ISSN impreso 1996-6660 / ISSN online 2519-5719
DOI: https://doi.org/10.31381/perfilesingenieria.v19i20.6029

COMPETENCIA DE LA LEY DE PROTECCIÓN DE DATOS EN LAS COMPAÑÍAS DE LA PROVINCIA DE SANTA ELENA

COMPETENCE OF THE DATA PROTECTION LAW IN COMPANIES OF THE PROVINCE OF SANTA ELENA

Javier Mauricio Muzzio Arguello
Universidad Ricardo Palma, Lima, Perú

RECIBIDO: 06 de octubre de 2023
ACEPTADO: 08 de diciembre de 2023

RESUMEN
Este artículo se centra en la importancia de la estrategia de cumplimiento en protección de datos y analiza las regulaciones más relevantes que impactan la privacidad de los usuarios. El objetivo es comprender el alcance global del Reglamento General de Protección de Datos (GDPR), explorar las leyes de protección de datos en los Estados Unidos y resaltar la relevancia de la regulación CPS 234 en Australia. La estrategia de cumplimiento es crucial para salvaguardar la confidencialidad y privacidad de los datos de los usuarios, a la vez que asegura el cumplimiento de las normativas y fortaleciendo la reputación de las organizaciones. En un mundo cada vez más regulado y digitalmente conectado, la inversión en una estrategia sólida de protección de datos no solo previene posibles multas, sino que también establece bases seguras para el futuro y genera confianza entre los clientes.
Palabras clave: estrategia, protección de datos, regulaciones, privacidad, GDPR, seguridad

Cómo citar
J. M. Muzzio Arguello, «Competencia de la ley de protección de datos en las compañías de la provincia de Santa Elena», Perfiles_Ingenieria, vol. 19, n.º 20, pp. 167–178, dic. 2023.

ABSTRACT
This article focuses on the importance of the data protection compliance strategy and analyzes the most relevant regulations that impact user privacy. The objective is to understand the global scope of the General Data Protection Regulation (GDPR), explore the data protection laws in the United States and highlight the relevance of the CPS 234 regulation in Australia. The compliance strategy is crucial to safeguard the confidentiality and privacy of user data, ensuring compliance with regulations and strengthening the reputation of organizations. In an increasingly regulated and digitally connected world, investing in a strong data protection strategy not only prevents potential fines, but also lays a secure foundation for the future and builds trust among customers.
Keywords: Strategy, Data Protection, Regulations, Privacy, GDPR, Security

1. Introducción

La protección de datos es el proceso de proteger la información confidencial de daños, pérdidas o corrupción. Dado que la cantidad de datos que se crean y almacenan ha aumentado a un ritmo sin precedentes, la protección de datos es cada vez más importante. Además, las operaciones comerciales dependen cada vez más de los datos, e incluso un breve período de inactividad o una pequeña pérdida de datos pueden tener consecuencias importantes en una empresa [1].

Las implicaciones de una violación de datos o un incidente de pérdida de datos pueden poner de rodillas a las organizaciones. La falta de protección de los datos puede causar pérdidas financieras, pérdida de reputación y confianza del cliente, y responsabilidad legal, considerando que la mayoría de las organizaciones en la actualidad están sujetas a algún estándar o regulación de privacidad de datos. La protección de datos es uno de los desafíos clave de la transformación digital en organizaciones de todos los tamaños [2].

Por eso, la mayoría de las estrategias de protección de datos tienen tres enfoques clave:

- Seguridad de datos: protección de datos contra daños malintencionados o accidentales
- Disponibilidad de datos: restauración rápida de datos en caso de daño o pérdida
- Control de acceso: garantizar que los datos sean accesibles para quienes realmente los necesitan y nadie más.

1.1 Principios de Protección de Datos

El principio básico de la protección de datos es garantizar que permanezcan seguros y disponibles para sus usuarios en todo momento. Son dos los principios clave de la protección de datos: disponibilidad de datos y gestión de datos. La primera garantiza que los usuarios puedan acceder a los datos que necesitan para hacer negocios, incluso si los datos se dañan o se pierden [3]. La segunda abarca dos áreas principales de protección de datos:

Gestión del ciclo de vida de los datos: distribuye automáticamente datos importantes al almacenamiento en línea y fuera de línea, según su contexto y sensibilidad.

En el entorno de big data actual, incluye métodos para identificar datos valiosos y ayudar a la empresa a obtener datos de ellos para informes, análisis, desarrollo y pruebas.

Gestión del ciclo de vida de la información: evalúa, clasifica y protege los activos de información para evitar errores de aplicaciones y usuarios, ataques de malware o ransomware, bloqueos o mal funcionamiento del sistema y fallas de hardware [4].

En relación a las últimas tendencias en política y tecnología de protección de datos, se destacan las siguientes:

1.2 Hiperconvergencia

Con la llegada de los sistemas hiperconvergentes, los proveedores están introduciendo dispositivos que pueden brindar respaldo y recuperación en un dispositivo que integra infraestructura de cómputo, redes y almacenamiento. Los sistemas hiperconvergentes están reemplazando muchos dispositivos en el centro de datos tradicional y brindan capacidades similares a las de la nube en las instalaciones [5].

1.3 Protección Contra Ransomware

El ransomware es un tipo de malware que infecta un sistema, cifra sus datos y exige una tarifa de rescate para liberarlo. Los métodos de copia de seguridad tradicionales son útiles para proteger los datos del ransomware. Sin embargo, los nuevos tipos de ransomware también pueden infectar los sistemas de respaldo y los inutiliza. Esto hace que sea muy difícil restaurar la versión original de los datos [6].

Para resolver este problema, las nuevas soluciones de copia de seguridad están diseñadas para estar completamente aisladas de la red corporativa y utilizan otras medidas, como el cifrado de datos en reposo, para evitar que el ransomware infecte las copias de seguridad.

1.4 Recuperación ante Desastres como Servicio

Disaster Recovery as a Service (DRaaS) es una solución basada en la nube que permite a una organización crear una copia remota de los sistemas locales o incluso un centro de datos completo y utilizarla para restaurar las operaciones en caso de desastre.

Las soluciones DRaaS replican continuamente los datos del centro de datos local para proporcionar un objetivo de tiempo de recuperación (RTO) bajo, lo que significa que pueden entrar en acción minutos o segundos después de una falla desastrosa [7].

1.5 Gestión de Datos de Copia (CDM)

Las soluciones CDM simplifican la protección de datos al reducir la cantidad de copias de datos almacenados por la organización. Esto reduce los costos generales, de mantenimiento y de almacenamiento. A través de la automatización y la gestión centralizada, CDM puede acelerar los ciclos de vida de desarrollo y aumentar la productividad de muchos procesos comerciales.

1.6 Estrategia de Protección de Datos

Toda organización necesita una estrategia de protección de datos. Aquí hay algunos pilares de una estrategia sólida:

- **Auditoría de Datos Sensibles:**

Antes de adoptar controles de protección de datos, primero se debe realizar una auditoría de los datos. Identifique las fuentes de datos, los tipos de datos y la infraestructura de almacenamiento utilizada en toda la organización.

Luego, es necesario clasificar los datos en niveles de confidencialidad y evaluar qué medidas de protección de datos ya existen en la organización, qué tan efectivas son y cuáles se pueden ampliar para proteger datos más confidenciales. A menudo, el mayor potencial está en aprovechar los sistemas de protección de datos existentes que están "por ahí" o que no se usan de manera consistente en toda la organización [8].

- **Evaluación de Riesgos Internos y Externos:**

El equipo de seguridad de la organización debe evaluar periódicamente los riesgos de seguridad que puedan surgir dentro y fuera de la organización. Los programas de protección de datos deben diseñarse en torno a estos riesgos conocidos.

Los riesgos internos incluyen errores en la configuración de TI o en las políticas de seguridad, la falta de contraseñas seguras, autenticación y gestión de acceso de usuarios deficientes, y acceso sin restricciones a los servicios o dispositivos de

almacenamiento. Una amenaza creciente son los internos malintencionados o las cuentas comprometidas que han sido tomadas por los actores de amenazas.

Los riesgos externos incluyen estrategias de ingeniería social, como phishing, distribución de malware y ataques a la infraestructura corporativa, como inyección SQL o denegación de servicio distribuida (DDoS). Estas, así como la mayoría de las amenazas de seguridad, son comúnmente utilizadas por los atacantes para obtener acceso no autorizado a datos confidenciales y exfiltrarlos [9].

1.7 Definición de una Política de Protección de Datos

Con base en el análisis de la organización de sus activos de datos y las amenazas más relevantes, se debe desarrollar una política de protección de datos que determine:

La tolerancia al riesgo para cada categoría de datos: la protección de datos tiene un costo y las medidas de protección deben aplicarse de acuerdo con la sensibilidad de los datos.

Política de autorización y autenticación: se usarán las mejores prácticas y la información histórica para identificar qué aplicaciones comerciales o cuentas de usuario deben tener acceso a datos confidenciales.

1.8 Estrategia de Seguridad

Con respecto a la protección de datos, la estrategia de seguridad de una organización debería:

- Tomar medidas para evitar que los actores de amenazas accedan a datos confidenciales,
- Asegurar que las medidas de seguridad no perjudiquen la productividad ni impidan que los empleados accedan a los datos cuando y donde los necesiten, y
- Administrar las copias de seguridad de manera efectiva para evitar el ransomware u otras amenazas, y garantizar la disponibilidad constante de los datos.

1.9 Estrategia de Cumplimiento

Finalmente, una estrategia de protección de datos debe considerar las obligaciones de cumplimiento. Las organizaciones o unidades comerciales específicas pueden estar sujetas a una variedad de regulaciones o estándares de cumplimiento específicos de la

industria. A continuación, se detallan las normativas más significativas que afectan a la protección de datos en la actualidad [10].

✓ **RGPD (Unión Europea):**

El Reglamento General de Protección de Datos (GDPR) se aplica a todas las organizaciones que hacen negocios con ciudadanos de la UE, independientemente de si la empresa está ubicada dentro o fuera de la UE. El incumplimiento puede resultar en multas de hasta el 4% de las ventas mundiales o 20 millones de euros. El RGPD protege datos personales como nombre, número de identificación, fecha o dirección de nacimiento, datos analíticos web, información médica y datos biométricos.

✓ **Leyes de Protección de Datos en los EE.UU.:**

EE. UU. no tiene una regulación de gran alcance equivalente al RGPD, pero sí varias regulaciones que afectan a la protección de datos. Entre estas, se puntualizan las siguientes:

La Ley de la Comisión Federal de Comercio exige que las organizaciones respeten la privacidad del consumidor y se adhieran a las políticas de privacidad.

La Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA, por sus siglas en inglés) regula el almacenamiento, la confidencialidad y el uso de la información médica.

La Ley Gramm Leach Bliley (GLBA) regula la recopilación y el almacenamiento de datos personales por parte de las instituciones financieras.

La Ley de Privacidad del Consumidor de California (CCPA) protege el derecho de los residentes de California a acceder a su información personal, solicitar que se elimine y solicitar que sus datos personales no se recopilen ni se revendan.

✓ **Leyes de Protección de Datos en Australia:**

La Autoridad Reguladora Prudencial de Australia introdujo una regulación de privacidad de datos obligatoria llamada CPS 234 en 2019. CPS 234 requiere que las organizaciones mejoren las medidas de seguridad de la información para proteger los datos personales de los ataques.

ISSN (Digital): 2519-5719

CPS 234 se aplica a las instituciones de depósito acreditadas (ADI), compañías de seguros generales, compañías de seguros de vida, organizaciones privadas de seguros de salud y compañías con licencia de RSE [2].

2. Metodología

El tipo de investigación que se planteó en este artículo se basó en el enfoque cualitativo y cuantitativo con el fin de obtener una visión extensa de los desafíos que presentan las empresas en cuanto a la protección de datos. En la parte de enfoque cualitativo se realizó entrevistas semiestructuradas ya que este modelo permite tener preguntas predeterminadas. Las preguntas claves de la entrevista fueron:

¿Cuáles consideras que son los principales desafíos que enfrenta la empresa en cuanto a la protección de datos?

¿Cuál es el nivel de conocimiento de los empleados sobre las regulaciones de protección de datos y las políticas internas?

¿La empresa ha enfrentado incidentes de seguridad o brecha de datos en el pasado? ¿Cuáles fueron las principales causas y como se solucionó?

¿Qué recursos se destinan para garantizar el cumplimiento de la regularización de protección de datos?

Las respuestas recolectadas entre los miembros del equipo de cumplimiento normativo, además de los empleados y otras personas que forman parte de la empresa, permitieron comprender profundamente sus experiencias relacionadas con la protección de datos. Entre los elementos a considerar en este apartado, se cuentan el tipo y diseño de investigación, la población y muestra (en los que se especifican el tipo de muestreo y los criterios de inclusión y exclusión); técnicas e instrumentos de recolección de datos, y la técnica de análisis de datos empleada [3].

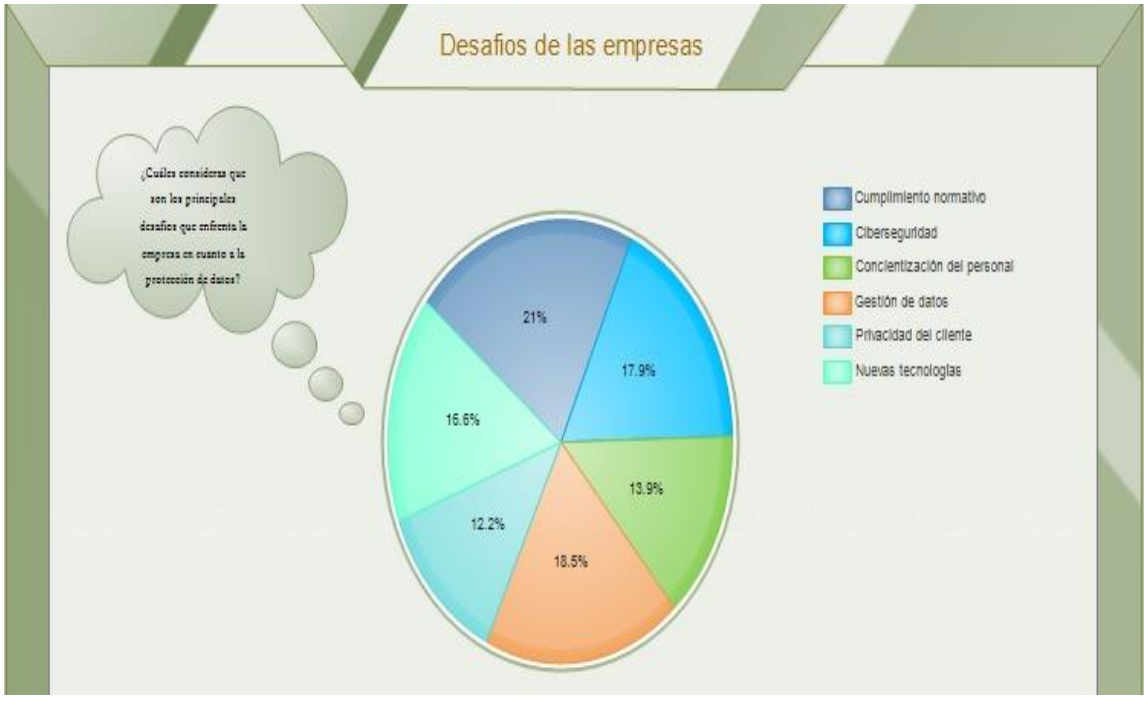
El estudio del caso se basó en los incidentes de seguridad o brechas de datos que enfrentó la empresa en el pasado, puesto que en la entrevista se mencionó un incidente relacionado al reseteo de las bases de datos de los empleados, lo que significó un gran problema para la empresa. Se buscaron soluciones tales como recolección de datos y el aumento de la seguridad en esa área para evitar futuras brechas de seguridad.

En el enfoque cuantitativo se realizaron encuestas estructuradas a los empleados y clientes que permitan tener una recolección de datos cuantitativos acerca del nivel de conocimiento de la ley de protección de datos además del cumplimiento de las políticas internas y su percepción de la seguridad de los datos en la empresa. Como en la parte de las entrevistas se recolecta datos, en este enfoque se obtienen datos numéricos de los incidentes ocurridos en el ámbito de la seguridad y niveles de cumplimiento. Las estadísticas son unas herramientas para calcular la tasa de cumplimiento y el tiempo de respuesta ante incidentes de seguridad.

Al combinar estos enfoques o metodologías se obtuvo una visión de los desafíos de la empresa en cuanto a la protección de datos [1].

3. Resultados

Figura **N°** 1**.** Resultados de la primera encuesta



Elaboración propia

Figura N° 2. Resultados de la segunda pregunta

Elaboración propia

4. Conclusiones

En conclusión, una sólida estrategia de cumplimiento en protección de datos es esencial en el entorno actual altamente regulado y digitalmente conectado. Las organizaciones deben comprender y cumplir con las regulaciones relevantes, como el GDPR, para garantizar la privacidad y seguridad de los datos de los usuarios. La protección de datos no solo es una responsabilidad legal, sino también una manera efectiva de mantener la confianza de los clientes y salvaguardar la reputación de la empresa. La inversión en medidas adecuadas de protección de datos no solo evita posibles multas, sino que también sienta las bases para un futuro digital seguro y confiable. Al adoptar una enfoque proactivo y centrado en la privacidad, las organizaciones pueden asegurar la confidencialidad de la información, protegerse contra posibles riesgos cibernéticos y fortalecer su posición en el mercado competitivo. La protección de datos se ha convertido en un pilar fundamental para el éxito empresarial y un compromiso con la seguridad y privacidad de los usuarios.

5. Referencias bibliográficas

[1] M. del C. Guerrero Picó, “El impacto de internet en el derecho fundamental a la protección de datos de carácter personal,” 2004, Accessed: Aug. 01, 2023. [Online]. Available: https://dialnet.unirioja.es/servlet/tesis?codigo=109448&info=resumen&idioma=SPA

[2] P. L. M. de la Cueva, “Informática y Protección de Datos Personales,” Revista Chilena de Derecho Informático, no. 2, Jan. 2003, doi: 10.5354/RCHDI.V0I2.10656.

[3] M. A. Ramiro and M. A. Ramiro, “El derecho fundamental a la protección de datos personales en Europa,” El derecho fundamental a la protección de datos personales en Europa, 2005.

[4] E. J. del Estado, “Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.” Mar. 25, 2021. Accessed: Aug. 01, 2023. [Online]. Available: https://hdl.handle.net/10421/9132

[5] A. Fúster, D. De La Guía, L. Hernández, F. Montoya, and J. Muñoz, “Técnicas Criptográficas De Protección De Datos 2 ª edición actualizada Criptología y Seguridad de la Información Actas de la VI Reunión Española de Criptología y Seguridad de la Información”.

[6] | Cuaderno, J. Y. Político, Y. Revista, C. Jurídica, Y. Política, and C. A. Arellano López, “El derecho de protección de datos personales,” Biolex, vol. 12, no. 23, pp. 163–174, Dec. 2020, doi: 10.36796/BIOLEX.V0I23.194.

[7] M. Rojas Bejarano, “Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales.,” Novum Jus, vol. 8, no. 1, pp. 107–139, Jan. 2014, doi: 10.14718/NOVUMJUS.2014.8.1.6.

[8] S. A. Machuca Vivar et al., “Habeas data y protección de datos personales en la gestión de las bases de datos,” Revista Universidad y Sociedad, vol. 14, no. 2, pp. 244–251, 2022, Accessed: Aug. 01, 2023. [Online]. Available: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218362020220002002 44&lng=es&nrm=iso&tlng=pt

[9] N. Remolina Angarita, “Aproximación constitucional de la protección de datos personales en Latinoamérica”. Revista Internacional de Protección de Datos Personales Revista Internacional de Protección de Datos Personales, 2012, Accessed: Aug. 01, 2023. [Online]. Available: http://www.habeasdata.org.co/.

[10] A. R. Lombarte, “Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma,” Revista de Derecho Político, no. 85, pp. 13–56, Sep. 2012, doi: 10.5944/RDP.85.2012.10244.

Javier Mauricio Muzzio Arguello

Universidad Estatal Península de Santa Elena, Ecuador.

Ingeniero en Electrónica, magíster en Telecomunicaciones, consultor en Tics y docente de la Universidad Estatal Península de Santa Elena, Ecuador.

Autor corresponsal: jmuzzio@outlook.com

ORCID: https://orcid.org/0000-0002-7610-6456

Financiamiento

Declaro que este trabajo no tiene fuentes de financiamiento

Conflicto de intereses

Declaro no tener conflictos de intereses para la elaboración del presente trabajo.

Responsabilidad ética y legal

La investigación se realizó de conformidad a los principios éticos en las ciencias de las ingenierías.

Correspondencia: jmuzzio@outlook.com