Pontificia Universidad Católica del Ecuador | Sede Ambato

ESCUELA DE INGENIERÍAS

Tema:

POLÍTICA DE PROTECCIÓN DE DATOS PARA UNA INSTITUCIÓN FINANCIERA DEL SEGMENTO 3

Proyecto de investigación previo a la obtención del título de Ingeniero en Sistemas de Información

Línea de investigación:

TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Autor:

José Raimi Pambazo Guaranga

Directora:

Mg. Verónica Maribel Pailiacho Mena

Ambato – Ecuador

Agosto 2025

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **JOSÉ RAIMI PAMBAZO GUARANGA** con cédula de ciudadanía **2000135158**, autor del trabajo de graduación titulado: "POLÍTICA DE PROTECCIÓN DE DATOS PARA UNA INSTITUCIÓN FINANCIERA DEL SEGMENTO 3", previo a la obtención del título profesional de **INGENIERO EN SISTEMAS DE INFORMACIÓN**, en la escuela de **INGENIERÍAS**.

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Ambato, agosto 2025

José Raimi Pambazo Guaranga
CC. 2000135158

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

APROBACIÓN DEL TRIBUNAL DE GRADO

Tema:

POLÍTICA DE PROTECCIÓN DE DATOS PARA UNA INSTITUCIÓN FINANCIERA DEL SEGMENTO 3

Línea de investigación:

TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Autor:

José Raimi Pambazo Guaranga

Verónica Maribel Pailiacho Mena, Ing. Mg. f._____

CC. 0602970238

CALIFICADOR

José Marcelo Balseca Manzano, Ing. Mg. f._____

CALIFICADOR

Liliana del Rocío Mena Hernández, Ing. Mg. f._____

CALIFICADOR

Darío Javier Robayo Jácome, Ing. Mg. f._____

DIRECTOR ESCUELA DE INGENIERÍAS

Diego Gonzalo Coca Chanalata, Dr. f._____

SECRETARIO GENERAL PUCESA

Pontificia Universidad Católica del Ecuador
SECRETARÍA GENERAL
PROCURADURÍA

Ambato – Ecuador

Agosto 2025

DEDICATORIA

Para Mariano Guaranga C. quien, con su infinito amor, paciencia e inteligencia, me crio y me enseño lo necesario para “Ser alguien en la vida”.

A Margarita Pambazo.

A Matías Pambazo y Tránsito Guaranga M. quienes me dieron la vida, y me amaron incondicionalmente.

A Elizabeth, Sisa y Jennifer mis queridas hermanas, Quienes fueron, son y serán mi sostén en los momentos de caída.

A mis tíos, sobrinos y primos que me han brindado su apoyo moral en cada una de mis etapas de la vida.

Por último, a mí, por no rendirme, por mantenerme fuerte y demostrar a quienes no creyeron en mí, que si pude y siempre podré.

AGRADECIMIENTO

A familiares, profesores, compañeros y amigos, que constituyeron un pilar fundamental, para cumplir con mis metas establecidas.

A la entidad financiera que me abrió sus puertas.

RESUMEN

Las cooperativas de ahorro y crédito del segmento 3 en Ecuador, desde la entrada en vigencia de la Ley Orgánica de Protección de Datos Personales (LOPDP), deben implementar políticas internas para la protección de los datos que garanticen la privacidad y seguridad de la información personal de sus socios y clientes. Muchas de las instituciones financieras aún no han implementado estas políticas que garanticen la privacidad y seguridad de los datos de sus socios y clientes.

Ante esta problemática, la presente investigación tiene como objetivo desarrollar una política de protección de datos personales para una institución financiera del segmento 3, con el fin de dar cumplimiento a la normativa y fortalecer la confianza institucional. La propuesta se justifica por la necesidad de establecer directrices claras para el tratamiento responsable de los datos personales.

La metodología empleada fue de tipo cualitativo con enfoque analítico-sintético, porque permite identificar las necesidades específicas de la institución y estructurar una solución normativa. Como resultado, se diseñó una “Política de Protección de Datos Personales”, basada en el marco de ciberseguridad del NIST-CSF y en la norma ISO/IEC 27001, los cuales permiten gestionar riesgos, establecer controles y garantizar la mejora continua en la protección de la información.

La validación de la propuesta de política se realizó mediante una rúbrica que consta de siete preguntas claves con una escala de 1 a 5 puntos. Los resultados obtenidos resaltan que la propuesta cumple con la pertinencia, calidad técnica, además, se cumple con las necesidades específicas de la entidad financiera.

Palabras clave: política, protección de datos, ciberseguridad, cooperativas del segmento 3, ley orgánica de protección de datos Ecuador.

ABSTRACT

Since the Organic Law on Personal Data Protection (LOPDP) came into force, Segment 3 Savings and Credit Cooperatives in Ecuador must implement internal data protection policies that guarantee the privacy and security of their members' and clients' personal information. Many financial institutions have yet to implement these policies.

Faced with this problem, this research aims to develop a personal data protection policy for a Segment 3 financial institution in order to comply with the regulations and strengthen institutional trust. The proposal is justified by the need to establish clear guidelines for the responsible processing of personal data.

The methodology used was qualitative with an analytical-synthetic approach, allowing the institution's specific needs to be identified and a regulatory solution to be structured. As a result, a "Personal Data Protection Policy" was designed, based on the NIST-CSF cybersecurity framework and the ISO/IEC 27001 standard, which allows for risk management, establishing controls, and ensuring continuous improvement in information protection.

The policy proposal was validated using a rubric consisting of seven key questions on a scale of 1 to 5 points. The results obtained highlight that the proposal meets the financial institution's relevance and technical quality requirements, and that it also meets the specific needs of the financial institution.

***Keywords**: policy, data protection, cyberscurity, segment 3 cooperatives*, *organic law on data protection Ecuador.*

ÍNDICE GENERAL DE CONTENIDOS

INTRODUCCIÓN

En el ciberespacio, los consumidores ceden datos personales a cambio de servicios en línea, y subestiman el valor que este representa. En 2017, 4.000 millones de personas usaban Internet, la mayoría mediante redes móviles 3G y 4G, además, hubo 175.000 millones de aplicaciones descargadas. A inicios de 2018, más de 5.000 millones de personas usaban teléfonos móviles, el 57% fueron smartphones. Además, 3.000 millones de usuarios accedían a redes sociales mensualmente y otros 1.800 millones compraban en línea, lo que refleja el creciente impacto global de las tecnologías digitales. Según las cifras en el mundo existe miles de millones de datos sueltos (libres), lo cuales no han sido tratadas de manera adecuada o simplemente no existía la preocupación por parte de los usuarios exponerse en la red (Porcelli, 2020).

En su estudio, Maqueo Ramírez, Moreno Gonzales, & Recio Gayo (2017) explican que en 1980, la Asamblea Parlamentaria del Consejo de Europa propuso al Comité de ministros considerar la inclusión del derecho a la protección de datos personales en la Convención Europea de Derechos Humanos. Esta recomendación surgió debido a que varios estados miembros de la actual Unión Europea adoptaban una legislación en esta materia. Sin embargo, la propuesta fue rechazada bajo el argumento de que “no era el momento adecuado”, porque en ese momento no se contaba con la experiencia suficiente en el tema y se tenía avances significativos hacia la aprobación del Convenio 108, el cual se consolidaría como el primer marco legal internacional en la materia de protección de datos personales.

En Latinoamérica, el Sistema Interamericano de Derechos Humanos no cuenta con una normativa que vele por la protección de datos personales, pese a los esfuerzos iniciales de la Organización de Estados Americanos (OEA) y la Revista Internacional de Derecho Público. Países como Argentina, México, Chile, Uruguay y Colombia reconocen a este derecho como autónomo, inspirado en el Reglamento General de Protección de Datos Personales de la Unión Europea, vinculándolo al derecho a la vida privada y a la información conocida como *habeas data*, Ecuador

no fue incluido en este análisis por estar en proceso de desarrollar la “Ley Orgánica de Protección de Datos Personales” (Maqueo Ramírez et al., 2017).

En el ámbito nacional, la carencia de un marco legal regule el tratamiento de los datos personales junto con la ausencia de una entidad reguladora ha generado problemas tanto para las empresas, especialmente en la transferencia internacional de datos, como para los ciudadanos, cuyos derechos fundamentales son vulnerados a través de prácticas como la venta ilegal de información o el acoso por parte de operadoras telefónicas. A nivel global, ha surgido la necesidad de establecer marcos normativos que garanticen la protección adecuada de los datos personales. Un ejemplo clave es el Reglamento General de Protección de Datos (RGPD), promulgado por el Consejo de Europa en abril de 2016, cuyo objetivo principal es fortalecer la normativa de protección de datos y adaptarla a los desafíos tecnológicos actuales (Hernández Alvarado, Pinguel Llanos, & Coello Avilés, 2023).

Entre los años 2006 y 2020, se evidenció un notable aumento en el acceso a Internet y el uso de tecnologías digitales en Ecuador. Como lo señalan Rovira Jurado, Robles Riera, & Castillo Méndez (2023) de acuerdo con datos proporcionados por el Instituto Nacional de Estadísticas y Censos (INEC), en el año 2006 apenas el 6% de los ecuatorianos tenían acceso a internet, cifra que se incrementó hasta el 60%, en 2012 esto gracias a estrategias gubernamentales como la implementación de infocentros y el acceso a internet en escuelas y colegios.

En el año 2018, el acceso a Internet incrementó a 14.7 puntos, en zonas urbanas y rurales, el mismo año, el 54.3% de la población tenía celulares activos y el 36% contaba con acceso a redes sociales. Entre 2008 y 2020, el uso de Internet creció hasta 7.7 puntos, este contexto resalta la transformación digital en Ecuador, lo que marca un punto clave para entender la evolución de la conectividad en el país.

En la Constitución ecuatoriana el derecho a la protección de datos personales se constituye como una medida que garantiza la vida privada, intimidad personal y familiar, y ofrece una protección frente al uso indebido o la difusión malintencionada

de información. Este derecho es de gran importancia debido a que el acceso y la divulgación de datos son más fáciles en la era digital actual. Por lo que se brinda, también, garantías integrales al definir qué datos son estrictamente personales, identificar responsables de su tratamiento, y regular aspectos como la obtención, almacenamiento, acceso, seguridad y confidencialidad, incluido la adopción medidas que previenen la transferencia o difusión ilegal (Novillo Arévalo & Jordán Naranjo, 2023).

La problemática de la investigación se enmarca en un entorno donde las instituciones financieras de Ecuador enfrentan a retos importantes relacionados a la protección de datos personales a raíz de la aprobación de la nueva Ley Orgánica de Protección de Datos Personales. A pesar de contar con un marco legal que busca proteger la privacidad de los usuarios, la gran mayoría de las cooperativas de ahorro y crédito del segmento 3 aún no han desarrollado políticas adecuadas para cumplir con estas normas, lo que genera una contradicción entre la situación actual marcada por una falta de cumplimiento y una gestión ineficaz de los datos, y la situación deseada, en la que se requiere que las instituciones implementen prácticas sólidas que garanticen que los datos personales de socios y clientes estén protegidos.

En el caso de estudio, se pudo evidenciar que el personal del área de Sistemas de la institución financiera tiene una idea general de las normativas relacionadas a la protección de datos personales. Sin embargo, al no contar con una política de protección de datos definida para el correcto tratamiento de los datos personales, la cooperativa se expone a incumplimientos regulatorios, posibles fallas en la seguridad y vulneración de la privacidad de los usuarios. La ausencia de un marco claro para la gestión de datos personales sugiere que los procedimientos actuales carecen de estandarización, lo que incrementa el riesgo de uso inadecuado de la información personal, fuga o pérdida de información sensible.

El problema científico se puede definir como la siguiente pregunta: ¿Cómo pueden las instituciones financieras del segmento 3 del Ecuador desarrollar políticas efectivas de protección de datos personales que cumplan con la Ley Orgánica de

Protección de Datos Personales? Esta pregunta refleja una contradicción entre el conocimiento actual sobre las normativas y las prácticas efectivas en el manejo de datos, esto indica una necesidad urgente de investigación. La solución a este problema no solo contribuirá a mejorar el cumplimiento legal, sino que también fortalecerá la confianza de los actores de negocio y optimizará la gestión institucional en el ámbito financiero.

¿Con la política de protección de datos, una institución financiera del segmento 3 puede cumplir las normativas ante los organismos reguladores? El objetivo general de esta investigación es desarrollar una Política de Protección de Datos para una institución financiera del segmento 3 en Ecuador, que cumpla con la Ley Orgánica de Protección de Datos Personales.

Del mismo modo, los objetivos específicos planteados para completar este trabajo de investigación son:

1. Fundamentar teóricamente las normativas vigentes que regulan la protección de datos en instituciones financieras del segmento 3.
2. Analizar la situación actual la institución financiera en cuanto a la materia de protección de datos personales, identificando las deficiencias y oportunidades de mejora para los procedimientos y políticas actuales.
3. Diseñar una política, que establezca el procedimiento para garantizar el cumplimiento de la Ley Orgánica de Protección de Datos Personales basada en la normativa legal vigente.

La metodología que se usa es basada en el marco del NIST *Cybersecurity Framework* que se complementará con el ISO/IEC 27001 como directrices, mismas que se adaptan a las necesidades de la Cooperativa de Ahorro y Crédito “Indígenas Galápagos” y a las normativas vigentes como la Ley Orgánica de Protección de Datos Personales, y la regulación de la Superintendencia de Economía Popular y Solidaria.

La urgente necesidad de garantizar la protección de los datos personales en de las instituciones financieras del segmento 3, y la ausencia de una política clara en esta materia representa riesgos legales y reputacionales en las cooperativas de ahorro y crédito, el estudio propone una solución integral basada en estándares internacionales, que además cumplen con la ley orgánica que rige la protección de los datos personales en Ecuador. Con el desarrollo de la política de protección de datos personales la cooperativa cumplirá con la obligación legal, además de que es probable que obtenga un mejor manejo interno lo cual ayuda a que sea una institución financiera segura y confiable.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Principios fundamentales de la protección de datos personales

Los principios fundamentales de protección de datos personales, definidos por el Reglamento General de Protección de Datos (RGPD) de Europa comprende los siguientes aspectos: la licitud, lealtad, transparencia, limitación de la finalidad, minimización de datos, exactitud, integridad y confidencialidad. Estos principios son los esenciales porque garantizan el tratamiento adecuado y seguro de la información (Unión Europea, 2021).

Tabla 1. Perspectiva de autores sobre los principios de la protección de datos personales

Autores	Descripción
Conde Ortíz (2005)	Menciona que el objetivo de este derecho es proteger cualquier dato relevante con el fin de que la persona pueda ejercer su derecho, sin limitarse a la intimidad, ideología o vida familiar. Además, proporciona al titular el control sobre sus datos personales, permitiéndoles exigir a terceros que se abstengan de intromisiones o usos indebidos, lo que amplía las garantías frente a la simple protección de la intimidad.
García González (2007)	Destaca la necesidad urgente de proteger los datos personales de los ciudadanos frente a los riesgos de la era digital. Para lo cual el autor propone un marco legal sólido que reconoce este derecho como fundamental y garantice a las personas el pleno ejercicio de sus derechos sobre sus propios datos.
Solove (2013)	Expone que los principios de licitud y transparencia son esenciales para generar confianza entre las organizaciones y los titulares de los datos, destaca la importancia de una política clara y accesible para los usuarios.

Fuente: elaboración propia

En vista de la concordancia de los autores en evidenciar el manejo adecuado de la información personal como un derecho fundamental destaca la necesidad de que todas las instituciones ya sean financieras, educativas, públicas o privadas implementen una política y marcos legales sólidos que garanticen la protección de datos personales. Estas normativas deben alinearse con los reglamentos y leyes donde operan.

Dentro del contexto histórico la Protección a los datos personales, Cazurro Barahona (2020) describe que fue en Estados Unidos donde se origina el concepto del derecho a la intimidad conocido también como *right of privacy*, luego con las

primeras normativas europeas como Alemania y Francia, y finalmente en España, donde no se considera el derecho a la intimidad como fundamento de la protección de datos hasta la Constitución de 1978. Esto evidencia qué países que influyeron en el desarrollo de las normativas acerca de la privacidad. Sin embargo, el avance no fue parejo, puesto que no se contaba con leyes internacionales que garanticen la gobernanza de la privacidad en un mundo cada vez más interconectado.

En la Tabla 2 se evidencia el recorrido histórico del protocolo de protección de datos:

Tabla 2. Evolución histórica de la Protección de Datos Personales

Año	Descripción
1967	Se constituye el seno del Consejo de Europa, con el fin de estudiar el potencial de las tecnologías de la información y su amenaza hacia el derecho a la privacidad de las personas.
1978	En Dinamarca se aprueban dos leyes, la primera sobre de los registros públicos y la segunda acerca de los registros privados. En Austria se aprueba la Ley de Protección de Datos, que consolida el Derecho fundamental sobre la confidencialidad y comunicación.
1979	"La tutela de los Derechos del individuo frente al creciente progreso técnico en el sector de la informática" es una de las primeras resoluciones que abogó por una gobernanza ética de la informática y fue aprobada el 8 de mayo. En ese mismo año en Luxemburgo, se aprueba la Ley sobre utilización de datos en tratamientos informáticos.
1981	El Consejo de Europa establece el Convenio núm. 108 el cual intenta concretar el derecho al respeto hacia la vida privada de las personas, agilita la colaboración internacional en la materia de protección de datos y establece límites para las desviaciones de las legislaciones nacionales.
1995	Se adopta la Directiva 95/46/CE del Parlamento Europeo y del Consejo Europeo. Esta directiva fue un marco legal clave para la protección de los datos personales dentro de la Unión Europea, además estableció las bases para garantizar la "libre circulación de datos personales" entre los estados que la conforman.
1999	Se introduce el concepto de valor económico de los datos personales. A medida que la economía se adapta a la globalización y digitalización, los datos personales se convierten en un activo valioso en las transacciones comerciales, lo que conlleva a la necesidad de que se garantice la libre circulación de datos dentro del mercado europeo, siempre que se respeten los derechos fundamentales de las personas, en especial el de la intimidad.
2000	Se abre una nueva etapa en la Unión Europea y España, en la protección de los datos de carácter personales se reconocen como un derecho propio, consolidándose como un derecho fundamental autónomo diferente al tradicional derecho a la intimidad. La innovación, que fue radical, surgió esencialmente de la Carta de Los Derechos Fundamentales de la Unión Europea, la misma fue proclamada en la Cumbre de Niza en diciembre del 2000 donde se dispone en el artículo 8 del capítulo relativo a las libertades lo siguiente: "Toda persona tiene Derecho a la protección de los datos de carácter personal que la conciernan."

Fuente: adaptado a partir de Piñar Mañas (2005).

Desde el año 1967 donde se tiene los primeros avances de las tecnologías de la información, hasta el año 2000, se cuenta con un gran avance en la materia de la protección de datos. Estos avances son significativos, porque se abarca la mayoría de los atributos que debería abordar una ley adecuada para la protección de datos. España se destacó como un ejemplo a seguir, al reconocer la protección de datos como un derecho fundamental que deberá ser respaldada por organismos dedicados a garantizar su cumplimiento en cualquier situación que implique el tratamiento de información personal.

Ahora bien, ¿Cuáles son los objetivos del “Reglamento (UE) 2016/679”? De acuerdo con el de la investigación realizada por Burzaco Samper (2020) esta norma define las normas acerca de la protección de las personas físicas frente al tratamiento de los datos personales y las demás normativas relacionadas a la libre circulación de esos datos. Vela por los derechos fundamentales y libertades de las personas especialmente a su derecho a la protección de datos personales.

El RGPD establece un marco jurídico para el tratamiento y el intercambio de los datos personales en la Unión Europea, también refuerza la protección de los derechos fundamentales de las personas. Si se aplica el reglamento de manera adecuada se garantiza que las organizaciones tomen medidas apropiadas para el manejo responsable de la información y al mismo tiempo se promueve el respeto a la privacidad. Esto destaca la importancia de una regulación clara y efectiva en relación con los avances tecnológicos.

Los principios relativos al tratamiento de datos personales, de acuerdo con la Unión Europea (2021), los datos personales deben ser:

1. Gestionados de tal manera que se respete los principios de legalidad, lealtad y transparencia hacia la persona interesada.
2. Recolectados con fines concretos, explícitos y legítimos, y no serán utilizados, más adelante, para fines distintos a los propósitos iniciales.
3. Estrictamente limitado al fin para los que han sido recolectados.

4. Exactos y actualizados, para lo cual se utilizará todas las medidas para su supresión o rectificación sin demora para aquellos datos que presenten incoherencias con relación a los fines del tratamiento.
5. Deben ser almacenados de manera que permita la identificación del titular de los datos únicamente el tiempo estrictamente necesario para cumplir con la finalidad del tratamiento. Los datos personales serán almacenados de manera prolongada con fines de registros de interés público, propósitos de investigación, históricos o estadísticos.
6. Tratados con un nivel adecuado de protección, donde se prevenga accesos no autorizados o ilegales, así como pérdidas, daños o destrucción, mediante medidas técnicas y organizativas adecuadas.

Cumplir con los principios descritos anteriormente aseguran que el tratamiento de los datos personales en organizaciones e instituciones, tanto privadas como públicas se hagan de tal manera que se respeten la dignidad, derechos y libertades de las personas. Los principios como los antes descritos establecen obligaciones no solo para quienes hacen uso o tratamiento de los datos sino también para los titulares sino, también otorgan control acerca de su información.

1.2. Evolución histórica de las normativas de protección de datos en Latinoamérica

En algunos países de América Latina era evidente la ausencia de una ley de protección de datos, pero en algunos otros incluían normativas constitucionales sobre la privacidad o *habeas data,* además de que en 1997 tuvo lugar la Conferencia euro iberoamericana sobre Protección de Datos Personales que contó con la participación de autoridades europeas en la materia y delegados de los países iberoamericanos. Donde se evidenció la falta de normativas específicas sobre el tema, lo que incitó a que los asistentes propusieran la implementación de medidas que resguarden los datos de las personas físicas, así como la elaboración de una legislación adecuada (Hernández, 2012).

En comparación con otras regiones, Latinoamérica ha mostrado más efectividad, con las cartas magnas que reconocen derechos y establecen medidas jurídicas para la defensa y protección de datos personales tanto en los sectores públicos como privados. Se ha logrado por dos acciones uno: reconociéndolo como un derecho independiente, y dos: establece mecanismos constitucionales para su salvaguardia. Entre los mecanismos de defensa de los derechos fundamentales se incluyen la “Acción de Tutela” en Colombia, Recurso de Protección en Chile y *Mandado de Segurança* en Brasil, como una acción específica conocida como *habeas data* (Bertoni, 2012).

Así la normativa ha sido aplicada de manera progresiva en distintos países del continente, específicamente Latinoamérica, es por ello que, se presenta la tabla 3 donde se resume lo más destacado de la ley de protección de datos personales en distintos países.

Tabla 3. Contexto de las normativas constitucionales en materia de protección de datos en Latinoamérica.

País	Año de promulgación	Ley específica	Descripción y Detalles
Argentina	2000	Ley 25.326 Ley Orgánica de Protección de Datos Personales	El objetivo de la ley proteger de manera integral los datos personales que están almacenados en archivos, registros, bancos y bases de datos. El Código Civil y Comercial de la Nación protege aspectos íntimos, considerados datos sensibles, como la imagen y la voz. Estos deben ser tratados si cuentan con el consentimiento expreso del afectado. Así también, la legislación dispone como regla general que todo tratamiento debe ser realizado con la autorización del titular de manera libre, expresa e informada según el caso, de manera escrita. (Juri, 2019); (Milanes, 2017).
Brasil	2018	Ley General de Protección de Datos (Ley N°13.709)	Implementada en 2020 es reconocida como una de las leyes más completas y avanzadas de la región. La Ley General de Protección de Datos Personales de Brasil se destaca por sus sanciones severas. Las sanciones podrían llegar al 2% por facturación anual por empresa en Brasil, con un tope de 50 millones de reales por infracción (Echeverria, Alarcón, Altamirano, & Usca, 2024).
Chile	1999	Ley 19.628	La Ley 19.628 contempla algunos derechos fundamentales de las personas en relación con la protección de datos personales, además de contar con mecanismos judiciales para su protección, conocida como *Habeas Data*. Derechos como el acceso, modificación, eliminación y bloqueo permiten que el titular de los datos pueda solicitar judicialmente la exhibición de sus datos. En caso

			de un mal uso de los datos personales el titular puede solicitar una indemnización por el daño causado, en pleno uso del *Habeas Data,* según lo dictamina el artículo 23 de la ley (Noguera Osorio, 2020)
Colombia	2008	Artículo 15 – Ley 12.66 (2008)	La protección de datos empezó con la norma especial 12.66 de 2008, y se solidifica con la Ley 1581 en 2012 medio por el cual se regula el *Habeas Data,* con el objetivo de proteger todos los datos que se encuentren inscritos en todas las bases de datos que realicen tratamiento de datos (Rojas Bejarano, 2014). La Superintendencia de Industria y Comercio se consagra como la entidad encargada de la protección de los datos personales, y mediante el decreto 1377 se actualiza parcialmente la ley, donde se incluye aplicaciones de regulaciones y procedimientos para reducir sanciones que se aplican a distintas entidades (Arcos Argudo, Matute Pinos, & Fernández Mora, 2023).
Costa Rica	2011	Ley No. 8968	Denominado “Protección de la Persona frente al Tratamiento de sus Datos personales y su Reglamento” cuyo fin es garantizar los derechos fundamentales de las personas. En el caso de existir alguna violación al derecho de Autodeterminación Informática, la Agencia de Protección de Datos de los Habitantes encargada de fiscalizar y regular las bases de datos, actuará de oficio o por petición del interesado (Rivera Barrantes, 2019).
Cuba	2019	Protección de Datos Personales	Según Gaytán (2023) evidencia que se reconoce el derecho de los ciudadanos al acceso a sus datos almacenados en registros, archivos o información pública. Así mismo, se considera la facultad de solicitar la no divulgación, así como la corrección, rectificación, modificación y actualización de dicha información conforme con lo dispuesto en la ley. Una nueva modificación de la constitución se dio el 14 de mayo del 2022, donde se aprobó la Ley de Protección de Datos Personales, donde se protege a la ciudadanía ante cualquier difusión de cualquier información que afecte la privacidad. Así el panorama cambia para bien porque se crearon las condiciones idóneas para prevenir cualquier situación de desprotección en un mundo más interconectado.
Ecuador	2021	Ley Orgánica de Protección de Datos Personales	Esta ley engloba todo lo relacionado al tratamiento de los datos personales, con la finalidad de que se garantice el derecho al resguardo de esta y para ello se establece el Registro Nacional de Protección de Datos Personales el cual establece las infracciones, medidas correctivas y regímenes sancionatorios. Incluye la creación de la primera autoridad de protección de datos personales que es la Superintendencia de Protección de Datos Personales. Como toda ley de protección de datos, la LOPDP cubre cualquier tratamiento técnico de datos ya sean automatizados, semi automatizados, o

			manuales, los cuales son la recolección, recopilación, registro, organización, conservación, adaptación, modificación, eliminación, indexación, extracción, consulta, utilización, distribución, comunicación o transferencia (Rovira Jurado et al., 2023).
México	2010	Ley Federal de Protección de Datos Personales en Posesión de los Particulares	Se hace mención a la protección de los datos personales en el Artículo 16 en junio de 2009 el cual se denomina como la Ley Federal de Protección de Datos Personales en Posesión de los Particulares aprobada en 2010 por el Congreso de la Unión a través de los derechos de Acceso, Rectificación, Cancelación u Oposición (ARCO) (Nieves Lahaba & Ponjuan Dante, 2021). Los derechos ARCO constituyen el mecanismo principal por el cual las personas ejercen su derecho a la protección de datos personales junto a los derechos de privacidad y libertad de expresión. El Instituto Nacional de Acceso a la Información y Protección de Datos Personales (INAI) es el organismo constitucional responsable de garantizar el derecho a la protección del derecho de los datos personales, cuya participación en el desarrollo y la creación de normas y guías que facilitan la protección de dicho derecho (Hernández Cruz, 2022) (Moreno Pérez, 2022).
Perú	2017	Ley de Protección de Datos Personales (LPDP)	La ley mediante la Autoridad Nacional de Protección de Datos Personales busca proteger, defender, garantizar y promover los derechos a la protección de los datos personales. De esta manera se garantiza que el tratamiento de datos sea de manera fidedigna, sin alteración de los hechos, dentro del límite legal y razonable. Para ello se cuenta con un método denominado procedimiento trilateral de tutela el cual se encuentra regulado en el artículo 24 de la LPDP (Lima Cervantes, 2021).
Uruguay	2008	Ley N° 18.331	La ley se orienta a la protección de los datos personales y su resguardo mediante la aplicación del *Habeas Data.* El organismo regulador de la protección de los datos personales es la Unidad Reguladora y de Control de Datos Personales (URCPD) el cual se consagra como la máxima autoridad de supervisión y control de este derecho (Ordóñez Pineda, Correa Quezada, & Correa Conde, 2022). En 2020 la presidencia del país presentó a la asamblea general el proyecto de ley con la finalidad de convalidar el Protocolo Modificatorio del Acuerdo para la Protección de las Personas Interesadas en el Tratamiento de Datos Personales, el cual se firmó el 10 de octubre de 2018. Esta normativa está designada a renovar los términos descritos en acuerdo original, estar a la par con las nuevas tecnologías y reforzar la protección de los datos personales. Además, Uruguay es uno de los países que cuenta con una certificación europea por su cumplimiento en la

			protección de los datos personales (Limones Zambrano & Peralta Peralta, 2023).
Paraguay	2001	Ley 1682	Esta ley promulgada por la presidencia el 16 de enero del 2001 precisa en un marco legal para el tratamiento de datos personales los cuales se consideraban de carácter licito si y solo sí los datos eran recolectados, almacenados, procesados para su publicación de datos o características personales, científicos o estadísticos. Estas publicaciones no debían individualizar al individuo u organización investigada. Esta ley, además, prohíbe la difusión de los datos sensibles que, por lo general, generan consecuencias negativas como prejuicios y discriminaciones, vulneraciones a su: dignidad, privacidad, la imagen del titular e intimidad doméstica. También determinaba que todo individuo posee el derecho al acceso a su información personal que se encuentren en registros públicos (Ferreira Aguilera, 2021).
Nicaragua	2012	Ley No. 787 "Ley de Protección de Datos Personales"	La ley se promulga con el objetivo de mantener un equilibrio con la Ley de Acceso a la Información Pública (Ley No. 621). Luego en el 2014, la Constitución Política realiza una reforma que fortalece la protección de datos personales, dándose a conocer que el derecho al acceso y el tratamiento de la información personal aplica para entidades públicas y privadas (Pérez Martínez, 2020).
Panamá	2019	Ley 81	El objetivo principal de esta ley es regular el tratamiento de los datos personales por parte de personas naturales y jurídicas, públicas o privadas. Esta ley se considera un avance mínimo, pero de gran importancia en el largo proceso de consolidación de una ley sólida y organizada en el ámbito de la seguridad de la información sensible (Guzmán, Palacios, & Palacios, 2023).

Fuente: elaboración propia

Como se evidencia en la Tabla 3, algunos países latinoamericanos han demostrado avances significativos en la formulación de normativas en la materia de protección de datos personales. A pesar de no hacer referencia explícita a la normativa de la Unión Europea (RGPD), se puede observar una clara influencia en algunas normativas con los principios de derechos al acceso, rectificación, cancelación, y la designación o creación de una autoridad autónoma de control.

Esto demuestra la importancia de contar con una Ley autónoma, actualizada y rigurosa para la protección de datos personales, misma que debe ser respaldada por un ente controlador independiente que vele por el cumplimiento de las normas

establecidas. Además, es importante fomentar la concientización pública para así cultivar una cultura de responsabilidad, transparencia y seguridad digital.

La constitución ecuatoriana ampara la protección de los datos personales de sus ciudadanos por lo que establece una normativa que garantiza los derechos de los titulares y, así mismo, dispone reglamentos para instituciones y empresas que hacen el tratamiento. De esta manera, la Ley Orgánica de Protección de Datos Personales se ajusta a las exigencias internacionales, aborda temas importantes como la autorización informada, privacidad de la información, las garantías establecidas para garantizar el derecho de las personas sobre su información personal y el intercambio internacional de la información. Para la supervisión y el cumplimiento de estos derechos el país cuenta con la Agencia de Regulación y Control de Datos Personales (ARCO) que se encarga de dar seguimiento para que se garantice y respete los estándares de seguridad en el tratamiento de los datos personales dentro de empresas e instituciones (Barahona Martínez, Barzola Plúas, & Peñafiel Muñoz, 2024).

1.3. Datos sensibles y su gestión en las instituciones financieras

Si bien es cierto que los datos personales hacen identificable a una persona, los datos sensibles son conocidos según Pfeiffer (2008) como: todos aquellos que identifican o permiten la identificación de la persona, estas pueden ser inclinaciones ideológicas, etnia, sexo, estado de salud o situación económica que pueda servir para la confección de su perfil, misma que puede llegar a constituir una amenaza para el individuo. Lo que demuestra que los datos sensibles que son manejadas en las instituciones financieras constituyen un riesgo referente a la elaboración de perfiles automatizados en base a su estatus económico.

A esto también se agrega la información genética la cual revela datos traducibles como las preferencias sexuales, salud física o psíquica e inclinaciones morales, lo cual caracteriza a este tipo de datos como una subcategoría de los Datos Personales. Para realizar cualquier tratamiento con este tipo de dato, se requiere el consentimiento expreso del titular de la información, en ocasiones de manera

escrita, y a su vez queda prohibida el almacenamiento en ficheros (Peyramo, 2020); (Pfeiffer, 2008).

El Instituto Nacional de Transparencia, Acceso al Información y Protección de Datos Personales (INAI) citado en el trabajo de Pimboza Ninacuri (2025) menciona que los datos sensibles y los datos patrimoniales o financieros son subcategorías de los datos personales, entonces se define a los datos sensibles como los datos que informan características íntimas del individuo cuyo tratamiento incorrecto puede ser capaz de injuriar a la persona. En cuanto a los datos patrimoniales son todos aquellos datos que informan acerca de las condiciones, recursos o activos que una persona posee.

La Ley Orgánica de Protección de Datos Personales (LOPDP) de Ecuador, según lo establecido en el Registro Oficial (2021) de la Asamblea Nacional, define a los datos sensibles aquellos que pueden servir para originar discriminación o vulnerar los derechos y libertades fundamentales de los ciudadanos. Asimismo, los datos crediticios corresponden al comportamiento económico de las naturales utilizada el análisis de su capacidad financiera. Ambos tipos de datos deben ser tratadas conforme a los principios de licitud, finalidad y proporcionalidad de la LOPDP, lo que garantiza el respeto a los derechos del titular.

Para una mejor garantía de este derecho, la LOPDP otorga a los titulares de los datos derechos como el acceso, rectificación, eliminación, oposición, portabilidad y a la no elaboración de perfiles automatizados. Ante cualquier vulneración de seguridad que puedan afectar los datos personales, sensibles o patrimoniales, la entidad financiera está obligada a notificar al ente regulador y a los titulares afectados dentro de un plazo de 72 horas, el incumplimiento de estas obligaciones pueden dar lugar a sanciones, multas, suspensión de actividades o inclusión prisión, y otras sanciones previstas en la LOPDP (SEPS, 2024)

La regulación de protección de datos es la obligatoriedad que impone a empresas u organizaciones realizar evaluaciones de impacto, es así que toda entidad que se dedica a realizar actividades financieras, de crédito, aseguradoras, farmacéuticas,

hospitales y clínicas, seguridad, comercializadoras, *e-commerce* o instituciones educativas deben realizar dicha evaluación (Gadea Soler, 2020).

Las entidades financieras deben recopilar los datos de las personas de manera lícita y consentida, y esta recopilación debe tener un fin, propósito específico y legal, y no se pueden utilizar para otros fines. Con el cumplimiento de este propósito, se logra la confianza y la seguridad por parte del titular al saber que sus datos no serán ocupados para otros fines ilícitos que vulneren los principios de la ley de protección de datos personales (Pacheco Bancayan, 2019).

Desde el momento en que una persona, ya sea natural o jurídica, decide abrir una cuenta de ahorros o corriente, en una entidad financiera esta brinda información de todos los datos personales, así como la autorización para acceder a su estado financiero (considerado como dato sensible), es por ello que se destaca la importancia de que se debe contar con una infraestructura informática robusta que asegura la protección de conectividad, redes, acceso a plataformas y servidores del banco, contar con políticas de seguridad informática. Todo esto debe ser acompañado de una correcta capacitación y concientización sobre la importancia del cuidado del tratamiento de datos personales de clientes o socios (Niño García, 2022).

Los datos financieros de una persona están sujetos a la no divulgación sin previa autorización expresa por parte del afectado. Sin embargo, en caso de que se dé un proceso judicial como, por ejemplo, un juicio de pensión alimenticia es posible solicitar la obtención de la información necesaria al órgano máximo de control competente, que es en este caso, la Superintendencia de Bancos (SB). Previa la autorización de la SB, obligatoriamente se deben aplicar los principios que rigen el tratamiento de los datos personales, tales como finalidad, necesidad e integridad (Abdo León, 2024).

En el *Hábeas Data* de Ecuador se garantiza el derecho a que la persona solicite que se intervenga en un tratamiento automatizado de los datos que incluyan la elaboración de perfiles o decisiones automatizadas que afecten al individuo.

Además, regula el nivel óptimo de seguridad para riesgos, como la seudonimización y el cifrado de datos personales, también la responsabilidad de notificar a la autoridad competente y al usuario acerca de cualquier posible falla en la seguridad que represente un riesgo hacia los derechos y libertades de las personas, es por ello que la Superintendencia de Economía Popular y Solidaria (SEPS) se pronuncia de manera anticipada a los ataques cibernéticos, y publicó un oficio donde se encuentran recomendaciones para las buenas prácticas de resguardo de la información de socios y clientes en entidades financieras (Arellano Veloz, 2023); (Martínez Pérez, Freire Gaibor, & Alzate Peralta, 2024).

La seudonimización se refiere a que el tratamiento de los datos personales se debe hacerlo de modo que no se puedan relacionar a una persona en específico sin algún otro dato que lo complemente, dicho dato complementario debe sujeta a medidas técnicas y organizativas adecuadas, y almacenadas por separado para que los datos no se asocien a otra persona identifica o identificable (Diario Oficial de la Unión Europea, 2016)

Dentro de las instituciones financieras existe un tipo característico que son las Cooperativas de Ahorro y Crédito (COAC), las cuales son organizaciones que pertenecen al sector de la economía popular y solidaria, y aportan al desarrollo económico de todos los sectores a nivel nacional con especial enfoque en las zonas rurales y tradicionalmente marginadas, es importante destacar el desarrollo de este tipo de entidades y lo que implica la digitalización progresiva en la protección de datos personales de los socios y clientes, especialmente a aquellas cooperativas que aún no cuentan con una política estructurada que garantice el correcto tratamiento de la información de los usuarios.

Debido a los avances tecnológicos las cooperativas se encuentran en un entorno de competencia en el cual los socios están cada vez más actualizados en el ámbito tecnológico, y un mercado financiero con opciones casi ilimitadas, debido a que cuentan con plataformas móviles que son más accesibles y menos costosas. Por lo cual las entidades financieras deben estar a la vanguardia para asegurar la permanencia en el mercado (Ojeda-Contreras, Moreno-Narváez, & Torres-Palacios,

2020). Algunas cooperativas cuentan con la opción de banca virtual para sus socios y clientes, además de contar con la emisión de tarjetas de crédito y débito que permite que los procesos sean más sencillos y con menor costo.

La Junta de Política y Regulación Monetaria y Financiera establece reformas en las normas para la segmentación de las entidades del Sector Financiero Popular y Solidario, es por lo que la SEPS en 2024 realizó las actualizaciones pertinentes, en su Artículo 1 menciona que las instituciones financieras se segmentarán de acuerdo con el tipo y liquidez de sus activos, por lo cual da como resultado 5 segmentos los cuales se detallan en la tabla 4:

Tabla 4. Segmentación del Sector Financiero Popular y Solidario.

Segmento	Activos
1	Mayor a 80’1000.000,00
2	Mayor a 20'000.000,00 hasta 80'000.000,00
3	Mayor a 5'000.000,00 hasta 20'000.000,00
4	Mayor a 1'000.000,00 hasta 5’1000.000,00
5	Hasta 1'000.000,00

Fuente: Superintendencia de economía popular y solidaria 2024.

Es evidente que las COAC’s manejan datos sensibles de todos los actores del negocio como: directivos, socios, colaboradores, empleados y clientes las cuales se utilizan en transacciones financieras tanto de manera presencial y, en algunos, casos de manera digital. Los datos que se recogen son datos personales, de contacto, laborales, económicos, referencias comerciales, datos biométricos, de género, de salud, y según productos que ofrecen algunas cooperativas, las mismas pueden recolectar datos personales de menores de edad. Existen diversas cooperativas de ahorro y crédito que aún no establecen medidas para el correcto tratamiento de datos personales en base a la Ley Orgánica de Protección de Datos Personales (Encalada Aguilar, 2024).

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1. Metodología de la investigación

Enfoque de Investigación

El enfoque cualitativo obtiene datos descriptivos los cuales serán presentados a través del discurso oral o de manera escrita. Este enfoque busca comprender la realidad social como una construcción histórica, percibido desde la lógica y el sentir de los autores, y considera la percepción y características propias del individuo. La relevancia radica en el estudio de fenómenos sociales complejos que resultan ser complicados de entender desde una perspectiva cuantitativa (Sandoval Casilimas, 1996); (Cueto Urbina, 2020).

La adopción del enfoque cualitativo a este estudio nos permite tener una comprensión profunda acerca de las perspectivas sociales relacionadas con la protección de datos personales en las cooperativas de ahorro y crédito del segmento 3 a demás, de su contexto normativo, operacional y organizacional debido a su flexibilidad y adaptabilidad. Resulta pertinente utilizar dicho enfoque debido a que la protección de datos personales no solo depende de las normas reguladoras, sino también, de la interpretación propia y la aplicación práctica en contextos específicos.

Resulta útil debido a que se busca una fundamentación teórica de las normativas vigentes, mediante al análisis documental, que permite determinar el contexto actual de la institución financiera en materia de protección de datos, así como la experiencia y percepción cada uno de los actores del negocio, lo cual permite obtener un enfoque íntegro del problema.

Método de investigación

El método analítico-sintético es una herramienta que permite al lector facilidades para la comprensión de textos argumentativos mediante el estudio por partes y de

forma individual (análisis) para luego integrarlos y estudiarlas de manera global e integral (síntesis), (Torres Salcedo, 2019).

El uso de este método se justifica porque permite comprender el tema de estudio de manera profundizada y organizada. Al indagar los diferentes componentes de la protección de datos personales por separado posibilita la comprensión de todos sus elementos. Posteriormente, todos los elementos estudiados se integran para tener un entendimiento general e íntegro del tema tratado. La combinación de estas dos partes permite determinar los elementos clave y establecer relaciones significativas lo que facilita la formulación de propuestas fundamentadas.

Tipo de Investigación

Se va a usar la investigación documental la cual permite recolectar, recopilar y seleccionar información proveniente de documentos, libros, revistas y artículos especializados. Su objetivo principal es orientar la investigación desde dos perspectivas: primero relaciona información existente de diversas fuentes, y la segunda, brinda una visión amplia y sistemática cobre un tema tratado en distintas fuentes (Reyes Ruiz & Carmona Alvarado, 2020).

Se realiza una investigación documental, porque permite la recopilación de información de diversas fuentes como leyes, reglamentes, artículos, libros y documentos institucionales. Resulta adecuado para desarrollar un marco teórico adecuado y solido acerca de la protección de los datos personales con especial énfasis en las instituciones financieras pertenecientes al segmento 3 en Ecuador. La revisión sistémica de documentación de distintas fuentes permite determinar el nivel de conocimiento actual, avances en las normativas y los estándares en la materia. La visión panorámica del tema de estudio es indispensable porque permite fundamentar propuestas que cumplen con los requisitos de la norma vigente.

La investigación de campo es la técnica la cual se hace directamente en el entorno de estudio. Tiene como propósito la recopilación de información directa de la fuente

original (fuente primaria), mediante la implementación de diversas técnicas como la observación, encuestas, entrevistas y prácticas de campo (UNAM, 2016).

Además de la investigación documental, se utilizará la investigación de campo porque permite la obtención de información real y de primera mano acerca del estado actual de las prácticas, procedimientos y nivel de cumplimiento con la normativa vigente directamente de la institución financiera.

Técnicas e instrumentos de investigación

La entrevista se emplea para entender la perspectiva del otro mediante una interacción comunicacional que busca la comprensión profunda acerca de un tema en particular. A través de la entrevista se pretende entender la perspectiva del otro con el fin de entender, describir y explicar sus experiencias de su entorno cotidiano o profesional (Hernández Carrera, 2014).

La entrevista permite comprender acerca del nivel del conocimiento del personal involucrado en el tratamiento de los datos personales en la institución financiera, en este caso el encargado del área de sistemas de la COAC Indígenas Galápagos. La obtención de información de primera mano será útil para la comprensión del nivel de conocimiento, de cómo se realiza el tratamiento, el cumplimiento con la normativa vigente y las practicas internas con relación a los datos personales. De este modo, se logra fortalecer la investigación documental con evidencia recolectada directamente del campo de estudio.

2.2. Metodología de desarrollo

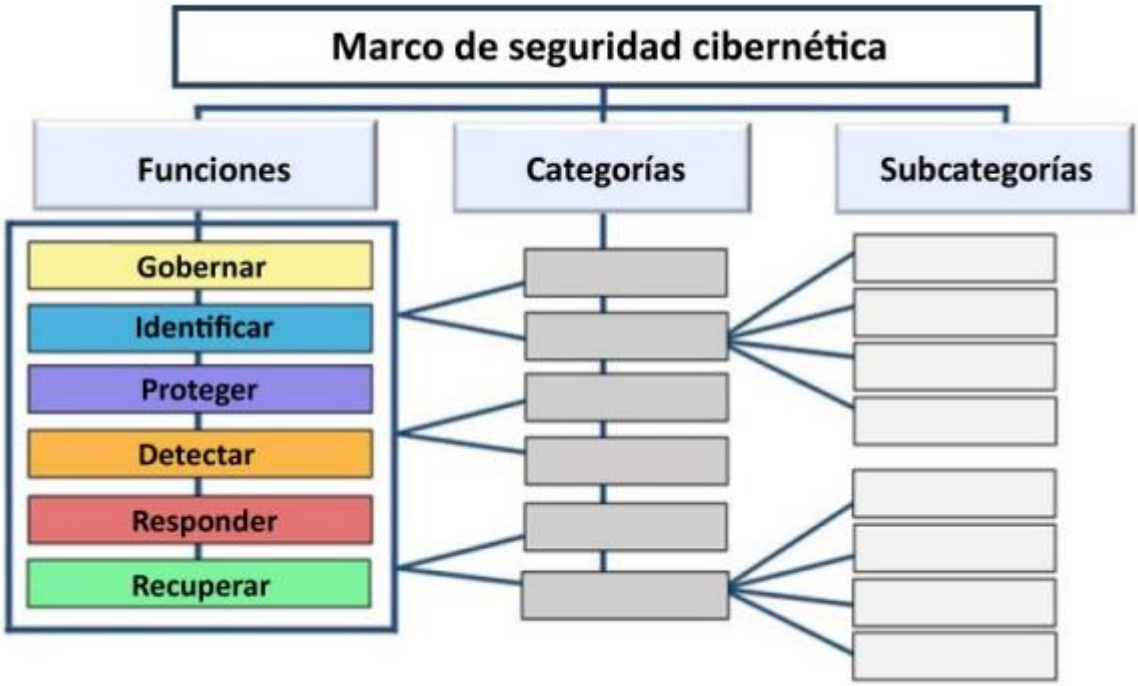
El desarrollo de la política se basa en el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnologías (NIST-CSF por sus siglas en inglés) y la norma internacional ISO/IEC 27001 porque proporcionan estructuras reconocidas a nivel global en materia de gestión de la seguridad de la información, por lo que es necesario comprender el contenido y la aplicabilidad de cada una de estas normativas.

Marco de Ciberseguridad (NIST-CSF):

NIST *Cybersecurity Framework* (CSF) es un marco de seguridad cibernética que fue desarrollado por el gobierno de Estados Unidos que brinda directrices sobre gestión y minimización de los riesgos relacionados a la ciberseguridad, al ámbito financiero, de privacidad, y tecnología a empresas y organizaciones de todo tipo. Es de gran ayuda puesto que se puede aplicar en empresas sin necesidad de determinar el nivel de madurez y sofisticación de sus sistemas de seguridad. Debido a su flexibilidad puede ser comprendida tanto por el personal especializado como el personal no técnico (Nist, 2024).

El núcleo del marco de privacidad consta de 3 elementos, que son funciones, categorías y subcategorías, su estructura se detalla en el Figura 1.

Figura 1. Estructura del Núcleo del Marco de ciberseguridad



Fuente: Nist (2024)

Las funciones de la CSF ordenan los resultados de la ciberseguridad en un rango alto, las cuales constan de lo siguiente:

1. **Gobernar (GV):** La Nist (2024) define a Gobernar como la función donde se establece las estrategias, expectativas y políticas para gestionar la seguridad de la información. Su objetivo principal es orientar y priorizar acciones que son necesarias para lograr los resultados de las demás funciones. Es de gran importancia debido a que permite comprender el contexto organizacional y operativo, definir responsables y autoridades, la política, y asegurar la adecuada supervisión de las estrategias para la seguridad de la información.
2. **Identificar (ID):** Esta función permite la identificación de oportunidades de mejora en las políticas, procesos y procedimientos relacionados con la gestión de los riesgos de la seguridad de la información. A través del reconocimiento de las brechas existentes, la comprensión sobre cuáles son los activos de la organización, y la evaluación de proveedores facilita la priorización de acciones de acuerdo con las misiones definidas en la función de Gobernanza (Nist, 2024).
3. **Proteger (PR):** Una vez que los riesgos y los activos han sido correctamente identificados, esta función se enfoca en utilizar medidas para mitigar los riesgos de seguridad de la información. Los resultados que se esperan son: el control de acceso y gestión de usuarios, mecanismos de autenticación, capacitación al personal, protección efectiva de los datos, plataformas aseguradas y una infraestructura tecnológica confiable y robusta (Nist, 2024).
4. **Detectar (DE):** En esta fase se detectan y se examinan ataques o situaciones que representen riesgos potenciales para la seguridad de la información. Permite identificar anomalías de manera oportuna lo que permite una respuesta rápida y efectiva. Esta función es muy importante porque brinda información necesaria para las siguientes funciones (Responder y Recuperar) (Nist, 2024)..
5. **Responder (RS):** Es la fase donde se aplica las medidas correctivas para mitigar los efectos del problema o ataque anteriormente detectado. Como se determina en la Nist (2024) aporta a la contención y gestión de los incidentes de seguridad de la información, para evitar un impacto no deseado. Los resultados esperados de esta fase son la gestión eficiente del

problema, su análisis, la disminución del daño ocasionado, así como la notificación y comunicación oportuna de los incidentes a las partes involucradas.

6. **Recuperación (RC):** La recuperación se enfoca en restablecer las operaciones del negocio, con el fin de minimizar al máximo el impacto y retomar la normalidad en el menor tiempo posible. Además, comunica a todas las partes involucradas, sobre las operaciones afectadas durante un incidente, para que se tenga conocimiento sobre el estado del sistema y las medidas adoptadas para su reutilización.

Todas las funciones trabajan de manera conjunta, es por ello por lo que la NIST CSF, las representa como una rueda, como se puede observar en el Figura 2, se destaca la función de gobernanza porque esta función es la encargada de comunicar acerca de cómo se implementarán las demás funciones. Las categorías del marco de ciberseguridad son subdivisiones de cada una de las funciones que organizan los resultados que se espera lograr, en grupos temáticos, que se relacionan con las necesidades específicas. Por su parte las subcategorías proporcionan un conjunto de resultados que contribuyen al logro de los resultados esperados de cada categoría.

Figura 2. Representación de tipo rueda de las funciones del NIST-CSF

Fuente: Nist (2024)

EL NIST-CSF es de gran utilidad porque permite identificar, protección, detectar, responder y recuperar las amenazas de privacidad y de ciberseguridad. En el contexto de la cooperativa, al ser una institución financiera que hace uso y tratamiento de datos personales y sensibles de todos los actores del negocio, es necesario adoptar un marco de seguridad claro, flexible y adaptable para gestionar los riesgos que esto conlleva. Además, es de fácil comprensión, y aporta al cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información.

Norma ISO/IEC 27001

La ISO/IEC 27001 es una norma internacional que define requerimientos para un buen Sistema de Gestión de la Seguridad de la Información (SGSI). Proporciona a empresas de todo tipo, guías para implementar, mantener y mejorar continuamente el SGSI. Esta norma engloba todos los aspectos que intervienen en un SGSI como personas, políticas y tecnología. Una política diseñada y aplicada con esta norma es apta para gestionar riegos, mantener la continuidad de negocio y la excelencia operativa (ISO, 2022).

Esta norma está destinada para que empresas de todo tipo adopten un sistema para la gestión de la seguridad de la información. Los puntos que se utilizarán para el desarrollo de la política de protección de datos personales son los siguientes:

1. **Entender la organización y su contexto (4.4.1):** Se determinan deficiencias tanto internas como externas que representan riesgos potenciales para el cumplimiento de su objetivo y de los resultados que se esperan obtener mediante la aplicación del sistema de seguridad de la información. Además, proporciona un diagnóstico sobre el contexto actual de la organización.
2. **Evaluación de riesgos de seguridad de la información (6.1.2):** Se definen los procesos para evaluar riesgos relacionados a la seguridad de la información. Esto incluye criterios de aceptación del riesgo y las reglas para evaluar los riesgos. Se aplican las reglas establecidas para identificar

riesgos que afecten a la integridad, confidencialidad y disponibilidad de la información y se determinan sus responsables. Abarca también la evaluación de las consecuencias, si se materializan los riesgos identificados. Todo lo anterior mencionada debe ser estrictamente documentado (ISO, 2022).

3. **Controles de seguridad de la información (Anexo A):** Los controles de seguridad de la información según ISO (2022) se refieren los controles de seguridad de la información que las organizaciones deben adoptar para la correcta protección de la información, de los cuales se toman en cuenta los siguientes:

    - Controles organizacionales.
    - Controles relacionados con las personas.
    - Controles físicos.
    - Controles tecnológicos.
    - Controles de acceso.
    - Controles de adquisición, desarrollo y mantenimiento.

4. **Liderazgo (5.1; 5.2; 5.3):** La alta gerencia debe demostrar respaldo total para implementación del SGSI. Esto se logra si la política de seguridad de la información coincide con: los objetivos estratégicos de la organización, con la disponibilidad de los recursos necesarios, con la comunicación acerca de la importancia del manejo eficaz y cumplimiento de los requisitos del SGSI (5.1 liderazgo y compromiso).

   La alta gerencia establece políticas que se adecuen a los propósitos de la empresa, por lo que se debe incluir a los objetivos de seguridad de la información, el compromiso de mejora continua. Esta política debe estar disponible, ser comunicada en todas las áreas de la organización, y disponible para todos los actores del negocio (5.2 Política).

   La alta gerencia establece responsabilidad y sus respetivas autoridades de los roles, y estas deben ser debidamente informadas a toda la empresa (5.3 Funciones, Responsabilidades y Autoridades de la Organización) (ISO, 2022).

5. **Soporte (7.1; 7.3; 7.4; 7.5):** En el caso de soporte la ISO (2022) menciona que la empresa debe proporcionar los recursos que sean necesarios para establecer, implementar, mantener y mejorar continuamente el SGSI (7.1 Recursos).

   Todos los involucrados con el negocio, directa o indirectamente, deben estar de acuerdo con la política de seguridad de la información, con la contribución para la mejora del desempeño y la eficacia del SGSI (7.3 Conciencia).

   La organización debe establecer qué información es esencial compartir tanto de manera interna como externa, en la información que se compartirá se debe incluir aspectos como: qué se debe informar, a quién, cuándo se debe informar y cómo o por cuales medios se realizará (7.4 Comunicación).

   El SGSI de contener: información documentada sobre los requisitos obligatorios de la norma (ISO 27001) y la que la empresa requiera. Al momento de la creación y actualización de la información documentada se debe garantizar que se determine autor(es), título, fecha, formato y deber ser aprobada mediante una revisión de suficiencia y adaptación para su aprobación. La información documentada que sea necesaria para el SGSI debe asegurarse que esté disponible, protegido contra casos de perdida, mal uso, o pérdida de integridad.

   Además de que se debe garantizar su distribución, acceso, recuperación, uso almacenamiento, controles de versión, retención y disposición (Información Documentada 7.5 y adyacentes) (ISO, 2022).

Metodología de desarrollo de la política de protección de datos personales

La razón por la que se complementa a NIST-CSF con la norma ISO/IEC 27001 es porque establece los requisitos para la correcta implementación de un SGSI seguro y sostenible. Lo que permite que la institución financiera estructure políticas, procesos y controles necesarios para la mitigación de riesgos relacionados a la vulneración de información crítica como son los datos personales de socios y empleados. Esta norma fomenta una cultura organizacional de mejora continua lo que mantiene a las empresas aseguradas frente a amenazas y cambios

tecnológicos constantes, y garantiza, por su enfoque íntegro, la seguridad de la información, continuidad operativa y el cumplimiento con los marcos regulatorios vigentes.

Ambas metodologías serán combinadas y adaptadas a las necesidades de la cooperativa, lo que permitirá diseñar una política realista, aplicable y alineada con los requisitos establecidos en la Ley Orgánica de Protección de Datos Personales (LOPDP) vigente en Ecuador. Este enfoque metodológico integrador garantiza que la política propuesta responda tanto a las exigencias de las normativas como a las necesidades operativas de la organización. La presente metodología integra tres normas fundamentales para obtener como resultado una política sólida y enfocada en las buenas prácticas internacionales que garantice una buena gestión de la seguridad de la información.

1. **Diagnóstico organizacional.**

   En base a la cláusula 4.1.1. Con el entendimiento organizacional y su contexto de la norma ISO/IEC 27001 junto con la función Identificar de la NIST-CSF, se espera obtener información acerca del contexto organizacional actual tanto de la parte interna como de la externa de la cooperativa. Esta etapa realiza una evaluación minuciosa sobre qué personal tanto interno como externo interactúa directa o indirectamente con los activos de información de la cooperativa, los riesgos derivados del tratamiento de los datos personales y la seguridad de la información, procesos críticos, tecnologías utilizadas y sobre todo qué riesgos pueden afectar a la integridad, disponibilidad y confidencialidad de la información. Como resultado se espera una base sólida sobre la cual diseñar una política de protección de datos personales, que va desde la evaluación del entorno institucional, tecnológico y normativo.

2. **Identificación de riesgos**

   El uso de las funciones Identificar y Controlar de la NIST-CSF, combinado con la cláusula 6.1.2 de la norma ISO/IEC 27001 que evalúa los riesgos de seguridad de la información se espera identificar y analizar qué datos se tratan, su sensibilidad, personal involucrado y las medidas necesarias que

garanticen su uso adecuado, además asegura la asignación de los propietarios de los riesgos.

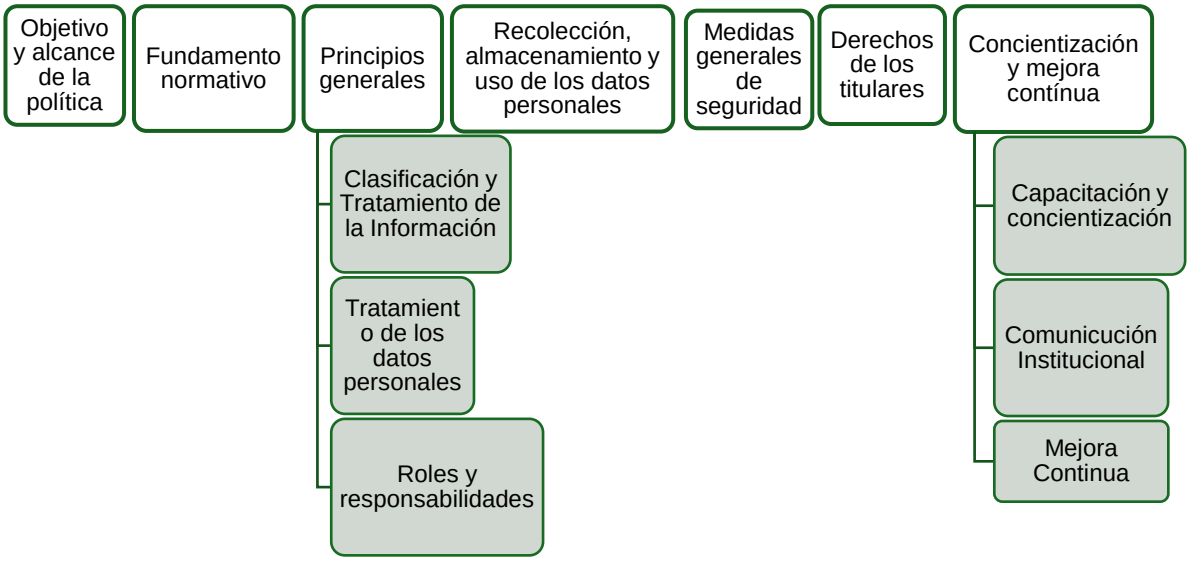
3. **Diseño de políticas**

   En esta fase se elabora la política y los procedimientos que permitirán reducir los riesgos que se identificaron en la fase anterior. Se toma en cuenta la función Proteger de la NIST-CSF, y los controles de seguridad de la información de la norma ISO/IEC 27001. En conjunto, estas dos normas abarcan áreas como la protección de identidad, controles físicos, controles de acceso, seguridad del personal y de las tecnologías, la gestión de archivos, criptografía y la protección de la información almacenada de manera física y digital.

   Política de protección de datos personales

   Para elaborar el diseño de la política interna, se consideraron aspectos claves como la Ley Orgánica vigente y el contexto actual de la cooperativa en relación al tratamiento de los datos personales. La entrevista realizada anteriormente sirvió para conocer qué datos son los que se recolectan, se hacen uso y se almacenan con el fin de determinar una estructura que evidencie el ciclo de vida de los datos personales, desde su recolección hasta su eliminación. A continuación, se presenta la estructura de la política interna de protección de datos personales en el Figura 3.

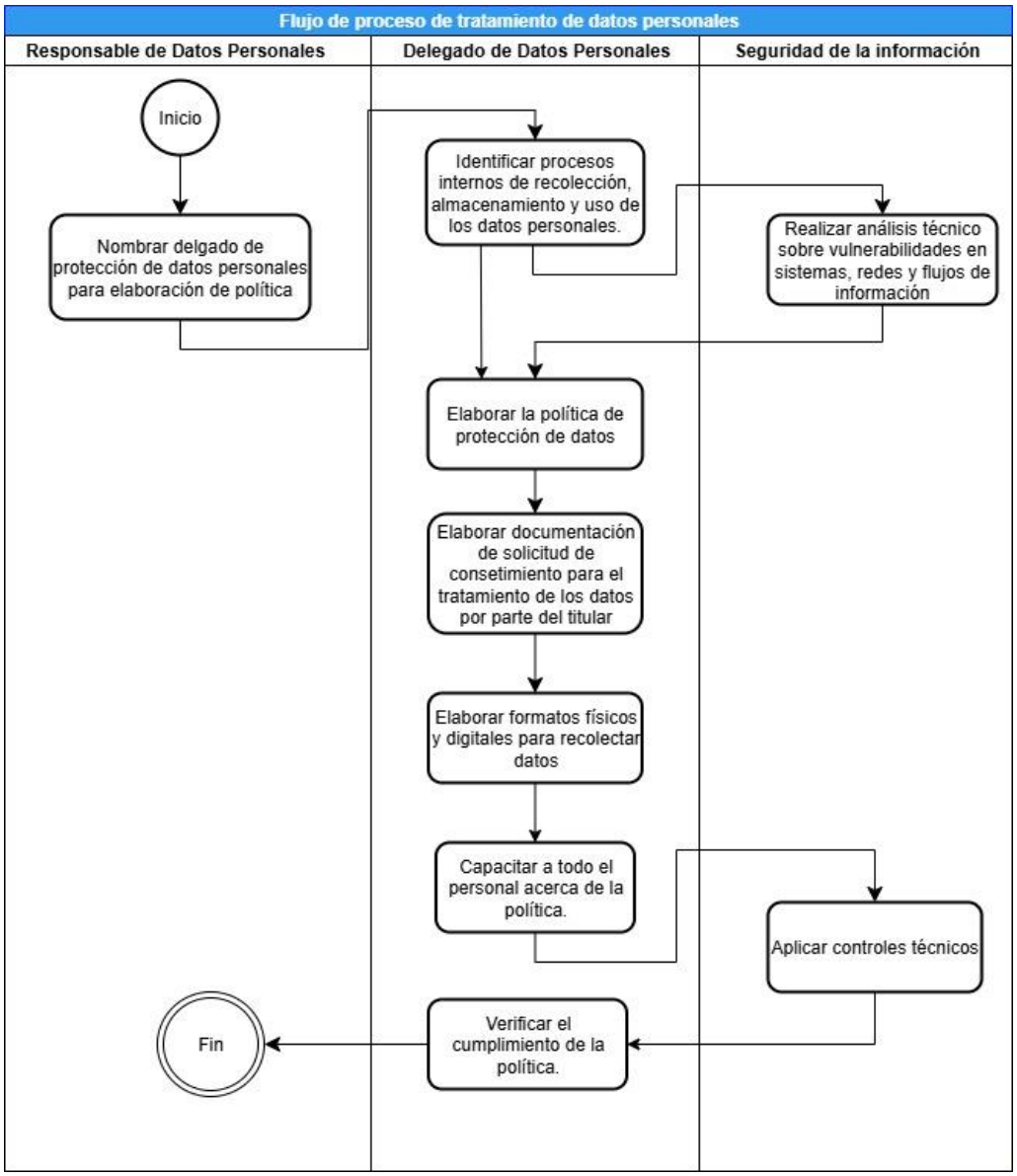
Figura 3. Estructura de la política interna de Protección de Datos Personales.



Fuente: elaboración propia.

El proceso que se propone para el diseño de la presente política de protección de datos personales en la cooperativa se presenta en la Figura 4, la cual detalla de manera sistematizada la gestión de los datos personales. El propósito de este flujo de procesos es el cumplimiento de las normativas vigentes junto con los marcos internacionales, en la figura 4 se identifican de manera clara los actores involucrados con sus respectivos procesos.

Figura 4. Flujo del proceso de tratamiento de datos personales



Fuente: elaboración propia

4. Monitoreo y mejora

Esta etapa se enfoca en la mejora continua de las medidas empleada para mitigar y contener los riesgos para la seguridad de la información. Con el uso de las funciones Detectar y Responder en conjunto con la cláusula de Soporte permiten la detección oportuna de los riesgos y la activación de las medidas de contención, análisis y comunicación. Además, garantizan que los recursos de la cooperativa estén disponibles, la concientización del personal, comunicación inter y externa, y un estricto control sobre la información documentada.

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

En este capítulo se describe a detalle sobre los hallazgos obtenidos durante el proceso de investigación, sobre el tratamiento de los datos personales dentro de la institución financiera. El cual se realiza según la metodología propuesta para el desarrollo de la política de protección de datos personales, propuesta en el capítulo anterior.

3.1. Diagnóstico organizacional

Caracterización de la empresa o institución

Historia

La Cooperativa de Ahorro y Crédito “Indígenas Galápagos” Ltda., (COACIG) (2016) “es una Institución Financiera creada por un grupo de visionarios migrantes Salasacas, aprobada mediante Acuerdo Ministerial N.- 0003 el 19 de septiembre del 2007, con una participación de 12 socios fundadores, inician su actividad el 22 de abril del 2008”. Su Matriz está ubicada en el barrio la Unión del Cantón Santa Cruz, Provincia de Galápagos, con Ruc No. 2091756679001.

La “COACIG” inició sus actividades con el fin de apoyar e impulsar la creatividad y el ingenio de gente que se propone desarrollar proyectos, trabajar, mejorar sus ingresos económicos, otorgando créditos de corto y largo plazo.

La institución financiera posee su Matriz en Galápagos Santa Cruz (Galápagos) y sus oficinas en Salasaca, San Cristóbal (Galápagos), Pelileo, Ambato, Quero, Riobamba y Salcedo.

La prioridad de la Cooperativa de Ahorro y Crédito Indígenas Galápagos Ltda., es apoyar activamente al desarrollo socioeconómico del sector indígena, rural y urbano, mediante la prestación de servicios y productos financieros de vanguardia, íntegros y sobre todo de calidad, dentro de los principios y valores corporativos que

orientan a la COAC - IG a un desarrollo integral, equitativo y constante en aspectos como el recurso humano y modelo administrativo eficiente.

Desde sus inicios la Cooperativa “INDIGENAS GALAPAGOS” Ltda., se ha caracterizándose como “una institución de prestigio por la confianza y credibilidad que brinda a sus socios, además en ofrecer apoyo mediante créditos en las áreas de microcrédito”. La cooperativa tiene dos enfoques que se mantienen desde el día su apertura: una es la de priorizar el desarrollo económico social, y la segunda es promover el crecimiento del sector de la economía popular y solidaria.

El entorno cultural en la década de los 70, debido a la crisis económica, la baja producción agrícola, la baja rentabilidad en la venta de artesanías y la coyuntura social, influenciaron a que miembros del pueblo kichwa Salasaca migren hacia las islas Galápagos, con un objetivo en mente, la de emplear su mano de obra en las construcciones de colonias, gracias al esfuerzo y sacrificio empleado por el Salasaca y Residentes de la isla se evidenció un desarrollo progresivo en varios sectores socioeconómicos.

Las Islas Encantadas, considerada internacionalmente como una de las islas más hermosas y maravillosas, por su ecosistema único y sorprendente, promulgándose como una de las joyas importantes en el ámbito científico y turístico; en las Islas existen numerosas etnias y culturas que coexisten en paz, respeto y armonía de los cuales se puede identificar un 40% mestizos, 40% indígenas, 15% blancos y un 5% de negros; dentro de la etnia indígena son Salasacas, Otavaleños, los Saraguros, entre otros., quienes participan activamente en el progreso de la región insular y el país.

Los principales objetivos de la cooperativa son:

1. Brindar servicios financieros a los sectores no atendidos por la banca tradicional.
2. Contribuir al mejoramiento socio económico de los socios de la Cooperativa.

3. Fortalecer y mantener los servicios financieros acorde a las necesidades de los sectores atendidos.
4. Generar satisfacción y compromiso de los socios.

Misión

Ofrecemos servicios financieros sostenibles que promueven el desarrollo económico y social.

Visión

Brindar servicios financieros de alta eficiencia con una perspectiva internacional.

Valores Corporativos

Para el cumplimiento de la Misión y el logro de la Visión la Cooperativa de Ahorro y Crédito Indígenas Galápagos (2016) estableció guías de conducta de todos quienes conforman la institución, mismos que se describen la Tabla 5:

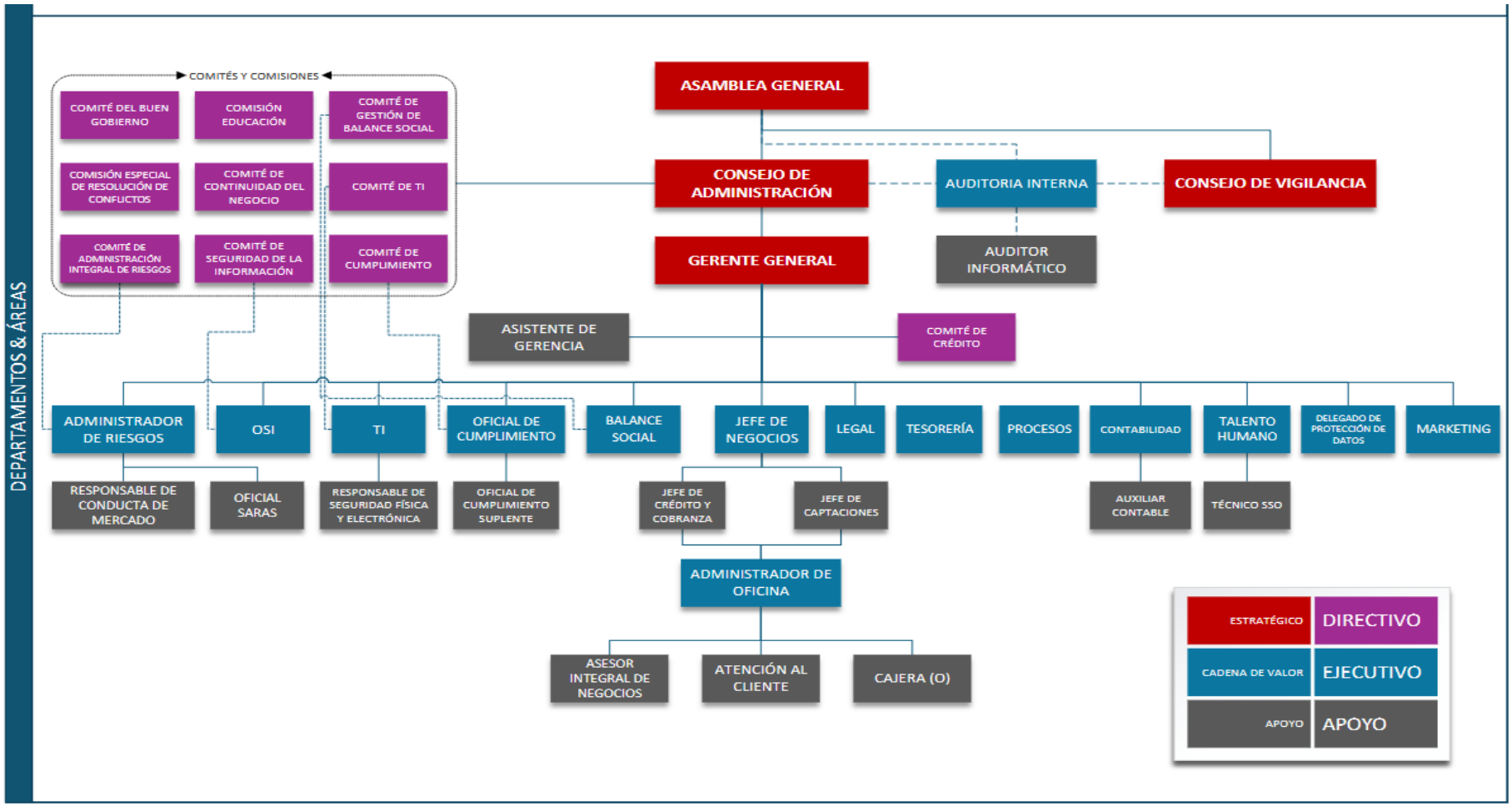
Tabla 5. Valores de la institución financiera.

Valores	Características
Transparencia	La institución proporciona a sus socios, autoridades de control y público en general toda la información concerniente a la Cooperativa y sus procesos internos.
Compromiso social	Promovemos valores cristianos, el progreso y desarrollo de la gente
Responsabilidad	El personal de la Institución cumple con todas las funciones y tareas asignadas de manera eficiente y oportuna.
Excelencia	El personal de la Cooperativa se caracteriza por los más altos estándares de calidad y puntualidad en el cumplimento de sus funciones y responsabilidades.
Satisfacción	La Cooperativa busca proveer a sus socios y clientes productos y servicios que satisfagan sus necesidades de una manera ágil, oportuna y con los más altos estándares de servicio al cliente.
Innovación	Los productos de la Cooperativa serán innovativos tanto en sus características como en la forma de proveerlos y se tiene en cuenta en todo momento las necesidades puntuales de los socios y clientes.
Calidad	La Cooperativa reconoce a la calidad como uno de los factores diferenciadores en el mercado, por lo que todos sus productos y servicios deberán ser desarrollados y proporcionados a sus socios y clientes con una calidad superior.

Fuente: Cooperativa de Ahorro y Crédito Indígenas Galápagos

Organigrama estructural

Figura 4. Organigrama Estructural de la Coop. Indígenas Galápagos



Fuente: Cooperativa de Ahorro y Crédito Indígenas Galápagos.

Una vez realizada la entrevista al encargado del departo de sistemas de la entidad financiera, se logra identificar aspectos importantes sobre el tratamiento de los datos personales de las cuales se destaca que:

1. La institución financiera en el contexto actual No cuenta con una política definida para la protección de los datos personales, por lo que incumple con las normativas vigentes.
2. Para evitar sanciones por parte de la SEPS, ente regulador de la protección de datos personales en las instituciones financieras del sector financiero popular y solidario, se designó a un empleado como responsable del tratamiento de los datos personales, el cual posee un conocimiento poco profundizado acerca de la ley vigente.
3. La cooperativa hace uso de sistemas terceros como Pago Ágil y Red Facilito para el cobro de servicios básicos que, posiblemente, no cuentan con políticas para la protección de datos.
4. La información que recolectada de los socios es muy extensa y en algunas ocasiones para cierta información, no se cuenta con el consentimiento de los afectados. Para el otorgamiento de préstamos el personal recolecta datos personales y sensibles, proceso cual según el entrevistado si se lo realiza con el consentimiento informado del titular, pero al mismo tiempo los asesores indagan sobre la vida privada de los solicitantes de crédito con el fin de elaborar perfiles que sean aptos para el otorgamiento del préstamo. (La información personal y financiera recolectada por parte de la cooperativa son muy extensas, y pocas veces informadas.)
5. Para la seguridad de la información, la cooperativa hace uso de medidas tecnológicas avanzadas como un firewall, segmentación de redes mediante VLANS servicio que está incluido en los servicios de Fortinet.
6. Como parte de la recolección de información se destaca que la cooperativa cuenta con limitaciones institucionales en cuanto a la falta de personal especializado, presupuesto restringidos y plazos de aplicación de políticas vencidos frente a la SEPS.

3.2. Identificación de riesgos

El proceso de identificación permitió el análisis de los datos recopilados por la cooperativa, su nivel de sensibilidad, personal involucrado, y las medidas existentes que garanticen el uso adecuado.

1. **Tipos de datos tratados:** La cooperativa hace uso de información personal y sensible como: número de cédula, nombres, apellidos, edad, dirección, estado financiero, situación crediticia, ingresos, egresos, y detalles de la situación familiar de los solicitantes de crédito.
2. **Ausencia de políticas internas**: Actualmente, la cooperativa no cuenta con una política interna que regule el tratamiento de los datos personales, lo que supone un riesgo a la cooperativa porque incumple con las regulaciones y se expone a sunciones por parte del ente regulador conforme a lo establecido en la Ley Orgánica de Protección de Datos Personales (LOPDP).
3. **Accesos no controlados:** El personal de diversas áreas posee acceso no limitado a la información personal de los socios, tanto en formatos digitales como físicos, lo cual representa un riesgo para la confidencialidad y tratamientos indebidos de información.
4. **Segmentación de redes:** La implementación de redes VLAN permite un control de acceso restringido, lo cual contribuye a limitar el riesgo de exposición de los datos personales.
5. **Asignación de responsable:** Con el fin de evitar sanciones la cooperativa ha designado a un responsable de los datos, dicho empleado o cuenta con conocimiento especializado en materia de protección de datos personales lo cual representa un riesgo para la implementación de principios y obligaciones establecidos por la ley.
6. **Limitaciones institucionales:** Las restricciones presupuestarias, la ausencia de personal especializado materia de protección de datos personales y el vencimiento de los plazos regulatorios evidencian que el contexto normativo y operativo es riesgoso, por lo cual se debe priorizar

acciones que fortalezcan la seguridad del tratamiento de los datos personales.

3.3. Diseño de política

La propuesta de política de protección de datos para la Cooperativa de ahorro y Crédito Indígenas Galápagos (COAC-IG) se fundamenta como una herramienta primordial para garantizar el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el fortalecimiento de la seguridad de la información dentro de la institución. El diseño basado en el estándar internacional ISO/IEC 27001 y el marco de ciberseguridad NIST – CSF, los cuales permiten establecer controles técnicos y organizativos orientaos a la protección de los datos personales desde su recolección hasta su eliminación.

Mediante la definición de principios sólidos, roles definidos, medidas de seguridad competentes, la inclusión de mecanismos para el ejercicio de los derechos de los titulares y el proceso de mejora continua favorecen a que la política contribuya a la reducción de riesgos, promover la confianza de los socios y cumplir con requisitos legales, establecidos por el ente regulador. Esta propuesta de política se encuentra a detalle en el Anexo 2, el cual establece bases para un tratamiento responsable, transparente y seguro de los datos personales, alineándolo a las exigencias legales actuales en materia de protección de datos personales.

3.4. Monitoreo y mejora

Como una parte importante del cumplimiento de la política, la cooperativa establece un enfoque de monitoreo y mejora continua con el fin de que se mantenga la eficacia de las medidas implementadas para la protección de los datos personales y la seguridad de la información.

El proceso de monitoreo y mejora se sustenta de las funciones Detectar y Responder del marco NIST-CSF y Soporte de la ISO/IEC 27001, los cuales permiten la identificación temprana de riesgos, reacción oportuna ante incidentes,

y la activación de mecanismos para la mitigación del riesgo de la seguridad de la información. Estas acciones incluyen la supervisión periódica de los controles técnicos y organizativos, auditorías internas y eternas, actualización de procedimientos controles y documentos, los cuales se actualizan conforme a cambios normativos, tecnológicos o estructurales dentro de la institución, revisión periódica y ajuste de riesgos mediante nuevas evaluaciones, comunicación y concienciación constante del personal y el registro y documentación de todo cambio, incidente o mejora aplicada en la política.

Esto garantiza a que el documento de la política no sea un documento estático, sino que sea una herramienta dinámica que cambia y se adapta según el entorno para garantizar una protección continua y eficaz de los datos personales.

Resultados obtenidos

Una vez revisada la propuesta de política por parte del responsable del departamento de TI de la cooperativa (revisor 1) y el responsable del tratamiento de los datos personales (revisor 2), se presenta una rubrica de evaluación que consta de siete preguntas clave donde se evalúan aspectos como: la estructura y la organización de la política, estructura y organización de la política, actualidad, claridad del objetivo y alcance, conceptualización, pertinencia, aplicabilidad, y redacción técnica y normativa.

El puntaje obtenido por parte del revisor 1 es de 35 / 35 puntos, se recibe esa puntuación debido a que la propuesta de política tuvo varias retroalimentaciones importantes donde se identificaron factores clave que no se incluyeron en las primeras versiones de la propuesta de la política, como: confidencialidad de terceros vinculados a la cooperativa, servicios informáticos contratados por la cooperativa, formatos de solicitud de consentimiento del titular de los datos y formato de evaluación de impacto de tratamiento de datos personales. En la Figura 5, se detallan los aspectos evaluados por parte del revisor 1. Para más detalle acerca de la rúbrica de evaluación evaluada véase el Anexo 3.

Figura 5. Tabla de evaluación de la propuesta de política por parte del Revisor 1

Criterio	Descripción	5	4	3	2	1
Estructura y organización de la política.	Claridad en la presentación, formato uniforme, numeración adecuada y secciones completas.	X				
Actualidad	Evalúa si la política se encuentra actualizada conforme a la legislación y contextos tecnológicos recientes.	X				
Claridad del objetivo y alcance	Explica con precisión el propósito de la política y los actores a los que aplica.	X				
Conceptualización	Se comprende los conceptos clave de marcos legales y metodologías empleadas.	X				
Pertinencia	La propuesta de política es adecuada con las necesidades de la cooperativa	x				
Aplicabilidad	Adaptación al contexto financiero, especialmente en cooperativas pequeñas o medianas.	X				
Redacción técnica y normativa	Uso de lenguaje técnico preciso, formalidad académica y coherencia normativa.	X				

Fuente: elaboración propia

El puntaje obtenido por parte del revisor 2 es de 31 / 35 puntos, la puntuación se acompaña de recomendaciones y retroalimentaciones importantes, las recomendaciones incluyeron necesidades específicas como la familiarización con la normativa vigente por parte del personal, socios y clientes, proporcionar información clara al titular sobre la finalidad del tratamiento y el tiempo que se mantendrán los datos personales, al igual que la implementación de controles que garanticen la protección de la información personal frente a accesos no autorizados, pérdidas, o divulgaciones mal intencionadas. Todas las recomendaciones fueron atendidas y aplicadas en la versión final de la política, mismos que fortalecieron la estructura, claridad y alineación con la LOPDP. En la Figura 6, se detallan los aspectos evaluados por parte del revisor 2. Para más detalle acerca de la rúbrica de evaluación evaluada véase el Anexo 4.

Figura 6. Tabla de evaluación de propuesta de política por parte del Revisor 2

Criterio	Descripción	5	4	3	2	1
Estructura y organización de la política.	Claridad en la presentación, formato uniforme, numeración adecuada y secciones completas.		x			
Actualidad	Evalúa si la política se encuentra actualizada conforme a la legislación y contextos tecnológicos recientes.		x			
Claridad del objetivo y alcance	Explica con precisión el propósito de la política y los actores a los que aplica.	X				
Conceptualización	Se comprende los conceptos clave de marcos legales y metodologías empleadas.	X				
Pertinencia	La propuesta de política es adecuada con las necesidades de la cooperativa		x			
Aplicabilidad	Adaptación al contexto financiero, especialmente en cooperativas pequeñas o medianas.	X				
Redacción técnica y normativa	Uso de lenguaje técnico preciso, formalidad académica y coherencia normativa.		x			

Fuente. elaboración propia

CONCLUSIONES

- La fundamentación teórica actualizada y formal sobre las normativas vigentes permitió identificar principios, entes reguladores y metodologías adecuadas que sirvieron como base para el desarrollo de la política de protección de datos personales para la cooperativa. La aplicación de estándares internacionales como la ISO/IEC 27001 y el marco internacional de ciberseguridad NIST-CSF no solo garantiza el cumplimiento de la LOPDP, sino que también fortalece la protección de la información de la entidad frente a amenazas que comprometan su seguridad. Asimismo, contribuye al cumplimiento de los lineamientos establecidos por la SEPS que es el ente regulador encargado.

- Las deficiencias identificadas mediante el uso de herramientas para la recolección de la información permitieron destacar que la entidad financiera no cumplía con las normas vigentes y que por ende quedaba expuesta a sanciones frente al ente regulador. El análisis determinó que la institución financiera no cuenta con una política formal definida que regule el tratamiento de los datos personales, el responsable designado no cuenta con conocimiento profundizado en la materia de protección de datos personales, todo el personal tiene acceso a la información personal de los socios lo que incrementa el riesgo de uso indebido o la difusión malintencionada de información.

- El análisis del contexto actual de la cooperativa junto con la identificación de los riesgos asociados al tratamiento de los datos personales permitió el desarrollo del diseño de la política basado en las necesidades específicas de la entidad, por lo cual el uso de la ISO/IEC 27001 y la NIST-CSF fueron cruciales porque permitieron generar controles técnicos y organizativos que garantizan el correcto tratamiento de los datos personales dentro de la institución, además de que se estableció roles y responsabilidades para la correcta gestión de la seguridad de la información.

RECOMENDACIONES

- Para tener una cultura organizacional adecuada se recomienda que empresas, organizaciones de toda índole adopten o implementen políticas, procedimientos, protocolos y manuales para un funcionamiento adecuado de todas las partes del negocio. Las políticas pueden ayudar a tener un mejor control sobre información manejada, así como la designación de responsables que velen por el cumplimiento de estas.

- Mantener una constante capacitación tanto en directivos como en empleados es crucial para que todos los involucrados en el manejo de información sensible de la organización tengan conocimiento acerca de las normativas y procesos que se deben utilizar en caso de un uso indebido de la información. Además, garantiza la concientización sobre cómo esto puede afectar la institución, así como a los titulares de los datos.

- El uso de normativas y marcos internacionales orientados a la seguridad y protección de la información contribuyen con un enfoque más detallado acerca de las necesidades de la empresa, por lo que se recomienda el uso de las funcionalidades o cláusulas que mejor se adapten al contexto actual. No toda empresa tiene necesidad de adaptar o usar todos los puntos de un marco normativo o un estándar internacional, aunque es recomendable. El enfoque de mejora continua de la norma ISO/IEC 27001 y las fases de la NIST-CSF permiten que la política se mantenga actualizada junto con los resultados de análisis de auditorías, mismas que permiten identificar nuevas deficiencias en cuanto a la seguridad de la información, por lo tanto, el proceso de tratamiento de datos personales se repite según cuanto sea necesario.

BIBLIOGRAFÍA

Abdo León, L. B. (2024). *RESPONSABILIDAD BANCARIA: MANEJO DE DATOS PERSONALES Y LA VIOLACIÓN A LA PRIVACIDAD DEL DEUDOR* (Universidad del Azuay). Universidad del Azuay, Cuenca – Ecuador. Recuperado de https://dspace.uazuay.edu.ec/bitstream/datos/15417/1/20933.pdf

Arcos Argudo, M., Matute Pinos, K., & Fernández Mora, M. (2023). Análisis comparativo de la Ley Orgánica de Protección de Datos Personales del Ecuador con la legislación colombiana desde un enfoque de ciberseguridad y delitos informáticos. *RISTI - Revista Ibérica de Sistemas e Tecnologías de Informação*, 100-114.

Arellano Veloz, C. E. (2023). *Seguridad de la información*. Recuperado de https://repositorio.puce.edu.ec/server/api/core/bitstreams/75d06c01-781e-49b7-aba0-b87b258deea8/content

Barahona Martínez, G. E., Barzola Plúas, Y. G., & Peñafiel Muñoz, L. V. (2024). El Derecho a la Protección de Datos y el Avance de las Nuevas Tecnologías en Ecuador: Implicaciones Legales y Éticas. *Journal of Economic and Social Science Research*, *4*(3), 46-64. https://doi.org/10.55813/gaea/jessr/v4/n3/113

Bertoni, E. A. (Ed.). (2012). *Hacia una Internet libre de censura: Propuestas para América Latina*. Buenos Aires: Universidad de Palermo, Facultad de Derecho, Centro de Estudios en Libertad de Expresión y Acceso a la Información.

Burzaco Samper, M. (2020). *Protección de datos personales: Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección del personal 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 producción de datos); Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos personales y garantía de los derechos digitales*. Madrid: Dykinson.

Cazurro Barahona, V. (2020). *Antecedentes y fundamentos del derecho a la protección de datos* (1.ª ed.). J.M Bosch. https://doi.org/10.2307/j.ctv14t46sm

Conde Ortíz, C. (2005). *La Protección de Datos Personales Conde Ortiz, Concepción*. Dykinson. Recuperado de http://www.dykinson.com/libros/la-proteccion-de-datos-personales/9788497725972/

Cueto Urbina, E. (2020). Investigación cualitativa. *Applied Sciences in Dentistry*, *1*(3). Recuperado de https://rhv.uv.cl/index.php/asid/article/download/2574/2500

Diario Oficial de la Unión Europea. (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)*.

Echeverria, D. A. M., Alarcón, F. P. M., Altamirano, E. E. C., & Usca, F. J. I. (2024). La protección de datos personales en Ecuador: Evolución legislativa y comparación con modelos regionales en Sudamérica. *Perspectivas Sociales y Administrativas*, *2*(2), 35-44. https://doi.org/10.61347/psa.v2i2.70

Encalada Aguilar, D. M. (2024). *Propuesta de Política interna alineada a la Ley de Protección de Datos Personales mediante estándar NIST para Cooperativas de Ahorro y Crédito.*

Ferreira Aguilera, V. M. (2021). Iniciativas para la institucionalización de la protección de datos personales en Paraguay. *REVISTA CIENTÍFICA UNE*, *4*(1), 1-13. Recuperado de http://revistas.une.edu.py/index.php/revista_une/article/view/101

Gadea Soler, E. (2020). Análisis de riesgos y evaluación de impacto relativa a la protección de datos: Su aplicación a las sociedades cooperativas. *Boletín de la Asociación Internacional de Derecho Cooperativo*, (56), 47-72. https://doi.org/10.18543/baidc-56-2020pp47-72

García González, A. (2007). La protección de datos personales: Derecho fundamental del siglo XXI. Un estudio comparado. *Boletín Mexicano de Derecho Comparado*. https://doi.org/10.22201/iij.24484873e.2007.120.3933

Gaytán, D. A. G. (2023). DIRECTORIO INSTITUCIONAL RECTOR: DR. SANTOS GUZMÁN LÓPEZ SECRETARIO GENERAL: DR. JUAN PAURA GARCIA DIRECTOR DE LA FACULTAD DE DERECHO Y CRIMINOLOGIA: MTRO. OSCAR P. LUGO SERRATO. . . *PP.*, *03*.

Guzmán, C., Palacios, D., & Palacios, E. (2023). Incidencias de los ciberdelitos y sus regulaciones en la ciudad de Panamá. *Revista Semilla Científica*, (4), 524-539. https://doi.org/10.37594/sc.v1i4.1296

Hernández Alvarado, V. J., Pinguel Llanos, O. F. P., & Coello Avilés, E. M. (2023). Ley Orgánica de Protección de Datos en Ecuador: Requerimiento de un reglamento ausente. *Dilemas contemporáneos: Educación, Política y Valores*. https://doi.org/10.46377/dilemas.v11iEspecial.3988

Hernández Carrera, R. M. (2014). La investigación cualitativa a través de entrevistas: Su análisis mediante la teoría fundamentada. *Cuestiones Pedagógicas. Revista de Ciencias de la Educación*, (23), 187-210. Recuperado de https://revistascientificas.us.es/index.php/Cuestiones-Pedagogicas/article/view/9815

Hernández Cruz, A. (2022). Derecho a la protección de datos personales. *Estudios en derecho a la información*, (13), 157-160. Recuperado de https://www.scielo.org.mx/scielo.php?pid=S2594-00822022000100157&script=sci_arttext

Hernández, J. C. (2012). La protección de datos personales en internet y el hábeas data. *Revista derecho y tecnología*, *13*, 61-85. Recuperado de https://www.corteidh.or.cr/tablas/r32012.pdf

ISO. (2022). ISO/IEC 27001:2022. Recuperado 19 de junio de 2025, de https://www.iso.org/standard/27001

Juri, Y. E. (2019). *Personal data protection. Special reference to the reform project of the argentine law Nº 25,326*.

Lima Cervantes, E. J. (2021). Preguntas y respuestas varias sobre la protección de datos personales en el Perú. *Advocatus*, (039), 253-264. https://doi.org/10.26439/advocatus2021.n39.5133

Limones Zambrano, J. M., & Peralta Peralta, J. A. (2023). *Análisis comparativo de la ley orgánica de protección de datos personales del Ecuador con la legislación uruguaya desde un enfoque de ciberseguridad y delitos informáticos* (Master's Thesis). Recuperado de https://dspace.ups.edu.ec/handle/123456789/25184

Maqueo Ramírez, M. S., Moreno Gonzales, J., & Recio Gayo, M. (2017). *Data Protection, Privacy and Private Life: The Challenging Search of a Needed Global Balance*. Recuperado de https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-09502017000100004&lng=en&nrm=iso&tlng=en

Martínez Pérez, O., Freire Gaibor, E. F., & Alzate Peralta, L. A. (2024). Desafíos del habeas data en la protección de datos personales en el ordenamiento jurídico ecuatoriano. *European Public & Social Innovation Review*, *9*, 1-21. https://doi.org/10.31637/epsir-2024-1842

Milanes, V. (2017). *DESAFÍOS EN EL DEBATE DE LA PROTECCIÓN DE DATOS PARA LATINOAMÉRICA*. Recuperado de https://www.consejotransparencia.cl/wp-content/uploads/2018/04/librocompleto__4.pdf#page=15

Moreno Pérez, I. J. (2022). *RETOS DE LOS DERECHOS A LA PRIVACIDAD Y A LA PROTECCIÓN DE DATOS PERSONALES EN MÉXICO*.

Nieves Lahaba, Y. R., & Ponjuan Dante, G. (2021). *Tratamiento de datos personales y acceso a la información. Visiones a partir de la academia*. Recuperado de http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-86342021000200167

Niño García, D. Y. (2022). Los datos personales y sus riesgos jurídicos a partir de la transformación digital en el comercio electrónico. *Revista CES Derecho*, *13*(1), 70-89. https://doi.org/10.21615/cesder.6386

Nist, G. M. (2024). *Spanish Translation of the NIST Cybersecurity Framework 2.0* (N.º NIST CSWP 29 spa; p. NIST CSWP 29 spa). Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29.spa

Noguera Osorio, M. (2020). *NUEVO MARCO REGULATORIO DE LA PROTECCIÓN DE DATOS PERSONALES Y PROTECCIÓN DE LA VIDA PRIVADA EN CHILE.* Recuperado de https://repositorio.uft.cl/server/api/core/bitstreams/784422bf-0d33-4429-bfc8-688cd6f7e180/content

Novillo Arévalo, W. V., & Jordán Naranjo, G. V. (2023). *La protección de datos personales y el otorgamiento de copias y compulsas ante el notario* (masterThesis). Recuperado de https://dspace.uniandes.edu.ec/handle/123456789/16622

Ojeda-Contreras, F. I., Moreno-Narváez, V. P., & Torres-Palacios, M. M. (2020). Gestión del riesgo y la ciberseguridad en el sector financiero popular y solidario del Ecuador. *CIENCIAMATRIA*, *6*(2), 192-219. https://doi.org/10.35381/cm.v6i2.366

Ordóñez Pineda, L., Correa Quezada, L., & Correa Conde, A. (2022). Políticas públicas y protección de datos personales en Ecuador: Reflexiones desde la emergencia sanitaria. *Estado & amp; comunes, revista de políticas y problemas públicos*, *2*(15), 77-97. https://doi.org/10.37228/estado_comunes.v2.n15.2022.270

Pacheco Bancayan, R. J. (2019). *EL TRATAMIENTO DE LOS DATOS PERSONALES DENTRO DE LAS EMPRESAS VINCULADAS AL SISTEMA FINANCIERO PERUANO*. Recuperado de https://tesis.usat.edu.pe/bitstream/20.500.12423/2332/1/TL_PachecoBancayanRonaldo.pdf

Pérez Martínez, M. R. (2020). Protección de datos personales y derecho a la autodeterminación informativa: Régimen jurídico. *Revista de Derecho*, (28), 107-138. https://doi.org/10.5377/derecho.v0i28.10146

Peyramo, G. (2020). *Datos sensibles: Perfiles y regulaciones. El impacto del desarrollo tecnológico. Dossier: Habeas Data, 511.*

Pfeiffer, M. L. (2008). *Derecho a la privacidad. Protección de los datos sensibles*. *3*.

Pimboza Ninacuri, H. D. P. (2025). *La protección de datos sensibles vs la protección de datos personales* (B.S. thesis). Recuperado de https://dspace.uniandes.edu.ec/handle/123456789/18973

Piñar Mañas, J. L. (2005). El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro. *Asamblea. Revista parlamentaria de la Asamblea de Madrid*, (13), 21-46. https://doi.org/10.59991/rvam/2005/n.13/604

Porcelli, A. M. (2020). La Protección de los Datos Personales en el Entorno Digital. Los Estándares de Protección de Datos en los Países Iberoamericanos. *REVISTA QUAESTIO IURIS*, *12*(2), 465-497. https://doi.org/10.12957/rqi.2019.40175

R32012.pdf. (s. f.). Recuperado de https://www.corteidh.or.cr/tablas/r32012.pdf Registro Oficial. (2021). *1162059_-_LEY_ORGÁNICA_DE_PROTECCIÓN_DE_DATOS_PERS_20210701124 8165227*. Recuperado de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf

Reyes Ruiz, L., & Carmona Alvarado, F. A. (2020). *La investigación documental para la comprensión ontológica del objeto de estudio*. Recuperado de https://bonga.unisimon.edu.co/items/cbb661ef-30e3-4263-b7b2-810e88237f5f

Rivera Barrantes, V. (2019). Realidad sobre la Privacidad de los Datos Personales en Costa Rica. *E-Ciencias de la Información*, *9*(2), 68-81. https://doi.org/10.15517/eci.v9i2.37503

Rojas Bejarano, M. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. *Novum Jus*, *8*(1), 107-139. https://doi.org/10.14718/NovumJus.2014.8.1.6

Rovira Jurado, Z. E., Robles Riera, L. E., & Castillo Méndez, J. A. (2023). Protección de datos en el contexto de la promulgación de la Ley Orgánica de Protección de Datos Personales en Ecuador. *Polo del Conocimiento*, *8*(8), 1355-1373. https://doi.org/10.23857/pc.v8i8.5908

Sandoval Casilimas, C. (1996). *Estudio de localidades*. Santafé de Bogotá: Icfes.

SEPS. (2024). *Normativa Sanciones*. Recuperado de https://www.seps.gob.ec/wp-content/uploads/2.-Capacitacio%CC%81n-normativa-de-sanciones-con-NOTAS.PPTX-modificado-final.pptx-15.pdf

Solove, D. J. (2013, mayo 20). Introduction: Privacy Self-Management and the Consent Dilemma. Recuperado 27 de mayo de 2025, de Harvard Law Review website: https://harvardlawreview.org/print/vol-126/introduction-privacy-self-management-and-the-consent-dilemma/

Torres Salcedo, G. del C. (2019). PLAN INFORMÁTICO 2019–2023, BASADO EN LA NORMA ISO/IEC 27001:2013 PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN, INFRAESTRUCTURA Y RECURSOS TECNOLÓGICOS EN EL CENTRO DE PROCESAMIENTO DE DATOS EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN QUININDÉ (GADMCQ), EN LA CIUDAD DE QUININDÉ. *UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES UNIANDES*. Recuperado de https://dspace.uniandes.edu.ec/xmlui/bitstream/handle/123456789/10924/PIUSDSIS008-2020.pdf?sequence=1&isAllowed=y#page=132

UNAM. (2016). Técnicas de Investigación de Campo. Recuperado 12 de junio de 2025, de https://repositorio-uapa.cuaed.unam.mx/repositorio/moodle/pluginfile.php/2796/mod_resource/content/1/UAPA-Tecnicas-Investigacion-Campo/recursos/opcion_multiple/index.html

Unión Europea. (2021). *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 ya la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE).* L 119/36. Recuperado de https://travesia.mcu.es/server/api/core/bitstreams/d5f3ef20-3dcc-4065-961a-f77ea31d6d55/content

ANEXOS

ANEXO 1. Instrumento de entrevista para identificar elementos clave en el diseño de una política de protección de datos personales

Pontificia Universidad Católica del Ecuador | Sede Ambato

Pontificia Universidad Católica del Ecuador Sede Ambato
Carrera de Ingeniería en Sistemas de Información
Instrumento de Entrevista para Identificar Elementos Clave en el Diseño de una Política de Protección de Datos Personales

Datos Generales del entrevistado:

Nombres: Autachi Shiri Masaquiza

Cargo: Responsable del área de TI

Área: TI

Fecha: 23/06/2025

Pregunta 1

- **¿Que conoce acerca de la ley de protección de datos?**

  Lo que el entrevistado conoce acerca de la Ley Orgánica de Protección de Datos Personales, es de que es una política reciente y que todas las empresas de todos los sectores están obligaos a implementarla para asegurar la protección de datos. Además, argumentó que casi ninguna cooperativa cumple con lo descrito en la ley.

Pregunta 2

- **¿La cooperativa cuenta con una política o protocolos internos que regulen el tratamiento de los datos personales?**

  Respondiendo a la pregunta el entrevistado aseguró que la cooperativa no cuenta con una política o protocolos definidos para el aseguramiento de los datos personales, y destacó la necesidad de la cooperativa el contar con procesos o políticas que aseguren la protección de los datos personales conforme con la ley.

Pregunta 3

- **¿Qué departamentos o áreas están implicadas en el manejo de datos personales?**

  En la cooperativa todas las áreas están involucradas en el tratamiento de lo/s datos personales. Destacó que se necesitan los datos de una persona para abrir una cuenta, otorgar préstamos, para una póliza, además de que utilizan sistemas externos que utilizan como Pago Ágil para el cobro de servicio básico como luz, internet, teléfono.

  En los pagos de Pago Agil y Red Facilito el entrevistado aseguró que al momento de realizar un pago no se genera un documento que conste que los servicios externos cuentan con políticas de protección de datos personales.

- **¿Existe un responsable designado que vele por el cumplimiento de la Ley Orgánica de Protección de Datos Personales?**

  Para cumplir parcialmente con la Ley Orgánica de Protección de Datos Personales, la gerencia designo a un responsable. Pero el responsable designado tiene conocimiento general acerca de la Ley, por lo cual la cooperativa no ha sido capaz de realizar una política o procedimientos adecuados como lo mencionado en la pregunta No. 2

Pregunta 4

- **¿Qué tipos de datos personales recolecta la cooperativa (de socios, clientes, empleados)? ¿Qué métodos utilizan para la recolección? (Ejemplo: nombres, cédula, direcciones, estados financieros, etc.)**

  Para la recolección de los datos el entrevistado mencionó que se obtiene por medio de una encuesta y se los ingresa directamente en el Core Financiero (Sistema central de la cooperativa) para su almacenamiento. Los datos que se recolectan son, principalmente la cédula como identificador único, nombres, apellidos, edad, dirección, estado financiero, situación crediticia, ingresos, egresos.

  Para el otorgamiento de un préstamo, en la información de los estados financieros de los socios también se indaga si la persona tiene alguna otra deuda en otra institución financiera, para ello se utiliza el sistema de Equifax para determinar si la persona es apta para el otorgamiento de un crédito. También menciono que los asesores de crédito pueden preguntar por la persona a vecinos cercanos para determinar la situación familiar del solicitante del préstamo como medida adicional que sirve como un filtro.

- **¿Cómo es el proceso de recopilación actualmente? ¿Se obtiene consentimiento explícito del titular?**

Pregunta 5

- **¿En qué formato se almacenan los datos personales: ¿físico, digital o ambos? ¿Qué sistemas o herramientas usan?**

  Se utilizan ambos formatos, tanto físico como en digital. De manera física lo guardan en una carpeta en un archivo, y el almacenamiento digital se lo realiza en un sistema denominado SoftBank que alemana la información en la base de datos. Los datos almacenados en dicho sistema se respaldan todos los días.

Pregunta 7

Pontificia Universidad Católica del Ecuador | Sede Ambato

tema la cooperativa ya venció el plazo y es por ello que se definió al responsable para no recibir sanción alguna.

Pregunta 12

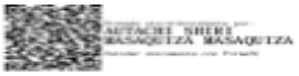
- **¿Cómo espera que la aplicación de una política de protección de datos beneficie a la cooperativa?**

  Con la regulación de la SEPS, la cooperativa está obligada a contar con una política para la protección de los datos personales, beneficiaría a la cooperativa de manera significativa puesto que se cumpliría con la ley y se evitarían multas o sanciones que pueden llegar a ser un tanto costosas.

Pregunta 13

- **¿Alguna información importante que se debe considerar en el diseño de la política?**

  Destacó que se debe tener en cuenta que en la cooperativa existen recursos limitados, hablando del área de finanzas, además de la infraestructura de red. En la infraestructura de la red destacó que se usa la red punto a punto que hace una red más segura, para evitar el robo de información.



Firma

Autachi Shiri Masaquiza

ANEXO 2. PROPUESTA DE POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES PARA UNA INSTITUCIÓN DEL SEGMENTO 3

(Ver documento adjunto)

COOPERATIVA DE AHORRO Y CRÉDITO

INDÍGENAS GALÁPAGOS

POLÍTICA INTERNA DE PROTECCIÓN DE DATOS PERSONALES

DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN

SALASACA, ECUADOR

JULIO 2025

ANEXO 3. Rúbrica de validación de la política

(Revisor 1)

Pontificia Universidad Católica del Ecuador | Sede Ambato

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR SEDE AMBATO

INGENIERÍA EN SISTEMAS DE INFORMACIÓN

RUBRICA DE EVALUACIÓN DE LA POLÍTICA

Objetivo:

El objetivo de la presente rubrica es evaluar la calidad, coherencia normativa, estructura y aplicabilidad de la propuesta de la propuesta de política de protección de datos personales para una institución del segmento 3 que se desarrolló utilizando los marcos internacionales como: NIST-CSF e ISO/IEC 27001 alineados con las necesidades de la cooperativa y la LOPDP.

Instrucciones:

Esta rubrica será aplicada por el evaluador durante su revisión. Cada criterio recibirá una calificación de tipo escala donde 1 Deficiente, 2 insuficiente, 3 aceptable, 4 bueno y 5 Excelente.

Tabla de evaluación

Criterio	Descripción	5	4	3	2	1
Estructura y organización de la política.	Claridad en la presentación, formato uniforme, numeración adecuada y secciones completas.	X				
Actualidad	Evalúa si la política se encuentra actualizada conforme a la legislación y contextos tecnológicos recientes.	X				
Claridad del objetivo y alcance	Explica con precisión el propósito de la política y los actores a los que aplica.	X				
Conceptualización	Se comprende los conceptos clave de marcos legales y metodologías empleadas.	X				
Pertinencia	La propuesta de política es adecuada con las necesidades de la cooperativa	x				

Pontificia Universidad Católica del Ecuador | Sede Ambato

Aplicabilidad	Adaptación al contexto financiero, especialmente en cooperativas pequeñas o medianas.	X				
Redacción técnica y normativa	Uso de lenguaje técnico preciso, formalidad académica y coherencia normativa.	X				

Observaciones:

La política está bien estructurada y cumple con los parámetros para una cooperativa de ahorro y crédito de segmento 3

Recomendaciones:

- Cumple con los requisitos de esta política.

Lugar y fecha de validación: Salasaca 8/07/2025

Firma

Autachi Shiri Masaquiza

Responsable de TI.

Coac. Indígenas Galápagos

Anexo 4. Rúbrica de validación de la política

(Revisor 2)

Pontificia Universidad Católica del Ecuador | Sede Ambato

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR SEDE AMBATO

INGENIERÍA EN SISTEMAS DE INFORMACIÓN

RUBRICA DE EVALUACIÓN DE LA POLÍTICA

Objetivo:

El objetivo de la presente rubrica es evaluar la calidad, coherencia normativa, estructura y aplicabilidad de la propuesta de política de protección de datos personales para una institución del segmento 3 que se desarrolló utilizando los marcos internacionales como: NIST-CSF e ISO/IEC 27001 alineados con las necesidades de la cooperativa y la LOPDP.

Instrucciones:

Esta rubrica será aplicada por el evaluador durante su revisión. Cada criterio recibirá una calificación de tipo escala donde 1 Deficiente, 2 insuficiente, 3 aceptable, 4 bueno y 5 Excelente.

Tabla de evaluación

Criterio	Descripción	5	4	3	2	1
Estructura y organización de la política.	Claridad en la presentación, formato uniforme, numeración adecuada y secciones completas.		x			
Actualidad	Evalúa si la política se encuentra actualizada conforme a la legislación y contextos tecnológicos recientes.		x			
Claridad del objetivo y alcance	Explica con precisión el propósito de la política y los actores a los que aplica.	X				
Conceptualización	Se comprende los conceptos clave de marcos legales y metodologías empleadas.	X				
Pertinencia	La propuesta de política es adecuada con las necesidades de la cooperativa		x			

Pontificia Universidad Católica del Ecuador | Sede Ambato

Aplicabilidad	Adaptación al contexto financiero, especialmente en cooperativas pequeñas o medianas.	X				
Redacción técnica y normativa	Uso de lenguaje técnico preciso, formalidad académica y coherencia normativa.		x			

Observaciones:

La normativa aplicable al momento de la presentación esta vigente, y que en lo futuro dependiendo de las reformas o actualizaciones lo hará los cambios pertinentes y la Institución financiera que también lo hará.

Recomendaciones:

- Las organizaciones deben familiarizarse con la LOPDP y sus principios,
- La obtención de consentimientos de datos debe ser informado al titular, explicando claramente la finalidad del tratamiento y el tiempo de conservación.
- Se debe implementar medidas de seguridad para proteger los datos personales contra accesos no autorizados, pérdidas o divulgaciones.

Lugar y fecha de validación: Salasaka 15 julio 2025.

KJULLIAR PFACCHA JEREZ MASAQUIZA

Firmado digitalmente por KJULLIAR PFACCHA JEREZ MASAQUIZA
Fecha: 2025.07.15 16:39:13 -05'00'

Asesor Jurídico
Coac Indigenas Galapagos