TRABAJO FIN DE GRADO
GRADO EN DERECHO Y ADE
CURSO ACADÉMICO 2024-2025
CONVOCATORIA SEPTIEMBRE

TÍTULO. La importancia de la ciberseguridad en las PYMES

AUTOR(A): Asimbaya Caiza, Allison Paloma
DNI (o documento equivalente, indicar en su caso): 05300104F

TUTOR(A): Álvarez Torres, Manuel

En (localidad), a (día) de (mes) de (año)

ÍNDICE DE CONTENIDOS

ÍNDICE DE ILUSTRACIONES

CAPÍTULO 1

ABREVIATURAS.

En este apartado se proporcionarán varias abreviaturas para la correcta descripción del trabajo.

- LOPDGDD: son siglas que responden a, Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales.

- OTAN: Organización del Tratado del Atlántico Norte

- **COMPUSEC:** Computer Security

- TRANSEC: Seguridad de las transmisiones

- INFOSEC: Seguridad de la información

- TIC.

- NETSEC

- ENS: Esquema Nacional de Seguridad

- STIC: Servicio de Tecnología de la Información y las Comunicaciones

- INFO ASSURANCE: Seguro de Información

- RGPD: Reglamento General de Protección de Datos

- LOPD: Ley Orgánica de Protección de Datos

- DP: Datos Personales

- DPO: Dirección de Datos Personales

- DUDH: Declaración Universal de los Derechos Humanos

- DDHH: Derechos Humanos

- L.O: Ley Orgánica

- C.E: Constitución Española

- TJUE: Tribunal de Justicia de la Unión Europea

- STJUE: Sentencia del Tribunal de Justicia de la Unión Europea

I. INTRODUCCIÓN

Este trabajo nace con la intención de investigar cuál es el calibre de que exista ciberseguridad o no en las empresas que conocemos como Pymes. El objetivo principal de este trabajo es que gracias a la investigación que realicemos podamos responder a una serie de preguntas. En concreto, al ser estudiante del doble grado de Derecho y Administración de empresas, mi intención es hacer dos trabajos, y que este sea la presentación del tema de investigación en el que se va a exponer los conceptos, y establecer las bases de la ciberseguridad, es decir, hacer una parte más teórica y jurídica ya que este es el de Derecho y el segundo trabajo será correspondiente al grado de ADE, en el que concretaré más el tema de estudio, se implementarán novedades y veremos aplicado el plan de ciberseguridad en una PYME.

Es razonable y en ningún caso cuestionable, que en una multinacional o grande empresa es necesaria la ciberseguridad porque depende de la actividad a la que esté dedicada dicha empresa o de la dimensión de esta, como, por ejemplo, el número de trabajadores. La ciberseguridad es fundamental en una empresa grande ya que es la que más probabilidad de recibir ataques cibernéticos tiene, ahí es donde surge la duda y gracias a ella nace este trabajo. De las dudas que surgen de la ciberseguridad, en primer lugar, hay que tener claro cuál es su significado, una vez tengamos esto claro, podemos investigar la relevancia, pero sin olvidarnos de que estamos actuando en España, por lo que debemos tener clara la base de regulación, qué leyes existen y cuál es la manera óptima de aplicarla.

Dos aspectos muy relevantes en los que nos vamos a centrar son: cómo va a afectar la ciberseguridad a los trabajadores, y cómo va a afectar ésta en las Pymes. Por eso, una de las preguntas que nos hacemos es: ¿es necesaria la ciberseguridad en una empresa pequeña o familiar? ¿Cómo y en qué proporción está relacionada ésta con los trabajadores? ¿y con la empresa ¿se vulnera los derechos fundamentales de los trabajadores imponiendo ciberseguridad? O, al contrario, ¿tiene algún beneficio para ellos?; ¿Cómo afecta la ciberseguridad a la empresa? ¿tiene algún riesgo? ¿qué medidas debería tomar una Pyme? Estas preguntas que nos vayan surgiendo a lo largo del trabajo serán resueltas gracias a la investigación que se irá detallando progresivamente.

En cuanto, a la metodología empleada para desarrollar la presente investigación y poder cumplir el objetivo planteado, se hará uso de varias modalidades de herramientas tanto de tipo cualitativo como cuantitativo. Tipo cuantito: Dialnet, Wos Scopus, Google Scholar, Estadísticas y de tipo cualitativo: información que proceda de organismos oficiales como (LOPD, C.E., RDPG, STJUE).

La investigación del presente trabajo se va a estructurar en tres bloques: en un primer bloque referido al primer epígrafe, en el cual se dará el significado y desarrollará de forma escueta la evolución histórica de la ciberseguridad; un segundo bloque en el que se hablará de la base de regulación y se hará un análisis normativo, y; un tercer bloque en el que ya ahondaremos más cómo afecta este tipo de seguridad a la empresa y qué relevancia tiene en los trabajadores, y terminaremos con las conclusiones de la investigación del trabajo.

II. CONCEPTOS Y EVOLUCIÓN DE LA CIBERSEGURIDAD.

En este apartado se estudiará el concepto y la evolución de la ciberseguridad a lo largo del tiempo.

La ciberseguridad o también conocida como seguridad informática se refiera a la protección de sistemas críticos y de información sensible frente a posibles ataques en el entorno

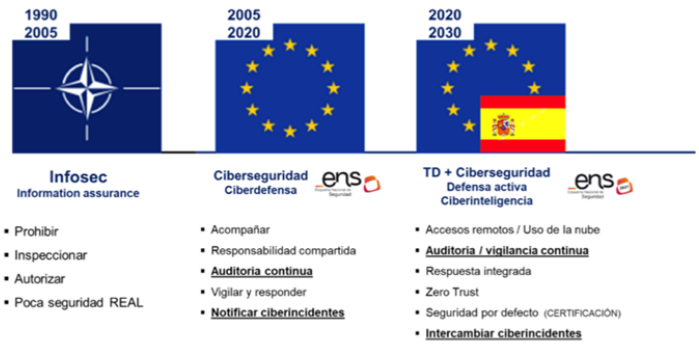
digital[1]. También conocida como seguridad de la tecnología de la información, abarca un conjunto de medidas que son destinadas a salvaguardar las redes y aplicaciones frente a amenazas, tanto internas como externas a las organizaciones[2]. Otra definición describe ciberseguridad como "*la defensa de los medios informáticos"*[3].

Desde la década de 1990, este concepto se ha convertido en un pilar esencial para la protección de infraestructuras críticas, se le ha considerado como una "quita dimensión" de seguridad que puede ser tanto física como virtual[4]. Por otro lado, la seguridad de la información se define como la no presencia de amenazas dirigidas o llevadas a cabo a través de las TIC y rus redes[5], aunque relacionada con la seguridad de la información, se enfoca en la defensa de redes y sistemas ante ciberataques. En las últimas 3 décadas, el concepto ha evolucionado significativamente, estableciendo un nuevo paradigma de seguridad global que abarca todas las áreas afectadas por el ciberespacio[6]. Además, también es conocida la ciberseguridad como seguridad digital, seguridad de la información, de datos, de sistemas o también seguridad en redes[7].

En cuanto a su evolución, el término de *"ciberseguridad* "ha experimentado una significativa evolución, sobre todo a largo de los últimos años. Empezó a tener relevancia en el siglo XX, cuando en 1990 la OTAN integró las definiciones de COMPUSEC, TRANSEC y NETSEC bajo el concepto unificado de seguridad de la información (INFOSEC). Esta seguridad se compone de tres dimensiones que se consideran clave como, la confidencialidad, disponibilidad de la información e integridad.

En Estados Unidos en 2002 se amplió el concepto de ciberseguridad porque incluyeron el "aseguramiento de la información" y además incorporaron dos elementos más, que fueron la autenticidad y la trazabilidad. Estos aspectos se añadieron a la Seguridad de la Tecnología de la Información y las Comunicaciones (STIC), lo que desencadenó en un enfoque más amplio y completo para la protección de datos y sistemas.

Ilustración 1: La evolución de la ciberseguridad.



[1] ROMERO, M. (2021). *La ciberseguridad y su importancia en el entorno digital.* Ed. Tecnología.
[2] Def Ciberseguridad. https://tep.pucmm.edu.do/. (3 febrero 2023).
[3] Revista ejército. Nº.837 extraordinario diciembre (2019). p.136.
[4] MOLERO, JUAN. (2016). Ciberseguridad: *La quinta dimensión de la seguridad. Ed. UG.*
[5] Una guía de aproximación para el empresario. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf.(12 febrero de 2023).
[6] RUFIÁN, MIKEL. Blog: Ciberseguridad y Ciberespacio en Distintas Organizaciones (2020). (Consultado 14 de febrero 2023)
[7] "¿Qué es la ciberseguridad? - Kaspersky" (2021). https://es.scribd.com/document/684269086/Que-es-la-ciberseguridad-Kaspersky (14 de febrero 2023).

Fuente: Ciberseguridad. Evolución y tendencias. ieee.es. Evolución del concepto de ciberseguridad[8].

A partir de 2005, la Unión Europea empezó a mostrar más interés en la seguridad de los sistemas, lo que llevó a la modificación del concepto inicial de INFOSEC/INFO ASSURANCE hacia el término de ciberseguridad. En ese mismo año, la OTAN volvió a definir la ciberseguridad como la implementación práctica de la garantía de la información, un enfoque más operativo basado en la responsabilidad compartida entre las autoridades encargadas de autorizar sistemas y quienes gestionan la información clasificada. Gracias y debido a esta evolución, la ciberseguridad ha adquirido un enfoque centrado en la vigilancia, la respuesta a incidentes, la auditoría continua y la notificación de incidentes.

Entre los principios clave que recogen las normativas nacionales de ciberseguridad se encuentra el Esquema Nacional de Seguridad (ENS), una norma pionera en la Unión Europea que establece principios fundamentales, requisitos mínimos y medidas de seguridad obligatorias. A nivel internacional, destacan las siguientes normativas, la Directiva de Seguridad en Redes de la UE[9] y Regulación de Protección de Datos.

La llegada del nuevo milenio ha traído consigo una mayor globalización y digitalización, transformando así el panorama de la ciberseguridad. La adopción masiva de Internet y la expansión de dispositivos conectados aumentaron las posibilidades para los ciberdelincuentes. En particular, en 2020, con la pandemia, la ciberseguridad adquirió un papel fundamental, ante el incremento del teletrabajo y el uso de dispositivos móviles como una nueva realidad en el mercado laboral, obligando a las empresas a adaptarse rápidamente a este nuevo escenario, ya que los ciberataques se multiplicaron y emergieron nuevas tecnologías, así como el Internet de las Cosas (IoT), que conectó dispositivos que antes en la red, presentando un desafío adicional para la protección digital.

Todo ello ha dado lugar a que hoy en día, la ciberseguridad sea un campo dinámico y esencial, con tecnologías avanzadas como la inteligencia artificial y el aprendizaje automático que se utilizan para detectar y prevenir ataques, adaptándose constantemente a las nuevas amenazas y tecnologías emergentes, con el objetivo de proteger la integridad y confidencialidad de la información en un mundo cada vez más digitalizado

III. BASE DE REGULACIÓN EN ESPAÑA DE LA CIBERSEGURIDAD

1. Relevancia o no del Reglamento General de Protección de Datos

El Reglamento General de Protección de Datos (RGPD), aprobado el 14 de abril de 2016, es una normativa de la Unión Europea que entró en vigor el 25 de mayo de 2018 que deben cumplir todas las organizaciones que operen en el ámbito de la UE, ya sea que hagan negocios con personas u organizaciones o que manejen datos personales de individuos o entidades dentro del ámbito comunitario, estableciendo un marco legal común para la recopilación, almacenamiento, tratamiento y uso de datos personales, garantizando así que los individuos tengan control sobre su información personal. Si bien, cada país miembro tiene libertad y posibilidad de complementarla con su propia legislación.

Entre las principales características de este RGPD es que fortalece los derechos ya establecidos e introduce nuevas disposiciones que otorgan a las personas un mayor control sobre sus datos personales En este sentido, uno de los cambios más significativos es la

[8] CANDAU, JAVIER (2021). Boletín IEE. N.º 23, 2021, pp. 460-494.
[9] Directiva NIS. (DOUE) L 194, de 19 de julio de 2016. Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016.

simplificación del acceso a la información que cada individuo tiene sobre sus propios datos, lo que incluye una comunicación más clara y accesible sobre cómo se están utilizando. Además, se ha implementado un nuevo derecho a la portabilidad de los datos, lo que permite a los usuarios transferir su información personal entre diferentes proveedores de servicios de manera más fluida[10].

Por otro lado, las organizaciones deben obtener el consentimiento claro y explícito de los usuarios antes de recopilar o procesar sus datos personales[11]. Otro aspecto clave es la clarificación del derecho a la supresión, conocido como derecho al olvido, que permite a los individuos solicitar la eliminación de sus datos cuando no haya una justificación válida para su conservación. Asimismo, se garantiza el derecho a ser informado en caso de que se produzca una violación de la seguridad de los datos personales, obligando a las organizaciones a notificar a las autoridades competentes y a los afectados en situaciones graves[12]. Por otra parte, todas aquellas entidades que no cumplan con esta normativa pueden enfrentarse a sanciones significativas, que pueden llegar a ser hasta el 4% de su facturación anual o 20 millones de euros, lo que sea mayor[13]. Una serie de derechos, en definitiva, que buscan empoderar a los ciudadanos y asegurar un tratamiento responsable de su información personal, garantizando un alto nivel de protección de datos personales, adaptándose a las nuevas tecnologías y prácticas en un mundo digital en constante evolución.

A nivel de normativa para las empresas se ha de destacar que el RGPD busca crear un entorno equitativo para todas las empresas que operan en el mercado interior de la Unión Europea, adoptando para ello un enfoque tecnológicamente neutral y fomentando la innovación al implementar un conjunto único de normas aplicables en toda la UE. De esta manera, al contar con una única ley de protección de datos, se incrementa la seguridad jurídica y se reduce la carga administrativa para las empresas, permitiéndoles operar de manera más eficiente en el ámbito digital[14]

Entre estas disposiciones, se incluye la obligación de designar un delegado de protección de datos en las entidades públicas y en aquellas empresas que manejen grandes volúmenes de datos, o que se dediquen al procesamiento de datos sensibles, como los relacionados con la salud. Además, el reglamento establece el principio de ventanilla única, lo que significa que las empresas solo necesitan interactuar con una única autoridad de control en el país donde tienen su sede principal, lo que facilita la colaboración entre autoridades competentes, especialmente en casos que involucren múltiples jurisdicciones[15].

Por otra parte, se introducen normas que favorecen la innovación, al exigir que se integren medidas de protección de datos desde las fases iniciales del desarrollo de productos y servicios, promoviendo el uso de técnicas como la seudonimización y el cifrado, que ayudan a proteger la privacidad de los datos. Asimismo, se reduce las obligaciones de notificación y los costes asociados, eliminando barreras a la libre circulación de datos personales dentro de la UE.

---

[10] EUR-Lex. (2022, enero). Reglamento general de protección de datos (RGPD). https://eur-lex.europa.eu/ES/legal-content/summary/general-data-protection-regulation-gdpr.html

[11] Agencia Española de Protección de Datos. (2024a, julio) Ejerce tus derechos. https://www.aepd.es/derechos-y-deberes/ejerce-tus-derechos

[12] Ibídem

[13] Agencia Española de Protección de Datos. (2024b). Guía del Reglamento General de Protección de Datos responsables de tratamiento.
https://www.aepd.es/guias/guia-rgpd-para-responsables-de-tratamiento.pdf

[14] EUR-Lex. (2022, enero). Reglamento general de protección de datos (RGPD).
https://eur-lex.europa.eu/ES/legal-content/summary/general-data-protection-regulation-gdpr.html

[15] Agencia Española de Protección de Datos. (2024c) ¿Qué es el principio de responsabilidad proactiva?
https://www.aepd.es/preguntas-frecuentes/2-rgpd/3-principios-relativos-al-tratamiento/FAQ-0208-que-es-el-prinipio-de-responsabilidad-proactiva

En este contexto, las organizaciones deben realizar evaluaciones de impacto cuando el tratamiento de datos represente un riesgo significativo para los derechos de los individuos, mientras que las PYMES tienen menos requisitos de mantenimiento de registros, a menos que sus actividades de tratamiento sean regulares o impliquen datos sensibles. Para las transferencias internacionales de datos, el RGPD proporciona diversas herramientas y mecanismos, asegurando que se mantenga un alto nivel de protección incluso fuera de la UE[16].

Con todo ello, se pretende alcanzar una serie de objetivos, entre los que cabe señalar garantizar que las personas tengan control sobre sus datos personales y que se respeten sus derechos fundamentales en relación con el tratamiento de estos datos. Así mismo, se pretende asegurar la libre circulación de datos personales dentro de la Unión Europea, asegurando al mismo tiempo un nivel elevado de los mismos. Para ello se establecen requisitos para garantizar la seguridad de los datos personales, incluyendo la implementación de medidas técnicas y organizativas adecuadas para prevenir violaciones de seguridad, junto con medidas para proteger los datos personales y que sean transparentes en sus prácticas de tratamiento, informando a los interesados sobre cómo se utilizan sus datos. En este sentido, dado que el RGPD proporciona un conjunto uniforme de reglas para el tratamiento de datos personales en todos los Estados miembros de la UE, la comprensión y la aplicación de la normativa es más sencilla, creando, así, un entorno de confianza en el tratamiento de datos personales y la protección de la privacidad de los ciudadanos en la era digital.

2. Análisis de la ley orgánica de protección de datos y garantía de derechos digitales: uso óptimo y fines.

El RGPD[17] es una ley que deben cumplir todas las organizaciones que operen en la Unión Europea UE), ya sea que hagan negocios con personas u organizaciones dentro de la UE o que manejen datos personales de individuos o entidades en la región. Esta normativa establece las directrices que deben seguirse en el tratamiento de datos personales de personas física y define las reglas para la libre circulación efectiva de estos datos. El RGPD fue aprobado el 14 de abril de 2016, aunque su aplicación efectiva comenzó en 2018. Se aplica a todos los países de la UE, aunque cada país miembro tiene libertad y posibilidad de complementarla con su propia legislación.

En este sentido, la confidencialidad de la información debe ser una prioridad constante en cualquier organización, de manera que, si los datos se almacenan en formato físico, es crucial implementar estrictas medidas de seguridad para protegerlos, como mantenerlos bajo llave y restringir el acceso únicamente al personal autorizado. Esto asegura que la información sensible no caiga en manos indebidas y se mantenga segura en todo momento[18]. Además, los clientes tienen el derecho de solicitar la eliminación y destrucción de sus datos personales. En caso de un incidente de seguridad o ciberataque, es imperativo informar de manera rápida y efectiva

[16] Agencia Española de Protección de Datos. (2021a). Gestión del riesgo y evaluación de impacto en tratamientos de datos personales. https://www.aepd.es/guias/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

[17] Parlamento Europeo y del Consejo. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). (DOUE), L 119, 1-88. Entró en vigor el 25 de mayo de 2018.

[18] Mailtek. (2021). Guía práctica RGPD/GDPR. https://mailcommsgroup.com/wp-content/uploads/2021/04/guia-practica-rgpd.pdf

tanto a las autoridades competentes como a los usuarios afectados. Esta respuesta rápida es esencial para minimizar los daños y mantener la confianza de los clientes en la capacidad de la organización para manejar sus datos de manera segura[19]

Además, es importante destacar que la ley permite el acceso a los datos de personas fallecidas y asume que las compañías pueden utilizar los datos de sus empleados con un interés legítimo. Toda vez que se pone especial énfasis en el derecho de cualquier persona a solicitar la eliminación de sus datos personales de las bases de datos de cualquier empresa. Un derecho que se extiende también a la protección de la privacidad personal y contra la vigilancia mediante sistemas de geolocalización en el entorno laboral[20].

Para asegurar una implementación adecuada de la ley, es fundamental que tanto las organizaciones públicas como privadas entiendan y se adhieran a sus disposiciones. Uno de los aspectos clave es la realización de Evaluaciones de Impacto en la Protección de Datos (EIPD), especialmente en casos donde el tratamiento de datos pueda representar un riesgo significativo para los derechos y libertades de las personas. Estas evaluaciones permiten identificar y mitigar potenciales amenazas, garantizando así una gestión más segura y responsable de la información personal.

Otro punto esencial es la designación de un Delegado de Protección de Datos (DPO). Se trata de un rol fundamental para supervisar el cumplimiento normativo, particularmente en organizaciones que manejan grandes volúmenes de datos o información sensible. Actúa como un enlace entre la organización, las autoridades de protección de datos y los interesados, asegurando que se mantenga un enfoque proactivo en la gestión de la privacidad y se minimicen los riesgos asociados al tratamiento de datos personales[21].

Adicionalmente, es vital obtener un consentimiento explícito, informado y verificable de los individuos antes de procesar sus datos. La transparencia en la comunicación es igualmente importante, ya que se debe informar a los interesados de manera clara y accesible sobre cómo se recogen, utilizan y protegen sus datos [22]

Las compañías también deben implementar las medidas de seguridad necesarias para resguardar la información y facilitar el ejercicio de los derechos de los interesados, como el acceso, la corrección y la eliminación de datos. Adoptar un enfoque de responsabilidad activa es clave para demostrar el compromiso con la protección de la privacidad y el cumplimiento de la legislación de protección de datos[23]

El propósito principal de esta legislación es crear un marco robusto y actual para la administración de los datos personales, promoviendo a la vez la circulación libre y efectiva de esta información. De esta manera, es enfoque busca no solo modernizar la gestión de los datos, sino también facilitar su uso responsable en un entorno cada vez más digitalizado. Además, se pretende asegurar el respeto de los derechos digitales, tal como se establece en el artículo 18.4

---

[19] Ibidem

[20] Agencia Española de Protección de Datos. (2024b). Guía del Reglamento General de Protección de Datos para responsables de tratamiento. https://www.aepd.es/guias/guia-rgpd-para-responsables-de-tratamiento.pdf

[21] Agencia Española de Protección de Datos. (2024c) ¿Qué es el principio de responsabilidad proactiva? https://www.aepd.es/preguntas-frecuentes/2-rgpd/3-principios-relativos-al-tratamiento/FAQ-0208-que-es-el-prinipio-de-responsabilidad-proactiva

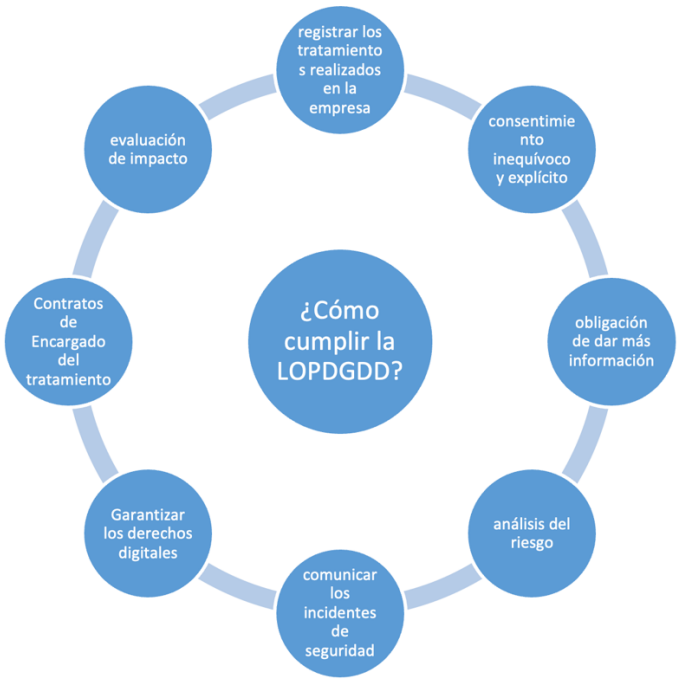
[22] Signaturit. (2024, febrero). GDPR: ¿cómo obtener el consentimiento del cliente? https://www.signaturit.com/es/blog/gdpr-como-obtener-el-consentimiento-del-cliente

[23] Apdcat. (2024). Guía para el cumplimiento del deber de informar en el RGPD. https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/V10-ES-Guia-sobre-el-deber-de-informar-en-el-RGPD-con-diseno.pdf

de la Constitución Española (CE) protegiendo la privacidad de los ciudadanos y fomentar un entorno donde la información personal sea tratada con la debida consideración y responsabilidad.

El Reglamento General de Protección de Datos RGPD, aprobado el 14 de abril de 2016, es una normativa de la Unión Europea que entró en vigor el 25 de mayo de 2018 que deben cumplir todas las organizaciones que operen en el ámbito de la UE, ya sea que hagan negocios con personas u organizaciones o que manejen datos personales de individuos o entidades dentro del ámbito comunitario, si bien cada país miembro tiene libertad y posibilidad de complementarla con su propia legislación.

Ilustración 2: Cumplimiento óptimo de la LOPDGDD



Fuente: Elaboración propia con datos extraídos de la guía de aplicación de la LOPDGDD[24].

IV. LA SEGURIDAD INFORMÁTICA: CÓMO AFECTA A LOS TRABAJADORES

1. La ejecución de las tecnologías de la información

El desarrollo de las nuevas tecnologías y las telecomunicaciones ha llevado a importantes transformaciones en los ámbitos económico y social. Así, más aspectos de la vida cotidiana se han digitalizado, con una tendencia que se acelera continuamente. Esto ha facilitado la creación y expansión de servicios y aplicaciones digitales que responden a diversas necesidades sociales, las cuales, aprovechando plataformas en línea como Twitter, TikToky Facebook, han dado lugar a una economía digital que supera barreras geográficas, fomentando

[24] Guía del cumplimiento de la LOPDGDD. https://www.aepd.es/guias/guia-rgpd-para-responsables-de-tratamiento.pdf. (3 de abril 2023)

una comunidad global con un acceso más fácil, esto empodera a las personas y abre un abanico de posibilidades[25].

No obstante, este entorno digital también presenta riesgos y desafíos, especialmente en lo que respecta a derechos humanos, subrayando la necesidad de que las autoridades adopten solucionen que estén en consonancia con la Declaración Universal de los Derechos Humanos[26] (DUDH), la cual, a lo largo de sus 30 artículos, establece un estándar universal para todas las personas y naciones, declarando que los derechos humanos son fundamentales para asegurar la libertad, la paz y la justicia[27]. Así, tanto la DUDH, al igual que la CE consideran estos derechos como representativos de los derechos que se poseen en el mundo tanto físico como digital. Brindando este último oportunidades de innovación que pueden mejorar la vida de las personas y tener así un impacto positivo en la sociedad. Aun cuando, su inadecuada utilización puede poner en peligro el interés general y vulnerar derechos fundamentales[28]

En este sentido, tal como se señaló en la Cumbre Mundial de la Sociedad de la Información (CMSI) de 2015, los principales desafíos son: asegurar que todos los derechos humanos sean respetados, tanto en línea como fuera de ella; incrementar el acceso a las TIC, reduciendo la brecha digital, mejorando la gestión del espectro radioeléctrico y permitiendo la expansión de las redes de telecomunicaciones; y fomentar la conciencia sobre la dimensión ética del uso de las TIC y promover un diálogo interdisciplinario[29]

Consecuentemente, si bien hay muchos desafíos y objetivos por conseguir, lo crucial es reconocerlos y afrontarlos de modo colaborativo, implicando a los diferentes actores sociales. Así, Internet y el ecosistema digital podrá desarrollarse, garantizando que se respetan los derechos fundamentales, sobre todo aquellos concernientes a la libertad de expresión, el acceso a la información, la privacidad y la protección de datos personales, así como los derechos de autor, tal y como establece la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital[30]

2. Posible vulneración de los derechos fundamentales en España

2.1. Libertad de expresión y acceso a la información

La era de la información lleva consigo un proceso de digitalización, caracterizado por la conectividad a Internet y la cada vez mayor relevancia de las plataformas digitales, ha transformado profundamente el modo en cómo las personas se comunican, actúan entre sí, comparten y crean contenido y acceden a la información desde cualquier tipo de dispositivos y lugar del planeta, lo cual antes estaba limitado únicamente a grandes medios de comunicación, los cuales eran centralizados, limitados por barreras geográficas y dependían de autorizaciones, lo que facilitaba su regulación y control.

---

[25] JIMÉNEZ, LUIS. (2018). *El impacto en las tecnologías digitales en la economía global.* Ed. Innovación Digital, p. 30.

[26] Organización de las Naciones Unidas. (s.f.). Declaración Universal de Derechos Humanos. (16 de abril 2023). https://www.un.org/es/about-us/how-to-donate-to-the-un-system

[27] Organización de las Naciones Unidas. (s.f.). Declaración Universal de Derechos Humanos. (16 de abril de 2023). https://www.un.org/es/about-us/how-to-donate-to-the-un-system

[28] Ibidem

[29] Unión internacional de telecomunicaciones. (2015). *Informe de la Cumbre Mundial de la Sociedad de la información* (CMSI). UIT

[30] Parlamento europeo (2023). Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital. Parlamento Europeo.

El acceso a este sistema de comunicación ofrece numerosas ventajas, como es el caso de poder acceder más fácilmente a todo tipo de información, contenidos y servicios, si bien existe una contraparte al también facilitar las conductas antisociales como la difamación, facilitar la creación y distribución de contenido inadecuado o ilegal, e inclusive poder utilizarse para efectuar actividades delictivas[31].

Así, mediante las plataformas digitales y de los distintos intermediarios, las personas tienen la capacidad de personalizar el contenido que consumen, a la vez que crear y distribuir el suyo propio o el de terceros, consiguiendo en pocos segundos tener un alcance global. Y, si bien, parte de dichos contenidos puedan resultar dañinos para la sociedad, la mayoría es provechosa, facilitando la difusión de noticias, contenidos educativos, y de temáticas especializadas, etc.

Sin embargo, dado el carácter global de Internet, el problema surge cuando se crea o se distribuye contenido peligroso para la sociedad, puesto que la información se difunde velozmente, siendo complicado poder eliminarla e identificar su autoría. Este aspecto ha generado preocupación entre las autoridades y reguladores, quienes han puesto su atención en la responsabilidad de los intermediarios y proveedores de acceso[32]. El desafío surge cuando se crea o se distribuye contenido antisocial o perjudicial. Esto se agrava debido a la naturaleza global de Internet, donde la información se propaga rápidamente, es difícil de eliminar y a menudo es complicado identificar con precisión al autor o editor. Este aspecto ha generado preocupación entre las autoridades y reguladores, que han puesto su atención en la responsabilidad de los intermediarios y proveedore de acceso. Esto ha llevado a que les exija filtrar o bloquear ciertos contenidos, así como revelar información que podría restringir el derecho a la libertad de expresión y el acceso a ideas e información, lo cual es esencial para la democracia moderna[33]

El entorno digital, la transmisión y el intercambio de contenidos dependen de varios actores que ofrecen servicios conocidos como "intermediarios". Aunque sus definiciones pueden variar, generalmente se refieren a cualquier entidad que facilita la comunicación[34], de información[35], como proveedores de servicios de Internet, motores de búsqueda, plataformas de blogs, redes sociales y servidores web[36]. Dado que controlan quién y cómo se comparte información a través de sus plataformas, tienen un papel crucial en la protección de la libertad de expresión, el acceso a la información y la privacidad[37]. A raíz de esto, varias regulaciones les asignan responsabilidades específicas.

Con respecto al plano internacional, hay muchos instrumentos que reconocen la libertad de expresión como un derecho humano esencial y fundamental. Por ejemplo, en el artículo 19 de la Declaración Universal de los Derechos Humanos (DUDH) enfatiza la relevancia de este derecho para la plena realización de otros derechos humanos y para fortalecer las sociedades democráticas. De manera similar, el artículo 11 de la Declaración Universal de Derechos del

[31] URIARTE, LUIS y RUIZ MANUEL. (2018). *Sociedad Red y Transformación digital, p 35-49*
[32] Barrero, A. (2021). Responsabilidad de los intermediarios de internet en el derecho de la UE. *Revista Española de Derecho Constitucional*, (123). Págs. 107 – 132
[33] ibidem
[34] Naciones Unidas. Asamblea General. (2011). Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue (Informe A/HRC/17/27). 16 de mayo de 2011, pp.38.
[35] UNESCO. (2014). Fostering freedom online: The role of internet intermediaries. UNESCO series on internet freedom (p. 19). Internet Society.
[36] Iniciativa global de la sociedad civil. (2015). Principios de Manila sobre Responsabilidad de los Intermediarios: Antecedentes. Versión 1.0. Mayo 2015, pp. 6.
[37] UNESCO. Fostering Freedom Online: The role of Intermediaries. UNESCO Series on Internet Freedom. Internet Society (2014). pp.23.

Hombre y del Ciudadano de 1789 subraya la importancia de la libertad de expresión en el desarrollo individual, el control del poder estatal y la participación democrática. A su vez, el artículo 19 del Pacto internacional de Derechos Civiles y Políticos de 1996 resalta el papel clave de este derecho en la promoción de la democracia, el acceso a la información, la diversidad de opiniones y la rendición de cuentas. Finalmente, el artículo 13 de la Convención Americana sobre Derechos Humanos refirma de este derecho, poniendo énfasis en el pluralismo de opiniones.

Asimismo, el artículo 10 del Convenio Europeo de Derechos Humanos (CEDH) y la Primera Enmienda de la Constitución de los Estados Unidos reconocen la libertad de expresión como un derecho esencial, para el desarrollo personal y la rendición de cuentas ante el poder, tanto estatal como privado. La principal diferencia entre la CEDH y la Primera Enmienda radica en las excepciones a la libertad de expresión: en Estados unidos, la libertad de expresión se prioriza más, buscando fomentar la autonomía individual y la tolerancia, mientras que en Europa se busca un equilibrio entre la libertad de expresión y la dignidad de las personas, estableciendo más excepciones.

En este contexto, los intermediarios tienen la responsabilidad de equilibrar la protección de la libertad de expresión con la necesidad de regular contenidos perjudiciales. Esto implica desafíos significativos, ya que deben filtrar o bloquear ciertos contenidos y, en algunos casos, revelar información que podría restringir el derecho a la libertad de expresión y el acceso a ideas e información, esenciales para la democracia moderna. Este equilibrio sigue siendo un desafío crucial en la era digital, donde la velocidad y el alcance de la información complican la regulación efectiva y justa[38]

En España, la Constitución también salvaguarda a estos derechos, tal y como se refiere en la Sección 1, "De los derechos fundamentales y de las libertades públicas", en su artículo 20 en el que se garantiza varios derechos, incluido el de expresar libremente pensamientos, ideas y opiniones a través de diversos medios junto con el derecho a transmitir y recibir información verídica sin restricciones previas. Sin embargo, está restringidos por la exigencia de respetar otros derechos esenciales como el honor, la privacidad, la imagen personal y la protección de los menores.

Se ha de tener en cuenta que los derechos concernientes con las comunicaciones son fundamentales, por lo que su regulación debe efectuarse mediante una Ley Orgánica, que exige una mayoría absoluta para su aprobación, modificación o derogación. Dado que una materia destinada a ser regulada por esta vía no lo have, podría declararse inconstitucional según el Tribunal Constitucional, en conformidad con el artículo 81 de la C.E. y el artículo 28.2 de la Ley Orgánica del Tribual Constitucional.

Nuestra Constitución también contempla un mecanismo preferente y rápido ante los tribunales ordinarios para salvaguardar los derechos fundamentales relacionados con la comunicación. En el artículo 53.2 de la Constitución Española se establece que cualquier ciudadano puede solicitar la protección de su libertades y derechos a través de un procedimiento ágil y prioritario. Este proceso tiene como objetivo resolver el conflicto de manera rápida, enfocándose exclusivamente en los derechos fundamentales involucrados, mientras que otros aspectos del caso pueden tratarse en un proceso más detallado posteriormente. Dependiendo de la naturaleza del asunto, se puede acudir a distintas jurisdicciones para estos procedimientos

[38] MacKinnon, R., Hickok, E., Bar, A., y Lim, H. I. (2015). *Fostering freedom online: The role of internet intermediaries*. UNESCO Publishing.

preferenciales[39]. Además, existe la posibilidad de solicitar amparo tanto ante los tribunales ordinarios como ante el Tribunal Constitucional[40].

Es importante mencionar la Sentencia N.º 159/1986 del Tribunal Constitucional[41], relacionada con el artículo 20 de la CE, ya que subraya la relevancia de la libertad de expresión y de comunicación como pilares esenciales en una sociedad democrática, permitiendo a los ciudadanos formar sus propias opiniones. Además, pone de manifiesto que el derecho a la información no solo es un derecho individual, sino también un elemento clave para el correcto funcionamiento de la opinión pública, estando estrechamente ligado al pluralismo. Igualmente, subraya que, en caso de que, de conflicto entre la libertad de información y otros derechos fundamentales, las limitaciones a esta libertad deben interpretarse de manera cuidadosa para no desnaturalizar su esencia[42]. Con la aparición de nuevos servicios, surgen más espacios que facilitan la expresión libre y el acceso a la información[43]. Dado el impacto que tienen estos derechos tanto para los individuos como para la sociedad, es crucial que las comunicaciones digitales también se consideren dentro de su ámbito de protección, en especial cuando puedan afectar los derechos de otros o generar perjuicios sociales[44]

Actualmente, los derechos de comunicación, la libertad de expresión y el acceso a la información están cobrando mayor importancia y difusión. Son fundamentales para el crecimiento personal, la formación de la opinión pública y el buen funcionamiento de una sociedad libre. No obstante, estos derechos no son ilimitados, ya que se establecen restricciones para proteger otros derechos fundamentales, como el honor, la privacidad, la imagen personal, y la protección de los menores. Además, se deben tener en cuenta factores como la seguridad nacional, el orden público, la salud y la moral pública. La libertad de expresión y el acceso a la información son cruciales para una democracia activa y para garantizar otros derechos. Con la creciente presencia de servicios digitales, es esencial proteger estos derechos en todos los formatos disponibles.[45]

En este contexto, en el año 2015 se aprobaron los Principios de Manila sobre Responsabilidad de los Intermediarios[46]. Estos principios operan como referente de buenas prácticas para precisar y delimitar la responsabilidad de los intermediarios en lo que se refiere al contenido de terceros e impulsar la libertad de expresión o de palabra y la innovación. Algunos de los principios incluyen: que la responsabilidad de los intermediarios tendría que estar legalmente respaldada; no se les debe obligar a restringir contenido sin una orden judicial; las solicitudes de eliminación de contenido es necesario que sean claras y precisas; las leyes y prácticas de restricción de contenido tienen que cumplir con los principios de necesidad y

[39] SANJURO, BEATRIZ (2015). "Manual de Internet y Redes Sociales", Dykinson, página 47 y 48.

[41] Tribunal Constitucional de España. (1986). Sentencia N.ª 159/1986, de 16 de diciembre de 1986. (BOTC), *BOE núm. 313, de 31 de diciembre de 1986)*

[43] Zinguer, M. A. (2014). Libertad de expresión y derecho a la información en las redes sociales en Internet. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, (12), 5.

[44] Echavarría, J. (1988). Aspectos constitucionales de la libertad de expresión y el derecho a la información. *Revista Española de Derecho Constitucional*, (23), Págs. 139-155.

[45] IBIDEM

[46] P Global Network Initiative. (2015). Principios de Manila sobre Responsabilidad de los Intermediarios. Recuperado de https://www.eff.org/files/2015/06/23/manila_principles_1.0_es.pdf. (Consultado el 3 de abril 2023).

proporcionalidad; y, por último, deben promover la transparencia y el compromiso en este tipo prácticas[47]

Teniendo en cuenta el valor de la libertad de expresión para la protección de otros derechos y libertades, es esencial considerar[48] que:

Reconociendo la importancia de la libertad de expresión en la protección de otros derechos y libertades, es fundamental que cualquier restricción a este derecho sea realmente necesaria y se aplique utilizando el método menos restrictivo posible, siguiendo los principios de necesidad y proporcionalidad. Además, el Tribunal de Justicia de la Unión Europea (TJUE), en el caso Satakunnan Markkinaporssi y Satamedia, afirmó que este derecho no se limita a los medios tradicionales, sino que también incluye a Internet como un medio de comunicación, independientemente del soporte utilizado para transmitir los datos[49]

Por su parte, el Tribunal Constitucional español ha destacado que cualquier medida que limite la creación o difusión de obras intelectuales, especialmente si depende de una evaluación previa oficial, constituye una forma de censura previa. Asimismo, el artículo 15 de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo establece que los Estados no pueden imponer una obligación general de supervisar los datos transmitidos o almacenados por los proveedores de servicios, ni obligarlos a buscar activamente actividades ilícitas.

El TJUE, en su sentencia del 24 de noviembre de 2011 (caso C-70/10 (Scarlet Extended SA contra SABAM), confirmó que el artículo 15 prohíbe categóricamente que las autoridades nacionales exijan a los proveedores de Internet supervisar de manera general los datos en sus redes o realizar búsquedas en curso de actividades ilícitas. Asimismo, advirtió que los sistemas de filtrado pueden vulnerar gravemente la libertad empresaria, al exigir la creación de sistemas complejos y costosos a cargo del intermediario, además de violar el derecho a la información. Este criterio fue reafirmado en la sentencia del TJUE del 16 de febrero de 2012 en el asunto C-360/10 (SABAM contra Netlog NV)[50].

Por otra parte, Si un proveedor de servicios colabora activamente con alguno de sus usuarios en la realización de actividades ilícitas, según la directiva, está sobrepasando su función de simple prestador de servicios, por consiguiente, no puede sacar provecho de la exención de responsabilidad. Además, las limitaciones de responsabilidad no impiden que se tomen medidas para detener cualquier infracción, como la eliminación de contenido ilegal o el bloqueo de acceso al mismo.

Así, para que un prestador de servicios pueda beneficiarse de la limitación de responsabilidad, debe actuar de manera inmediata una vez que tenga un conocimiento claro de la actividad ilegal[51]. Este conocimiento se adquiere cuando una autoridad competente emite una

[47] Electronic Frontier Foundation. (2015). Principios de Manila sobre Responsabilidad de los Intermediarios. https://www.eff.org/files/2015/06/23/manila_principles_1.0_es.pdf

[48] SIGÜENZA, ALICIA. (2016) "La libertad de expresión en Internet" en El Derecho de Internet, Atelier Libros Jurídicos. Barcelona. pp. 57 y ss.

[49] IBIDEM

[50] Tribunal de Justicia de la Unión Europea. (2012). STUJE, caso C-360/10, SABAM y Netlog NV, de 16 de febrero de 2012. Citado por Sigüenza, A. (Obra citada, pp. 57 y ss.)

[51] Parlamento Europeo y Consejo de la Unión Europea. (2000). Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), Considerandos 44 a 46.

resolución declarando la ilegalidad, ordenando la retirada del contenido o el bloqueo del acceso, o confirmando la existencia de una infracción, y el proveedor esté al tanto de dicha resolución[52].

En la práctica, el contenido puede ser restringido tanto por ley como por autorregulación o políticas privadas de las compañías. Estas políticas pueden incluir términos y condiciones de uso claros y transparentes que definan el tipo de contenido no deseado susceptible de ser removido, los criterios considerados para ello, el método de implementación y los recursos disponibles para el usuario. Siendo por ello importante que estas políticas no impliquen prácticas discriminatorias ni vulneren los derechos humanos[53].

Dado la naturaleza global de Internet, sería beneficioso establecer una estructura clara en cuanto a la responsabilidad de los proveedores de servicios, y esto permitiría garantizar un Internet abierto y accesible para todos[54].Internet y las plataformas digitales han facilitado la libertad de expresión, el intercambio de ideas y el acceso a información, aspectos esenciales para el desarrollo individual y colectivo en una sociedad democrática. Sin embargo, es crucial establecer límites que respeten el equilibrio adecuado, garantizado que cualquier restricción esté prevista por la ley, persiga un objetivo legítimo reconocido internacionalmente y sea necesaria para lograr dicho objetivo[55].

2.2. Privacidad y datos personales[56]

Se vive en la actualidad una era llena de oportunidades, donde gran parte de la población mundial está conectada y numerosos aspectos de la vida están digitalizados, a la vez que las nuevas tecnologías están transformando el mundo a gran velocidad, generando cambios disruptivos. Esta transformación digital ha supuesto evolucionar del mundo físico a uno digital, lo que, junto con una mayor capacidad de almacenamiento y procesamiento de información, y la expansión del acceso a las telecomunicaciones y la integración de diversas tecnologías como la inteligencia artificial, el Big Data, el aprendizaje automático, la robótica, la computación en la nube y la tecnología Blockchain, está acelerando los avances, convirtiendo los datos y la información en elementos cruciales[57]

La innovación tecnológica ha desarrollado herramientas que permiten almacenar, procesar y analizar grandes cantidades de datos de manera rápida, simple, económica y automatizada, facilitando el tomar de decisiones en el momento, pasando a ser un preciado activo para el comercio. Así, numerosas empresas recopilan datos y los utilizan para asesorar a

[52] SIGÜENZA, ALICIA. (2016) "La libertad de expresión en Internet" en El Derecho de Internet, Atelier Libros Jurídicos. Barcelona. pp. 57 y ss.
[53] Lanza, E. (2017). Estándares para una Internet libre, abierta e incluyente. *Relatoría Especial para la Libertad de Expresión. Comisión Interamericana de Derechos Humanos, Organización de los Estados Americanos. OAS Cataloging-in-Publication Data*.
[54] Comisión Interamericana de Derechos Humanos en estándares para un Internet Libre, Abierto e Incluyente. (1959 se creó la CIDH). https://www.cidh.org/annualrep/99span/capitulo2.htm#:~:text=La%20CIDH%20fue%20creada%20en,para%20investigar%20una%20situación%20particular. (5 de marzo 2023).
[55] IBIDEM
[56] Garriga, A. (2016). Nuevos retos para la protección de datos personales: en la Era del Big Data y de la computación ubicua.
[57] Lima, D. D. (2023). Transparencia y protección de datos personales en el ámbito universitario: ¿avance o retroceso? *Revista española de la transparencia, Núm. 17. Número Extraordinario 2023.* Págs. 201 -224.

otras entidades, además de conocer mejor a su clientela, atraer a nuevos segmentos de mercado y crear ventajas competitivas.

Aunque todo esto ofrece grandes beneficios, también conlleva ciertos riesgos. Entre estos riesgos está el desafío de categorizar los datos porque que la mayoría de los sistemas actuales no pueden distinguir entre información sensible y no sensible. Es crucial, por tanto, encontrar formas eficaces de proteger los derechos fundamentales de las personas, incluyendo su privacidad y su intimidad[58]

Según el Diccionario de la RAE, la se define la "privacidad" como el derecho a proteger aspectos de la vida privada frente a la divulgación de información, mientras que la "intimidad" se refiere a la esfera más personal y reservada de la vida de una persona o grupo, especialmente en el ámbito familiar. Es decir, la privacidad es un término más extenso, el cual incluye diversos y variados aspectos de la vida de una persona, que al conectarse pueden mostrar una imagen completa de su personalidad, la cual tiene derecho a mantener en confidencialidad[59].

En esta etapa, la protección de la privacidad ha ganado una relevancia significativa. Los datos personales están estrechamente vinculados con la dignidad y la privacidad de los individuos, siendo su resguardo considerado un derecho fundamental, respaldado por varios tratados internacionales. Entre ellos se encuentran el artículo 12 de la Declaración Universal de Derechos Humanos (DUDH), el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, el artículo 8 del Convenio Europeo de Derechos Humanos (CEDH) y el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea. Estos textos conforman el marco normativo internacional que protege a la privacidad y la seguridad de los datos personales, resaltando su importancia para preservar la dignidad humana y el respeto a la vida privada.

Por su parte en España, la Protección de Datos de Carácter Personal está reconocida como un derecho fundamental bajo el artículo 18.4 de la Constitución, y se encuentra regulada por la *Ley Orgánica N.º 3/2018 (LOPDGDD)* promulgada de 6 diciembre de 2018. A nivel normativo, la base de este derecho tiene sus raíces en la L*ey Orgánica 5/1992*, que regulaba el tratamiento automatizado de datos de carácter persona. Esta normativa fue posteriormente sustituida por la *Ley Orgánica 15/1999, la* cual implementó la *Directiva 95/46/CE del Parlamento Europeo y del Consejo*, que aborda la protección de las personas en relación con el tratamiento de datos personales y su libre circulación.

De acuerdo con el artículo 4 del RGPD, se entiende por "*datos personales*" toda la información que esté relacionada con una persona física identificada o identificable, también conocida como "*interesado*". Se considera identificable a cualquier individuo cuya identidad puede ser determinada, ya sea de manera directa o indirecta, a través de identificadores como el nombre, número de identificación, datos de localización, o identificadores en línea, entre otros. El término *"tratamiento*" hace referencia a cualquier acción u operación realizada sobre datos personales, ya sea por medios automatizados o manuales, incluyendo su recolección, registro, almacenamiento, modificación, consulta, uso y transmisión.

Este RGPD es aplicado a la gestión de cualquier dato personal incluido en archivos o destinado a ser incluido en los mismos, independientemente de si el tratamiento es automatizado o no, según refiere el artículo 2 de este RGPD. En este sentido, una de las novedades de este reglamento es que su ámbito de aplicación territorial avala una mayor protección para las

[58] De Miguel, P. A. (2015). *Derecho privado de Internet*. Thomson Reuters-Civitas.

[59] Diccionario de La Real academia española, definición de Privacidad. URL: https://dle.rae.es/privacidad. (6 de marzo de 2023).

personas. Se adapta, por tanto, a la realidad digital actual, asegurando que quienes traten datos personales en la UE cumplan con los requerimientos de protección referidos en la normativa europea, incluso si se hallan fuera de sus fronteras. De este modo, el RGPD busca afrontar las nuevas necesidades del entorno digital y salvaguardar los derechos esenciales de las personas, sin importar dónde se transfieran dichos datos personales.

El artículo 5 del RGPD establece los principios fundamentales para el tratamiento de los datos personales y la responsabilidad proactiva de quienes los gestionan. Entre estos principios se incluyen: licitud, transparencia y lealtad en el tratamiento; minimizar el uso de datos, se delimita a los necesarios; exactitud y actualización de los datos, así como la limitación del tratamiento con fines legítimos y claros. Por lo tanto, el artículo 5 del RGPD no solo establece los principios fundamentales para el tratamiento de datos personales, sino que también introduce el concepto de responsabilidad proactiva, exigiendo a las organizaciones que adopten una actitud consciente, diligente y proactiva en la protección de los datos personales[60]

En lo referente a la seguridad, el Considerando (85) del RGPD resalta la importancia de actuar rápidamente en caso de vulneraciones de la seguridad de los datos personales con el propósito de minimizar el impacto potencial de la brecha, prevenir daños adicionales, además de cumplir con las obligaciones legales de notificación. En este sentido, se destaca que se pueden generar daños tanto de carácter material e inmateriales, además de considerables consecuencias económicas y sociales[61]

2.2.1. La protección de los Datos Personales en España y el Impacto del RGPD

España lleva años implementando una normativa exhaustiva en materia de protección de datos destacando espacialmente la Ley Orgánica 3/2018[62] que regula la Protección de Datos Personales y garantía de los derechos digitales. Esta ley tiene como objetivo principal alinear la legislación española con el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, además de asegurar la protección de los derechos digitales de los ciudadanos.

La ley, estructurada en 97 artículos, comienza en su Título I regulando las disposiciones generales, con el propósito de adaptar la normativa española al RGPD y garantizar los derechos digitales conforme al artículo 18.4 de la CE. A la vez que también aborda la regulación de los datos de personas fallecidas, permitiendo a familiares o allegados solicitar acceso, modificación o eliminación de estos datos, siempre respetando la voluntad del fallecido. El Título II, por su parte, establece los principios generales de la protección de datos, como la precisión y confidencialidad, y regula que el tratamiento de datos personales debe contar con el consentimiento del afectado, fijando en 14 años la edad mínima para el consentimiento de menores. Mientras que el Título III reglamenta los derechos de las personas, acentuando el principio de transparencia con una orientación de "información por capas". Por otra parte, los ciudadanos pueden ejercer directamente o mediante un representante derechos como el acceso, rectificación, supresión, portabilidad y oposición de los datos, tal y como figura recogida en los artículos 15 a 22 de este RGPD.

El Título IV de la ley regula situaciones específicas relacionadas con el tratamiento de datos, sin pretender abarcar de manera exhaustiva todos los tratamientos lícitos. Por su parte, el Título V se centra en las obligaciones del responsable y del encargado del tratamiento. En su

[60] Álvarez, C. y Paricio, M. (2023, mayo). RGPD y las claves de la responsabilidad proactiva para su aplicación. KPMG. https://www.tendencias.kpmg.es/2023/05/rgpd-claves-responsabilidad-proactiva-aplicacion/
[61] GDPR-text. (2024). Considerando 85. https://gdpr-text.com/es/read/recital-85/
[62] Gobierno de España. (2018). Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales, N.º 3/2018. Boletín Oficial del Estado.

Capítulo I, se exige a los responsables y encargados la adopción de medidas técnicas y organizativas adecuadas para asegurar que el tratamiento de los datos cumpla con las normativas vigentes, siguiendo los lineamientos de los artículos 24 y 25 del RGPD. El Capítulo II detalla las responsabilidades específicas del encargado del tratamiento, mientras que el Capítulo III se enfoca en el papel del delegado de protección de datos. Finalmente, el Capítulo IV subraya la relevancia de los códigos de conducta y la certificación, estableciendo que serán vinculantes para quienes las adopten y que incluirán mecanismos de resolución extrajudicial de disputas.

El Título VI de la ley aborda la transferencia internacional de datos personales, estableciendo las normativas aplicables a ese tipo de operaciones. Por otro lado, el Título VII se centra en las autoridades responsables de la protección de datos, destacando el papel de la Agencia Española de Protección de Datos (AEPD), que actúa bajo las directrices del RGPD, la LOPDGDD y sus reglamentos. También se menciona la existencia de organismos de protección de datos en el ámbito autonómico, que pueden tener atribuciones específicas en ciertas áreas. Además, se fomenta la colaboración entre estas autoridades para asegurar una gestión coordinada y eficiente.

Por último, el Título X reafirma los derechos digitales, estableciendo en su artículo 79 que los derechos fundamentales presentes en la Constitución y en los tratados internacionales también se extienden al entorno digital. Los proveedores de servicios digitales y de Internet están obligados a asegurar el respeto y cumplimiento de estos derechos en sus plataformas y operaciones.

En el contexto de los derechos digitales en España, se han establecido y garantizado varios derechos alineados con el artículo 18.4 de la Constitución. Se destaca:

- La Ley 3/2018 establece el derecho a la neutralidad en la red, lo que significa que los proveedores de servicios deben ofrecer sus servicios de manera transparente y sin discriminaciones, ya sean por motivos técnicos o económicos[63].
- En el contexto de los derechos digitales en España, se han establecido y garantizado varios derechos alineados con el artículo 18.4 de la CE. Entre ellos, LOPDGDD establece el derecho a la neutralidad en la red, lo que implica que los proveedores de servicios deben ofrecer sus servicios de manera transparente y sin discriminación, ya sea por motivos técnicos o económicos. Además, la ley garantiza el derecho universal al acceso a Internet, independientemente de la condición social, económica o geográfica. Por ello, este acceso debe ser asequible, de calidad y no discriminatorio[64].
- La Ley también garantiza el derecho a la seguridad digital, exigiendo que los proveedores informen adecuadamente a los usuarios sobre la seguridad de sus comunicaciones[65].
- En cuanto a la educación digital, se promueve la inclusión de todos en la sociedad digital, asegurando la enseñanza de la utilización segura de las tecnologías y respetando los valores constitucionales, la dignidad humana, los derechos fundamentales y la privacidad. A este respecto, está previsto que los docentes reciban la formación precisa en competencias digitales y que los planes de estudio se adecúen para contener este tipo de formación[66].

[63] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del Estado. (5 de marzo de 2023)
[64] Ibidem, pp 119854 BOE
[65] Ibidem, pp 119851 BOE
[66] Ibidem, pp 119851 BOE

En lo que respecta a la protección de los menores en Internet, la ley fomenta un uso responsable y equilibrado de las tecnologías digitales para asegurar su desarrollo personal, salvaguardando su dignidad y sus derechos fundamentales. El uso no autorizado de imágenes o datos de menores en redes sociales puede considerarse una infracción de sus derechos, lo que podría motivar la intervención del Ministerios Fiscal. También se contempla la puesta en marcha de un plan de acción orientado a educar, concienciar y formar a los menores sobre el uso responsable de las redes sociales, los dispositivos digitales y los servicios de la sociedad de la información. Asimismo, se garantiza la protección de los datos de los menores en línea, siempre priorizando su interés superior y sus derechos fundamentales[67]. Entre otros derechos digitales que se destacan:

- Derecho de rectificación en Internet. Se asegura el derecho a la libertad de expresión, y se exige que las plataformas y redes sociales adopten protocolos que permitan ejercer el derecho de rectificación[68]
- Derecho de actualización. Los usuarios tienen el derecho de solicitar a los medios digitales que incluyan una nota de actualización claramente visible junto a las noticias o contenido que ya no reflejan la realidad actual.
- Derechos digitales en el entorno laboral: los empleadores están obligados a definir normas para el uso de dispositivos digitales, garantizando el respeto por la privacidad de los trabajadores. Los representantes de los trabajadores deben participar en la elaboración de estos criterios, y si se permite el uso privado de dispositivos laborales, los empleadores deben especificar los límites y garantizar la protección de la intimidad, incluyendo periodos de uso privado.[69]
- Derecho a la desconexión digital. Este derecho busca garantizar el respeto al tiempo de descanso, permisos y vacaciones, así como proteger la privacidad fuera del horario laboral, dependiendo de la naturaleza de la relación laboral[70].
- Derecho a la privacidad en la videovigilancia. Los empleadores están obligados a informar claramente a los trabajadores sobre el uso de cámaras, y estas no pueden instalarse en áreas de descanso, como comedores o vestuarios[71].
- Protección de datos en el ámbito laboral: Las empresas están obligadas a notificar a sus empleados sobre los dispositivos que recopilan datos personales y a informales sobre sus derechos relacionados, como el acceso, la rectificación, la limitación del tratamiento y la eliminación de dichos datos. Además, los convenios colectivos pueden incluir salvaguardias adicionales para proteger estos derechos
- Derecho al olvido: El derecho al olvido se aplica específicamente a las búsquedas en internet y servicios de redes sociales. Este derecho es fundamental para proteger la privacidad en la era digital, está regulado en el RGPD y fue establecido por el Tribunal de Justicia de la Unión Europea en el caso Google España vs AEPD y María Costeja

[67] Romero, N. (2021, septiembre). Derechos digitales de los niños: cómo protegerlos mientras exploran internet. INEAF. https://www.ineaf.es/tribuna/derechos-digitales-de-los-ninos-como-protegerlos-mientras-exploran-internet/

[68] Calvo, J. M. (2020). El derecho de rectificación ante informaciones falsas o inexactas, con especial mención a las publicadas en Internet. Revista de Derecho civil, 7(4), Págs. 137-181.

[69] Andrés, M. B. (2021). Génesis y desarrollo de los derechos digitales. Revista de las Cortes Generales, Págs. 197-233.

[70] Portero, M. (2023). Derecho a la desconexión digital. Temas laborales: Revista andaluza de trabajo y bienestar social, (168), Págs. 393-413.

[71] Andrés, M. B. (2021). Génesis y desarrollo de los derechos digitales. Revista de las Cortes Generales, Págs. 197-233.

González (C-131/12)[72]. Según esta sentencia, los motores de búsqueda tienen que eliminar de sus resultados los enlaces a páginas web que tengan información personal de una persona, incluso si la información sigue siendo legalmente accesible en esas páginas. Esto asegura que los individuos puedan controlar la visibilidad de su información personal en línea[73].

- Derecho a la portabilidad en servicios de redes y servicios semejantes. Los usuarios tienen derecho a recibir y transmitir el contenido generado a través de estos servicios.
- Derecho al testamento digital. Los familiares autorizados pueden decidir si los perfiles de personas fallecidas en redes sociales se mantienen o se eliminan, a menos que la persona haya dejado instrucciones claras[74].

En conclusión, la legislación española ha avanzado considerablemente en la protección de los derechos digitales, no solo adaptando el RGPD, sino yendo más allá para responder a los retos que plantean las innovaciones y garantizar el amparo de los derechos fundamentales.

2.3. Derechos de autor.

La "*propiedad industrial*" está definida por la RAE como el derecho exclusivo de explotación de obras literarias o artísticas, el cual es reconocido por la legislación a su creador durante un tiempo determinado. Por su parte, el "Derecho de autor" es el derecho legal otorgado el autor de una obra intelectual o artística, que le permite autorizar su reproducción y obtener beneficios económicos de ella [75].

En este escenario, la Organización Mundial de la Propiedad Intelectual (OMPI) asocia la propiedad intelectual con las obras del ingenio humano, que incluyen invenciones, obras literarias y artísticas, así como símbolos, nombres e imágenes empleados en el comercio. Su misión es proteger estas creaciones para estimular la creatividad y la innovación, utilizando diversas herramientas como patentes, derechos de autor y marcas registradas[76].

Esto que se ha expuesto, está respaldado, por el artículo 27.2 de la DUDH, que establece que *"toda persona tiene derecho a la protección de los intereses morales y materiales que le correspondan por razón de las producciones científicas, literarias o artísticas de que sea autora*", así como en el artículo 17.2 de la Carta de Derechos Fundamentales de la Unión Europea. El primero reconocimiento formal de estos derechos ocurrió en el Convenio de País para la protección de la Propiedad Industrial de 1883 y en el Convenio de Berna para la Protección de Obras Literarias y Artísticas de 1886[77].

En este sentido, se diferencia entre la propiedad industrial, que hace referencia a patentes, marcas, diseñados industriales e indicaciones geográficas, y el derecho de autor, que

---

[72] Tribunal de Justicia de la Unión Europea. (2014). Sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014, asunto C-131/12.
[73] Agencia Española de Protección de Datos. (2024a, julio) Ejerce tus derechos. https://www.aepd.es/derechos-y-deberes/ejerce-tus-derechos
[74] Imbernón, N. M. (2020). El testamento digital en la nueva Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. *Anuario de derecho civil*, *73*(1), Págs. 241-281.
[75] Diccionario de la Real Academia Española, URL: https://dle.rae.es/derecho?m=form#CUr4nPg.
(23 de marzo de 2023)
[76] Organización Mundial de la Propiedad Intelectual: https://www.wipo.int/portal/es/
(23 de marzo de 2023)
[77] OMPI: ¿Qué es la Propiedad Intelectual? (23 de marzo de 2023) URL:
https://mision.sre.gob.mx/oi/index.php/areas-tematicas/propiedad-intelectual.

circunscribe, entre otros a obras literarias y artísticas música, películas, diseños arquitectónicos, etc. Las ideas están protegidas por la propiedad intelectual[78]

2.3.1. Protección jurídica en España.

La base esencial es que el titular de la creación original posee el derecho a reproducirla y a controlar si otros la copian. Esta protección se activa desde el momento en que la creación se expresa en algún formato. La tecnología influye considerablemente en este derecho, haciendo que el sistema evolucione para adaptarse a las nuevas realidades y formas de expresión.

En España la protección de los derechos de autor se encuentra garantizada por la Constitución Española (artículo 20,1 b), por la Ley de Propiedad Intelectual (LPI), por el Real Decreto Legislativo 1/1996, sus normas reglamentarias, así como por el Código Civil y el Penal. Es relevante señalar que una parte de la doctrina considera derechos fundamentales, adquiriendo esta categoría gracias a los tratados internacionales ratificados por el país. Para los propósitos de este análisis, los abordaremos como derechos fundamentales, conforme a los dispuesto en el artículo 10.2 de la Constitución. La legislación establece que la propiedad intelectual de cualquier obra literaria, artística o científica corresponde al autor por su creación, quien posee el derecho exclusivo para explotar la obra, así como derechos personales y patrimoniales asociados.

Todas las obras originales en los ámbitos literario, artístico o científico, independientemente del medio o formato en que se presenten, ya sea físico, digital o en alguna forma aún no conocida, gozan de protección. Esto incluyendo:

a) Publicaciones, textos, charlas, panfletos, presentaciones y otros materiales parecidos.

b) Composiciones musicales, con o sin letra.

c) Obras dramáticas, coreografías, pantomimas y otras obras teatrales.

d) Obras cinematográficas y audiovisuales.

e) Esculturas, pinturas, dibujos, grabados, litografías, cómics y otras obras plásticas.

f) Trabajos, modelos y propuestas vinculados a la cartografía, esquemas

g) Obras fotográficas y similares.

h) Programas de software

Las obras derivadas, tales como adaptaciones, traducciones, revisiones, actualizaciones, compendios, arreglos musicales, anotaciones, resúmenes y cualquier modificación de una creación literaria, científica o artística, también cuentan con protección. Igualmente, se consideran protegidas las colecciones y bases de datos, que, con conjuntos de obras, datos u otros elementos independientes organizados de manera sistemática y accesibles de forma individual[79].

Es esencial que la obra sea original, creativa y se exprese mediante cualquier formato. La originalidad se refiere a la forma en que se presenta la idea, la cual no puede ser reproducida

[78] Organización Mundial de la Propiedad Intelectual. (2024c). ¿Qué es la Propiedad intelectual?. https://www.wipo.int/edocs/pubdocs/es/wipo_pub_450_2020.pdf

[79] Registro de la Propiedad Intelectual. (2024, junio). Propiedad Intelectual. https://www.cultura.gob.es/cultura/areas/propiedadintelectual/mc/rpi/que-es/pi.html

de un trabajo existente; no se requiere que la idea sea novedosa. La Ley de Propiedad Intelectual (LPI) excluye de esta protección a normativas o reglamentos, así como sus borradores, decisiones de tribunales, y actos, acuerdos, deliberaciones y dictámenes de entidades públicas, incluyendo traducciones oficiales de los mencionados documentos[80].

Se considera "autor" a la persona, tanto natural como jurídica, que es la responsable de producir una obra de carácter literario, científico o artístico. Dicha obra puede ser desarrollada de manera individual, en conjunto con otros autores, de forma colectiva, compuesta o independiente. Además, es necesario considerar las circunstancias en las que una obra es creada por un empleado, así como los aspectos particulares que involucran la elaboración de un sotfware. Si el autor es una persona física, la protección de la obra se extiende a lo largo de toda su vida y por 70 años después de su fallecimiento. En el caso de una persona jurídica, la protección dura 70 años a partir del 1 de enero del año siguiente a su creación o divulgación[81].

Según Susana Checa Prieto, la protección de los derechos de autor se extiende también a las bases creadas como obras intelectuales, bajo las mismas características que cualquier otra obra susceptible de protección. El derecho sui generis protege la disposición y el formato de la obra impidiendo así que se descargue, ya sea completa o parcialmente, el contenido de la base de datos usando un buscador para crear otra base con una apariencia distinta y obtener beneficios comerciales de ella. Esto significa que, al adquirir una base de datos, se permite su uso, pero no su comercialización posterior. Además, los autores de las obras incluidas en la base de datos se conservan derechos adicionales en función de cada caso[82].

Los derechos de autor también se aplican a las bases de datos creadas como obras intelectuales, bajo las mismas condiciones que cualquier otra obra protegida. El derecho sui generis protege la organización y estructura de la base de datos, prohibiendo la descarga total o parcial de su contenido mediante un motor de búsqueda para crear otra base de datos con una interfaz diferente y explotarla comercialmente. Esto significa que, al adquirir una base de datos, se permite su uso, pero no su reventa comercial. Además, los autores de las obras incluidas en la base de datos mantienen derechos adicionales según cada caso específico[83]

En consecuencia, España debería modificar la LPI para alinearse con las nuevas directrices, lo que fomentará la investigación y el desarrollo. Estas modificaciones reflejarán las nuevas realidades y abordarán futuras regulaciones relacionadas con la inteligencia artificial y la robótica, asegurando que la legislación esté actualizada y adecuada a los avances tecnológicos.

V. LA SEGURIDAD EN EL MUNDO DIGITAL: CÓMO AFECTA A LA EMPRESA

El uso adecuado de la tecnología e internet aporta grandes ventajas para todos, pero su mal uso puede generar daños y comprometer la seguridad de individuos, empresas, gobiernos, e incluso de dispositivos y sistemas.

---

[80] García, T. (2016). Análisis del criterio de originalidad para la tutela de la obra en el contexto de la ley de propiedad intelectual. *Anuario Jurídico y Económico Escurialense, XLIX (2016).* Págs. 251-274

[81] Corzo, M. (2006). Derecho de Autor en las Obras Creadas Por Encargo y en el Marco de Una Relación Laboral, El. *-11 Rev. Prop. Inmaterial*, *10*, 45.

[82] CHECA SUSANA, 2019). Los derechos de autor. En Nota Técnica 3, Máster de Acceso a la Abogacía, Derecho Informático y Nuevas Tecnologías, Universidad de Nebrija.

[83] Casas, R y Xalabarder, M. (2022). Introducción a la propiedad intelectual. https://openaccess.uoc.edu/bitstream/10609/147156/3/RegimenJuridicoDeLaComunicacion_Modulo5_IntroduccionALaPropiedadIntelectual.pdf

Mar Goodman en su obra "Future Crimes", destaca a un aspecto que a menudo se considera ignorado: los delincuentes están continuamente perfeccionando sus métodos y utilizando las últimas innovaciones tecnológicas en sus actividades delictivas se comportan como "primeros usuarios" de tecnologías emergentes, lo que ha llevado al aumento del cibercrimen en áreas como la robótica, la realidad virtual y la inteligencia artificial. A medida que nos volvemos más dependientes del entorno digital, la tecnología se convierte en un arma de doble filo, facilitando que quienes poseen ciertos conocimientos puedan causarnos daño si no tomamos las medidas necesarias para protegernos. La interconexión total aumenta nuestra vulnerabilidad, lo que facilita que los ataques cibernéticos desestabilicen la seguridad a nivel global[84]

1. Riesgos asociados a las PYMES y fugas de información

Existen tres tipos principales de filtración de datos: accidental, intencionada o mediante un ataque externo. Cuando la filtración es intencional, aunque su prevención completa puede ser complicada, se pueden aplicar medidas de seguridad para rastrear quién tuvo acceso a la información y así identificar al responsable. En el caso de filtraciones accidentales, estas representan un problema considerable para la empresa; la mejor forma de prevenirlas es capacitar a los empleados en medidas de seguridad que minimicen los errores. Por otro lado, si la fuga de información resulta de un ataque externo, se deben establecer sistemas que dificulten al máximo el acceso no autorizado y que aseguren que, incluso si se logra extraer información, esta no pueda ser leída fácilmente[85].

Es crucial también tener en cuenta otros riesgos, como las filtraciones de datos por mal uso de la nube, correo electrónico o ataques de ingeniería social, como soporte técnico falso o la explotación de la página web de la empresa para instalar software malicioso. Para abordar estos riesgos, la organización debe establecer una lista de buenas prácticas y cumplir con los requisitos legales para proteger su seguridad. La implementación de políticas de seguridad adecuadas y la promoción de buenas prácticas son esenciales para proteger la información y los sistemas de la empresa[86].

El objetivo principal es salvaguardar la información y los sistemas mediante acciones como: aplicar medidas de seguridad para asegurar un acceso protegido tanto a los equipos como a los servicios en la nube, clasificar la información según su nivel de importancia, establecer permisos de usuario específicos, mantener el software actualizado, usar antimalware robusto, involucrar al equipo en las tareas de ciberseguridad, e implementar una política de seguridad clara que todos los empleados comprendan y con la que se comprometan. En caso de un incidente de seguridad, este debe ser notificado a la autoridad competente y a los afectados en un plazo máximo de 72 horas, conforme al RGPD, del cual se tratará en detalle más adelante[87].

2. Medidas de ciberseguridad que debe llevar a cabo una PYME

Las grandes empresas, por su tamaño, volumen de negocio y su internalización, fueron las primeras en comprender la importancia de protegerse de las amenazas cibernéticas tras sufrir

---

[84] GOODMAN, MARC, (2016) "Future Crimes. Inside the digital underground and the Battle for Our Connected World", Anchor Books, United States, New York, January. pp 6 y ss.

[85] INCIBE. (2023). Gestionar fuga de información. https://www.aepd.es/guias/guia-incibe-aepd-gestionar-fuga-de-informacion.pdf

[86] INCIBE. (2019a, mayo). Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse. https://www.incibe.es/empresas/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse

[87] INCIBE. (2023a). Guía de ciberseguridad. La ciberseguridad al alcance de todoshttps://www.incibe.es/sites/default/files/docs/senior/guia_ciberseguridad_para_todos.pdf

ataques. Sin embargo, las pequeñas y medianas empresas (PYMES) tardaron más en darse cuenta de que también son objetivos atractivos para los cibercriminales. Hoy en día, se estima que aproximadamente el 50% de los ataques informáticos afectan a las pymes. Mientras que las grandes corporaciones cuentan con recursos suficientes para destinar importantes cantidades de dinero a la ciberseguridad, las PYMES[88].deben recurrir a soluciones más simples, económicas, pero igualmente eficaces. Diversas instituciones, tanto públicas como privadas, ofrecen recomendaciones y datos relevantes en este ámbito.

- El Instituto Nacional de Ciberseguridad (INCIBE) destaca la importancia de contar con un protocolo eficaz que todos los empleados puedan seguir correctamente
- Sophos enfatiza la importancia de vigilar los controles de acceso, los permisos, la red empresarial, los puertos abiertos, las conexiones y los recursos compartidos. También desaconseja la descarga de archivos desde sitios no seguros.
- Kaspersky se enfoca en la prevención del phishing y alerta sobre el uso de dispositivos USB o discos duros de origen desconocido.
- Randed informa que el coste promedio para una empresa tras un ciberataque exitoso es de 35.000€, una cifra inasumibl para muchas pymes. Este dato explica por qué el 60% de las empresas no se recupera después de sufrir un ataque ditial
- Según el Centro Criptológico Nacional (CNN), en 2021 se registraron más de 25.000 incidentes de ciberseguridad.

Es crucial entender que los cibercriminales explotan las vulnerabilidades de nuestras redes, por lo que es esencial priorizar su protección. Contar con programas antimalware y antivirus con firewall es fundamental para dificultar su actividad ilícita. También es importante que los empleados tengan conocimiento sobre los riesgos informáticos, ya que una gran parte de las amenazas provienen de errores o negligencias cometidas por ellos. La amenaza de los malware está estrechamente relacionada con lo anterior; son programas que, a simple vista, parecen legítimos pero que en realidad crean una “puerta trasera” en el sistema, permitiendo a los individuos malintencionados acceder a la información. Para prevenirlo, es clave evitar la instalación de dichos programas, pero muchos empleados no son conscientes de estos riesgos y puedan cometer imprudencias costosas[89].

Es esencial que las empresas, especialmente aquellas que manejen información estratégica y financiera, se tomen en serio estas recomendaciones y adopten medidas como la encriptación segura de datos sensibles. Confiar en plataformas que han demostrado buenas prácticas y han ganado una sólida reputación puede enviar un mensaje claro de que quienes no se tomen la ciberseguridad en serio quedarán fuera del mercado. Esto ayudará a fortalecer la seguridad de los servicios en general.

2.1. Correo digital o electrónico.

En nuestros días, el correo electrónico se ha convertido en una herramienta indispensable para las empresas debido a su versatilidad. Sin embargo, su utilidad lo ha transformado también en un medio atractivo para quienes cometen fraudes y ciberataques. A

[88] GÓNZALEZ ROCÍO. (2018, 1 de octubre). Más de la mitad de las pymes sufren ciberataques. *Cinco Días*. (25 de abril 2023) https://cincodias.elpais.com/cincodias/2018/09/28/pyme/1538169199_927487.html

[89] ISMS. (2023). Guía para la gestión de la ciberseguridad en el entorno industrial de una PYME. https://www.ismsforum.es/ficheros/descargas/guia-entornos-industriales-20231686772410.pdf

continuación, se presentan los principales tipos de fraude relacionados con el correo electrónico que las empresas deberían conocen y sobre los que es fundamental educar a los empleados[90].

⇒ Phishing. Se conoce "phshing" como el método que emplea la falsificación de identidad a través de correos electrónicos engañosos para obtener información sensible, en particular detalles financieros o bancarios. Las acciones preventivas recomendadas incluyen[91]:

- Comprobar las URL con las que se está interactuando
- Desconfiar de correos electrónicos de entidades bancarias que soliciten información personal
- Verificar los enlaces que se incluyen en los correos
- Ignorar mensajes sospechosos que pidan datos personales, ya sea por email o SMS

⇒ Scam: consiste en engañar a la víctima haciéndole creer que ha ganado un premio, un concurso o ha recibido una herencia, con el objetivo de cobrar una tarifa para liberar los fondos. También se utiliza para obtener información privada[92]

⇒ Malware: Estos correos tienen archivos adjuntos peligrosos creados para infectar el sistema del receptor. Los ciberdelincuentes los envían masivamente, con la esperanza de que algún empleado los abra. Las medidas más efectivas para prevenir ese tipo de ataque son formar adecuadamente a los empleados y usar software antivirus confiable.

⇒ Spam: es el envío masivo de correos electrónicos no deseados, generalmente con fines publicitarios o fraudulentos. Afortunadamente, hoy en día existen filtros de spam avanzados que nos permiten evitar la mayoría de estos correos.

⇒ Fake: se refiere a la difusión masiva de noticias falsas a través de correo electrónico, WhatsApp o Telegram. Estos mensajes suelen estar acompañados de enlaces peligrosos. Para protegerse, es crucial contar con un equipo de trabajo entrenado en ciberseguridad y con herramientas de protección como antivuris y antimalware[93].

⇒ Correo electrónico desechable: al navegador por internet, muchas webs solicitan un correo electrónico para acceder a ciertos servicios. A menudo, esto genera una sobrecarga de correos no deseados en la bandeja de entrada. Aunque existen filtros antispam, en ocasiones no funciona correctamente. Para evitar estos problemas, se pueden utilizar cuentas de correo temporales, que son generadas

[90] INCIBE. (2018, octubre). El correo electrónico como canal para el fraude digital. https://www.incibe.es/empresas/blog/el-correo-electronico-canal-el-fraude-digital
[91] Google. (2020). Panorama actual de la Ciberseguridad en España. https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf
[92] INCIBE. (2019, julio). La formación como elemento imprescindible en ciberseguridad. https://www.incibe.es/empresas/blog/formacion-elemento-imprescindible-ciberseguridad
[93] I Vosoughi, S., Roy, D., y Aral, S. (2018). The spread of true and false news online. science, 359(6380), Págs. 1146-1151.

automáticamente y destruidas después de un tiempo. Las ventajas de utilizar estas cuentas incluyen:

- Proteger nuestros datos de hackers
- Usarlas para registrarse en redes WIFI públicas
- Evitar la inclusión en bases de datos de correo electrónico
- Recibir correos no deseados de manera temporal para obtener algún beneficio, sin usar nuestra dirección principal
- Hacer los ensayos pertinentes en sitios web antes de su publicación oficial
- Enviar correos de forma anónima

Hoy en día, existen numerosas plataformas que ofrecen la posibilidad de crear correos temporales, como 10minutemail, Mohmail y Tempmail entre otras. Estas plataformas se pueden encontrar fácilmente mediante una búsqueda rápida en Internet.

2.2. Seguridad criptográfica.

En el momento de usar servicios de almacenamiento en la nube, uno de los mayores peligros es el acceso no autorizado a la información. Para evitarlo, se deben tomar medidas como las que mencionaremos a continuación[94].

- Establecer credenciales seguras
- Activar la autenticación de doble factor
- Mantener el software siempre actualizado
- Usar un antivirus potente y asegurarse de tener activo el cortafuegos
- Evitar abrir correos sospechosos, especialmente si contienen archivos adjuntos o enlaces
- Priorizar el uso de datos móviles sobre redes WiFi-públicas y, en caso de necesidad, utilizar una red VPN para asegurar la conexión

El trabajo en la nube ofrece muchas ventajas, pero también presenta ciertos riesgos. Entre las ventajas, podemos destacar[95]

a. Hay una alta competencia en el mercado de la nube, lo que motiva a las empresas a mejorar constantemente sus servicios, incluyendo la seguridad a precios accesibles.

[94] Microsoft. (2024, julio). ¿Qué es la seguridad en la nube? https://www.microsoft.com/es-es/security/business/security-101/what-is-cloud-security
[95] Gutiérrez, A. (2018). Almacenamiento en la nube. https://www.acta.es/medios/informes/2018004.pd

b. Según Zinko Colombia, la nube facilita el trabajo colaborativo, permitiendo que varias personas trabajen simultáneamente en un mismo archivo, lo que incrementa la productividad y apoya el trabajo remoto

Por otro lado, las desventajas incluyen:

- La necesidad de una conexión a Internet fiable y de buena calidad. Sin una buena conexión, es difícil aprovechas al máximo las ventajas de la nube.
- La posibilidad de que existan vulnerabilidades en el sistema de la empresa, lo que hace crucial la elección cuidadosa del proveedor de servicios de almacenamiento.

La criptografía es una herramienta clave para proteger los datos en la nube, ya que permite que un archivo sea ilegible a menos que se cuente con la clave de descifrado. Esta técnica es esencial para el manejo de información sensible y es fundamental para evitar que una empresa segura fugar de información. A reputación de una empresa depende en gran medida de su capacidad para proteger la confidencialidad de los datos que maneja, por lo que la criptografía se ha convertido en una medida de seguridad indispensable.

2.3. Gestión de accesos

El recurso más valioso de cualquier organización es la información que se maneja. Muchas empresas u organizaciones invierten avanzadas técnicas de cifrado, equipamiento informático de última generación y software de seguridad integral, pero a menudo descuida el control sobre las personas que tienen acceso a dicha información. A partir de aquí es donde el control de accesos se vuelve esencial. La primera pregunta que debemos hacernos para empezar a proteger adecuadamente la información es: ¿quién la gestiona dentro de la empresa? Pronto nos daremos cuenta de los retos a los que nos enfrentamos, entre ellos, el crecimiento del enfoque BYOD (Bring Your Own Device)[96], permite a los empleados manejar información sensible incluso después de que finalice su relación laboral.

Para prevenir riesgos potenciales, es esencial implementar una serie de medidas clave:

1. Política de usuarios y permisos: se trata de asignar a cada usuario permisos basado en su función dentro de la empresa, asegurándose de que cada empleado tenga acceso únicamente a una información necesaria y limitada para cumplir con sus deberes o responsabilidades. Este principio de "*mínimo privilegio*" reduce el riesgo de accesos innecesarios.
2. Gestión de cuentas de acceso. Un administrador designado tiene que encargarse de la creación, actualización y eliminación de las cuentas de acceso, siendo responsable de otorgar credenciales a los nuevos empleados, así como de garantizar que estas contraseñas se actualicen periódicamente. El administrador también tendrá la

[96] Método de trabajo que consiste en prescindir de los equipos informáticos proporcionados por la empresa, haciendo que sea el propio trabajador quien emplee los suyos propios trasladándolos diariamente desde su vivienda a su oficina y viceversa.

capacidad de ajustar los permisos de acceso según cambien las funciones de los empleados a lo largo del tiempo.[97]

3. Cuentas de administrador: a diferencia de las cuentas estándar, las cuentas de administrador tienen un control total sobre el sistema, lo que las convierte en un activo valiosos. Por esta razón, deben ser especialmente protegidas siguiendo estos pasos:
    a. Primer paso: utilizar contraseñas fuertes y autenticación de doble factor, además de cambiarlas periódicamente
    b. Limitar su uso únicamente a situaciones necesarias
    c. Realizar auditorías frecuentes y mantenerlas bajo constante supervisión
    d. Realizar auditorías frecuentes y mantenerlas bajo constante supervisión
    e. Registrar todas las acciones realizadas desde estas cuentas mediante un registro detallado (logs)
4. Mecanismo de autenticación. Se tienen que evaluar los diversos métodos e autenticación disponibles y seleccionar los más adecuados según las necesidades de la empresa.
5. Registro de actividad: Es crucial registrar los cambios importantes en una base de datos, detallando el momento, la fecha y el usuario que realizó la modificación.

2.4. Credenciales de usuario

Es fundamental revisar periódicamente los permisos de los usuarios para identificar y eliminar aquellos que ya no sean necesarios para sus tareas diarias. Esta revisión constante ayudará a optimizar la seguridad y aplicar una política de ciberseguridad cuidadosamente adaptada a la empresa

2.5. Conciencia de ciberseguridad en la organización

La ciberseguridad en una organización es como una cadena: "*una cadena es tan fuerte como su eslabón más débil*". En este contexto, el eslabón más débil suele ser el propio empleado. Aunque es relativamente fácil equipar a la empresa con sistemas informáticos avanzados y robustos, son los empleados quienes finalmente deben operarlos. Si los trabajadores no están conscientes de la importancia de la ciberseguridad o carecen de la formación adecuada, todos esos esfuerzos pueden resultar inútiles[98].

Aunque los empleados pueden ser considerados el eslabón más frágil de la cadena, también son el más crucial. Conseguir que cada trabajador esté comprometido con la ciberseguridad de la empresa, y que sus labores diarias se alineen con los estándares de protección, es un reto, pero es una inversión que vale la pena.

2.5.1. Establecer cultura de ciberseguridad en la empresa

[97] INCIBE. (2022). Uso de técnicas criptográficas. Políticas de seguridad para la PYME. https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-_tecnicas-criptograficas.pdf
[98] INCIBE. (2019, julio). La formación como elemento imprescindible en ciberseguridad. https://www.incibe.es/empresas/blog/formacion-elemento-imprescindible-ciberseguridad

En cualquier organización, los empleados suelen tener rutinas y métodos de trabajo bien establecidos. Por lo tanto, cuando se introducen nuevas directrices, es común que surjan dudas y que estas indicaciones sean percibidas como un obstáculo innecesario. Es en este punto donde la empresa debe tomar medidas específicas para superar esa resistencia, como las siguientes[99]:

- Capacitación de los empleados: en la realidad empresarial, los cursos de formación en ciberseguridad tienden a ser sesiones generales donde se agrupa a empleados de distintas áreas lo que provoca una baja implicación. Para mejorar esta situación, se recomienda ofrecer una formación personalizada que se ajuste a las responsabilidades de cada grupo dentro de la empresa. Además, la capacitación debe ser continua, con actualizaciones periódicas, especialmente para el personal técnico, que debe contar con los recursos necesarios para mantener un sistema de ciberseguridad eficaz.
- Definición de políticas y protocolos de ciberseguridad. Es esencial que cada empresa cuente con documentos formales que establezcan los pasos a seguir tanto en situaciones rutinarias como en caso de incidentes de ciberseguridad
- Supervisión: se debe designar a un responsable de ciberseguridad dentro de la organización, encargado de asegurar que todas las acciones y políticas se cumplan según lo previsto
- Concienciación: para que las políticas sean exitosas, es fundamental que todos los empleados se vean a sí mismos como piezas clave en la seguridad de la empresa

2.5.2. La ciberseguridad en los distintos sectores empresariales

La ciberseguridad es una prioridad para todas las empresas, no solo para proteger su actividad comercial, sino también para garantizar la confianza y seguridad de las personas que interactúan con ellas. Según el sector en el que opere la empresa, ciertos aspectos de la ciberseguridad requerirán mayor atención debido a las particularidades de cada industria. Algunas de las amenazas más comunes por sectores incluyen: industria, salud, construcción, distribución tanto minorista como mayorista, ocio y tiempo libre, educación logística y servicios profesionales y asociaciones.

Los mayores desafíos en ciberseguridad es conciencias a todos sobre su relevancia. En muchas organizaciones, debido a la falta de información, existe la percepción de que los datos que manejen no son valiosos para otros. Sin embargo, la información es un recurso sumamente valioso que puede convertirse en una ventaja competitiva o en una vulnerabilidad. Un ejemplo de ello son empresas como Facebook o Google que generan ingresos significativos mediante la venta de información a terceros. Por otro lado, existen actores malintencionados que intentan acceder de manera ilegal a datos aprovechando las debilidades de los sistemas.

De acuerdo con el Centro Nacional de Seguridad Cibernética (National Security Centre), de Estados Unidos, las principales medidas de ciberseguridad que debe implementar una empresa incluyen:

- gestión adecuada de riesgos
- mantener los Softwares actualizados

[99] INCIBE. (2024b). Gestión RRHH Política de seguridad para PYMES. https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/2024/Gestion_RRHH_Pol%C3%ADtica_de_seguridad_2024.pdf

- proteger la red
- tener un plan de protección contra software maliciosos
- controlar los Privilegios de usuario
- gestionar los dispositivos externos de forma segura
- monitorear redes y servicios en tiempo real
- conciencias a los usuarios sobre los riesgos cibernéticos
- establecer protocolos claros sobre el uso de dispositivos móviles
- garantizar la continuidad del negocio en caso de incidentes

VI. DESAFÍOS Y POSIBILIDADES LEGALES EN LA ERA DIGITAL

Como hemos visto anteriormente, existen multitud de desafíos a los que esta nueva realidad digital debe de hacer frente tanto para las personas como las empresas y las administraciones públicas. Dicha transición digital tiene una influencia en todos, mientras que las personas piensan de forma lineal debido a la educación que recibimos, la tecnología progresa de manera exponencial esto va a producir una gran diferencia entre los que aprovechan este cambio y se adaptan a la innovación frente a los que se mantienen reticentes al cambio, aferrados a lo tradicional[100].

El modelo vertical en la nueva realidad digital se incorpora debido a la interoperabilidad, lo que permite manejar la información de manera más ordenada. Esto incrementa la velocidad de los procesos y genera una mayor eficiencia, reduciendo tiempos, costos y errores. Además, la digitalización fragmenta los procedimientos y negocios tradicionales, permitiendo la especialización en distintas partes de la cadena de valor. Este progreso se refleja en el aumento del valor de industrias tradicionales como la banca, el entretenimiento y las telecomunicaciones[101]

En esta nueva situación, el factor tiempo es un elemento clave. Por lo que es fundamental actuar de una forma correcta y veloz para poder así transformarse y competir justamente. También es necesario realizar una evaluación continua para poder calcular el progreso y obtener los resultados de dicha innovación adoptada, esto se hace con el fin de actuar en consecuencia de lo conseguido para que la digitalización verdaderamente se universalice y todas las personas puedan formar parte y saber adaptarse.

Es un necesario tan cambiante y en el que todo ocurre a una desmesurada rapidez, actuar con diligencia es esencial, sin embargo, debido a que existen grandes oportunidades que permiten el crecimiento de todos los países hay que tener precaución con respecto a la regulación de esta nueva realidad ya que pueden provocar inseguridad y esta a su vez desencadenar en una pérdida de inversiones de talentos, junto con el desarrollo e innovación. Cada vez es más indispensable: sintetizar, escuchar, reconocer los riesgos e inconvenientes,

[100] Cámara de Comercio de España. (2020). Una iniciativa para la transición digital. https://www.camara.es/sites/default/files/publicaciones/inciativa-transicion-digital.pdf

[101] Grant Thorton. (2018). Ciberseguridad: protegiendo el valor de los datos. https://www.grantthornton.es/globalassets/1.-member-firms/spain/folletos/2018-ciberseguridad_protegiendo-el-valor-de-los-datos.pdf

producir valor, adaptarse junto con la transición, entender que modelos han variado, que las barreras se han borrado en muchos casos en los diferentes mercados y por lo tanto surgen nuevos competidores, enseñar y defender a los clientes.

Como hemos visto anteriormente, sin duda los reguladores tienen que hacer frente a considerables desafíos, pero también pueden colaborar en contribuir en el apropiado crecimiento, fomentar la innovación, otorgando previsibilidad y contribuyen de forma directa el poder conseguir capitalistas.

Tal y como la Dra. Cristina Vázquez[102], señala en su análisis sobre los desafíos regulatorios en el contexto de la digitalización, la regulación juega un papel clave en mantener el equilibrio dentro del sistema regulador. Sin embargo, es un proceso complicado debido a la naturaleza de las relaciones entre las partes involucradas, en los que cada grupo busca satisfacer sus propios intereses, lo que dificulta una satisfacción plena para todos. Tanto la teoría como práctica indican que es esencial reforzar estos organismos mediante un mayor presupuesto, más información y mayor autonomía. Además, las normativas se complementan con servicios administrativos específicos, enfrentándose a retos importantes, como la falta de acceso a información completa, el riesgo de captura política o de los agentes regulados, y la debilidad en el apoyo por parte de los consumidores. Es fundamental que los objetivos de la regulación prioricen la protección de los derechos de los usuarios, mientras que la sostenibilidad, la eficiencia y la equidad deben ser metas adicionales. Asimismo, las normativas deben de cumplir con el principio de proporcionalidad, evaluando cuidadosamente la idoneidad y la necesidad de las decisiones adoptadas.

La regulación se presenta como un proceso complejo, caracterizado por relaciones interdependientes que requieren un enfoque equilibrado. Para lograrlo, es fundamental que los organismos reguladores cuenten con los recursos necesarios, tanto en términos de presupuesto como de capacitación, para operar de manera autosuficiente. Además, las normativas deben estar fundamentadas en principios de proporcionalidad, asegurando que cada decisión adoptada sea adecuada, necesaria y proporcional a los fines que se persiguen, como la protección de los derechos de los consumidores y la promoción de la sostenibilidad y la equidad[103].

Entre los retos actuales, Aramendía identifica la necesidad de crear marcos regulatorios ágiles que se adapten rápidamente a las innovaciones del entorno. La fragmentación y la superposición de regulaciones representan un obstáculo significativo, al igual que el riesgo de traspasar límites regulatorios que podrían generar confusiones. Asimismo, la privacidad y la seguridad digital requieren un balance cuidadoso, así como la necesidad de abordar la opacidad de los algoritmos y los sesgos que pueden surgir en la implementación de tecnologías de inteligencia artificial. En este contexto, la regulación debe ser reflexiva y adaptativa, evitando tanto la lentitud como la inmediatez sin análisis previo.

Por tanto, ante la rápida transformación que se vive actualmente, resulta fundamental que la regulación se adapte a la evolución constante de las tecnologías. La innovación y el progreso son motores clave en este proceso, lo que hace necesario establecer normas claras que ofrezcan seguridad y previsibilidad. Sin embargo, regular sin un entendimiento profundo del contexto puede acarrear riesgos significativos, limitando el avance y el desarrollo tecnológico. Por ello, es esencial que las regulaciones sean flexibles y adaptables, y que se revisen

[102] Vázquez, Cristina. (2018). Desafíos regulatorios ante la digitalización. En Estudios sobre desafíos jurídicos ante la digitalización (pp. 57 y ss.). UM.

[103] Aramendía, M. M. (2021). Retos y oportunidades jurídicas ante la digitalización. Tesis doctoral. Universidad de Granada.

continuamente para reflejar la realidad dinámica del entorno[104]Para llevar a cabo una regulación efectiva, es crucial identificar claramente los aspectos que se desean regular y los problemas que se pretenden abordar. La sostenibilidad, la eficiencia y la equidad deben estar en el centro de este análisis, considerando si las normativas existentes o las propuestas son adecuadas y necesarias. Este proceso implica evaluar los derechos e intereses de todas las partes involucradas, siempre respetando el principio de proporcionalidad, que garantiza un equilibrio justo entre los diversos intereses[105]

En definitiva, como señala Aramendí, la regulación debe ser un facilitador de la innovación y no un obstáculo. Para desempeñar este rol, es vital que los reguladores actúen de manera ágil, iterativa y colaborativa, enfocándose en resultados concretos y dispuestos a experimentar con nuevos modelos de regulación, siempre bajo un marco de control que asegure la transparencia y el acceso a la información[106].

VII. CONCLUSIONES

A lo largo de este trabajo, hemos analizado el impacto de la ciberseguridad en las pequeñas y medianas empresas (pymes), así como su relación con los trabajadores. A medida que las amenazas cibernéticas se vuelven más sofisticadas y omnipresentes, se plantea la necesidad de que incluso las empresas más pequeñas adopten medidas para proteger sus activos digitales. Sin embargo, la implementación de estas medidas plantea interrogantes entorno a la privacidad y los derechos fundamentales de los empleados. Este apartado tiene como objetivo responder a las preguntas que fueron clave para nuestra investigación, evaluando tanto los beneficios como los posibles desafíos que la ciberseguridad suponen para las pymes y sus trabajadores.

En la primera pregunta se planteaba si era necesaria la ciberseguridad en una empresa pequeña o familiar, y a lo largo del trabajo se ha podido ver que a pesar de que las pymes suelen tener menos recursos y pueden pensar que no son un objetivo de ciberataques, la ciberseguridad es igual de crucial para ellas. Los cibercriminales no discriminan por el tamaño de la empresa, y las pymes pueden ser especialmente vulnerables debido a la falta de medidas de seguridad robustas. Implementar ciberseguridad ayuda a proteger información valiosa, como datos financieros, información de clientes y propiedad intelectual, evitando pérdidas económicas significativas y daños a la reputación.

Por otro lado, nos preguntábamos acerca la relación existente entre la ciberseguridad y los trabajadores y es que la ciberseguridad tiene un impacto directo en los trabajadores, ya que a menudo son el primer eslabón de defensa en la cadena de seguridad de una empresa. Capacitar a los empleados en buenas prácticas de ciberseguridad es clave para minimizar los riesgos de errores humanos, como el phishing o la descarga de malware. Al mismo tiempo, los sistemas de seguridad no deberían vulnerar los derechos fundamentales de los trabajadores, como la privacidad. Con una implementación correcta y respetuosa, la ciberseguridad no solo afecta

[104] Cubo, A., Hernández, J. L., Porrúa, M., y Roseth, B. (2022). Guía de transformación digital del gobierno: resumen ejecutivo. Inter-American Development Bank. United States of America

[105] Torrijos, J. V. (2022). Los derechos en la era digital. *Nuevos retos en materia de derechos digitales en un contexto de pandemia: perspectiva multidisciplinar*, 25-45.

[106] Aramendía, M. M. (2021). Retos y oportunidades jurídicas ante la digitalización. Tesis doctoral. Universidad de Granada.

negativamente a los empleados, sino que puede proteger su entorno de trabajo y la estabilidad laboral a largo plazo.

También nos planteábamos si los derechos fundamentales de los trabajadores se veían vulnerados imponiendo ciberseguridad. La implementación de ciberseguridad debe ser respetuosa con los derechos de los trabajadores, especialmente en cuanto a la privacidad. Aunque algunas medidas de seguridad, como la monitorización de los correos electrónicos o la navegación por Internet, podrían interpretarse como una invasión a la privacidad, éstas deben estar claramente justificadas, ser proporcionales y transparentes. En muchos casos, los beneficios de una mayor protección contra ciberataques superan cualquier inconveniente, siempre que los derechos fundamentales sean respetados.

Entre otros interrogantes estaban los beneficios de la ciberseguridad para los trabajadores. Los sistemas de ciberseguridad bien diseñados ofrecen beneficios claros para los trabajadores, como un entorno laboral más seguro y protegido de amenazas externas que podrían comprometer su información personal o afectar el funcionamiento de la empresa. Además, la ciberseguridad reduce la posibilidad de que se produzcan interrupciones significativas en las operaciones de la empresa, lo que protege tanto los puestos de trabajo como la estabilidad financiera de la organización.

Y otro de los interrogantes más relevantes era cómo afectaba la ciberseguridad a la empresa. Como ya hemos visto, la ciberseguridad es esencial para la continuidad correcta del negocio. La ciberseguridad es esencial para la continuidad del negocio. Un ciberataque exitoso puede causar importantes pérdidas financieras, daños a la reputación y pérdida de confianza por parte de los clientes. Para las pymes, que a menudo operan con márgenes más estrechos, las consecuencias de un ataque pueden ser devastadoras. Sin embargo, con una correcta gestión de la ciberseguridad, estas empresas pueden mitigar riesgos y ganar en competitividad al demostrar un compromiso con la protección de sus datos y los de sus clientes.

Y respecto a la última pregunta planteada, era qué medidas de ciberseguridad debería tomar una pyme. Desde mi punto de vista, las pymes deben aportar un enfoque estratégico en la implementación de medidas de ciberseguridad. Algunas acciones clave incluyen como hemos visto en el desarrollo del trabajo: capacitar a los empleados en buenas prácticas de seguridad, implementar soluciones básicas de protección, como cortafuegos, antivirus y actualizaciones regulares de software; realizar copias de seguridad periódicas; aplicar políticas claras sobre el uso de contraseñas y la gestión de accesos; desarrollar un plan de respuesta ante incidentes cibernéticos para actuar rápidamente en caso de un ataque.

Como reflexión final de todo lo visto y expuesto en este trabajo, quiero que se vea reflejada la idea que he extraído de esta investigación, la ciberseguridad no solo es necesaria para las pymes, sino que también puede beneficiar tantos a los trabajadores como a la empresa si se implementa de manera correcta y respetuosa. Las medidas de seguridad deben ser vistas como una inversión en la estabilidad y el futuro de la organización. Podemos ver que la ciberseguridad ha evolucionado para convertirse en un aspecto central de la estrategia empresarial, no solo por la necesidad de proteger los datos y activos, sino también por su potencial para impulsar la competitividad y el crecimiento de las empresas.

En un mundo cada vez más digitalizado, creo que sería conveniente implementar de una manera más eficaz y rápida la inteligencia artificial (IA) y así mismo, el Big data ya que estos dos factores están redefiniendo el funcionamiento de las organizaciones, la ciberseguridad no puede verse simplemente como una medida reactiva para suavizar riesgos, sino como una oportunidad para generar valor y optimizar procesos.

La inteligencia artificial ha transformado significativamente el campo de la ciberseguridad, proporcionando capacidades avanzadas para la detección y respuesta a amenazas. Los sistemas basados en IA permiten a las empresas analizar grandes cantidades de datos en tiempo real, identificar patrones de acciones atípicas y prevenir posibles ataques antes de que ocurran. Sin embargo, esta misma tecnología también plantea riesgos, como la posibilidad de que los atacantes utilicen IA para lanzar ataques más sofisticados. Por ello, la integración de la IA en las estrategias de ciberseguridad debe ir acompañada de un enfoque integral que considere no solo las amenazas tecnológicas, sino también las políticas y procesos internos de cada empresa.

El Big data, por su parte, ofrece a las empresas una herramienta poderosa para gestionar y analizar la información crítica. A través del análisis masivo de datos, las organizaciones pueden no solo detectar vulnerabilidades, sino también optimizar sus operaciones, mejorar la eficiencia de sus procesos y personalizar sus servicios para los clientes. Sin embargo, la acumulación y gestión de grandes cantidades de datos también aumenta la exposición a riesgos cibernéticos, lo que hace esencial que las empresas implementen medidas de protección adecuadas.

Otro punto que hemos destacado a lo largo del trabajo y en el que nos hemos centrado significativamente, ha sido el aspecto jurídico y creo que el papel de las instituciones nacionales e internacionales es crucial para conseguir crear un marco de protección que permita salvaguardar no solo los activos digitales que tienen las empresas, sino que también los derechos fundamentales de los trabajadores como ya hemos visto que son la privacidad, y la protección de datos personales. Creo que es fácil de ver que al estar en un entorno cada vez más interconectado, las amenazas cibernéticas logran trascender fronteras, y esto exige una cooperación y regulación efectiva entre naciones y organismos internacionales. A nivel internacional, hemos dado relevancia a marcos normativos como el Reglamento General de Protección Datos (GDPR) de la UE que ha establecido precedentes importantes, imponiendo estrictas obligaciones sobre la forma en que las empresas manejan los datos personales. Lo que más destaco de este tipo de regulación es que aparte de proteger a los usuarios, también obliga a las empresas a adoptar prácticas robustas de ciberseguridad para evitar sanciones legales y considero muy importante la armonización de normativas entre países para combatir el ciberdelito global y asegurar que las empresas cumplan con estándares de protección de datos y seguridad informática. Por otro lado, hablando del ámbito nacional, la Ley de Protección de Datos de nuestro país busca adaptarse a las particularidades que existen hoy en día en el mercado y establecer requisitos que las empresas deben cumplir para operar de forma segura. Viendo esto, considero importante la creación de un entorno regulatorio que proteja tanto a las empresas como a los individuos ya que con estas normativas no solo se previenen vulnerabilidades, sino que también actúan como incentivo para que las empresas adopten políticas más responsables y transparentes respecto al manejo de los datos y que de esta forma se consiga crear un marco en el cual la innovación tecnológica puede florecer de manera segura y sostenible.

En definitiva, la ciberseguridad no debe percibirse únicamente como un coste necesario para protegerse de las amenazas digitales, sino como una inversión estratégica que permite a las empresas adaptarse a un entorno global cada vez más interconectado. La integración de tecnologías como la IA y el Big data, el cumplimiento de normativas internacionales y la adaptación a las nuevas tecnologías pueden no solo garantizar la protección de los activos críticos, sino también abrir nuevas oportunidades de crecimiento y eficiencia.

VIII. FUENTES

⇒ BIBLIOGRAFÍA

ANTONOPOULOS, ANDREAS M. Mastering Bitcoin (2ª ed.). O´Reilly Media, California, 2017.

CANDAU, JAVIER. (2021). Boletín IEE, No 23, pp. 460-494.

ARAMENDÍA, MERCEDES. *"La revolución digital: telecomunicaciones, servicios digitales y la sociedad de la información*". En Estudios de Telecomunicaciones y Sociedad de la Información.

ARAMENDIA, MERCEDES. (2021). *La protección de los datos personales es esencial para el desarrollo del mundo digital: Primeras aproximaciones al nuevo reglamento general de datos de la Unión Europea.* En Estudios de Información Pública y datos Personales (Tomo III).

GOODMAN, MARC, *Future Crimes: Inside the digital underground and the Battle for Our Connected World.* Anchor Books, New York, 2017.

GÓNZALEZ ROCÍO. (2018, 1 de octubre). "*Más de la mitad de las pymes sufren ciberataques". Cinco Días*. (25 de abril 2023)

Iniciativa global de la sociedad civil. (2015). *Principios de Manila sobre Responsabilidad de los Intermediarios*: Antecedentes. Versión 1.0, mayo 2015, pp. 6.

Jiménez, M. F. (2018). Presente y futuro de las plataformas digitales. Revista de estudios de juventud, (119), 63-74.

LANZA, E. (2017). Estándares para una Internet libre, abierta e incluyente. *Relatoría Especial para la Libertad de Expresión. Comisión Interamericana de Derechos Humanos, Organización de los Estados Americanos. OAS Cataloging-in-Publication Data*.

LIMA, D. D. (2023). Transparencia y protección de datos personales en el ámbito universitario: ¿avance o retroceso? *Revista española de la transparencia, Núm. 17. Número Extraordinario 2023.* Págs. 201 -224.

PAZ PENDÉS JAVIER Y MARTÍNEZ VELENCOSO, LUZ. "*Nuevos retos jurídicos de la Sociedad Digital".* Thomson Reuters, Aranzadi, Navarra, 2017.

PEREZ-SEBRABONA GONZALEZ, JOSE LUIS, "*Entorno a la interpretación de las condiciones generales del seguro".* Editorial Universal de Granada, España, 1987.

SANJURO, BEATRIZ (2016). *"Manual de Internet y Redes Sociales*", Dykinson, pp. 47 y 48.

SIGÜENZA, ALICIA, "*La libertad de expresión en Internet*" en *El Derecho de Internet.* Atelier Libros Jurídicos, Valencia, 2016.

SIGÜENZA, ALICIA. (2016) "*La libertad de expresión en Internet*" en El Derecho de Internet, Atelier Libros Jurídicos, Barcelona, pp. 57 y ss.

REGISTRO DE LA PROPIEDAD INTELECTUAL. (2024, junio). Propiedad Intelectual. https://www.cultura.gob.es/cultura/areas/propiedadintelectual/mc/rpi/que-es/pi.html

ROMERO, J. C. (2021). Ciberseguridad: Evolución y tendencias. *bie3: Boletín IEEE*, (23), Págs. 460-494.

ROMERO, N. (2021, SEPTIEMBRE). Derechos digitales de los niños: cómo protegerlos mientras exploran internet. INEAF. https://www.ineaf.es/tribuna/derechos-digitales-de-los-ninos-como-protegerlos-mientras-exploran-internet/

RUFIÁN, MIKEL. Blog: *"Ciberseguridad y Ciberespacio en Distintas Organizaciones"* (2020). (Consultado 14 de febrero 2023)

VALLS PRIETO, JAVIER, *Retos Jurídicos por la Sociedad Digital,* Thomson Reuters, Aranzadi 2018.
VÁZQUEZ, CRISTINA. (2018). "*Desafíos regulatorios ante la digitalización*". En Estudios sobre desafíos jurídicos ante la digitalización (pp. 76 y ss.). UM.
VOSOUGHI, S., ROY, D., Y ARAL, S. (2018). The spread of true and false news online. *science*, *359*(6380), Págs. 1146-1151.
ZINGUER, M. A. (2014). Libertad de expresión y derecho a la información en las redes sociales en Internet. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, (12), 5.

⇒ REFERENCIAS WEB

Alemán, M. (2017). *Correo electrónico temporal*: Qué es, para qué sirve y cómo crearlo. https://www.misaelaleman.com/correo-electronico-temporal

Blanco, A (2019) *"La Tienda de las Licencias*: Cómo crear cuentas de correo temporales". Consultado el 23 de abril de 2023. https://blog.latiendadelaslicencias.com/crear-cuentas-de-correo-temporales/
Dataseg consultores y auditores. (2021). *Ya está aquí la nueva LOPD, la LOPDGDD.* https://dataseg.es/ya-esta-aqui-la-nueva-lopd-la-lopdgdd/
10 minutemail. (2024). *Bienvenido al 10 Minute Mail*. Consulta el 3 de mayo de 2023, https://10minutemail.net/
Def Ciberseguridad. Página principal https://tep.pucmm.edu.do/.
González, R. (2018, 1 de octubre). Más de la mitad de las pymes sufren ciberataques. *CincoDías*. https://cincodias.elpais.com/cincodias/2018/09/28/pyme/1538169199_927487.html
INCIBE. (2020b, junio). Cómo proteger la información personal de los clientes en la empresa. https://www.incibe.es/empresas/blog/proteger-informacion-personal-los-clientes-empresa
INCIBE. (2021a, julio). Políticas de seguridad para la pyme. https://www.incibe.es/empresas/herramientas/politicas
INCIBE. (2021b) Concienciación y formación. https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/concienciacion-y-formacion.pdf
INCIBE. (2022). Uso de técnicas criptográficas. Políticas de seguridad para la PYME. https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-_tecnicas-criptograficas.pdf
INCIBE. (2023). Gestionar fuga de información. https://www.aepd.es/guias/guia-incibe-aepd-gestionar-fuga-de-informacion.pdf
INCIBE. (2023a). Guía de ciberseguridad. La ciberseguridad al alcance de todoshttps://www.incibe.es/sites/default/files/docs/senior/guia_ciberseguridad_para_todos.pdf
INCIBE. (2023b). Una guía de aproximación para el empresario. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware.pdf
INCIBE. (2023c, agosto). La ciberseguridad desde los inicios: evolución de la seguridad. https://www.incibe.es/empresas/blog/la-ciberseguridad-desde-los-inicios-evolucion-de-la-seguridad

EAE Business School (2019). Diez claves sobre ciberseguridad en pymes. Consultado en 25 de abril de 2023.

https://www.eaeprogramas.es/blog/negocio/tecnologia/diez-claves-sobre-ciberseguridad-en-pymes
Kaspersky. (2021) "¿Qué es la ciberseguridad?
https://es.scribd.com/document/684269086/Que-es-la-ciberseguridad-Kaspersky.
Instituto Nacional de Ciberseguridad (INCIBE). *El correo electrónico como canal para el fraude digital* (blog).
https://www.incibe.es/empresas/blog/el-correo-electronico-canal-el-fraude-digital
Instituto Nacional de Ciberseguridad (INCIBE) (2028). *Desarrollar Cultura en Seguridad*.
https://www.incibe.es/empresas/que-te-interesa/desarrollar-cultura-en-seguridad
National Cyber Security Centre (NCSC). (2018). *10 steps to cyber security. Guidance on how organizations can protect themselves in cyberspace, including the 10 steps to cyber*space
https://www.ncsc.gov.uk/collection/10-steps

Revista ejército. (2019) Nº.837 extraordinario diciembre, p.136.

Una guía de aproximación para el empresario.
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf.
RAE. (2024a). Privacidad. https://dle.rae.es/privacidad
RAE. (2024b). Propiedad intelectual. https://dle.rae.es/propiedad#FNaj5bL
RAE. (2024c). Derecho de autor. https://dle.rae.es/derecho#CUr4nPg

Zinko Colombia (2019). *Ventajas y desventajas de trabajar en la nube informática.*
http://www.zinkocolombia.com/nube-informatica. (2 de mayo 2023)

⇒ Normativa consultada

Constitución Española. (1978) Boletín Oficial del Estado, núm. 311, de 29 de diciembre.

Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo (2018). Por la que se establece el Código de las Comunicaciones Electrónicas, 11 de diciembre.

Directiva (UE) 2019/789 del Parlamento Europeo y del Consejo (2019). Por la que se establecen normas sobre el ejercicio de los derechos de autor y derechos afines aplicables a determinadas transmisiones en línea de los organismos de radiofrusión y a las retransmisiones de programas de radio y televisión. WIPO Lex - World Intellectual Property Organization.

Tribunal de Justicia de la Unión Europea. (2014). Sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014, asunto C-131/12.