	V
Se transmiten los datos al nuevo responsable que el interesado determina, si es	V

posible técnicamente	
DERECHOS DEL INTERESADO. DERECHO DE OPOSICIÓN	
Se atienden las solicitudes de oposición y se dejan de tratar los datos	V
Se atienden las solicitudes de oposición pero no se dejan de tratar los datos por motivos legítimos imperiosos para el tratamiento que prevalecen sobre los intereses, los derechos y las libertades o para la formulación, el ejercicio o la defensa de reclamaciones	V
Se ponen los medios necesarios para que pueda ejercer su derecho a oponerse por medios automatizados	V
DERECHOS DEL INTERESADO. DECISIONES INDIVIDUALES AUTOMATIZADAS, INCLUIDA LA ELABORACIÓN DE PERFILES	
No se realizan tratamientos que supongan la toma una decisión basada únicamente en el tratamiento automatizado y que produzca efectos jurídicos	V
Se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos porque es necesario para la celebración o la ejecución de un contrato	V
Se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos porque están autorizados en Derecho	V
Se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos porque se cuenta con el consentimiento explícito	V
Si se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento y que producen efectos jurídicos se adoptan las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos	V
Si se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos se adoptan medidas adecuadas para salvaguardar el derecho a obtener intervención humana por parte del responsable	V
Si se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos se adoptan medidas adecuadas para dar al interesado ocasión de expresar su punto de vista e impugnar la decisión	V
Se toman decisiones individuales automatizadas, incluida la elaboración de perfiles, que se basen en las categorías especiales de datos personales porque se cuenta con el consentimiento del interesado	V
Se toman decisiones individuales automatizadas, incluida la elaboración de perfiles, que se basen en las categorías especiales de datos personales porque se cuenta con habilitación legal	V
Se informa a los interesados acerca de estas decisiones individuales automatizadas y de la habilitación legal de las mismas	V

Se toman decisiones individuales automatizadas, incluida la elaboración de perfiles, que se basen en las categorías especiales de datos personales porque se han tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado	V
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	V
Se tienen en cuenta los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas	V
Se aplican medidas técnicas y organizativas apropiadas	V
Las medidas se revisan y actualizan cuando es necesario	V
Se han confeccionado políticas de protección de datos	V
Se aplican las políticas de protección de datos	V
PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO	
Se analizan las medidas técnicas y organizativas apropiadas antes de determinar los medios de tratamiento	V
Durante el diseño del tratamiento se tienen en cuenta las medidas técnicas y organizativas apropiadas para cumplir con el RGPD	V
Durante el tratamiento se aplican las medidas que han sido determinadas	V
Durante el tratamiento se comprueba la efectividad de las medidas aplicadas	V
Se aplican medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo se tratan datos necesarios para cada uno de los fines	V
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	V
Las medidas garantizan que, por defecto, los datos no son accesibles a un número indeterminado de personas físicas, sin la intervención de personal	V
CORRESPONSABLES DEL TRATAMIENTO	
Se han determinado de modo transparente, y de mutuo acuerdo, las responsabilidades respectivas de los corresponsables en el cumplimiento de las obligaciones impuestas por el RGPD	V
El acuerdo fija las respectivas obligaciones de suministro de información al interesado	V
El acuerdo entre corresponsables del tratamiento refleja las funciones y relaciones respectivas de ambos en relación con los interesados	V
Los aspectos esenciales del acuerdo están a disposición del interesado	V
ENCARGADO DEL TRATAMIENTO	
Se eligen los que ofrecen garantías suficientes conforme con los requisitos del	V

RGPD y garantizando la protección de los derechos del interesado	
El encargado del tratamiento no recurre a otro encargado sin la autorización previa por escrito	V
El tratamiento por el encargado se rige por un contrato u otro acto jurídico vinculante con arreglo a las normas de Derecho	V
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	V
El contrato establece que se tratan los datos personales únicamente siguiendo instrucciones documentadas del responsable	V
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	V
El contrato establece que se tomarán las medidas de seguridad necesarias	V
El contrato establece que se respetarán las condiciones indicadas para recurrir a otro encargado del tratamiento	V
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	V
El contrato establece que se suprimirán o devolverán los datos personales una vez finalice la prestación	V
de los servicios, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales	V
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	V
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	V
El contrato consta por escrito	V
Sólo se accede a los datos siguiendo instrucciones del responsable	V
REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO	
Se lleva un registro de las actividades de tratamiento	V
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	V
El registro recoge los fines del tratamiento	V
Recoge una descripción de las categorías de interesados y de las categorías de	V

datos personales	
Recoge las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales	V
Recogen las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional	V
Incluye los plazos previstos para la supresión de las categorías de datos	V
Incluye una descripción general de las medidas técnicas y organizativas apropiadas al riesgo de los tratamientos	V
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	V
Se aplican las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo	V
Se han incluido medidas para asegurar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento	V
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	V
Existe un proceso de verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento	V
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	V
Se han tomado medidas para garantizar que las personas autorizadas a acceder a datos sólo los tratan siguiendo instrucciones	V
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	V
Existe un procedimiento para que los encargados del tratamiento notifiquen las brechas al responsable en el momento en que tengan conocimiento de ellas	V
Existe un procedimiento para notificar a la autoridad de control en el plazo de 72 horas	V
Existe un procedimiento para documentar los motivos por los que no se puede notificar en el plazo de 72 horas	V

Existe un procedimiento para facilitar la información de manera gradual cuando no es posible facilitarla simultáneamente	V
Se documenta cualquier brecha de seguridad de los datos personales	V
En la documentación se incluyen los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas	V
Se ha comprobado que el procedimiento de notificación funciona	V
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	V
La comunicación al interesado, se lleva a cabo en un lenguaje claro y sencillo, describe la naturaleza de la brecha	V
EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS	
Se recaba el asesoramiento del DPD	V
Se realiza EIPD antes del tratamiento cuando es probable que entrañe un alto riesgo para los derechos y libertades de las personas	V
Se realiza una EIPD antes en tratamientos a gran escala de categorías especiales de datos o relativos a condenas e infracciones penales	V
Se realiza una EIPD antes de tratamiento que suponen una observación sistemática a gran escala de una zona de acceso público	V
Se realiza una EIPD en operaciones de tratamiento incluidas en la lista publicada por la autoridad de control	V
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	V
Incluye una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad	V
La EIPD incluye una evaluación de los riesgos para los derechos y libertades	V
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	V
Incluye las medidas previstas para afrontar los riesgos, garantías y mecanismos para garantizar la protección de datos	V
Se reexaminan las EIPD siempre que es necesario y cuando exista un cambio de los riesgos que representen las operaciones de tratamiento	V
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	V
Se informa de las responsabilidades respectivas de los implicados en el tratamiento en la consulta a la autoridad de control	V
Se informa de los fines y medios del tratamiento previsto en la consulta	V

Se informa de las medidas y garantías establecidas para proteger los derechos y libertades en la consulta	V
Se facilitan los datos de contacto del delegado de protección de datos	V
Se incluye la evaluación de impacto	V
Cuando se consulta se facilita cualquier información adicional que solicite la autoridad de control	V
DELEGADO DE PROTECCIÓN DE DATOS	
Se ha designado un DPD por requerimiento legal	V
Se ha designado un DPD atendiendo a sus cualidades de profesionalidad, conocimientos y competencias en la materia	V
Se han publicado los datos de contacto del DPD y se ha comunicado a la autoridad de control	V
Se garantiza que el DPD participa de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales	V
Se da respaldo en el desempeño sus funciones	V
Se le facilitan los recursos necesarios para el desempeño de sus funciones, el acceso a los datos personales y a las operaciones de tratamiento	V
Se le facilitan los recursos necesarios para mantener sus conocimientos	V
Se garantiza que el DPD no recibe ninguna instrucción en lo que respecta al desempeño de sus funciones	V
No se puede destituir ni sancionar al DPD por desempeñar sus funciones	V
El DPD rinde cuentas directamente al más alto nivel jerárquico	V
El DPD atiende las solicitudes de los interesados	V
El DPD está obligado a mantener la confidencialidad en el desempeño de sus funciones	V
Si el DPD desempeña otras funciones, se garantiza que no dan lugar a conflicto de intereses	V
Las funciones del DPD son informar, asesorar y formar al personal de las obligaciones que les incumben	V
El DPD coopera y actúa como punto de contacto con la autoridad de control	V

Respecto al primer apartado de “principios relativos al tratamiento” podemos observar cómo nuestro site cumple con todos los requisitos salvo en el caso de “Se mantienen durante más tiempo del necesario respecto de la finalidad”, en el que en el caso de nuestra empresa estos para un intento de correcto uso se destruyen una vez cumplida su función, por tanto no se cumple este requisito, cabe resaltar que dicho criterio ha sido

seguido en pro de desarrollar la actividad de la mejor manera posible, sin embargo se deberá de modificar para cumplir con la normativa.

Para los apartados de “licitud del tratamiento” y “condiciones para el consentimiento” comprobamos cómo se cumplen todos los requisitos en cada uno de ellos, esto quiere decir que nuestra empresa desarrolla la actividad de tratamiento de los datos en la web informando con carácter previo, con consentimiento del tratamiento solicitando el mismo previamente de forma inteligible y con fácil acceso, usando un lenguaje claro y sencillo y solicitando únicamente los datos necesarios, requisitos que podemos considerar como los más importantes de estos apartados y como hemos comentado se cumplen todos ellos.

Respecto al apartado de “tratamiento de categoría especial de datos” encontramos cómo nuestra empresa no cumple con los siguientes requisitos. En primer lugar, no cumple con el requisito: “Se tratan datos que el interesado ha hecho manifiestamente públicos”, puesto que en el caso de nuestra empresa dichos datos del usuario no se consideran de carácter público porque este los ha cedido a nuestra entidad obviamente de manera privada, es por ello que no se cumple este requisito. El siguiente requisito que encontramos que no se cumple es “Es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social”, obviamente dicho requisito no se cumple puesto que los datos tratados en ningún momento serán de carácter médico o sanitario, dicho requisito podría haber sido eliminado pero es un buen ejemplo de cómo dependerá de la actividad desarrollada por la empresa que se cumplan unos requisitos u otros. Y por último encontramos que no se cumple el requisito “Es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos en base a normas de derecho” puesto que los datos tratados nunca tendrán una finalidad científica, histórica, etc. Este apartado es similar al anterior y no se cumple por la misma regla. Respecto al resto de requisitos comprobamos como nuestra web de empresa cumple con todos ellos.

En el siguiente apartado de “tratamientos que no requieren identificación” encontramos cómo nuestra empresa cumple con todos esos requisitos en su web salvo con “Se mantiene información adicional con vistas a identificar al interesado cuando los fines no requieren esa identificación”, puesto que en nuestra página únicamente se mantiene aquella información que sea pertinente, es decir, no se mantendrá ninguna otra

información adicional para identificar al propietario de los datos. Por lo tanto no se cumple dicho requisito pero en este caso no se incumple la normativa.

Posteriormente en el apartado de “derechos del interesado. Transparencia de la información” vemos cómo nuestra web cumple con todos estos requisitos de toma de medidas para facilitar al interesado toda la información tratada, que dicha información se facilita de forma concisa, transparente e inteligible, que se usa n lenguaje claro y sencillo, etc. Por tanto nuestra web se ajusta a la perfección a la normativa en este apartado.

De igual forma comprobamos cómo en los apartados restantes referentes a los derechos del interesado se cumple en todos ellos la totalidad de los requisitos, demostrado pues que nuestra empresa se encuentra totalmente ajustada al cumplimiento de la normativa en términos de derechos del interesado al cual se le están tratando los datos, los apartados a los que se hace referencia son los siguientes: “derechos del interesado. Información a facilitar cuando los datos se obtienen del interesado”, “derechos del interesado. Derecho de acceso”, “derechos del interesado. Derecho de rectificación”; “derechos del interesado. Derecho de supresión («el derecho al olvido»)”, “derechos del interesado. Derecho a la limitación del tratamiento”, “información al interesado ante rectificación, supresión o limitación en el tratamiento”, “derechos del interesado. Derecho a la portabilidad de los datos”, “derechos del interesado. Derecho de oposición”, “derechos del interesado. Decisiones individuales automatizadas, incluida la elaboración de perfiles”,

A continuación y ya fuera de las categorías de requisitos vinculadas a los derechos pasamos a aquellas en las que se comentan aspectos relacionados con los cargos responsables del tratamiento como son el responsable del tratamiento, el corresponsable del tratamiento o el encargado del tratamiento. En estos casos nuestra empresa cumple con todos los requisitos de la normativa demostrando que cuenta con esos roles cubiertos y acorde a la normativa vigente, siendo los apartados mencionados: “responsabilidad del responsable del tratamiento”, “corresponsables del tratamiento”, “encargado del tratamiento” y “delegado de protección de datos”.

Finalmente en los apartados restantes se cumple con la totalidad de requisitos por parte de nuestra web de empresa los cuales son: “protección de datos desde el diseño y por defecto”, “registro de las actividades de tratamiento”, “seguridad del tratamiento”, “notificación de brechas de la seguridad de los datos personales a la autoridad de control”, “comunicación de una brecha al interesado” y “evaluación de impacto relativa

a la protección de datos". Concluyendo pues que en el caso de nuestra web también se mantienen acorde a la normativa todos aquellos aspectos relacionados con el registro de las actividades de tratamiento, los protocolos de actuación en caso de una brecha de seguridad así como la comunicación de la misma al interesado en dichos datos y la evaluación del impacto generado por la misma.
En definitiva, comprobamos cómo nuestro site se encuentra adaptado casi a la perfección a la normativa vigente de protección de datos salvo algunos aspectos puntuales.

3. Conclusiones

Gracias a la elaboración de este trabajo he podido conocer en profundidad toda la normativa vigente actual de protección de datos de carácter personal con el Reglamento General de Protección de Datos en nuestro país, así como la normativa vigente previa con la Ley Orgánica de Protección de Datos, y conocer como estas se complementan y cubren la totalidad del marco legal actual.

Además, he podido obtener una idea general del funcionamiento y características de las instituciones que se encuentran detrás de su cumplimiento a través de una serie de fuentes bibliográficas y conocer la importancia que tiene en nuestro panorama actual la AEPD.

Sin duda la elaboración de este trabajo ha sido una experiencia enriquecedora en la que he podido aumentar mis conocimientos de todo lo relacionado con la protección de datos, dicho sea de paso considero que estos deben de ser la base del desarrollo de cualquier empresa dada la repercusión de cualquier tipo de falla y de su impacto económico.

Una vez estudiados los aspectos más relevantes que se han destacado durante la práctica y habiendo sido evaluada y auditada nuestra web mediante la guía que habíamos elaborado, puedo concluir que la misma cumple prácticamente en su totalidad con la normativa vigente de protección de datos salvo pequeñas incidencias que hemos resaltado como que deben ser corregidas. Espero que este trabajo sirva de ayuda a la empresa y les permita corregir esos pequeños errores.

5. Bibliografía

Agencia Española de Protección de Datos (2021). Consultado el 18 de agosto de 2021: https://www.aepd.es/es

Agencia Española de Protección de Datos (2021). *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales.* Consultado el 18 de agosto de 2021: https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

CEUPE magazine. (s.f.). *Seguridad informática y protección de datos.* Consultado el 2 de octubre de 2021. https://www.ceupe.com/blog/seguridad-informatica-y-proteccion-de-datos.html

Clicks Informáticos. (2020, 24 de septiembre). *Seguridad Informática: 02 Concepto seguridad y objetivos.* [Archivo de vídeo]. Consultado el 19 de septiembre de 2021. Youtube. https://www.youtube.com/watch?v=l7gyyMr95xg

Clicks Informáticos. (s.f.) *Seguridad informática: 03 Clasificación tipos seguridad.* [Archivo de vídeo]. Consultado el 19 de septiembre de 2021. Youtube https://www.youtube.com/watch?v=0j0gB8wl3dQ

Elogia. (2021). *Claves del Estudio Anual eComerce 2021*. Consultado el 16 de agosto de 2021. https://blog.elogia.net/claves-del-estudio-anual-ecommerce-2021-iab-by-elogia.

Ergo, Hackers. (2020, 30 de abril). *Análisis de riesgo - Introducción a la seguridad informática – Parte #4.* [Archivo de vídeo]. Consultado el 19 de septiembre de 2021. Youtube https://www.youtube.com/watch?v=ENyydJAsQZk

Ionos. (2018). *La protección de datos personales en el eCommerce.* Consultado el 3 de octubre de 2021. https://www.ionos.es/digitalguide/paginas-web/derecho-digital/la-proteccion-de-datos-personales-en-el-ecommerce/

ISOTools (s.f.) *Sistemas de Gestión de Riesgos y Seguridad.* Consultado el 25 de septiembre de 2021. https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001

Jefatura del Estado (2018, 5 de diciembre). *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*. Consultado el 20 de agosto de 2021. https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

Procem Consultores. (s.f.). ISO 27001-Seguridad de la Información [Archivo de vídeo]. Consultado el 19 de septiembre de 2021. Youtube. https://www.youtube.com/watch?v=BNdPQU32p2Y

Sage. (2019). *11 errores de protección de datos que la web de tu empresa no debe cometer*. Consultado el 2 de octubre de 2021. https://www.sage.com/es-es/blog/11-errores-de-proteccion-de-datos-que-la-web-de-tu-empresa-no-debe-cometer/

Schulz M., Hennis Plasschaert J.M (2016, 17 de abril). *Reglamento (ue) 2016/679 del Parlamento Europeo y del Consejo*. Consultado el 27 de agosto de 2021. https://www.boe.es/doue/2016/119/L00001-00088.pdf

Signaturit. (s.f.). *RGPD/GDPR: ¿Qué es el Reglamento Europeo de Protección de Datos?* [Archivo de vídeo]. Consultado el 20 de agosto de 2021. Youtube https://www.youtube.com/watch?v=heKapvVLjng

Villanova Blanco, L. (2018, 29 de enero). ISO27001 y GDPR (Parte ½). [Archivo de vídeo]. Consultado el 20 de agosto de 2021. Youtube. https://www.youtube.com/watch?v=tELvT9fJZMI

WEBOPOSITER. (2019, 5 de febrero). *RGPD: Cómo adaptar tu web al nuevo Reglamento General de Protección de Datos [Parte I]*. [Archivo de vídeo]. Consultado el 20 de agosto de 2021. Youtube https://www.youtube.com/watch?v=OpNFNEg5_GM

6. Anexos

Abreviaturas

AEPD Agencia Española de Protección de Datos

LOPD Ley Orgánica de Protección de Datos

RGPD Reglamento General de Protección de Datos de la Unión Europea

ISO Internacional Organization for Standardization

SEO Search Engine Optimization

SEM Search Engine Marketing

SGSI Sistema de Gestión de Seguridad de la Información

EIPD Evaluaciones de Impacto de Protección de Datos