Vol.8 No.3 (2024): Journal Scientific Investigar ISSN: 2588–0659
https://doi.org/10.56048/MQR20225.8.3.2024.3624-3638

Management of personal data protection in the popular and solidarity financial sector

Gestión de protección de datos personales en el sector financiero popular y solidario

Autores:

Bermeo-Pérez, Shirley Katherine
UNIVERSIDAD CATÓLICA DE CUENCA
Cuenca – Ecuador
bshirleyk@psg.ucacue.edu.ec
https://orcid.org/0009-0007-9250-2778

Ureta Arreaga, Laura Alexandra
UNIVERSIDAD CATÓLICA DE CUENCA
Docente Maestría en Ciberseguridad
Cuenca – Ecuador
laura.ureta@ucacue.edu.ec
https://orcid.org/0000-0001-5328-8085

Yamba-Yugsi, Marco
UNIVERSIDAD CATÓLICA DE CUENCA
Docente Tutor Maestría en Ciberseguridad
Cuenca – Ecuador
marco.yamba@ucacue.edu.ec
https://orcid.org/0000-0003-4095-1444

Fechas de recepción: 30-JUN-2024 aceptación: 21-AGO-2024 publicación:15-SEP-2024

https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

Resumen

La protección de datos personales es fundamental en el sector financiero popular y solidario, que maneja información sensible de socios y clientes. En este sentido, el presente estudio aborda la implementación del estándar ISO/IEC 27701:2019 en una institución financiera de este sector en Ecuador, de acuerdo con la Ley Orgánica de Protección de Datos Personales (LOPD) y su Reglamento General. El objetivo principal de este estudio es garantizar la protección de los datos personales a través de la gestión basado en el estándar ISO/IEC 27701:2019, cumpliendo así con la LOPD. De esta forma, se busca identificar actividades de tratamiento de datos personales, gestionar los riesgos, adoptar medidas de seguridad y fomentar una cultura organizacional de cumplimiento de la ley. Se empleó una metodología aplicada y descriptiva con un enfoque mixto, dentro del proceso se identificaron las actividades del tratamiento de datos personales y artefactos jurídicos necesarios para el cumplimiento normativo. Para finalizar se realizó una evaluación exhaustiva identificando y evaluando los riesgos asociados al procesamiento de datos personales. Los resultados muestran que la implementación de una gestión de protección de datos personales permitió identificar y mitigar riesgos significativos, mejorando la seguridad y la confianza de los usuarios. Además, este enfoque cumple con los requisitos legales, estableciendo un marco sólido para la protección de la información, alineado con estándares internacionales. El cumplimiento de la LOPD demuestra un compromiso integral, que debe mantenerse a través de revisiones periódicas, evaluaciones de riesgos y adaptaciones a los cambios normativos y tecnológicos.

PALABRAS CLAVE: Instituciones financieras; datos personales; gestión de datos; ISO/IEC 27701:2019

Abstract

The protection of personal data is fundamental in the popular and solidarity financial sector, which handles sensitive information from partners and clients. In this regard, the present study addresses the implementation of the ISO/IEC 27701:2019 standard in a financial institution of this sector in Ecuador, in accordance with the Organic Law on Personal Data Protection (LOPD) and its General Regulation. The main objective of this study is to ensure the protection of personal data through management based on the ISO/IEC 27701:2019 standard, thus complying with the LOPD. In this way, the study aims to identify personal data processing activities, manage risks, adopt security measures, and promote an organizational culture of legal compliance. A descriptive and applied methodology with a mixed approach was used; within the process, personal data processing activities and the necessary legal artifacts for regulatory compliance were identified. Finally, a comprehensive evaluation was conducted to identify and assess the risks associated with personal data processing. The results show that the implementation of personal data protection management enabled the identification and mitigation of significant risks, enhancing the security and confidence of users. Additionally, this approach complies with legal requirements, establishing a solid framework for information protection, aligned with international standards. Compliance with the LOPD demonstrates a comprehensive commitment, which must be maintained through periodic reviews, risk assessments, and adaptations to regulatory and technological changes.

KEYWORDS: Financial institutions; personal data; data management; ISO/IEC 27701:2019

Introducción

La información es un activo valioso para las organizaciones y debe ser protegida adecuadamente. Si bien el avance tecnológico ha impulsado el desarrollo de las organizaciones, también ha incrementado el riesgo de pérdida, robo de información o mal uso de la información *(Castillo y Zavala, 2019).* Por lo tanto, es fundamental implementar medidas de seguridad efectivas para mitigar estos riesgos.

En el sector financiero popular y solidario, la protección de los datos de socios y clientes es fundamental garantizar la seguridad y calidad de los productos y servicios ofrecidos, a la vez que se fomenta la confianza. Un ejemplo alarmante de la magnitud del riesgo lo ilustra el informe *vpnMentor (2023),* que reveló la filtración de 18 GB de datos de 20 millones de ecuatorianos en 2019 debido a una violación en los servidores de *Novaestrat.*

Este tipo de incidentes pone de manifiesto la necesidad de implementar medidas de seguridad efectivas para mitigar los riesgos asociados a la información. En este sentido, la gestión de datos personales bajo el estándar ISO/IEC 27701:2019 se presenta como una herramienta fundamental para las entidades financieras populares y solidarias.

Desde 1948, la protección de datos personales ha ganado importancia a nivel internacional, y muchos países han implementado leyes para proteger estos datos. Cada nación ha adaptado estas regulaciones a sus propias condiciones culturales, económicas y políticas *(Cevallos & Delgado, 2023).* Ecuador no es la excepción, ya que aprobó la Ley Orgánica de Protección de Datos Personales (LOPD) en 2021 y su Reglamento General en 2023.

Si bien la LOPD establece un marco legal sólido para la protección de datos, *Aguilar et al. (2022)* advierten que la ley por sí sola no es suficiente. Se requiere un cambio cultural en las organizaciones y en la sociedad en su conjunto para garantizar una efectiva protección de los datos personales.

Es fundamental determinar cómo influye la gestión de datos personales bajo el estándar ISO/IEC 27701:2019 en la efectividad de la protección de datos personales en el sector financiero popular y solidario, en consonancia con los requisitos legales. Por consiguiente, las entidades financieras del sector popular y solidario están obligadas a implementar medidas de protección de datos para cumplir con la LOPD y prevenir sanciones económicas y daños a su reputación.

El sector financiero popular y solidario (SFPS) representa más del 20% del Producto Interno Bruto (PIB) del Ecuador *(Hernández, 2023).* Está conformado por cooperativas de ahorro y crédito, entidades asociativas o solidarias, cajas y bancos comunales, y cajas de ahorro, que realizan actividades de intermediación financiera y de responsabilidad social con sus socios (LOEPS, 2011).

Toda información que pueda ser utilizada para identificar a una persona física, directa o indirectamente, se considera dato personal (LOPD, 2021). En el contexto del SFPS, los datos

personales pueden incluir información sobre los socios, clientes y empleados de las entidades financieras. Asimismo, la privacidad es el derecho de todos los titulares de la información a proteger sus datos personales y la información clasificada que se hayan entregado o esté en poder de una entidad *(Montoya, 2020).*

La protección de datos personales implica un conjunto integral de medidas que aseguran el tratamiento lícito, leal y transparente de los datos personales, así como su seguridad y confidencialidad *(LOPD, 2021).* La ley Orgánica de protección de datos personales fue aprobada el 26 de mayo de 2021 y publicado en registro oficial No. 459, tiene como objetivo principal regular y proteger el ejercicio del derecho a la protección de datos personales. Para garantizar la implementación efectiva de la LOPD y la protección de los derechos y libertades fundamentales de las personas cuyos datos personales son tratados, se establece el Reglamento General de la LOPD, aprobada el 11 de noviembre de 2023 y publicado en registro oficial No. 435 *(RGLOPD, 2023).*

La norma ISO/IEC 27701:2019 actúa como complemento de las ISO/IEC 27001 y 27002, diseñada para proporcionar directrices específicas sobre el establecimiento, implementación, mantenimiento y mejora continua de un Sistema de Gestión de Información de Privacidad (PIMS). Esta norma aborda la gestión de riesgos de privacidad y ayuda a las organizaciones al cumplimiento de regulaciones de protección de datos. La implementación esta norma permite a las organizaciones demostrar su compromiso con la protección de datos personales a través de la implementación de controles específicos y la mejora continua de sus prácticas de privacidad *(International Organization for Standardization, 2019).*

El análisis de riesgos es una metodología empleada para identificar riesgos asociados al manejo de datos personales y evaluar la probabilidad e impacto de su ocurrencia. Esto ayuda a las organizaciones a tomar decisiones sobre cómo mitigar dichos riesgos y asignar recursos de manera eficaz *(Asana, 2024).* Además, la gestión de datos abarca el ciclo de vida completo de los datos personales, desde su recopilación inicial hasta su eliminación final, asegurando el cumplimiento de las leyes y regulaciones de privacidad en cada etapa *(Congreso de la República de Colombia, 2012).*

Debido a que la protección de datos es un tema reciente en Ecuador y hay una escasez de talento cualificado, el abogado Pablo Arteaga ofrece las siguientes recomendaciones: Definir el rol de la empresa en el tratamiento de datos, designar y capacitar a un responsable interno de protección de datos, comprender tanto la normativa como los procesos internos, inventariar las actividades de tratamiento, aplicar medidas de seguridad específicas para cada actividad, identificar las bases legales para cada tratamiento, gestionar contratos de protección de datos y establecer un canal para atender los derechos de los titulares.

El objetivo de este proyecto es garantizar la protección de los datos personales a través de la gestión bajo el estándar ISO/IEC 27701:2019, cumpliendo así con la ley de protección de datos personales de Ecuador. Entre los objetivos específicos incluyen identificar actividades de tratamiento de datos personales, gestionar el riesgo de tratamiento de datos, establecer

medidas de seguridad técnicas y organizativas para proteger los datos personales frente a los riesgos identificados, generar cultura y conciencia organizacional para el cumplimiento de la ley de protección de datos personales de Ecuador.

Para responder a los objetivos planteados se realiza las siguientes actividades: realizar un inventario de todas las actividades de tratamiento que se lleva a cabo dentro de la institución con los lideres de los procesos, evaluar los riesgos asociados a cada actividad de tratamiento de datos personales, implementar medidas de control para mitigar los riesgos identificados, como medidas técnicas, organizativas y contractuales, sensibilizar y capacitar al personal de la institución sobre la importancia de la protección de datos personales y sus obligaciones legales. Es importante destacar que la implementación efectiva de estas medidas requiere un compromiso continuo por parte de la organización y una revisión periódica para garantizar su adecuación y eficacia.

Material y métodos

Este estudio se desarrolló utilizando una metodología aplicada y descriptiva con un enfoque mixto, adecuada para los diversos análisis necesarios para alcanzar los objetivos propuestos. La investigación se llevó a cabo en una entidad financiera del “segmento 1 del sector financiero popular y solidario”, enfocándose en los procesos que implican el tratamiento de datos personales.

Para gestionar la protección de los datos personales, se cumplió con la normativa legal vigente en Ecuador, utilizando como referencia la norma ISO/IEC 27701:2019. Con la cual, se identificaron las actividades de tratamiento de datos personales realizadas en la institución en colaboración con los líderes de cada proceso operativo, de apoyo y estratégico por medio de entrevistas. Además, se determinó la licitud de cada tratamiento y se identificaron los artefactos jurídicos necesarios para asegurar el cumplimiento de los principios y derechos de los titulares de datos personales.

Asimismo, se realizó una evaluación exhaustiva para identificar y evaluar los riesgos asociados al procesamiento de datos personales y su potencial impacto en los derechos y libertades de los individuos. A partir de esta evaluación, se diseñaron medidas de seguridad y privacidad, tanto tecnológicas como organizativas, para mitigar los riesgos de incumplimiento de la ley y de impacto sobre los derechos y libertades de los interesados.

Luego, se implementaron políticas y procesos específicos, además de actualizar documentos informativos y legales para incluir cláusulas de protección de datos personales. Se definieron procedimientos claros y accesibles para que los titulares de datos pudieran ejercer sus derechos de acceso, rectificación, cancelación, oposición y revocatoria del tratamiento de sus datos personales. Todo el personal de la institución recibió la capacitación y sensibilización en materia de protección de datos personales para garantizar el cumplimiento de las normativas y procedimientos establecidos.

El análisis de datos se enfocó en identificar las actividades de tratamiento de datos que representan riesgos significativos y evaluar el impacto potencial de estos riesgos sobre los derechos y libertades de los titulares de los datos. Además, se evaluó la eficacia de las medidas implementadas para mitigar dichos riesgos, asegurando el cumplimiento de la normativa vigente. Esta evaluación permitió determinar la efectividad de las políticas, procedimientos y controles establecidos, así como identificar áreas de mejora para fortalecer la protección de datos personales en la institución.

La Gerencia de la institución brindó su consentimiento para llevar a cabo la investigación. Sin embargo, debido a la naturaleza sensible de la información recopilada, se decidió mantener el anonimato de la institución para resguardar su privacidad. De igual manera, se garantizó que todos los procedimientos cumplieran con las normativas éticas y legales vigentes, asegurando la protección de los datos personales y los derechos de los individuos involucrados.

Resultados

Se creo la política de protección de datos personales estableciendo los principios y lineamentos generales que regirán el tratamiento de datos personales en la institución, se designó un encargado de protección de datos que será el responsable de velar por el cumplimiento de la normativa y la gestión de protección de datos personales.

Se identificó 35 actividades de tratamiento de datos personales en coordinación con los líderes de los procesos, de las cuales 2 actividades de tratamiento con categorías especiales de datos personales (Exámenes médicos preocupaciones y Aperturas de cuenta de menores de edad). A continuación, se presenta las actividades de tratamiento identificadas:

Tabla 1.

Actividades de tratamiento de datos personales

N.	Actividad de tratamiento
1	Apertura de Cuentas de ahorro
2	Brindar Servicio al cliente
3	Convenios de débito
4	Depósitos a plazo fijo
5	Recaudaciones
6	Quejas y reclamos
7	Apertura de cuentas de menores de edad
8	Solicitud de Créditos.

9 Créditos CONAFIPS

10 Gestión de colocación

11 Grabación de llamadas telefónicas

12 Posicionamiento de marca

13 Campañas de generación leads.

14 Evaluación de satisfacción de servicio en la página web.

15 Publicidad a través de emails masivos

16 Servicio al cliente mediante chatbot

17 Proceso de selección de personal

18 Exámenes médicos preocupacionales

19 Capacitaciones y gestión de nómina

20 Exámenes médicos de campaña

21 Uso de imagen de los empleados para fines publicitarios

22 Exámenes médicos periódicos, reintegro y Desvinculación del personal.

23 Gestión de seguridad física

24 Videovigilancia.

25 Actividades de Auditoría

26 Gestión de proveedores

27 Servicios gestionados de administración de base de datos

28 Acreditación de sueldos (convenio de cooperación institucional)

29 Reclamaciones de seguro de vida y mortuorio

30 Envío de reportes y estructuras

31 Prevención de lavado de activos.

32 Educación financiera

33 Notificar e informar sobre el uso de canales electrónicos.

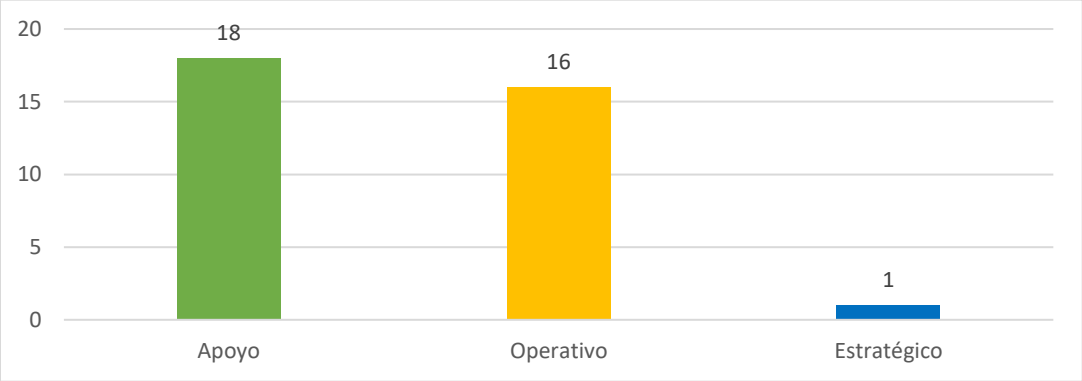
34 Validación de transacciones realizadas.

35 Gestión jurídica y atención a requerimientos judiciales.

Las actividades de tratamiento de datos personales están clasificadas por tipo de proceso. En total, se identificaron 18 actividades de tratamiento en los procesos de apoyo, 16 actividades de tratamiento en los procesos operativos y 1 actividad de tratamiento en el proceso estratégico.

Figura 1.

Actividades de Tratamiento de Datos Personales por Tipo de Proceso



Para cada tratamiento de datos personales, se analizó la legitimidad y licitud de acuerdo con la base legal establecida en la normativa vigente. Las bases legales consideradas incluyen: Consentimiento del titular, Cumplimiento de obligaciones legales, Orden judicial, Interés público, Cumplimiento de medidas contractuales solicitadas por el titular, Protección de intereses vitales del interesado, Tratamiento de datos personales contenidos en bases de datos de acceso público y Satisfacción del interés legítimo del responsable del tratamiento.

Tabla 2.

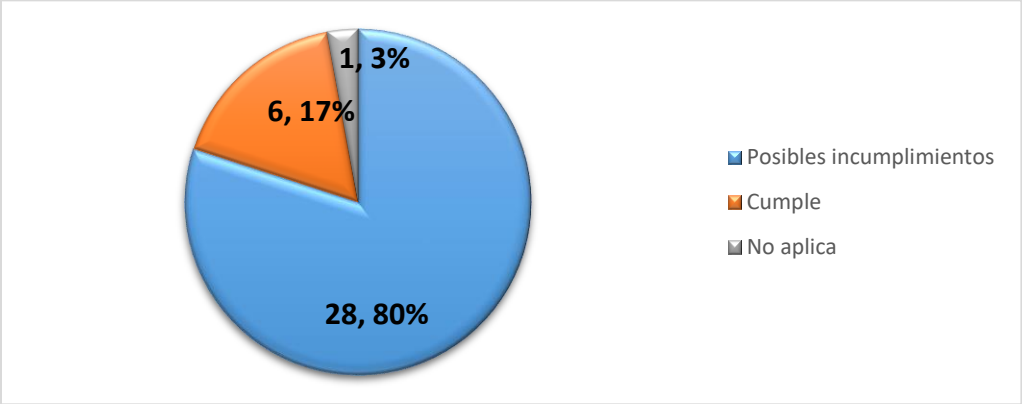
Licitud de tratamientos

Licitud de tratamiento	**Total, Licitud de tratamiento**
Cumplimiento de obligaciones legales	16
Cumplimiento de medidas contractuales solicitadas por el titular	8
Consentimiento del titular	6
Satisfacción del interés legítimo del responsable del tratamiento	2
No se determina la condición de licitud	2
Satisfacción de un interés legítimo del responsable del tratamiento	1
Total, general	**35**

Para demostrar el cumplimiento de los principios y derechos de los titulares de datos personales en cada actividad de tratamiento, se analizaron exhaustivamente documentos contractuales de socios, clientes, empleados y proveedores, así como los procesos y políticas asociados a cada actividad. Los resultados de este análisis se presentan en la *figura 2*.

Figura 2.

Cumplimiento de principios y derechos

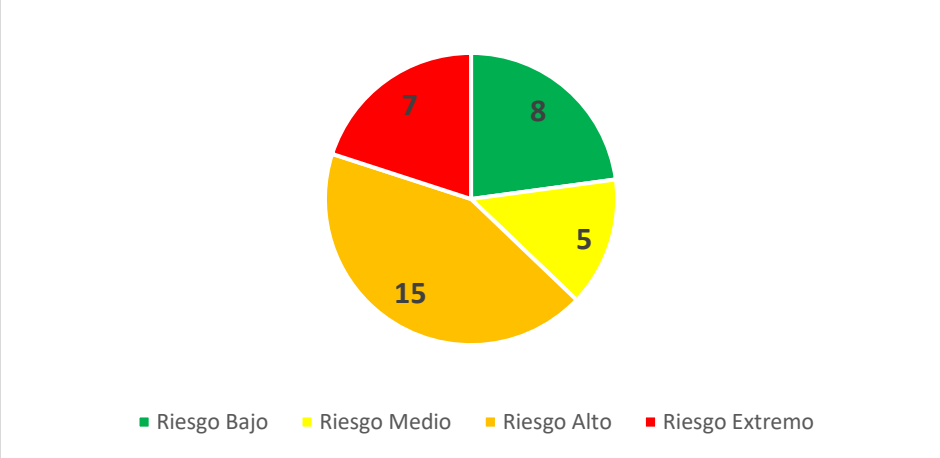


El análisis realizado determinó que seis actividades de tratamiento se ajustan a los principios y derechos establecidos. No obstante, se identificaron 28 actividades de tratamiento con posibles incumplimientos que afectan dichos principios y derechos. Además, 1 actividad de tratamiento no pudo ser evaluada en cuanto a su licitud debido a la falta de claridad legal en el tratamiento de datos personales en el entorno cibernético. En este caso específico, la institución utiliza cookies para generar tráfico publicitario a través de Google Ads en las redes sociales de los usuarios que visitan su sitio web.

Después de realizar la evaluación de riesgos, se identificaron 7 riesgos de nivel extremo, 15 de nivel alto, 5 de nivel medio, y 8 nivel bajo, para los derechos y libertades de los individuos, como se puede observar en la *figura 3.*

Figura 3:

Numero de riesgos pretramineto



Los responsables de gestionar los riesgos identificados fueron: Jefe de Captaciones, Coordinador de Marketing, Jefe de Talento Humano, Coordinador de Seguridad de la Información, Coordinador de Seguridad Física, Coordinador de Seguridad Ocupacional y Jefe de Crédito. Estos responsables implementaron medidas de seguridad y privacidad para

mitigar los riesgos extremos, altos y medios, incluyendo políticas, procesos y actualizaciones de documentos informativos y legales.
Todo el personal de la institución, un total de 400 empleados participó en el programa de capacitación y sensibilización en materia de protección de datos personales. Este programa incluyó un taller presencial dirigido a los 23 líderes de procesos y la distribución de materiales educativos, como videos, para el resto del personal. Cada empleado completó un total de 2 horas de formación.

Discusión y Conclusiones

La implementación de la gestión de datos personales bajo la norma ISO/IEC 27701:2019 ha tenido logros significativos en la institución. Se destaca la creación de una política de protección de datos personales, la designación de un encargado y la identificación de 35 actividades de tratamiento de datos. El análisis de estas actividades permitió determinar su base legal y verificar su cumplimiento con los principios y derechos de los titulares.

Si bien se identificaron seis actividades de tratamiento que se ajustan a la normativa, se encontraron 28 actividades con posibles incumplimientos. Un aspecto relevante a mencionar es la falta de claridad legal en el tratamiento de datos personales en el entorno cibernético, ejemplificado en el uso de cookies para publicidad. La evaluación de riesgos también arrojó resultados que requieren atención, identificándose 7 riesgos de nivel extremo y 15 de nivel alto para los derechos y libertades de los individuos.

Para fortalecer la protección de datos personales, la institución deberá enfocar sus esfuerzos en abordar los incumplimientos identificados en las 28 actividades de tratamiento. Se recomienda revisar los procesos y documentos legales asociados a estas actividades para garantizar su adecuación a la normativa. En el caso del uso de cookies, se sugiere buscar alternativas publicitarias que no requieran el tratamiento de datos personales sensibles.

Además, la institución debe continuar con su programa de capacitación y sensibilización para todo el personal. Es importante mantener actualizado el conocimiento de los empleados sobre sus responsabilidades en materia de protección de datos. Realizar evaluaciones periódicas del programa permitirá medir su efectividad y realizar ajustes necesarios.

Este estudio se encuentra en línea con investigaciones previas que han demostrado la efectividad de la gestión de protección de datos personales para mitigar los riesgos asociados al tratamiento de datos. Por ejemplo, *Jiménez Gómez & Hernández Franco (2019)* realizó un estudio para la protección de datos personales basado en la ISO 27001, donde demostró que un análisis de riesgo cualitativo y un plan de acción puede mitigar los riesgos. *Montoya (2020)* analizó un modelo de seguridad y privacidad de la información en una entidad pública, identificando riesgos y proponiendo un plan de acción. Al igual que *Girbau (2022)* diseñó un sistema de gestión basado en ISO/IEC 27701:2019 para mejorar la gestión de privacidad de datos.

Por tanto, estos estudios encontraron que la implementación de un sistema de gestión de protección de datos personales resultó en una reducción significativa de los incidentes de seguridad y en una mayor confianza de los interesados.

Los resultados del estudio demuestran la importancia de implementar la gestión de protección de datos personales basado en la normativa vigente y estándares internacionales. La gestión implementada ha permitido identificar y clasificar los riesgos asociados al tratamiento de datos personales, así como implementar medidas de control adecuadas para mitigar dichos riesgos. Esto contribuye a proteger los derechos y libertades de los individuos y a cumplir con las obligaciones legales en materia de protección de datos.

Se ha realizado un análisis exhaustivo para identificar los riesgos asociados al tratamiento de datos personales, clasificándolos en niveles de riesgo extremo, alto, medio y bajo. Esta identificación permitió implementar medidas de control adecuadas para mitigar los riesgos y proteger los derechos y libertades de los individuos. Estas medidas incluyen políticas, procesos y actualizaciones de documentos informativos y legales, lo que contribuye a proteger los datos personales y reducir la probabilidad de incidentes de seguridad.

La implementación de la política de protección de datos personales en la institución ha sido un paso significativo hacia el cumplimiento de las normativas vigentes y la protección de los datos de los titulares. La designación de un encargado de protección de datos es una medida clave para asegurar el monitoreo continuo y la gestión adecuada de los datos personales adoptando los cambios normativos y tecnológicos.

El análisis de la legitimidad y licitud de las actividades de tratamiento conforme a las bases legales es fundamental para asegurar el cumplimiento de las normativas de protección de datos. Las bases legales incluyen el consentimiento del titular, cumplimiento de obligaciones legales, órdenes judiciales, interés público, entre otros. La mayoría de las actividades (16) se basan en el cumplimiento de obligaciones legales, seguido por el cumplimiento de medidas contractuales solicitadas por el titular (8) y el consentimiento del titular (6). Esto muestra una dependencia significativa en el marco legal para la justificación de las actividades de tratamiento, lo cual es positivo desde el punto de vista del cumplimiento normativo.

Recomendaciones

Se recomienda a las instituciones financieras del sector popular y solidario que manejan datos personales implementar este tipo de gestión para garantizar la protección de los datos personales.

Dado que la protección de datos es una responsabilidad compartida, es crucial continuar con programas de capacitación y sensibilización para todo el personal. Estos programas deben actualizarse regularmente para reflejar nuevos desarrollos legales y tecnológicos en el campo de la protección de datos.

La institución debe priorizar la protección de datos desde el diseño y por defecto, integrando medidas de seguridad y privacidad en todas las etapas de desarrollo de productos y servicios. Este enfoque proactivo fortalece la confianza de los socios, minimiza los riesgos de seguridad y previene infracciones costosas.

La evaluación de riesgos identificó varios niveles de riesgo, desde extremos hasta bajos. Es fundamental mantener un sistema robusto de monitoreo y gestión de riesgos que permita la identificación temprana y mitigación de posibles amenazas a la seguridad de los datos personales.

Se recomienda mantener una política de actualización constante basada en investigaciones recientes y cambios en la normativa de protección de datos. Esto permitirá a la institución estar a la vanguardia en la protección de datos personales y garantizar el cumplimiento continuo de las obligaciones legales.

Referencias bibliográficas

Aguilar Martínez, M. R., Gordillo Cevallos, D. P., Paredes López, J. A., & León Burgos, G. P. (2022). La protección de datos personales en Ecuador. Revista Electrónica Estudios del Desarrollo Social: Cuba y América Latina, 10(Especial 1), 369-382. https://www.revflacso.uh.cu/

Arteaga, P. (02 de 2023). Ley de protección de datos personales en Ecuador. (K. Matute, & M. Fernandez, Entrevistadores)

Asana, T. (2024, 3 de febrero). Cómo realizar un análisis de riesgos y ejemplos. Asanas. https://asana.com/es/resources/project-risks

Calle, A., & Baño, F. (2018). Modelo de Gestión de la Información para la Protección de Datos Personales en la Carrera de Ciencias Policiales de la Universidad Central del Ecuador (Proyecto de Examen Complexivo para la obtención del título de Magíster en Informática Empresarial). Universidad Regional Autónoma de los Andes, UNIANDES, Ambato, Ecuador.

Castillo Fonseca, J. M., & Zavala Juárez, B. (2019). Ciberseguridad y vigilancia tecnológica: Un reto para la protección de datos personales en los archivos. Revista Académica de Investigación Tlatemoani, (31), 219-246. https://www.eumed.net/rev/tlatemoani/index.html

Cevallos, L., y Delgado J. (2023). Ley de Protección de Datos Personales: Impacto en la promoción del ODS 16 en el Ecuador. Reincisol, 2(4), 271-303. https://doi.org/10.59282/reincisol.v2(4)271-303

Departamento Administrativo de la Función Pública. (2020). Decreto 1377 de 2020. https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981

Girbau, C. (2022). Diseño de un Sistema de Gestión de Protección de Datos Personales Basado en La Norma ISO/IEC 27701:2019. https://n9.cl/91s2i0

Hernández, M. (2023). "El sector financiero popular y solidario representa un tercio del sistema financiero nacional". Boletines SEPS. https://n9.cl/0myhr

Organización Internacional de Normalización (ISO). (2019). ISO/IEC 27701:2019: Security techniques. Privacy information management.

Jiménez Gómez, P., & Hernández Franco, C. (2019). Implantación del Reglamento General de Protección de Datos y adaptación al Esquema Nacional de Seguridad de manera integrada en el Sistema de Gestión de Seguridad de la información basado en la ISO.

Ley Orgánica de Economía Popular y Solidaria [LOEPS]. (2011). Registro Oficial Suplemento 444. Quito: Gobierno de Ecuador. https://www.seps.gob.ec/wp-content/uploads/Ley-Organica-de-Economia-Popular-y-Solidaria.pdf

Ley Orgánica de Protección de Datos Personales del Ecuador [LOPD]. (2021). Registro Oficial Suplemento 459. Quito: Gobierno de Ecuador. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf

Montoya, J. (2020). Análisis para la implementación de un modelo de seguridad y privacidad de la información a una entidad pública del orden Territorial en el departamento del Valle del Cauca. https://repository.unad.edu.co/bitstream/handle/10596/40178/jjmontoyac.pdf?sequence=3&isAllowed=y

Mora, J., Díaz, R., Zhuma, E., & Díaz, I. (2020). El sistema de gestión de seguridad de la información bajo la norma NTE ISO/IEC 27001 en instituciones de Educación Superior (Ecuador). ROCA: Revista Científico - Educacional De La Provincia Granma, 16, 546–548. https://dialnet.unirioja.es/servlet/articulo?codigo=7414351

Reglamento General de la Ley Orgánica de Protección de Datos Personales [RGLOPD]. (2023). Registro Oficial Tercer Suplemento 435. Quito: Gobierno de Ecuador. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2023/11/Decreto-Ejecutivo-No.-904.pdf

vnpMentor. (2023, 17 de julio). Informe: Violación de seguridad en Ecuador revela datos personales confidenciales. vpnMentor. https://www.vpnmentor.com/blog/report-ecuador-leak/

Conflicto de intereses:

Los autores declaran que no existe conflicto de interés posible.

Financiamiento:

No existió asistencia financiera de partes externas al presente artículo.

Agradecimiento:

N/A

Nota:

El artículo no es producto de una publicación anterior.