UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES INSTITUTO DE POSTGRADO

TÍTULO

Plan De Seguridad De Datos Para Cooperativas Segmento 1 En Ecuador Basado En La Ley Orgánica De Protección De Datos Personales

AUTOR
Caillamara Encalada, David Antonio

TRABAJO DE TITULACIÓN

Previo a la obtención del grado académico en
MAGÍSTER EN CIBERSEGURIDAD

TUTOR
Cruz Carrillo, Henry Omar

Santa Elena, Ecuador
Año 2026

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TRIBUNAL DE SUSTENTACIÓN

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ALICIA GERMANIA ANDRADE VERA

Ing. Alicia Andrade Vera, Mgtr.
COORDINADORA DEL PROGRAMA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
HENRY OMAR CRUZ CARRILLO

Ing. Henry Cruz Carrillo, Ph.D.
TUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
BYRON WLADIMIR OVIEDO BAYAS

Ing. Byron Oviedo Bayas, Ph.D.
DOCENTE ESPECIALISTA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
DIEGO EDUARDO BENAVIDES ASTUDILLO

Ing. Diego Benavides Astudillo, Ph.D.
DOCENTE ESPECIALISTA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MARIA MARGARITA RIVERA GONZALEZ

Abg. María Rivera González, Mgtr.
SECRETARIA GENERAL
UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por **CAILLAMARA ENCALADA DAVID ANTONIO**, como requerimiento para la obtención del título de Magíster en Ciberseguridad.

TUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
HENRY OMAR CRUZ CARRILLO

Ing. Henry Omar Cruz Carrillo, Ph.D.

Santa Elena, 16 de junio de 2026

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

DECLARACIÓN DE RESPONSABILIDAD

Yo, **CAILLAMARA ENCALADA DAVID ANTONIO**

DECLARO QUE:

El trabajo de Titulación, "**PLAN DE SEGURIDAD DE DATOS PARA COOPERATIVAS SEGMENTO 1 EN ECUADOR BASADO EN LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES**", previo a la obtención del título en Magíster en Ciberseguridad, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, 16 de junio de 2026

EL AUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
DAVID ANTONIO
CAILLAMARA ENCALADA

Caillamara Encalada David Antonio

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE CIENCIAS DE LA INGENIERÍA
INSTITUTO DE POSTGRADO

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado **PLAN DE SEGURIDAD DE DATOS PARA COOPERATIVAS SEGMENTO 1 EN ECUADOR BASADO EN LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES**, presentado por el estudiante, **DAVID ANTONIO CAILLAMARA ENCALADA** fue enviado al Sistema Antiplagio COMPILATIO, presentando un porcentaje de similitud correspondiente al 6%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.

Informe de análisis
Compilatio Magister+ | ESPE-ECU

Formato - Examen Complexivo - Componente Practico v3 Rev HC 16062026
ID : 48cdd311351422923e2a225e9963f3da28cbc4d3

6%
Textos sospechosos

Nombre del fichero : Formato - Examen Complexivo - Componente Practico v3 Rev HC 16062026.txt
Tamaño del archivo original : 511,67 kB
Número de palabras : 7834
Número de caracteres : 53849

Depositante : HENRY OMAR CRUZ CARRILLO
Fecha de depósito : 16 de junio de 2026
Tipo de carga : interface
fecha de fin de análisis : 16 de junio de 2026

TUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
HENRY OMAR CRUZ CARRILLO

Ing. Henry Omar Cruz Carrillo, Ph.D.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

AUTORIZACIÓN

Yo, **DAVID ANTONIO CAILLAMARA ENCALADA**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de examen de carácter complexivo con fines de difusión pública, además apruebo la reproducción de este examen de carácter complexivo dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Santa Elena, 16 de junio de 2026

EL AUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
DAVID ANTONIO
CAILLAMARA ENCALADA

David Antonio Caillamara Encalada

AGRADECIMIENTO

Manifiesto mi agradecimiento en primer lugar a mi familia que con su apoyo y comentarios de aliento fueron de inspiración para seguir adelante.

Agradezco la Universidad de la Península de Santa Elena y sus docentes que compartieron su conocimiento y experiencia a lo largo del periodo educativo, además agradecer al Doctor Henry Cruz, tutor de este trabajo de titulación, por ser de guía, compartir su conocimiento, brindarme su ayuda y dedicación en cada etapa del proceso, agradezco a los compañeros de maestría por los momentos compartidos y el apoyo mutuo.

También agradezco a mis compañeros de trabajo que con sus incentivos apoyaron esta nueva meta.

Finalmente agradezco a cada una de las personas que de una u otra forma contribuyeron a la realización exitosa de este proyecto.

David Antonio, Caillamara Encalada

DEDICATORIA

El presente trabajo de investigación lo dedico especialmente a mi madre Piedad que con su apoyo y comentarios que me sirvieron de aliento para seguir adelante y brindarme ese cariño para cumplir esta nueva meta, a mis hermanos/as, mi cuñada y cuñado que fueron un apoyo, por sus consejos y siempre decirme sigue adelante que ya viene lo mejor, va dedicado a cada una de las personas que me dieron su apoyo y me impulsan a ser mejor persona.

Finalmente dedico este trabajo a mi persona que pese a momentos complejos supe resolver y seguir con el proceso sin dar un paso atrás.

David Antonio, Caillamara Encalada

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La investigación tiene como objetivo plantear un plan de seguridad de datos para cooperativas del segmento 1 en Ecuador basado en la ley orgánica de protección de datos personales, la investigación es cuantitativa de tipo exploratorio, diagnóstico y propositivo, como primer punto se ejecutó el análisis de las normativas vigentes y el estándar internacional ISO 27001, permitiendo identificar procesos críticos de las cooperativas en base al tratamiento de datos que se realiza en cada proceso, los cuales son: crédito, cobranza, recursos humanos y tecnologías de la información se identificaron riesgos de protección de datos, dando como resultado la elaboración de una matriz de riesgos en conjunto de controles de mitigación, los cuales sirven de base para el diseño del plan de seguridad, finalmente, se obtiene el plan de seguridad de datos que se estructura en cuatro puntos documentales clave administrativos, organizativos, tecnológicos y jurídicos, donde se integran políticas, procedimientos para el cumplimiento normativo.

Palabras claves: Protección de datos personales, Seguridad de la información,
Plan de seguridad de datos personales

ABSTRACT

The objective of this research is to propose a data security plan for Segment 1 cooperatives in Ecuador based on the “Ley orgánica de protección de datos personales”. The research follows a quantitative approach and is exploratory, diagnostic, and propositional in nature. As a first step, an analysis of the current regulations and the international ISO 27001 standard was conducted, allowing the identification of critical cooperative processes based on the data processing carried out within each process. These processes include lending, collections, human resources, and information technology. Data protection risks were identified, resulting in the development of a risk matrix together with mitigation controls, which serve as the foundation for the design of the security plan. Finally, a data security plan was developed, structured around four key documentary components: administrative, organizational, technological, and legal, integrating policies and procedures to ensure regulatory compliance.

Keywords: Personal Data Protection, Information Security, Personal Data Security Plan.

INTRODUCCIÓN

El presente trabajo de investigación se basa en la protección de datos personales en las entidades financieras como son las cooperativas del Segmento 1 del Ecuador, en las cuales el principal punto a abordar es que dichas entidades gestionan grandes volúmenes de datos personales y sensibles donde los principales actores son: socios, clientes y empleados.

La LOPDP en el Art. 37 de la seguridad de datos personales, dice que "El responsable o encargado del tratamiento de datos personales, deberá implementar un proceso de verificación, evaluación y valoración continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole, implementadas con el objeto de garantizar y mejorar la seguridad del tratamiento de datos personales" (Asamblea Nacional, 2021)

A raíz de lo citado las entidades que manejan datos personales tienen la necesidad de implementar medidas técnicas, jurídicas, organizativas y administrativas las cuales deben estar alineadas al cumplimiento de la LOPDP y dichas medidas cumplan con el modelo fundamental de ciberseguridad para la protección de la información, el cual se enfoca en la confidencialidad, integridad, disponibilidad de la información.

El estudio se enfocó en el diseño de un Plan de Seguridad de Datos Personales para las cooperativas del Segmento 1 y dicho plan cuente con los lineamientos de las normativas vigentes y estándares internacionales, el Plan de Seguridad al ser de carácter referencial, se realizó con un enfoque documental el cual se basa en la revisión de la LOPDP, su reglamento y demás lineamientos normativos emitidos por la Superintendencia de Protección de Datos Personales (SPDP), además de alinearse con la "norma de control respecto a la seguridad de la información en las entidades del financieras alineadas por segmentos, la cual es emitida por la Superintendencia de Economía Popular y Solidaria (SEPS)" (Superintendencia de Economia Popular y solidaria, 2022).

El estudio además de estar alineado con las normas y leyes vigentes, la investigación se basó en estándares internacionales como la ISO/IEC 27001, el cual tiene como objetivo "establecer, implementar, mantener y mejorar continuamente un SGSI dentro del contexto de la organización o entidad" (ISO/IEC, 2022).

El alcance de la investigación es de tipo exploratorio, diagnóstico y propositivo. Es exploratorio porque permite comprender el contexto del tratamiento de datos personales; diagnóstico, al identificar riesgos y brechas potenciales; y propositivo, al plantear el diseño de un plan de seguridad. Asimismo, se emplean métodos analítico, inductivo y deductivo, que permiten descomponer la normativa y procesos, identificar patrones de riesgo y aplicar estándares internacionales al contexto cooperativo.

En base al análisis del tratamiento de datos personales se identificó los procesos críticos que tienen las cooperativas en donde se manejan datos personales y se deben implementar medidas de mitigación, los procesos son: Crédito, Cobranza, Recursos humanos y TI, respecto a la recopilación de información se realizó la revisión de leyes y normativas vigentes, validación de buenas prácticas, la revisión del ciclo de vida del dato en los procesos para finalmente obtener la matriz de riesgos y controles, teniendo en cuenta que el enfoque es técnico y normativo.

Con el fin de mejorar la seguridad del tratamiento de datos personales la investigación tiene como aportes de carácter técnico, legal y social, técnico porque brinda un plan de seguridad de los datos personales enfocado al cumplimiento de la LOPDP, legal porque no solo se cumplen las leyes y normas vigentes si no que se enfoca en el cumplimiento de la ley a nivel contractual con la adición de cláusulas, obtención de consentimientos y adendum para el tratamiento de datos personales y social porque al contar con dichas medidas que fortalecen el tratamiento de datos personales las entidades crean seguridad y confianza en los clientes, socios y empleados.

El presente trabajo se estructurará por capítulos, el capítulo uno hace referencia a la fundamentación donde se abordan los antecedentes, la descripción del proyecto, los objetivos del proyecto, la justificación y el alcance, el capítulo dos trata el marco teórico en el cual se enfatizan conceptos respecto a la protección de datos personales, la Ley Orgánica de Protección de Datos, los principios de la protección de datos personales la seguridad de la información, el estándar ISO/IEC 27001, la gestión de riesgos en seguridad de la información, la seguridad de la información en el sector financiero enfocado en las cooperativas de ahorro y crédito y finalmente el plan de seguridad de datos personales, como capítulo tres se tiene la metodología del proyecto donde se detalla la metodología de la investigación y las técnicas de recolección de datos, finalmente, se

tiene el capítulo cuatro donde se tiene la propuesta y la sección para las conclusiones y recomendaciones.

CAPÍTULO I

1 FUNDAMENTACIÓN

1.1 ANTECEDENTES

La Ley Orgánica de Protección de Datos Personales (LOPDP), fue aprobada el 26 de mayo del 2021, en Ecuador, y a partir de esta fecha la Superintendencia de Protección de Datos Personales ha ido generando y publicando reglamentos, resoluciones y guías para que las empresas puedan manejar los datos personales del titular de forma correcta.

La ley no solo se centra en como una empresa maneja la información y la resguarda, si no que va más allá, se enfoca en proteger los derechos y libertades del titular de los datos, ya sea que dichos datos se manejen de forma física o de forma digital.

La Ley Orgánica de Protección de Datos Personales al ser relativamente nueva obliga a las entidades a aplicar medidas, controles y reforzar la seguridad, debido a que pueden surgir riesgos como: el acceso no autorizado a la información, perdida de la información o el uso indebido de los datos personales que vulneren los derechos y libertades de los titulares.

Las Cooperativas son entidades que se rigen bajo las leyes y el control de la Superintendencia de Economía Popular y Solidaria (SEPS), el cual tiene como objetivo "asegurar que las entidades de ahorro y crédito trabajen de forma correcta y protejan al socio evitando diferentes riesgos como son los fraudes, perdida de dinero." (Superintendencia de Economia Popular y solidaria, 2022)

Dentro de las normas que emite la SEPS, una de ellas es la "Norma de control respecto a la seguridad de la información en las entidades del sector financiero popular y solidario bajo control de la superintendencia de economía popular y solidaria", la cual clasifica a las cooperativas bajo regímenes los cuales son: régimen general, régimen especial, régimen simplificado, dichos regímenes clasifican a las cooperativas por segmentos en base a los servicios que prestan, va del segmento 1 al 5. (Superintendencia de Economia Popular y solidaria, 2022)

El eje de negocio de las cooperativas es la información que recopilan para sus procesos internos, independientemente del segmento que tenga una cooperativa recaba información para otorgar un crédito, para abrir una cuenta de ahorros, para trabajar dentro de la institución, entre otros procesos, hay que tener en cuenta que en cada proceso se realizan tratamiento de datos personales y por esta razón se debe incrementar las medidas

de seguridad de la información, aplicación de estándares internacionales como la ISO 27001 y estas medidas estén enfocadas y alineadas a lo que requiere la Ley Orgánica de Protección de Datos Personales.

Los actores principales que conforman el sistema de protección de datos personales son: titular, responsable, encargado, destinatario, autoridad de protección de datos y delegado de protección de datos, en este punto y para el escenario nos enfocaremos en el titular y el responsable, el titular es la persona dueña de los datos y el responsable es la entidad que recepta, resguarda y trata los datos personales, las entidades al ser responsables tienen un papel importante dentro del manejo de los datos personales, el cual es proteger los datos ante posibles amenazas ya sean físicas o tecnológicas, que puedan afectar la confidencialidad, integridad y disponibilidad de la información para el titular de los datos. (Dinarp, 2021)

Ante lo mencionado al ser la ley una regulación que surgió recientemente y al estar consolidándose bajo reglamentos y resoluciones recientes, no se tiene el diseño de plan directamente propuesto para solventar su implementación dentro de las entidades, es decir, que si bien la ley, el reglamento y sus resoluciones generan lineamientos para su implementación, aún existe una brecha al no tener un plan específico que haga cumplir la ley en las cooperativas.

1.2 DESCRIPCIÓN DEL PROYECTO

La entidades financieras tienen la necesidad de manejar la información de forma segura y respaldarla ofreciendo a sus clientes confianza, enfocándose en este punto nace el objetivo del proyecto que es el diseñar un plan de seguridad de datos personales alineado con las normas, leyes y regulaciones vigentes, en este sentido se seleccionarán procesos críticos donde se tratan datos personales en una cooperativa que son: crédito, cobranzas, TI y talento humano, con el fin de identificar de posibles riesgos y proponiendo controles y medidas de mitigación alineadas con la ISO 27001, para finalmente generar la estructura del plan donde se detalle el cumplimiento esta ley.

1.3 OBJETIVOS DEL PROYECTO

1.3.1 OBJETIVO GENERAL

Diseñar un Plan de Seguridad de Datos Personales de carácter referencial para las cooperativas del Segmento 1 del Ecuador, que permita garantizar la alineación con el principio de seguridad establecido en la Ley Orgánica de Protección de Datos Personales.

1.3.2 OBJETIVOS ESPECÍFICOS

- Analizar el marco normativo, técnico y conceptual relacionado con la protección de datos personales, considerando la norma vigente, sus disposiciones y estándares internacionales de seguridad de la información aplicables a las cooperativas del Segmento 1.
- Identificar los riesgos, las vulnerabilidades y las brechas potenciales en la gestión de los datos de carácter personal para los procesos ordinarios de las cooperativas del Segmento 1, a partir de una metodología de análisis de riesgos de enfoque documental y referencial.
- Elaborar un Plan de Seguridad de los Datos Personales que integre políticas, procedimientos, controles técnicos y organizativos que estén orientados a mitigar el riesgo y a reforzar el cumplimiento del principio de seguridad que establece la normativa que se encuentra en vigor.

1.4 JUSTIFICACIÓN DEL PROYECTO

El desarrollo del presente proyecto se justifica en la creciente necesidad de garantizar la protección de los datos personales en las organizaciones del sector financiero popular y solidario del Ecuador, particularmente en las cooperativas de ahorro y crédito del Segmento 1, las cuales gestionan grandes volúmenes de información sensible de socios, clientes y empleados. La Ley Orgánica de Protección de Datos Personales establece obligaciones claras para los responsables del tratamiento, especialmente en lo relacionado con la implementación de medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información.

Desde el punto de vista técnico, el proyecto tiene una gran importancia, ya que se basa en un enfoque estructurado para la gestión de la seguridad de los datos personales, que se encuentra fundamentada en el estándar internacional ISO/IEC 27001, permitiendo de esta

forma identificar riesgos, vulnerabilidades y definir controles para su tratamiento. Con esta forma, el proyecto contribuirá a mejorar las prácticas de seguridad de la información en un sector que, por la índole de su actividad, está expuesto a múltiples amenazas que pueden dañar la información de los datos personales.

Desde la perspectiva legal, la investigación proporciona una herramienta que facilita la interpretación y la aplicación de la normativa vigente, permitiendo a las cooperativas adecuar sus procesos al principio de seguridad que establece la Ley Orgánica de Protección de Datos Personales, disminuyendo de esta forma los riesgos de incumplimiento normativo y las sanciones que pueden derivar de las mismas al momento de promover la protección de datos.

Desde el punto de vista social, el proyecto tiene una gran importancia, ya que genera confianza entre los socios y usuarios de las cooperativas que facilitan su información a estas entidades.

De ese modo, la investigación se encuentra justificada por el aporte práctico que otorga la elaboración del Plan de Seguridad de Datos Personales, de carácter referencial, pues podrá servir de herramienta orientadora y adaptable para las cooperativas del Segmento 1, ayudando así a la implementación de políticas, procedimientos y mecanismos de control sin necesidad de haber diseñado totalmente desde su principio dicha política, haciendo fácil la aplicación en organizaciones que presenten las características indicadas.

1.5 ALCANCE DEL PROYECTO

El presente trabajo tiene un carácter analítico y también propositivo pues se espera dar lugar a un Plan de Seguridad de Datos Personales de carácter referencial para las cooperativas del Segmento 1 del Ecuador como resultado de la investigación, la cual comenzará por estudiar la Ley Orgánica de Protección de Datos Personales, su normativa complementaria y referencias de estándares internacionales relacionados con la seguridad de la información, tal como puede ser el caso de la norma ISO/IEC 27001, para así conocer los requisitos que le resulten aplicables al tratamiento de los datos personales que realizaban los trabajadores en esta forma de organización empresarial.

El alcance proyectado incluye el examen y el análisis de los procesos generales que se llevan a cabo en las cooperativas del Segmento 1, todos y cada uno de los siguientes, el crédito, la cobranza, los recursos humanos y la tecnología de la información, procesos en

los cuales se realiza el tratamiento de los datos personales de los trabajadores de la cooperativa. A partir del examen y análisis anterior se podrá identificar una serie de posibles riesgos, vulnerabilidades y brechas en la seguridad, datos todo ello que servirán de fundamentos a partir de los cuales construir un conjunto de políticas, procedimientos y controles aliados a la protección de la información.

El trabajo desembocará en la construcción de un Plan de Seguridad de Datos Personales sustentado en los lineamientos técnicos, administrativos y organizacionales cuales son los que están permitidos por el cumplimiento de la normativa vigente y los estándares internacionales de seguridad de la información. Así este Plan de Seguridad de Datos Personales tendrá un carácter referencial, con el fin de que cada cooperativa pueda adecuarlo de acuerdo con sus propias particularidades institucionales.

Hay que hacer notar que el presente trabajo no contempla la implementación del mismo en una cooperativa, no contempla la aplicación de herramientas tecnológicas, ni la realización de auditorías de campo o levantamiento de información directa. Por lo tanto, el presente trabajo será fundamentalmente un trabajo de análisis y de un desarrollo conceptual de modelo de seguridad de datos personales.

CAPÍTULO 2

2 MARCO TEORÍCO

2.1 Protección de Datos Personales

En cuanto a la protección de datos personales, hay que comenzar por establecer qué se entiende por dato personal, que es la información que puede llegar a identificar o hacer identificable a una persona física (Asamblea Nacional, 2021)

La Comisión Europea se hace eco de la idea de que no sólo engloban la información que identifica de forma directa a un sujeto, como el nombre, las direcciones o los distintos números de identificación, sino que además contempla cualquier información que dada la relación o combinación con otros datos puede identificar al titular (Comisión Europea, 2024)

Finalmente, la protección de datos personales también es entendida como el conjunto de principios, normas o medidas que garantizan el tratamiento correcto de la información relativa a personas físicas identificadas o identificables. La protección de datos personales también es un derecho fundamental para la protección de la vida privada y de la posibilidad de que las personas puedan controlar su propia información a través de evitar usos inadecuados o tratamientos que puedan poner en serio riesgo la información a la cual esas personas tienen acceso (Vera, 2025)

Con el paso de los años, el interés por la protección de datos personales ha ido en aumento, teniendo en cuenta que las propias organizaciones gestionan un alto volumen de información. De ahí que la implementación de los mecanismos requeridos para garantizar la triada de CID sea absolutamente relevante al objeto de reducir el riesgo de accesos no autorizados o de tratamientos inadecuados de la información.

2.2 Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador

La LOPDP es un marco jurídico que valida el tratamiento de datos en Ecuador, no solo se centra en como una empresa maneja la información y la resguarda, si no que establece deberes y responsabilidades de quienes realizan el tratamiento de esta información. La Ley Orgánica de Protección de Datos Personales también establece una serie de lineamientos que las organizaciones y empleadores deben observar, tales como la implementación de medidas de seguridad, la gestión del riesgo y la aplicación de criterios

de responsabilidad en el manejo de la información, en especial en aquellos casos relacionados con datos sensibles (Asamblea Nacional, 2021)

2.3 Principios de la Protección de Datos Personales

La Ley Orgánica de Protección de Datos Personales (LOPDP) tiene su base en ciertos principios que permiten llevar a cabo el tratamiento adecuado de los datos personales, destacando el principio de seguridad que trae como consecuencia la obligación de implementar medidas que permitan proteger la información (Curay & Flores, 2025)

Así también, la Organización de los Estados Americanos expresa múltiples principios vinculados de alguna manera a la protección de datos personales que, entre otros, emanan de sus normas, tales como finalidades lícitas y lealtad, transparencia y consentimiento, pertinencia y necesidad, limitación del tratamiento y conservación, confidencialidad, seguridad de los datos, exactitud de la información, acceso, protección de datos sensibles, transferencia transfronteriza de datos, responsabilidad, excepciones y la intervención de autoridades de protección de datos (Organización de los Estados Americanos, 2021)

Todos ellos permiten llevar a cabo la actividad del tratamiento de datos personales adecuada, y, además, conforme a criterios de protección, asegurando la confidencialidad de la información y reduciendo así los riesgos de que no se utilicen o no se autoricen los datos personales (Curay & Flores, 2025)

2.4 Seguridad de la Información

La seguridad de la información tiene por objeto garantizar la protección de la información frente a amenazas que pongan en riesgo su confidencialidad, su integridad y su disponibilidad, los que son considerados principios básicos en la gestión de la información. La correcta implementación de los mecanismos de seguridad permite a las organizaciones proteger sus activos de información y garantizar la continuidad de los procesos de la organización (International Organization for Standardization, 2022)

2.5 Estándar ISO/IEC 27001

La norma ISO/IEC 27001 establece los requisitos necesarios para crear un SGSI, basado en la identificación, evaluación y tratamiento de riesgos de la información. Así, con esta norma, las organizaciones obtienen un marco de trabajo que les permite gestionar la

seguridad de la información con eficiencia y en base a las buenas prácticas internacionalmente aceptadas (Calder, 2008)

La norma ISO 27001:2022, es un estándar internacional que organiza la seguridad de los datos, su confidencialidad e integridad, así como de los procesos que tienen los sistemas que los procesan, y permite que las organizaciones identifiquen sus riesgos que presentan esos datos y a partir de este último, poder aplicar controles para poder mitigar y/o eliminar. Tomar la norma 27001 también es una ventaja competitiva y ayuda a la imagen institucional al ser un compromiso organizativo relacionado con la información a proteger, mientras que la gestión de la seguridad de la información también se acompaña de las buenas prácticas y controles facilitados por la norma ISO 27002. (Encalada, 2024)

En la Figura 1 se muestran los controles establecidos por la norma ISO 27001 y los organiza según las diferentes áreas de aplicación como los son: gobernanza, activos, control de accesos, seguridad del personal, seguridad física, operaciones, redes, desarrollo del sistema, incidentes, continuidad del negocio, cumplimiento. Esto se hace con el fin de poder mejorar la seguridad de la información y poder mantener un correcto alineamiento con lo dispuesto a la Ley Orgánica de Protección de Datos Personales, constituyendo un referente en el diseño del Plan de seguridad de datos de carácter personal.

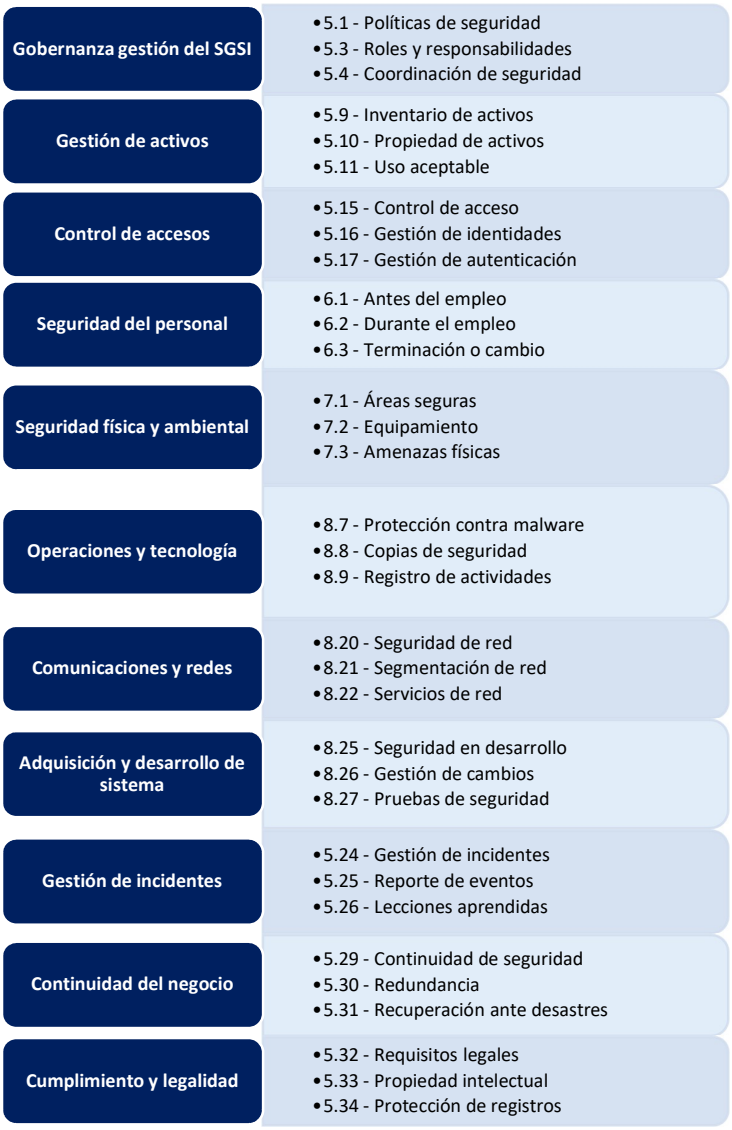

Figura 1. Controles ISO 27001

2.6 Gestión de Riesgos en Seguridad de la información

La gestión de riesgos es el procedimiento de identificar, analizar y minimizar los riesgos relacionados con la seguridad de la información que llevan a las organizaciones a tomar decisiones orientadas a la protección de sus activos importantes (Superintendencia de Protección de Datos Personales, 2026)

En este sentido, la gestión de riesgos es realmente necesaria para prevenir incidentes de seguridad para reducir el efecto que podrían tener de forma negativa el tratamiento y la

gestión de la información a una en la protección que se genera en las organizaciones (Stoneburner, Goguen, & Feringa, 2002)

Para la gestión de riesgos se ha tomado la escala que plantea la Superintendencia de Económica Popular y solidaria en la normativa (Superintendencia de Economia Popular y solidaria, 2022), en el que se determina el nivel del riesgo inherente y con el nivel de criticidad, así como su calificación de acuerdo con la siguiente ecuación:

Niveles de criticidad:

- Crítico = 5
- Alto = 4
- Medio = 3
- Bajo = 2
- Muy bajo = 1

Fórmula para determinar el riesgo inherente:

$$\textit{Probabilidad}\ \boldsymbol{x\ Impacto}\ = \textit{nivel de Riesgo de seguridad}$$

2.6.1 Niveles de impacto

Los niveles de impacto se crean en base a la documentación de la SPDP, que detalla como ejemplo dentro de la Guía de gestión de riesgos, define los niveles de criticidad que son: muy alto, alto, medio, bajo y muy bajo, para cada nivel de criticidad se enfoca en una categoría del dato, que tratan en una entidad como vulnerable, personal, sensible. El nivel de criticidad dado ayuda a calificar como afecta un incidente dentro de la entidad y como afecta en los derechos del titular. (Enríquez, 2026)

La Figura 2 hace referencia a los criterios cualitativos de evaluación de impacto.

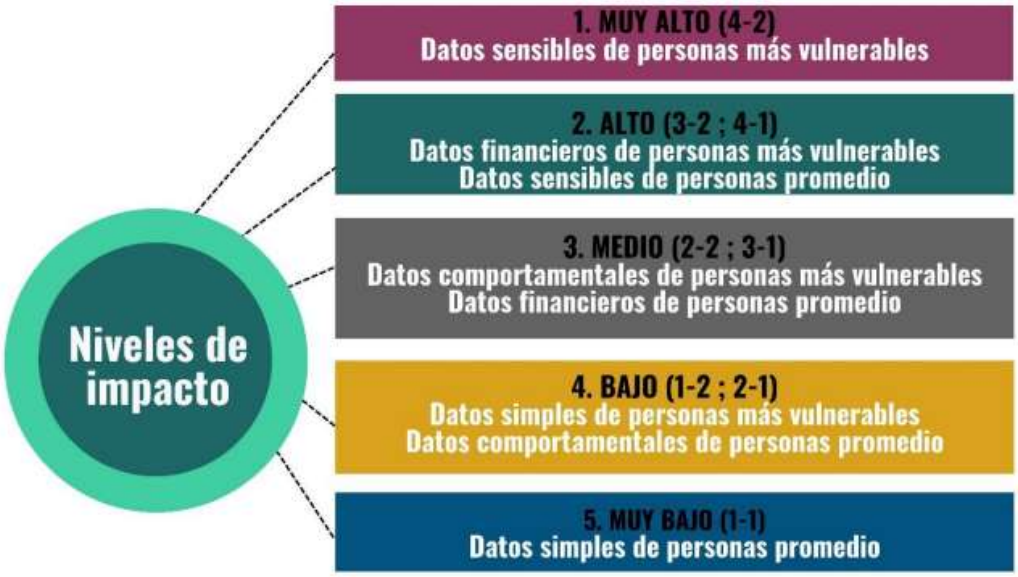

Figura 2. Niveles de impacto

Tomada del documento Guía de Gestión de Riesgos y Evaluación de impacto del Tratamiento de datos personales. Pág. 18. (Enríquez, 2026)

Teniendo así la Tabla 1 en la que se muestra los niveles de criticidad y valoraciones que se utilizan para la calificación del impacto.

Impacto	
Muy alto	5
Alto	4
Medio	3
Bajo	2
Muy bajo	1

Tabla 1. Niveles de criticidad del impacto.

2.6.2 Niveles de probabilidad

En la Figura 3 tomada de la guía gestión de riesgos, donde los criterios de probabilidad se establecieron en función de la frecuencia estimada de ocurrencia de un evento de riesgo dentro de un periodo establecido, utilizando rangos porcentuales que permiten clasificar los riesgos desde insignificantes hasta inminentes. Esta valoración facilita identificar qué riesgos requieren atención prioritaria, de acuerdo con la posibilidad real de que se materialicen durante la operación del proceso.

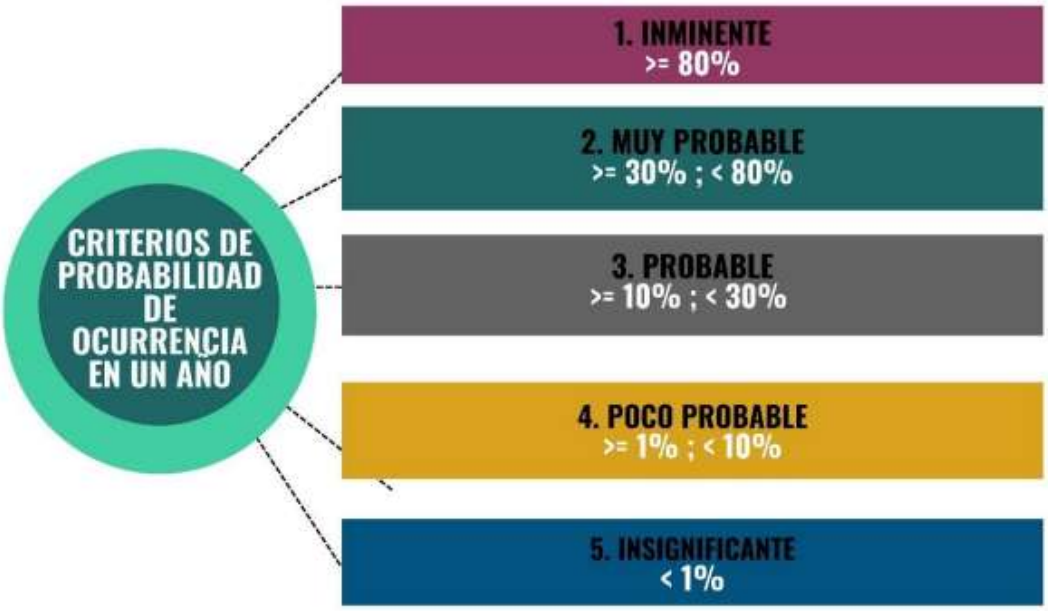

Figura 3. Criterios de probabilidad

Tomada del documento Guía de Gestión de Riesgos y Evaluación de impacto del Tratamiento de datos personales. Pág. 20 (Enríquez, 2026)

Teniendo así la Tabla 2 en la que se muestra los niveles de criticidad y valoraciones que se utilizan para la calificación de la probabilidad.

Probabilidad		
>=80%	Inminente	5
>=30% <80%	Muy probable	4
>=10% <30%	Probable	3
>=1% <10%	Poco probable	2
1%	Insignificante	1

Tabla 2. Niveles de criticidad de la probabilidad.

2.6.3 Mapa de calor

En la Tabla 3 se colocan los niveles de criticidad de cada ponderación para el impacto vs la probabilidad y poder determinar el valor del riesgo inherente.

MAPA DE CALOR			PROBABILIDAD				
			Insignificante	Poco probable	Probable	Muy probable	Inminente
			1	2	3	4	5
IMPACTO	Muy alto	5	5	10	15	20	25
	Alto	4	4	8	12	16	20
	Medio	3	3	6	9	12	15
	Bajo	2	2	4	6	8	10
	Muy bajo	1	1	2	3	4	5

Tabla 3. Mapa de calor

2.7 Seguridad de la información en el Sector Financiero (Cooperativas)

Las cooperativas de ahorro y crédito, sobre todo las del Segmento 1, manejan importantes volúmenes de información personal y financiera, lo que hace imprescindible la puesta en práctica de medidas de seguridad robustas y adecuadas para preservar dicha información (Superintendencia de Economia Popular y Solidaria, 2022)

En este sentido, la aplicación de sistemas de gestión de la seguridad de la información se convierte en un factor que colabora en garantizar la seguridad de los datos, a menudo incluso llegan a prevenir incidentes de seguridad y a permitir generar una mayor confianza en los socios o clientes (López, 2025)

2.8 Plan de Seguridad de Datos Personales

Un plan de seguridad de datos personales es la organización de un conjunto de políticas, procedimientos y controles operativos que permitan proteger la información dentro de una organización (ISO, 2022)

Este tipo de planes ayuda a establecer pautas definidas tanto para la gestión de los riesgos en la protección de datos de carácter personal como para el cumplimiento de la normativa actual, sobre todo cuando se basa en estándares internacionales, como la norma ISO 27001. En igual sentido, la planificación de un plan de seguridad de datos personales implica contemplar las amenazas y las vulnerabilidades existentes dentro de la organización con la voluntad de lograr un modelo global de seguridad de la información y que está basado en tres principios básicos: la confidencialidad, la integridad y la disponibilidad de los datos (Aguasanta, 2024).

CAPÍTULO 3

3 METODOLOGÍA DEL PROYECTO

La siguiente investigación presenta un enfoque propositivo y centrado en el diseño de un Plan de Seguridad de los Datos Personales dirigido a las cooperativas del Segmento 1 del Ecuador, sin incluir la recogida de información mediante trabajo de campo; se basa en el análisis documental, técnico y normativo en relación con el tratamiento de datos personales.

La propuesta metodológica se plantea en tres etapas básicas (diagnóstico, análisis de riesgos y diseño del plan) mediante las cuales se pueden detectar requerimientos, necesidades y posibles brechas en la gestión de datos personales para las cooperativas. Al efecto, se toman en cuenta los procesos estratégicos y críticos del sector como el crédito, TI, recursos humanos y cobranza.

Igualmente, la investigación plantea un enfoque de la gestión de riesgos tomando como base la norma ISO/IEC 27001, además de las guías del marco NIST, en tanto que permite detectar, analizar y valorar los riesgos de tratamiento de datos personales y añadir un soporte técnico a la propuesta.

La propuesta del estudio es la revisión de la normativa vigente (Ley Orgánica de Protección de Datos Personales (LOPDP), el reglamento y la normativa de la Superintendencia de Economía Popular y Solidaria (SEPS), estándares internacionales de seguridad de la información (ISO/IEC 27001:2022, entre otros).

3.1 METODOLOGÍA DE INVESTIGACIÓN

La investigación se desarrolla bajo un enfoque exploratorio, diagnóstico y propositivo. Se considera exploratoria porque permite entender el contexto en el que se desarrolla el tratamiento de los datos personales en el sector cooperativo; es diagnóstica porque permite descubrir brechas, vulnerabilidades y riesgos asociados a la gestión de la información; y propositiva porque permite alcanzar un objetivo principal: el diseño de un Plan de Seguridad de Datos Personales.

Con ayuda de diferentes métodos se desarrolló la investigación como lo es el analítico que se enfocó en entender el contexto de la normativa y el cómo es el proceso del tratamiento de datos, el método inductivo que ayudó a enlistar los riesgos y el método deductivo que ayudó a aplicar controles y puntos de mitigación con ayuda los controles de la ISO 27001.

La unidad de análisis corresponde a los procesos críticos del sector cooperativo, se analizan el crédito, la tecnología de la información (TI), los recursos humanos y la cobranza, dentro de una visión referencial aplicable a las cooperativas del Segmento 1 del Ecuador, las reguladas por la Superintendencia de Economía Popular y Solidaria del Ecuador.

En el análisis de riesgos, se consideran como elementos principales los activos de información (datos personales), amenazas, vulnerabilidades y controles existentes. La valoración del riesgo se realiza en función de criterios de probabilidad e impacto, permitiendo establecer niveles de riesgo (alto, medio, bajo) que facilitan la priorización de medidas de seguridad.

3.2 TECNICAS DE RECOLECCIÓN DE INFORMACIÓN

En la fase de desarrollo de la investigación, se recurrió a técnicas de recolección documental y normativa, sumadas a un enfoque técnico centrado en el análisis de riesgos. Las principales técnicas utilizadas fueron:

- Revisión normativa: fue el análisis de Ley Orgánica de la Protección de Datos Personales (LOPDP), su reglamento, las normativas emitidas por la Superintendencia de la Economía Popular y Solidaria (SEPS) y normas internacionales relacionadas con la seguridad de la información, tal como la norma ISO/IEC 27001:2022.
- Análisis documental: fue la revisión de mejores prácticas, guías técnicas y marcos de referencia respecto a la seguridad de la información y protección de datos personales.
- Identificación de procesos: permitió determinar los procesos críticos del sector cooperativo como lo son crédito, tecnología de la información, recursos humanos y cobranza, a partir de los cuales se desarrolló el análisis del tratamiento de los datos personales y de la información que se gestiona en esos procesos.
- Análisis de riesgos: se realizó, considerando el enfoque de la norma ISO 27001. Esto implicó, identificar amenazas, vulnerabilidades y los posibles impactos relacionados con la triada de CID.
- Construcción de matrices de riesgos y controles: incluyó la elaboración de matrices orientadas a valorar el riesgo mediante criterios de probabilidad e

impacto, así como la definición de controles de seguridad alineados a la norma ISO 27001.

La ejecución de estas técnicas posibilitó la fundamentación del diseño del plan presentado y que, de esta manera, tuviera correspondencia técnica, validez metodológica y aplicabilidad al sector financiero cooperativo.

CAPÍTULO 4

4 PROPUESTA

La propuesta consistió en la identificación de los procesos que manejan datos personales dentro de las cooperativas, donde los procesos analizados fueron créditos, cobranzas, talento humano y tecnología de la información, en conjunto con los tratamientos de datos personales que enlista la Ley Orgánica de protección de datos personales se generó el ciclo de vida del dato en conjunto con los tratamientos como se muestra en el Anexo 1: Ciclo de vida del dato, realizado este punto se identificaron los riesgos, vulnerabilidades y brechas de seguridad dando como resultado la creación de una matriz de riesgos enfocada a la protección de datos personales y alineada a la LOPDP como se muestra en el Anexo 2: Matriz de riesgos el cual tuvo como objetivo Identificar los riesgos, poder colocar una calificación referencial en base a las consecuencias de cada riesgo y presentar la mitigación los controles que se deben aplicar para cada riesgo enlistado, para finalmente, desarrollar el Plan de Seguridad de Datos Personales de carácter referencial como se presenta en el Anexo 3: Plan de protección de datos, orientado a las cooperativas del segmento 1 del Ecuador, con el objetivo de garantizar el cumplimiento del principio de seguridad establecido en la normativa vigente, donde el plan está diseñado con una estructura de cuatro dimensiones: administrativa, organizativa, técnica y jurídica, integrando políticas, procedimientos, controles y mecanismos de gestión de riesgos. El presente modelo permite realizar un tratamiento de la información personal de forma completa, abarcando no solo los aspectos normativos, sino también los aspectos operativos, manteniéndose a su vez alineado a los estándares internacionales y a los controles que indica la norma ISO 27001 y que existen en relación con la seguridad de la información.

De la misma manera, en el desarrollo del plan se introducen una serie de elementos exigidos por la Superintendencia de Protección de Datos Personales mediante su normativa, entre los que se encuentran el Registro de Actividades de Tratamiento (RAT), el inventario de datos personales, la matriz de riesgos, las estrategias de mitigación, el Modelo Técnico de Gran Escala (MTGE), el plan de capacitación y manuales de políticas y procedimientos acordes con la norma ISO 27001. De la misma forma se incluyen documentos legales como son los consentimientos informados, los contratos, las cláusulas de protección de datos y los adendum respecto del tratamiento de la información personal.

El modelo propuesto posee un carácter referencial, por lo que se le puede facilitar la posibilidad de adaptarla a las diferentes cooperativas de ahorro y crédito permitiendo una implementación gradual en función de las necesidades de cada institución, así como del grado de madurez de las organizaciones a nivel de seguridad de la información.

CONCLUSIONES

El estudio realizado ha permitido conocer que las cooperativas del segmento 1 gestionan datos personales en distintos procesos que son críticos como el de crédito, el de tecnología de la información, el de recursos humanos o el de cobranza sin tener, en muchos casos, un tratamiento estructurado formal unificado.

A partir del análisis del ciclo de vida del dato personal, se identificaron puntos críticos de riesgo en las etapas de recolección, procesamiento, almacenamiento y transferencia con la información, lo que da cuenta de la exposición a vulnerabilidades en su tratamiento.

Se evidenció que existen brechas en el tratamiento de los datos personales en los ámbitos administrativo, técnico, organizativo y jurídico, lo que pone de manifiesto la necesidad de adoptar un enfoque integral para garantizar el cumplimiento del principio de seguridad presente en la normativa vigente.

La aplicación de una metodología fundamentada en normativa y buenas prácticas permitió identificar potenciales riesgos y estructurar de manera clara el tratamiento de los datos personales en el ámbito de las cooperativas.

Como resultado, se elaboró un Plan de Seguridad de Datos Personales de tipo referencial y alineado a la Ley Orgánica de Protección de Datos Personales que abarca políticas, procedimientos y controles orientados a la mitigación de riesgos y el fortalecimiento del cumplimiento normativo.

RECOMENDACIONES

Se sugiere a las cooperativas del segmento 1 que utilicen el Plan de Seguridad de Datos Personales como una guía básica a partir de la cual deben estructurarse la gestión de los datos personales de forma práctica. En este sentido, las cooperativas pueden adaptar el plan a sus necesidades y nivel de madurez organizacional.

Se recomienda aplicar el plan de forma progresiva, comenzando por los riesgos identificados y asignando personal a la protección de datos personales en la cooperativa.

Se puede potenciar la cultura institucional de protección de datos y seguridad de la información mediante la formación continua del personal hacia el cumplimiento de la normativa vigente y las buenas prácticas de la seguridad de la información.

También se recomienda adoptar controles tanto técnicos como organizativos que garanticen la protección de la información (gestión de accesos, backups, gestión de auditorías y control de vulnerabilidades...).

Finalmente, se propone que la documentación de la gestión de datos personales sea mantenida al día, realizar auditorías frecuentes y establecer un proceso de mejora continua que ajuste el plan en función de cambios normativos y de los avances tecnológicos.

Finalmente, se recomienda establecer un proceso de mejora continua que permita ajustar el modelo en función de cambios normativos y tecnológicos.

REFERENCIAS

Aguasanta, A. (2024). *Universidad regional Autónoma de los Andes.* Obtenido de https://dspace.uniandes.edu.ec/bitstream/123456789/17649/1/UA-SIS-PDI-001-2024.pdf

Asamblea Nacional. (2021). *Dirección Nacional de Registros Publicos.* Obtenido de https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Calder, A. (2008). *ISO/IEC 27001: A Pocket Guide.* IT Governance Publishing. Obtenido de https://itgusa.blob.core.windows.net/files/download/2020-iso270002_1%20final%20ebook.pdf

Comisión Europea. (2024). *Web Oficial de la Comisión Europea.* Obtenido de https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en?prefLang=es

Curay, F., & Flores, C. (2025). Impacto de la Ley Orgánica de Protección de Datos y la ISO 27001 en la ciberseguridad empresarial ecuatoriana. *Religación*. Obtenido de https://revista.religacion.com/index.php/religacion/article/download/1588/2144/

Dinarp. (2021). *Dirección Nacional de Registros Públicos.* Obtenido de Ley de protección de datos personales:: https://www.registrospublicos.gob.ec/programas-servicios/servicios/proyecto-de-ley-de-proteccion-de-datos/

Encalada, D. (2024). *UNIVERSIDAD TECNOLÓGICA ISRAEL.* Obtenido de https://repositorio.uisrael.edu.ec/bitstream/47000/4185/1/UISRAEL-EC-MASTER-SEG-INF-ART-%20378.242-2024-004.pdf

Enríquez, L. (2026). *SuperIntendenicia de Protección de Datos Personales.* Obtenido de SuperIntendenicia de Protección de Datos Personales: https://spdp.gob.ec/wp-content/uploads/2026/03/ggrispdp2026v2.pdf

Fuel, G. (2024). *Universidad Técnica del Norte.* Obtenido de https://repositorio.utn.edu.ec/bitstream/123456789/16197/2/PG%201875%20TRABAJO%20GRADO.pdf

International Organization for Standardization. (2022). *ISO/IEC 27001: Information security management systems.* Obtenido de https://www.iso.org/standard/27001

ISO. (2022). *ISO/IEC 27001: Information security management systems — Requirements.* Obtenido de https://www.iso.org/standard/27001

ISO/IEC. (2022). *ISO/IEC 2022.* Obtenido de https://www.danielbonina.com/wp-content/uploads/ISO-IEC-27001-2022.Espanol.pdf

López, A. (2025). *Universidad Técnica del Norte.* Obtenido de https://repositorio.utn.edu.ec/bitstream/123456789/17802/2/PG%202168%20TRABAJO%20DE%20GRADO.pdf

Organización de los Estados Americanos. (2021). *OEA.* Obtenido de https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems (NIST SP 800-30).* Obtenido de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf

Superintendencia de Economia Popular y Solidaria. (2022). *Constitución de la República del Ecuador.* Obtenido de https://www.seps.gob.ec/wp-content/uploads/SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002.pdf

Superintendencia de Economia Popular y solidaria. (2022). *Superintendencia de Economia Popular y solidaria.* Obtenido de https://www.seps.gob.ec/wp-content/uploads/SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002.pdf

Superintendencia de Protección de Datos Personales. (2026). *Guía de Gestión de riesgos y Evaluación de Impacto en el Tratamiento de Datos Personales.* Obtenido de https://spdp.gob.ec/wp-content/uploads/2026/03/ggrispdp2026v2.pdf

Vera, B. (2025). *Pontificia Universidad Católica del Ecuador.* Obtenido de https://repositorio.puce.edu.ec/server/api/core/bitstreams/c57c8f1a-a929-4c93-9c96-91995557a3b2/content

ANEXOS

Anexo 1: Ciclo de vida del dato.

Anexo 2: Matriz de riesgos y medidas de mitigación.

DESCRIPCION DEL RIESGO				Impacto	Probabilidad	Valor de Riesgo	Tratamiento	Mitigación/Controles (Plan de Trabajo)	Responsable (Rol)	Criterios del Tratamiento de datos a gran escala			
Código Evento de riesgo	Evento y/o Amenaza	Causa y/o Vulnerabilidad	Consecuencia							Permanencia	Frecuencia	Categoría del titular de datos	Alcance geográfico
T1	Incumplimiento de la normativa al no tener implementado un Sistema de Gestión Seguridad de la Información	Ausencia de controles dispuestos en las normativas de la SEPS	1) Sanciones del ente regulador 2) Afectación de la imagen institucional 3) Afectaciones y vulneraciones a la Seguridad de la Información	Alto	Alta	Crítico	Mitigar	1) Implementar el SGSI para la institución acorde a lo estipulado en la resolución de a SEPS para régimen simplificado.	OSI	Prolongada	Continua	Datos personales Datos sensibles Datos salud Datos identificativos	Nacional
T2	Incumplimiento de normativa por no contar con el Plan de Continuidad de negocio para toda la institución30	No existe un Plan de Continuidad del Negocio y existe un Plan de Contingencia incompleto para TI	1) Indisponibilidad de servicios críticos 2) Sanciones del ente regulador 3) Afectación de la imagen institucional	Alto	Alta	Crítico	Mitigar	1) Generar el Plan de Continuidad de Negocio para la institución. 2) Generar un Plan de Contingencia para TI.	Administrador de Riesgos Área de Tecnología	Prolongada	Continua	Datos personales Datos sensibles Datos salud Datos identificativos	Nacional
T3	Ataque de phising o malware por correo electrónico33-34	El servidor de correo electrónico no garantiza la detección de phishing/malware o es insuficiente o ineficiente.	1) Robo de información 2) Sanciones del ente regulador 3) Afectación de la imagen institucional 4) Afectación a sistemas de información	Alto	Alta	Crítico	Mitigar	1) Solicitar al proveedor configurar el control de phishing/malware por correo electrónico. 2) Analizar la opción de cambiar sistema de correo electrónico. 3) Capacitación constante a los funcionarios	OSI jefe de TI	Prolongada	Continua	Datos personales Datos sensibles Datos salud Datos identificativos	Nacional

T4	No contar con todos los respaldos de la información que gestiona la Cooperativa 40-41-42	El alcance en el proceso de respaldos no cubre toda la información que maneja la Cooperativa	1) Pérdida de información 2) Indisponibilidad del sistema 3) Afectación de la imagen institucional	Alto	Moderada	Alto	Mitigar	1) Crear la política de respaldos en la cual se defina el alcance de la información a respaldar, así como el proceso de validación de los mismos en restauraciones controladas y resguardo de los medios en sitios alternos.	OSI Jefe de TI	Prolongada	Continua	Datos personales Datos sensibles Datos salud Datos identificativos	Nacional
T5	Robo o Accesos no autorizados a información contenida en equipos del personal 40	La información se encuentra en las estaciones de trabajo y la información no se encuentra cifrada.	1) Robo de información 2) Sanciones del ente regulador 3) Afectación de la imagen institucional	Moderado	Moderada	Medio	Mitigar	1) Implementar tecnología de encriptación confiables (AES, 3DES - 128 o 256 bits, TDE) a nivel de archivos y/o discos de equipos que salgan de la institución como laptops.	OSI Jefe de TI	Prolongada	Continua	Datos personales Datos sensibles Datos salud Datos identificativos	Nacional
T6	Robo de información por medio de dispositivos de almacenamiento externo o el correo 37	Ausencia o falta de controles que permita saber que tipo de información se descarga a medios externos (memorias usb) o adjuntos a los correos.	1) Pérdida de información 2) Robo de información 3) Sanciones del ente regulador 4) Afectación de la imagen institucional	Moderado	Alta	Alto	Mitigar	1) Política de uso de memorias USB y correo institucional. 2) Ajustes tecnológicos para bloquear el puerto USB 3) Soluciones tecnológicas para la prevención de perdida de datos (DLP)	OSI Jefe de TI	Prolongada	Continua	Datos personales Datos sensibles Datos salud Datos identificativos	Nacional
T7	Acceso a la información de datos personales por personas no autorizadas en la base de datos 47	Ausencia de controles o tecnologías para el control de acceso por parte de un proveedor	1) Robo de información 2) Sanciones del ente regulador 3) Afectación de la imagen institucional	Alto	Alta	Crítico	Mitigar	Nacional	Jefe de TI	Prolongada	Continua	Datos personales Datos sensibles Datos salud Datos identificativos	Nacional

T8	Información desactualizada del Hardware y Software43	No contar con la información actualizada de los equipos y software de la institución	1) Pérdida de Información 2) Afectación de la imagen institucional 3) Afectación al rendimiento de los equipos informáticos 4) Mantener brechas de ciberseguridad	Alto	Alta	Crítico	Mitigar	1) Generar un inventario de hardware y software con la información relevante de la misma y llevar un control del tiempo soporte, garantías, fechas de compra al menos. 2) Revisar software innecesario en los dispositivos finales.	OSI Jefe de TI Responsable de Activos	Prolongada	Continua	Datos personales Datos sensibles Datos salud Datos identificativos	Nacional
T9	Indisponibilidad o Ataques de ciberseguridad por vulnerabilidades en el software 49	Ausencia de una política y automatización de actualización de parches de seguridad.	1) Pérdida de información 2) Robo de información 3) Sanciones del ente regulador 4) Afectación de la imagen institucional 5) Mantener brechas de ciberseguridad	Alto	Alta	Crítico	Mitigar	1) Implementar una política para el proceso de parches de seguridad a la infraestructura tecnológica. 2) Configurar el Windows Update en los equipos y servidores Windows.	Jefe de TI	Prolongada	Continua	Datos personales Datos sensibles Datos salud Datos identificativos	Nacional
T10	Ataques cibernéticos por vulnerabilidades en los equipos/servicios expuestos a Internet 31-32	No se cuenta con una política para chequeos periódicos de vulnerabilidades o Ethical Hacking	1) Pérdida de información 2) Robo de información 3) Sanciones del ente regulador 4) Afectación de la imagen institucional 5) Afectación a la disponibilidad del sistema	Catastrófico	Alta	Crítico	Mitigar	1) Implementar una política para el proceso de escaneos de vulnerabilidades. 2) Ejecutar un proceso de Ethical Hacking conforme a la normativa.	OSI Jefe de TI Auditor de TI	Prolongada	Continua	Datos personales Datos sensibles Datos salud Datos identificativos	Nacional

T11	Accesos indebidos a datos personales por perfiles inadecuados 49	Ausencia de una política para redefinir los roles y perfiles basados en la gestión de datos personales. Sistemas de información no contemplan roles y perfiles de usuarios basados en datos personales	1) Robo de información 2) Afectación de la imagen institucional	Alto	Alta	Crítico	Mitigar	1) Política de gestión de roles y perfiles de usuarios en los sistemas de información basados en el uso de datos personales. 2) Ajustes a los sistemas de información para creación de roles/perfiles basados en la gestión de datos personales	OSI Jefe de TI	Prolongada	Continua	Datos personales Datos sensibles Datos salud Datos identificativos	Nacional
T12	Accesos indebidos o fraudulentos por claves débiles en ausencia de doble factor de autenticación51	Ausencia de política de doble factor de autenticación o gestión de claves fuertes	1) Pérdida de información 2) Robo de información 3) Afectación de la imagen institucional 4) Accesos no autorizados	Alto	Moderada	Alto	Mitigar	1) Actualizar la política de gestión de claves de usuario considerando si existe o no doble factor de autenticación. 2) Terminar de Implementar/Configurar los sistemas de información con doble factor de autenticación donde aplique.	OSI Jefe de TI	Prolongada	Continua	Datos personales Datos sensibles Datos salud Datos identificativos	Nacional
T13	Perdida de visibilidad de la transaccionalidad de los usuarios en el sistema de información core48	No se está usando las opciones de log o auditoría que permita obtener la suficiente información en caso de incidencias de seguridad relacionado a datos personales.	1) Pérdida de información 2) Afectación de la imagen institucional 3) Fraudes	Alto	Alta	Crítico	Mitigar	1) Solicitar al proveedor del sistema se capacite o active las opciones de auditoria y reportes de control conforme necesidades de la institución.	OSI Jefe de TI	Prolongada	Continua	Datos personales Datos sensibles Datos salud Datos identificativos	Nacional
T14	Acceso no autorizado a equipos de los funcionarios38	Ausencia de control de bloqueo de la pantalla por un tiempo de inactividad	1) Pérdida de Información 2) Robo de información 3) Accesos no autorizados	Catastrófico	Alta	Crítico	Mitigar	1) Configurar en el AD los controles de seguridad de bloqueo de pantalla.	OSI Jefe de TI	Prolongada	Continua	Datos personales Datos sensibles Datos salud Datos identificativos	Nacional

T15	Falla en los equipos del cuarto técnico49	No todos los equipos tienen contrato de soporte y mantenimiento	1) Indisponibilidad de la información 2) Pérdida de Información 3) Afectación de la imagen institucional	Alto	Alta	Crítico	Mitigar	1) Contratar soporte y mantenimiento a equipos de centro de cómputo o al menos garantizarse que en caso de incidencias de los equipos, tengan un proveedor que le respalden.	OSI jefe de TI	Prolongada	Continua	Datos personales Datos sensibles Datos salud Datos identificativos	Nacional

Anexo 4: Plan de protección de datos

DOCUMENTACIÓN		CUMPLIMIENTO DE LA LOPDP Y RGLOPDP				
		COOPERATIVA	Procesos			
			Crédito	Recursos humanos	Cobranzas	TI
ADMINISTRATIVOS						
Registro de actividades y tratamientos (RAT)						
Inventario de datos personales						
Matriz de riesgos						
Estrategia de mitigación						
Modelo de Tratamiento a gran escala (MTGE)						
Anexos						
	Solicitud de derecho de información					
	Respuesta solicitud de derecho de información					
ORGANIZATIVOS						
Perfil del DPDP						
Plan de capacitación						
Política general de PDP						
Manual de políticas						
	Obtención de consentimiento socios y clientes					
	Obtención de consentimientos empleados y administradores					
	Uso de categorías especiales de datos personales					
	Derechos de los titulares					
	Gestión de datos personales por parte del encargado o tercero					
	Notificación de incidentes de seguridad					
	Protección de datos desde el diseño y por defecto					
Manual de Procedimientos						
	Obtención de consentimientos de socios/clientes					
	Obtención de consentimientos de empleados y administradores					
	Gestión de datos personales por parte del encargado o tercero					
	Actualización de los datos personales conforme al derecho del titular					
	Derechos de los titulares					
	Notificación de incidentes de seguridad en la entidad de control					
TÉCNICOS						
Manual de políticas						
	Gestión de roles y perfiles					
	Respaldos y restauración					
	Gestión de claves de usuarios considerando si existe o no doble factor de autenticación					

	Uso de memorias USB y Correo institucional					
	Actualización de parches					
	Escaneo de vulnerabilidades en ambientes internos y externos					
	Indicadores claves de rendimiento					
Manual de Procedimientos						
	Gestión de claves de usuarios considerando si existe o no doble factor de autenticación					
	Gestión de roles y perfiles de usuarios					
	Uso de memorias USB y Correo institucional					
	Actualización de parches					
	Indicadores claves de rendimiento					
JURIDICO						
Consentimientos						
	Consentimiento Socios					
	Consentimientos colaboradores					
	Consentimientos garantes					
	Consentimiento socios menores de edad					
Contractuales						
	Adendum Colaboradores					
	Contratos Adhesión / Contrato de pactación Encaje / Orden de Pago Licitud de fondos Formatos que contengan datos personales.					
Cláusulas y avisos						
	Mensajería instantánea					
	Cookies					
	Pie de firma de correos electrónicos					
	Anuncio Web					
	Uso de imagen					
	Convocatoria oferta de trabajo					
	Notificación de utilización de uso de datos personales					