FACULTAD DE DERECHO

ESCUELA PROFESIONAL DE DERECHO

PROTECCIÓN JURÍDICA DE LOS DATOS PERSONALES EN EL ÁMBITO EMPRESARIAL Y LA REVISIÓN SISTEMÁTICA DE LAS IMPLICANCIAS DELICTIVAS

Trabajo de investigación para obtener el grado académico de Bachiller en Derecho

Autor

MANCO RAMIREZ, Jusan Enrique Junior (ORCID: 0000-0002-2023-5304)

Asesor

AYBAR IZAGUIRRE, Gerardo Manuel (ORCID: 0000-0003-3547-7602)

Línea de investigación del programa

Defensa y promoción de derecho humanos

Línea de acción RSU

Salud y bienestar

LIMA, PERÚ, NOVIEMBRE DE 2024

Referencia bibliográfica

Manco Ramirez, J. E. J. (2024). *Protección jurídica de datos personales en el ámbito empresarial y la revisión sistemática de las implicancias delictivas* [Trabajo de investigación, Universidad Autónoma del Perú]. Repositorio de la Universidad Autónoma del Perú.

HOJA DE METADATOS

Datos del autor	
Nombres y apellidos	Jusan Enrique Junior Manco Ramirez
Tipo de documento de identidad	DNI
Número de documento de identidad	76361676
URL de ORCID	https://orcid.org/0000-0001-9204-7882
Datos del asesor	
Nombres y apellidos	Gerardo Manuel Aybar Izaguirre
Tipo de documento de identidad	DNI
Número de documento de identidad	44823980
URL de ORCID	https://orcid.org/0000-0003-0128-0123
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Yurela Kosett Yunkor Romero
Tipo de documento	DNI
Número de documento de identidad	20118250
Secretario del jurado	
Nombres y apellidos	Yda Rosa Cabrera Cueto
Tipo de documento	DNI
Número de documento de identidad	06076309
Vocal del jurado	
Nombres y apellidos	Jessica Patricia Huali Ramos
Tipo de documento	DNI
Número de documento de identidad	42686844
Datos de la investigación	
Título de la investigación	Protección jurídica de datos personales en el ámbito empresarial y la revisión sistemática de las implicancias delictivas
Línea de investigación Institucional	Persona, Sociedad, Empresa y Estado
Línea de investigación del Programa	Promoción y Defensa de los Derechos Humanos en el Ámbito Nacional e Internacional
Línea de acción RSU	Salud y Bienestar

URL de disciplinas OCDE	https://purl.org/pe-repo/ocde/ford#5.09.01

FACULTAD DE DERECHO

ESCUELA PROFESIONAL DE DERECHO

ACTA DE SUSTENTACIÓN DEL TRABAJO DE INVESTIGACIÓN

En la ciudad de Lima, el jurado de sustentación del trabajo de investigación conformado por: la Dra. Yurela Kosett Yunkor Romero como presidente, la Dra. Yda Rosa Cabrera Cueto como secretario y la Mg. Jessica Patricia Huali Ramos como vocal, reunidos en acto público para dictaminar el trabajo de investigación titulado:

PROTECCIÓN JURÍDICA DE LOS DATOS PERSONALES EN EL ÁMBITO EMPRESARIAL Y LA REVISIÓN SISTEMÁTICA DE LAS IMPLICANCIAS DELICTIVAS

Presentado por el egresado:

JUSAN ENRIQUE JUNIOR MANCO RAMIREZ

Para obtener el **Grado académico de bachiller en derecho**; luego de escuchar la sustentación de la misma y resueltas las preguntas del jurado se procedió a la calificación individual, obteniendo el dictamen de **aprobado-bueno** con una calificación de **QUINCE (15).**

En fe de lo cual firman los miembros del jurado, el 20 de noviembre del 2024.

PRESIDENTE	**SECRETARIA**	**VOCAL**
DRA. YURELA KOSETT YUNKOR ROMERO	DRA. YSA ROSA CABRERA CUETO	MG. JESSICA PATRICIA HUALI RAMOS

ACTA DE APROBACIÓN DE ORIGINALIDAD

Yo Gerardo Manuel Aybar Izaguirre docente de la Facultad de Derecho de la Escuela Profesional de Derecho de la Universidad Autónoma del Perú, en mi condición de asesor del trabajo de investigación titulado:

PROTECCIÓN JURÍDICA DE LOS DATOS PERSONALES EN EL ÁMBITO EMPRESARIAL Y LA REVISIÓN SISTEMÁTICA DE LAS IMPLICANCIAS DELICTIVAS

Del egresado Jusan Enrique Junior Manco Ramirez certifico que el trabajo de investigación tiene un índice de similitud de 18% verificable en el reporte de similitud del software Turnitin que se adjunta.

El suscrito revisó y analizó dicho reporte a lo que concluyó que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender el trabajo de investigación cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad Autónoma del Perú.

Lima, 21 de Noviembre de 2024

Gerardo Manuel Aybar Izaguirre

DNI: 44823980

Protección jurídica de los datos personales en el ámbito empresarial y la revisión sistemática de las implicancias delictivas

Legal Protection of Personal Data in the Business Sector and a Systematic Review of Criminal Implications

Jusan Enrique Junior Manco Ramirez[1]

RESUMEN

La protección jurídica de los datos personales en el ámbito empresarial se ha convertido en una necesidad urgente debido al aumento de ciberataques y las consecuencias del mal manejo de datos en las organizaciones. Este estudio ha tenido como objetivo analizar los riesgos delictivos asociados a la gestión de datos en el sector empresarial, identificándose las áreas de vulnerabilidad y proponiendo mecanismos de protección eficaces.

Para este análisis, se llevó a cabo una revisión sistemática de la literatura especializada en la protección de datos y ciberseguridad, utilizando antecedentes científicos del estudio en referencia. Se examinaron los sistemas regulatorios y las estrategias de seguridad aplicadas en diversas jurisdicciones para resguardar la información en el entorno empresarial.

Los resultados de esta investigación destacan que las empresas enfrentan desafíos constantes debido a la sofisticación de los ataques y a las lagunas regulatorias en ciertas jurisdicciones, lo cual compromete la protección de datos personales.

Entre las recomendaciones principales, se sugiere fortalecer los marcos regulatorios, promover la educación continua en ciberseguridad para el personal, y fomentar la colaboración público-privada para optimizar las estrategias de seguridad de datos. En este sentido las empresas pueden reducir significativamente los riesgos y cumplir con las normativas vigentes.

Palabras clave: protección de datos, ciberseguridad empresarial, delitos informáticos

[1] Universidad Autónoma del Perú. Orcid: 0000-0002-2023-5304. Correo: jmancor@autonoma.edu.pe

ABSTRACT

The legal protection of personal data in the business environment has become an urgent necessity due to the increase in cyberattacks and the consequences of poor data management within organizations. This study aimed to analyze the criminal risks associated with data management in the business sector, identifying areas of vulnerability and proposing effective protection mechanisms. For this analysis, a systematic review of specialized literature on data protection and cybersecurity was conducted, using scientific background from referenced studies. Regulatory systems and security strategies applied in various jurisdictions to safeguard information in the business environment were examined.

The results of this research highlight that companies face constant challenges due to the sophistication of attacks and regulatory gaps in certain jurisdictions, compromising the protection of personal data. Among the main recommendations, it is suggested to strengthen regulatory frameworks, promote continuous cybersecurity education for personnel, and encourage public-private collaboration to optimize data security strategies. In this way, companies can significantly reduce risks and comply with current regulations.

Keywords: data protection, corporate cybersecurity, cybercrime

I. **INTRODUCCIÓN**

El artículo titulado Protección jurídica de los datos personales en el ámbito empresarial y la revisión sistemática de las implicancias delictivas examina un tema crucial en el actual entorno digital: la manera en que los datos personales son protegidos jurídicamente en las empresas y las diversas implicancias delictivas que pueden surgir del uso inadecuado o ilícito de tecnologías avanzadas.

La llegada de la Cuarta Revolución Industrial, concepto introducido por Klaus Schwab, marca un cambio trascendental en cómo las tecnologías digitales impactan a la humanidad. Hoy en día, la tecnología no solo cumple un papel auxiliar en la vida de las personas y las empresas, sino que se ha convertido en una pieza fundamental e integral en sus operaciones y decisiones. Esto ha traído beneficios significativos, como mayor accesibilidad y eficiencia, pero también ha incrementado notablemente los riesgos, especialmente en lo que respecta a la privacidad y seguridad de los datos personales en el ámbito empresarial.

De esta forma, el estudio aborda la protección de estos datos, que no solo son valiosos para las empresas en términos de información, sino que también constituyen un derecho fundamental para los individuos.

Este tema tiene una importancia considerable tanto en el ámbito académico como en la sociedad. En la academia, se ha convertido en un área de investigación activa, dado que la protección de datos personales y la ciberseguridad son temas de interés que afectan múltiples disciplinas, incluyendo el derecho, la informática, y la administración empresarial.

A nivel social, la protección de datos es fundamental para mantener la confianza en el ecosistema digital. La pandemia de COVID-19, que impulsó el uso de servicios en línea y sistemas de trabajo remoto, también elevó las oportunidades para los ciberdelitos.

Como resultado, los delitos informáticos se incrementaron drásticamente, afectando tanto a individuos como a empresas a nivel global. Esta realidad ha generado una urgente necesidad en los estados de derecho de formular estrategias que aseguren la protección de bienes jurídicos, tales como la identidad personal y la propiedad empresarial, frente a las nuevas modalidades delictivas que se aprovechan de los avances tecnológicos (Vega & Arévalo, 2022).

La creciente exposición de las empresas y sus datos críticos exige un marco legal y preventivo robusto que proteja tanto a los ciudadanos como a las organizaciones.

Históricamente, el concepto de ciberdelito y la necesidad de proteger los datos personales en el ámbito empresarial han evolucionado en respuesta a los rápidos avances tecnológicos. Desde la década de 1990, los países han comenzado a legislar en torno a los delitos informáticos, adaptando sus códigos penales para incluir categorías específicas de delitos vinculados a la tecnología digital.

Por ejemplo, en 1995, el Código Penal español introdujo nuevas disposiciones sobre delitos informáticos, y en 2013, Perú promulgó la Ley N° 30096, que regula el uso indebido de tecnologías de información y crea la División de Investigación de Delitos de Alta Tecnología (Divindat). Estas iniciativas reflejan el reconocimiento de la importancia de los datos personales y de la necesidad de establecer protecciones legales específicas que se adapten a las amenazas de la era digital.

A nivel internacional: El derecho a la protección de datos personales ha evolucionado significativamente desde la Convención 108 de 1981, que fue la primera norma internacional vinculante sobre protección de datos. Esta convención buscaba establecer un marco común para la protección de la privacidad de las personas ante los riesgos derivados del tratamiento automatizado de sus datos personales. Posteriormente, la evolución normativa alcanzó un hito importante con el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, que entró en vigor en 2018. El GDPR establece estándares globales de protección de datos personales y pone un fuerte énfasis en la ciberseguridad, responsabilizando a las organizaciones por el manejo adecuado de los datos, la transparencia en su uso, y la implementación de medidas técnicas y organizativas para prevenir brechas de seguridad.

En América Latina, la protección de datos personales ha ido tomando relevancia en los últimos años, especialmente con la creación de leyes nacionales que buscan homologarse a los estándares internacionales. Un ejemplo destacado es la Ley General de Protección de Datos (LGPD) de Brasil, que entró en vigor en 2020, y que establece un enfoque integral sobre la privacidad, imponiendo responsabilidades a empresas y organismos que tratan datos personales, con un fuerte enfoque en la ciberseguridad. Otros países de la región, como Argentina, México y Colombia, han seguido este modelo adaptando sus propias legislaciones y

trabajando en la implementación de medidas para fortalecer la seguridad de los datos personales en el entorno digital, fomentando así un espacio más seguro para el intercambio de información personal.

En el contexto de Perú, el derecho a la protección de datos personales se consolidó con la promulgación de la Ley N° 29733 en 2011, conocida como la Ley de Protección de Datos Personales. Esta ley establece los principios y normas para el tratamiento de datos personales en el país, garantizando los derechos de las personas sobre su información personal y promoviendo la responsabilidad de las entidades que procesan esos datos. Además, el D.L. 03-2013-JUS, que aprobó el Reglamento de la Ley de Protección de Datos Personales, regula los procedimientos y las medidas técnicas y organizativas necesarias para proteger los datos, especialmente en lo que respecta a la seguridad de la información. Aunque Perú ha avanzado en este campo, la ley y su reglamento continúan adaptándose a los nuevos desafíos planteados por la transformación digital y las crecientes amenazas cibernéticas.

A medida que la tecnología avanza, también lo hacen las tácticas de los ciberdelincuentes, lo cual impone un desafío continuo para los legisladores que deben actualizar y fortalecer las normativas vigentes para proteger los derechos de los individuos y la estabilidad de las empresas (García, 2012).

El marco teórico y conceptual sobre delitos informáticos muestra que, si bien existen ciertos acuerdos sobre su definición, aún hay áreas de debate en la literatura académica. Desde una perspectiva doctrinal, estos delitos se han conceptualizado de varias maneras y los describe como aquellas acciones delictivas que utilizan la tecnología electrónica como medio o fin (De la Luz,1984)

En un contexto más reciente, el papel de las nuevas tecnologías es esencial en la creación y expansión de estos delitos, ya que facilita la comisión de crímenes en ámbitos como el financiero y el empresarial. A pesar de que el uso de tecnología como medio para la comisión de delitos es la característica distintiva de los ciberdelitos, existen distintos puntos de vista respecto a las modalidades específicas y los bienes jurídicos protegidos (Bloissiers, 2022)

Esta multiplicidad de opiniones refleja un campo en evolución donde los académicos, legisladores y expertos en seguridad buscan un consenso sobre las herramientas más efectivas para prevenir y sancionar estos delitos, especialmente

cuando afectan a empresas que gestionan grandes volúmenes de datos personales y financieros.

En términos prácticos, este tema tiene implicaciones importantes para los profesionales en el ámbito empresarial, así como para los formuladores de políticas y los encargados de velar por la seguridad en entornos digitales. La protección jurídica de los datos personales es crucial no solo para la privacidad y seguridad de los individuos, sino también para preservar la integridad y confianza en las operaciones empresariales.

En un mundo donde la reputación de una empresa y la confianza de sus clientes pueden verse gravemente afectadas por incidentes de ciberseguridad, este estudio destaca la necesidad de políticas preventivas y un marco legal sólido que permita responder con efectividad a las amenazas que plantea el cibercrimen. Asimismo, la importancia de este tema influye en la formulación de políticas públicas, ya que los estados deben equilibrar la innovación tecnológica con la salvaguarda de derechos fundamentales.

En conclusión, esta introducción proporciona una base sólida para comprender los desafíos legales actuales en la protección de los datos personales en el ámbito empresarial y subraya la importancia de una respuesta integrada que incluya tanto medidas jurídicas como preventivas para enfrentar los desafíos de la era digital.

II. MÉTODO

En todo caso respecto de la metodología analizada para el trabajo de investigación es importante tener presente que se ha utilizado el método inductivo la misma que ha tratado de la revisión de elementos científicos como casos, artículos, libros y ensayos particulares, teniendo en cuenta que habiendo partido de estos análisis se ha llegado a la generalización de la conclusión planteada, habiéndose contribuido con la misma investigación la respectiva observación del problema planteado.

En este sentido este método se vincula con el enfoque cualitativo para efectos de entender y comprender el problema planteado, dentro de la sociedad, a razón de hacer una adecuada exploración de los fenómenos de la problemática encausada en la sociedad, esto en razón de la interpretación y comprensión de la realidad social con la realidad, de la controversia en cuestión del tema analizado.

El proceso de análisis en este trabajo se centra en la recopilación rigurosa de datos específicos relacionados con el tema de investigación. Estos datos se obtuvieron a través de una diversidad de fuentes, tales como informes, tesis, artículos académicos, revistas especializadas y leyes relevantes, siguiendo las recomendaciones metodológicas de Flick, quien destaca la importancia de una recolección de datos diversificada y bien documentada para garantizar la validez de los resultados (Flick, 2022).

La información recopilada se utilizó para extraer conclusiones fundamentadas que sustentaron las discusiones presentadas en el estudio, asegurando que el análisis sea comprensivo y meticulosamente respaldado por la evidencia.

Se revisaron un total de 30 estudios de investigación pertinentes al tema abordado en este trabajo, obtenidos mediante la búsqueda de fuentes confiables procedentes de Scielo, Google Académico y repositorios, siendo aplicables 15 al estudio propuesto porque contenían al menos una de las dos categorías y, además, eran igual o superiores al año 2019; y excluidos 10 por ser anteriores, publicados antes del año 2019.

III. ANÁLISIS E INTEGRACIÓN DE LA INFORMACIÓN

Para realizar el análisis sobre la protección jurídica de los datos personales en el ámbito empresarial y las implicancias delictivas que pueden derivarse de la falta de ciberseguridad, se realizó una revisión sistemática de artículos científicos cualitativos utilizando los descriptores “protección de datos personales” (PDP) y “ciberseguridad empresarial” (CE). Estos términos se combinaron con los conectores booleanos AND y OR (Arazimendi & Huampiri, 2021).

El análisis comparativo de los estudios seleccionados se centró en identificar similitudes y diferencias en los enfoques regulatorios adoptados por distintas jurisdicciones para proteger la privacidad y en las estrategias utilizadas para mitigar los riesgos específicos que enfrentan las empresas (Ojeda-Pérez et al., 2011).

Se subrayan que el desconocimiento o la falta de capacitación en ciberseguridad entre empleados representa una vulnerabilidad crítica para la protección de datos personales. Explica que, aunque las empresas puedan adoptar tecnologías avanzadas, es la falta de formación continua lo que puede poner en riesgo la seguridad de la información (García, 2012)

Además, se expone cómo la capacitación en ciberseguridad no solo reduce los riesgos de incidentes de seguridad, sino que también fortalece la "primera línea de defensa" contra amenazas internas, haciendo de la formación un elemento fundamental de protección en el entorno empresarial (García, 2016).

EUROPOL (2020) destaca el rol de plataformas como Microsoft Teams en la protección de la confidencialidad de la información empresarial. Según EUROPOL, el uso de estas herramientas de comunicación, que integran funciones avanzadas de encriptación y autenticación multifactor, protege la confidencialidad de los datos personales, reduciendo considerablemente los riesgos de exposición a amenazas externas. Este hallazgo resalta la efectividad de implementar tecnología avanzada para garantizar la seguridad en la comunicación y almacenamiento de datos dentro de las empresas.

Ojeda-Pérez et al. (2011) señalan la importancia de la colaboración entre el sector público y privado en la implementación de políticas de ciberseguridad efectivas. La cooperación entre gobiernos, instituciones académicas y empresas permite el desarrollo de medidas y estrategias de protección innovadoras, contribuyendo a una defensa cibernética más robusta.

También Ojeda-Pérez et al. (2011) apoyan esta perspectiva y sugieren que el intercambio de recursos y conocimientos fortalece la infraestructura de seguridad digital, lo cual es esencial para la protección de datos personales en el contexto empresarial globalizado.

Ojeda-Pérez et al. (2011) también destacan las diferencias en la aplicación de normativas de ciberseguridad en distintas jurisdicciones. En algunos países europeos, como señalan los autores, se aplica un enfoque riguroso con normativas como el Reglamento General de Protección de Datos, que exige altos estándares de protección para el manejo de datos personales.

Arocena (2011) complementa esta visión al comparar este enfoque con otras jurisdicciones, donde las regulaciones son más flexibles y permiten una mayor adaptación a las capacidades y necesidades de cada empresa, especialmente en sectores con menos recursos.

Sosa (2022) identifican una brecha en la capacidad de las pymes para implementar tecnologías avanzadas de ciberseguridad debido a sus limitados recursos. Schwab observa que las pequeñas y medianas empresas enfrentan desafíos adicionales para invertir en infraestructura de ciberseguridad, exponiéndolas a mayores riesgos en comparación con las grandes corporaciones. Sosa respalda esta idea y sugiere que la diferencia de recursos entre empresas de distinto tamaño representa una disparidad significativa en la implementación de medidas de protección de datos.

Minchola & Vega (2022) concluyen que la protección jurídica de los datos personales en el entorno empresarial exige un enfoque integral que incluya marcos regulatorios sólidos, innovación tecnológica, educación continua y colaboración activa entre el sector público y privado. Estos elementos, como mencionan los autores, conforman una “primera línea de defensa” esencial para mitigar amenazas de ciberseguridad y proteger la privacidad en el ámbito corporativo globalizado.

Ante ello, este análisis permitió identificar áreas de consenso y desacuerdo entre los estudios, así como inconsistencias en los resultados obtenidos por diferentes autores. Un hallazgo importante fue la identificación de vacíos en la investigación, como la falta de estudios que exploren en profundidad las estrategias de ciberseguridad adaptadas a las necesidades de las pequeñas y medianas empresas, que suelen tener recursos limitados para enfrentar amenazas avanzadas (Schwab, 2016).

Se observó un consenso general sobre la importancia de adoptar medidas preventivas robustas y tecnologías avanzadas para mitigar los riesgos de vulneración de datos personales (Minchola & Vega, 2022). En particular, se destacó la efectividad de políticas de seguridad digital implementadas en plataformas empresariales, como los sistemas de gestión de datos y comunicaciones en la nube.

Algunos estudios resaltaron la efectividad de plataformas como Microsoft Teams en la protección de la confidencialidad de la información, subrayando la importancia de contar con infraestructura tecnológica adecuada para enfrentar los riesgos de seguridad digital (EUROPOL, 2020).

La revisión de la literatura también mostró que la educación y concienciación de los empleados y directivos en temas de ciberseguridad desempeñan un papel fundamental en la protección de datos personales en el ámbito empresarial.

Los estudios señalaron que, aunque las empresas adopten tecnologías avanzadas, el desconocimiento o la falta de formación en ciberseguridad entre el personal pueden comprometer la seguridad de la información, convirtiendo a la capacitación continua en una medida crucial de protección (García, 2012).

Finalmente, la colaboración público-privada en el campo de la ciberseguridad empresarial fue destacada como una estrategia esencial para enfrentar los riesgos de seguridad. Los estudios sugieren que la cooperación entre gobiernos, instituciones académicas y el sector privado es crucial para el desarrollo de políticas de ciberseguridad efectivas y para el intercambio de conocimientos y tecnologías que fortalezcan las capacidades de defensa en el ámbito empresarial (EUROPOL, 2022).

Así, la revisión de la literatura sobre protección de datos personales y ciberseguridad empresarial muestra una convergencia significativa en la recomendación de implementar marcos regulatorios sólidos y medidas preventivas avanzadas para salvaguardar la privacidad en el entorno corporativo (Arazamendi & Huampiri, 2022).

Los estudios concuerdan en la necesidad de una infraestructura tecnológica robusta y de la educación continua de empleados y directivos como elementos clave para la prevención de incidentes de seguridad, ya que estos factores crean una "primera línea de defensa" ante amenazas cibernéticas (García, 2012).

Asimismo, se destaca un consenso sobre la relevancia de fomentar la colaboración entre el sector público y privado, reconociéndose que los desafíos

globales de ciberseguridad requieren de un esfuerzo conjunto para el desarrollo de políticas y la transferencia de tecnologías de protección (Schwab, 2016)

Estas similitudes subrayan la importancia de una acción coordinada y multifacética en la lucha contra las vulnerabilidades de seguridad digital en las empresas.

Sin embargo, también presentan diferencias importantes en cuanto a la implementación de regulaciones y prácticas de ciberseguridad en distintas jurisdicciones. En algunos países europeos, el enfoque es más estricto y se enfatiza el cumplimiento detallado de normativas específicas como el Reglamento General de Protección de Datos (RGPD), mientras que en otras jurisdicciones existen regulaciones más flexibles que permiten una adaptación mayor a las características y recursos de cada empresa (Arocena, 2011).

Esta variabilidad responde en parte a los niveles de desarrollo de cada región, afectando la efectividad de las políticas de protección de datos en función de las necesidades empresariales y los recursos disponibles (García, 2012). La literatura señala también una brecha en la adopción de tecnologías avanzadas entre grandes empresas y pymes, con estas últimas enfrentando desafíos adicionales debido a sus limitados recursos para invertir en ciberseguridad (Sosa, 2022).

En cuanto a las tendencias actuales en ciberseguridad empresarial, se observa una diferencia en la adopción de tecnologías avanzadas entre grandes empresas y pymes, con estas últimas enfrentando desafíos adicionales debido a la falta de recursos para invertir en sistemas de protección sofisticados (Sosa, 2022). La brecha tecnológica entre ambos sectores refleja la necesidad de políticas diferenciadas para atender las particularidades de cada grupo empresarial en la protección de datos personales.

Estos contrastes reflejan las prioridades y capacidades diferenciadas de los distintos sectores y tamaños de empresas en la implementación de medidas de protección de datos.

Por ello, el fortalecimiento de la protección jurídica de los datos personales en el ámbito empresarial requiere de un enfoque integral que incluya marcos regulatorios sólidos, innovación tecnológica, educación continua y una colaboración activa entre el sector público y privado para asegurar la seguridad y privacidad de los datos en el entorno corporativo globalizado (Minchola & Vega, 2022).

Por esta razón, las futuras investigaciones deben enfocarse en explorar estrategias efectivas para incrementar la adopción de medidas preventivas de ciberseguridad en empresas de todos los tamaños, particularmente en pequeñas y medianas empresas, que, como señalan Sosa (2022), enfrentan desafíos específicos debido a recursos limitados. Esto podría incluir incentivos económicos o fiscales para fomentar el uso de tecnologías avanzadas de protección de datos.

Además, se deben investigar los efectos de la implementación de marcos regulatorios flexibles frente a normativas más estrictas, como el Reglamento General de Protección de Datos en Europa. También Arocena (2011) muestra cómo las distintas jurisdicciones aplican enfoques divergentes, afectando los niveles de seguridad en función de los recursos y la adaptabilidad de cada contexto empresarial. Un análisis comparativo entre sistemas de regulación estrictos y adaptativos podría revelar beneficios y limitaciones en términos de protección de datos y operatividad empresarial.

IV. CONCLUSIONES

Primera: La revisión evidencia que la protección de datos personales es fundamental en el ámbito empresarial, no solo para cumplir con la normativa, sino también para mantener la confianza de los clientes y evitar daños económicos y reputacionales derivados de posibles brechas de seguridad.

Segunda: Existen diferencias significativas entre las normativas de protección de datos y ciberseguridad en distintas jurisdicciones. Esto afecta la efectividad de las medidas de protección empresarial, ya que algunos países cuentan con marcos legales avanzados y recursos regulatorios adecuados, mientras que otros presentan lagunas y limitaciones en su implementación y supervisión.

Tercera: La formación continua en ciberseguridad es esencial para proteger los datos personales dentro de las empresas. La falta de conocimientos en ciberseguridad por parte de empleados y directivos puede comprometer seriamente la seguridad de los datos, incluso cuando se han implementado tecnologías avanzadas.

En cuanto a las recomendaciones se precisa lo siguiente:

Primero: Se recomienda que los gobiernos fortalezcan sus marcos regulatorios y proporcionen recursos adecuados a las autoridades regulatorias para mejorar la aplicación y supervisión de las políticas de protección de datos en las empresas. Esto asegurará una mayor uniformidad y efectividad en las medidas de ciberseguridad a nivel internacional.

Segundo: Implementar programas de capacitación continua en ciberseguridad. Las empresas deben establecer programas de formación y sensibilización para todos los niveles de personal, desde empleados hasta directivos, con el objetivo de crear una cultura organizacional de seguridad de datos que prevenga riesgos y responda efectivamente ante amenazas emergentes.

Tercero: Fomentar la colaboración público-privada para mejorar la ciberseguridad empresarial. Se sugiere que el sector privado colabore estrechamente con el sector público y académico para desarrollar y compartir tecnologías y estrategias avanzadas de ciberseguridad.

REFERENCIAS

Acosta, G., Mendoza, L., & Zamora, P. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana De Gerencia, 17*(21), 351-368. https://doi.org/10.37960/revista.v25i89.31534

Aider, H., Patrini, G., Cavalli, F., & Cullen, L. (2019). *The State of Deepfakes: Landscape, Threats, and Impact.* http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S004186332012000300002&lng=es&tlng=es

Arismendi, L., & Hunmpiri, J. (2022). *Ruta para hacer una tesis en derecho*. Editorial Grijley.

Arocena, G. (2011). La regulación de los delitos informáticos en el Código Penal argentino: Introducción a la Ley Nacional núm. 26.388. *Boletín Mexicano de Derecho Comparado, 10*(12), 945-988. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S004186332012000300002&lng=es&tlng=es

Bloisser, J. (2010). *Delitos informáticos en la Banca.* Editora RAOS.

Carbajal, M. (2021). *Las fiscalías especializadas en delitos informáticos como mecanismo para la lucha contra el cibercrimen* [Tesis de maestría, Universidad San Martín de Porres]. Repositorio Institucional USMP. https://repositorio.usmp.edu.pe/

Casabona, C. (2019). *Delitos Informáticos de carácter patrimonial*. Universidad de La Laguna.

Caycho, D. (2019). *Infracciones administrativas elevadas a la categoría de delito: ¿La no rendición de cuentas de viáticos justifica una sanción penal por peculado?* [Tesis de maestría, Pontificia Universidad Católica del Perú]. Repositorio Institucional PUCP. https://tesis.pucp.edu.pe/repositorio/

Curay, P. (2018). *Diagnóstico en la investigación del delito contra el patrimonio en la modalidad de receptación en el año 2015 en la Ciudad de Lima efectuado por la división de investigación de robos de la DIRINCRI Lima* [Tesis de maestría, Pontificia Universidad Católica del Perú]. Repositorio Institucional PUCP. https://tesis.pucp.edu.pe/repositorio/

EUROPOL. (2020). *Internet organised crime threat assessment (IOCTA*). https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

EUROPOL. (2023). *ChatGPT: The impact of Large Language Models on Law Enforcement.* Luxembourg: Publications Office of the European Union.

EUROPOL. (2022). *Facing reality? Law enforcement and the challenge of deepfakes.* Luxembourg: European Union Agency for Law Enforcement Cooperation.

García, C. (2012). *Derecho Penal: Parte General* (2ª ed.). Juristas Editores.

García, J. (2012). El fraude informático en España e Italia: Tratamiento jurídico-penal y criminológico. Icade. *Revista de la Facultad de Derecho.* https://revistas.comillas.edu/index.php/revistaicade/article/view/357

Jakobs, G. (1997). *Derecho Penal: Parte General.* Marcial Pons.

Jiménez, I. (2020). *El delito de fraude informático (art. 248.2.a CP): Aspectos problemáticos en relación con su interpretación y aplicación.* http://hdl.handle.net/10045/130801

Joo, Ki, & Sung, H. (2005). *Method for electronic commerce using security token and apparatus thereof.* http://hdl.handle.net/10045/130801

Minchola, M., & Vega, J. (2022). *Ciberdelitos: Análisis del sistema penal.* Iustitia.

Ninasivincha, M., & Gutiérrez, E. (2023). *Inadecuada gestión de información para reducir la alta incidencia de delitos contra el patrimonio en los Departamentos de Investigación Criminal de Lima* [Tesis de maestría, Pontificia Universidad Católica del Perú]. Repositorio Institucional PUCP. https://tesis.pucp.edu.pe/repositorio/

Ojeda-Pérez, J. E., Rincón-Rodríguez, F., Arias-Flórez, M. E., & Daza-Martínez, L. A. (2011). Delitos informáticos y entorno jurídico vigente en Colombia. *Cuadernos de Contabilidad, 35*(128), 41-66. www.org.co/scielo.php?script=sci_arttext&pid=S0123147220100002000 03&lng=en&tlng=es

Pardo, A. (2018). *Tratamiento jurídico penal de los delitos informáticos contra el patrimonio* [Tesis de maestría, Universidad César Vallejo]. Repositorio de Institucional UCV.

https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/20372/Pardo_VA.pdf

Perez López, J. (2019). *Delitos regulados en leyes especiales.* Gaceta Jurídica.

Prasad, N., & Panigrahi, S. (2016). *Security Issues over E-Commerce and their Solutions.* Oxford Publications.

Robles, J., & Figueroa, S. (2020). Delitos contra el patrimonio genético nacional desde la perspectiva del COESCCI. *Revista de la Facultad de Derecho y Ciencias Políticas, 50(132)*, 80-99. https://doi.org/10.18566/rfdcp.v50n132.a04

Schwab, K. (2016). *La cuarta revolución industrial.* Editorial Debate.

Sosa, O. (2022). *Phishing como modalidad de delitos informáticos: A propósito de la suplantación y robo a los beneficiarios del Bono Universal en el Perú*. Iuris tántum Editores.

Velita, A. (2021). *Problemas de la valoración fiscal en la etapa de investigación preliminar de los delitos de fraude informático en Lima* [Tesis de maestría, Universidad San Martín de Porres]. Repositorio Institucional USMP. https://repositorio.usmp.edu.pe/

Vitteri, G. (2022). *Mecanismos jurídicos para implementar la Ley 30096 en los delitos informáticos contra el patrimonio frente a las nuevas tecnologías informáticas* [Tesis de maestría, Universidad Inca Garcilaso de la Vega]. Repositorio Institucional UIGV. https://roar.eprints.org/15208/

Zambrano, A. (2022). *El uso de banca móvil en los delitos informáticos contra el patrimonio en la ciudad de Arequipa* [Tesis de maestría, Universidad César Vallejo]. Repositorio Institucional UCV. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/20372/Pardo_VA.pdf