REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

IMPLEMENTACIÓN DE LA LEY ORGANICA DE PROTECCIÓN DE DATOS PERSONALES EN LA COOPERATIVA DE AHORROY CRÉDITO "PABLO MUÑOZ VEGA" CONSIDERANDO LOS ESTÁNDARES ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC27701:2019 Y EL SGSI INSTITUCIONAL

Trabajo de Titulación previo a la obtención del Título de Magíster en Computación conmención Seguridad Informática

AUTOR:

Ing. Gerzon Vladimir Fuel Rodríguez

DIRECTOR:

MSc. Xavier Mauricio Rea Peñafiel

Ibarra, julio 2024

UNIVERSIDAD TÉCNICA DEL NORTE

DIRECCIÓN DE BIBLIOTECA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega delpresente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	0401201025		
APELLIDOS Y NOMBRES:	Fuel Rodríguez Gerzon Vladimir		
DIRECCIÓN:	Tulcán, calles Cabras e Iguan		
EMAIL:	gvfuelr@utn.edu.ec		
TELÉFONO FIJO:		TELÉFONO MÓVIL:	0993935485

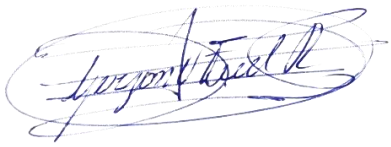
DATOS DE LA OBRA	
TÍTULO:	Implementación de la ley orgánica de protección de datos personales en la cooperativa de ahorro y crédito “Pablo Muñoz Vega” considerando los estándares ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 27701:2019 y el SGSI institucional.
AUTOR (ES):	Fuel Rodríguez Gerzon Vladimir
FECHA: DD/MM/AAAA	26/06/2024
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	( ) GRADO (X)POSGRADO
TITULO POR EL QUE OPTA:	Magister en Computación con mención en Seguridad Informática
ASESOR /DIRECTOR:	MSc. Cusme Fabian, MSc. Rea Mauricio

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y sela desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 9 días del mes de julio de 2024

EL AUTOR:



Gerzon Vladimir Fuel Rodríguez

APROBACIÓN DEL TUTOR

Yo MSc. Xavier Mauricio Peñafiel Rea en calidad de director de la tesis titulada IMPLEMENTACIÓN DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN LA COOPERATIVA DE AHORRO Y CRÉDITO "PABLO MUÑOZ VEGA" CONSIDERANDO LOS ESTÁNDARES ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 27701:2019 Y EL SGSI INSTITUCIONAL de la autoría del Ing. Gerzon Vladimir Fuel Rodríguez, para optar por el grado de Magister en computación con Mención en Seguridad Informática, doy fe de que dicho trabajo reúne los requisitos y méritos suficientes para ser sometidos a presentación privada y evaluación por parte del jurado examinador que se designe.

En la ciudad de Ibarra, a los 26 días del mes de junio del 2024

Lo certifico

Firmado electrónicamente por:
XAVIER MAURICIO REA PEÑAFIEL

MSc. Xavier Mauricio Rea Peñafiel

DIRECTOR DE TESIS

INDICE DE CONTENIDOS

INDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN EJECUTIVO

PROGRAMA DE MAESTRÍA EN COMPUTACIÓN CON MENSIÓN EN SEGURIDAD INFORMATICA

IMPLEMENTACIÓN DE LA LEY ORGANICA DE PROTECCIÓN DE DATOS PERSONALES EN LA COOPERATIVA DE AHORRO Y CRÉDITO "PABLO MUÑOZ VEGA" CONSIDERANDO LOS ESTÁNDARES ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 27701:2019 Y EL SGSI INSTITUCIONAL

Autor: Ing. Gerzon Vladimir Fuel Rodríguez
Director: MSc. Xavier Mauricio Rea Peñafiel
Año: 2024

La Cooperativa de Ahorro y Crédito Pablo Muñoz Vega enfrenta desafíos significativos en cuanto al tratamiento y protección de los datos personales de sus clientes. La falta de un adecuado análisis de riesgos, así como la ausencia de personal designado para el tratamiento y protección de datos, incluyendo un delegado de protección de datos, son preocupaciones clave que deben abordarse de manera urgente. Donde el objetivo principal de la cooperativa es cumplir con la Ley Orgánica de Protección de Datos Personales, aplicando estándares ISO/IEC para garantizar el cumplimiento del registro oficial N° 459. Se adoptó un enfoque cuantitativo para el análisis, basado en modelos que emplean aproximaciones numéricas y análisis estadísticos para identificar patrones de comportamiento y evaluar hipótesis. El proyecto se desarrolló en varias fases, incluyendo diagnóstico, modelado, control y ejecución. Se utilizó la metodología de Gestión por Procesos de Negocio (BPM) para diseñar, ejecutar, analizar y mejorar continuamente los procesos relacionados con la protección de datos. Se realizaron encuestas entre 15 empleados para recopilar información relevante. Se estableció el perfil del delegado de protección de datos, definiendo claramente sus funciones, responsabilidades y cronograma de capacitación para el personal. Se concluyó que se cumplió con las normas y regulaciones pertinentes, y se diseñó un plan estructurado de capacitación, involucrando a expertos y utilizando diversos métodos de aprendizaje. El proceso de creación del delegado de protección de datos también se completó con éxito, detallando el perfil y las responsabilidades del puesto.

Palabras Claves: Protección de datos personales, delegado de protección de datos, Gestión por Procesos de Negocio, responsabilidades del puesto.

ABSTRACT

PROGRAMA DE MAESTRÍA EN COMPUTACIÓN CON MENSIÓN EN SEGURIDAD INFORMATICA

IMPLEMENTATION OF THE ORGANIC LAW ON PERSONAL DATA PROTECTION IN THE SAVINGS AND CREDIT COOPERATIVE PABLO MUÑOZ VEGA, CONSIDERING THE STANDARS ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 27001:2019 AND THE INSTITUTIONAL SGSI

Author: Gerzon Vladimir Fuel Rodríguez
Director: Nombre completo del director
Year: 2024

The Pablo Muñoz Vega Savings and Credit Cooperative faces significant challenges regarding the treatment and protection of its customers' personal data. The lack of adequate risk analysis, as well as the absence of designated personnel for data treatment and protection, including a data protection officer, are key concerns that must be urgently addressed. The main objective of the cooperative is to comply with the Organic Law on Personal Data Protection, applying ISO/IEC standards to ensure compliance with Official Registry No. 459. A quantitative approach was adopted for the analysis, based on models that employ numerical approaches and statistical analysis to identify behavioral patterns and evaluate hypotheses. The project was developed in several phases, including diagnosis, modeling, control, and execution. Business Process Management (BPM) methodology was used to design, execute, analyze, and continuously improve processes related to data protection. Surveys were conducted among 15 employees to gather relevant information. The profile of the data protection officer was established, clearly defining their functions, responsibilities, and training schedule for staff. It was concluded that relevant standards and regulations were complied with, and a structured training plan was designed, involving experts and utilizing various learning methods. The process of creating the data protection officer was also successfully completed, detailing the profile and responsibilities of the position.

Keywords: Personal data protection, data protection officer, Business Process Management, job responsibilities.

CAPITULO I

EL PROBLEMA

1.1. Problema de investigación

1.1.1. Contextualización

A nivel mundial, la protección de datos tienen políticas establecidas, donde los principios vinculados con el procesamiento de los datos personales, son de interés del Alto Comisionado de las Naciones Unidas para los Refugiados (ACNUR), el cual protege a las personas forzadas a huir de sus hogares así como a las repatriadas, por lo que este comisionado, trabaja en más de 100 países, con su sede está en Ginebra, Suiza, estableciendo la confidencialidad de los datos personales, garantizando e implementando un alto nivel de seguridad de los datos, que se adecue a los riesgos que entraña la naturaleza y el procesamiento, cubriendo dichos nombramientos de forma segura, evitando la divulgación no autorizada o acceso a los datos personales en forma accidental, ilícita e ilegítima (ACNUR, 2015).

Referente a Latino América, la protección de datos, en países como en Argentina se da la reforma a la Ley Nº 25.326 útil para alinear sus disposiciones; la cual tiene por objeto la protección integral de los datos personales, que busca incorporar derechos a oponerse o restringir el tratamiento de sus datos personales y el derecho a la portabilidad. (Pascual et al., 2000) En tanto que, en Brasil, a partir del año 2018, se aplica la Ley General de Protección de Datos de Brasil, obligando a las empresas, a tratar los datos de protección de datos, pudiendo imponer una multa de hasta el 2% de los ingresos en el último año fiscal; así como en Colombia se establece un doble régimen de protección de datos personales, descritas en las Leyes de Privacidad Colombianas, en la Ley 1581 del 2012. (Blake, 2019)

Mientras que en Ecuador, se tiene la Ley Orgánica de Protección de Datos Personales, definida, en el Registro Oficial 459 del 26 de mayo del 2021; el cual se da en el capítulo I, en el ámbito de Aplicación Integral, en el artículo 1, el cual indica el objeto y la finalidad de la presente ley, la cual debe garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección, Para dicho efecto regula, prevé y desarrolla

principios, derechos, obligaciones y mecanismos de tutela; mientras que en el artículo 7, indica el tratamiento legítimo de datos de personas, si se cumple con el consentimiento del titular, para el tratamiento de sus datos personales. En tanto que en el capítulo IV, están las categorías especiales de datos, donde se consideran datos sensibles, datos de niñas, niños y adolescentes, datos de salud y datos de personas con discapacidad. En tanto que en el capítulo VI, en seguridad de datos personales, registradas en el artículo 37, indica que el responsable o encargado del tratamiento de datos personales según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos (Asamblea Nacional de la República del Ecuador, 2021).

Se debe tener, presente que el Ecuador, es uno de los pocos países que no ha firmado el Acuerdo de Budapest, que le permite rastrear a los ciber-delincuentes internacionales (Zavala, 2021, pág. 1). Por lo que el Convenio de Budapest sobre la Ciberdelincuencia, se trata de un acuerdo internacional, útil para combatir la delincuencia organizada transnacional, especialmente la delincuencia informática, con el objetivo de establecer un derecho y procedimiento penal uniforme para los estados miembros. Por lo que se considera un punto de referencia, indispensable en los esfuerzos, de la comunidad internacional, para fortalecer el estado de derecho en el ciberespacio. Por lo que su objetivo principal, es crear un código penal internacional, para salvaguardar contra el ciberdelito. Además de aprobar una legislación específica, la cual tiene como objetivo desarrollar nuevos métodos de colaboración internacional en la lucha contra el ciberdelito (Convenio de Ciberdelincuencia del Consejo de Europa, 2014, pág. 1).

Esta ley orgánica, ha sido motivada para el cumplimiento del derecho a la protección de datos personales garantizado en la Constitución de la República del Ecuador; en uno de los ejes de la estrategia acordado en el año 2016 de la red Iberoamericana de Datos Personales 2020; en los estándares de Protección de Datos Personales para los estados Iberoamericanos, aprobados el 2 de junio de 2017; en la propuesta de declaración de principios de privacidad y protección de datos personales en las Américas, adoptado por el comité jurídico de la Organización de Estados Americanos; con el objetivo de precautelar el derecho que tienen los ciudadanos a relacionarse electrónicamente con el Estado; y , en la Estrategia tres del programa de gobierno abierto del Plan Nacional de

Gobierno electrónico apunta a "Impulsar la protección de la información y datos personales (Alonso, 2023).

La Cooperativa de Ahorro y Crédito Pablo Muñoz Vega, no dispone de un correcto tratamiento para el análisis de riesgos, vulnerabilidades y amenazas de los datos personales de los clientes, de igual manera no se cuenta con el personal responsable encargado del tratamiento de datos personales ni el delegado de protección de datos personales.

1.1.2. Planteamiento del problema

En Ecuador hablar de protección de datos, parece un tema relativamente nuevo, aunque desde el 2008 la constitución de la República garantiza a los ecuatorianos el derecho a que sus datos sean protegidos. A pesar de que durante muchos años se limitó la previsión legal sobre el mencionado derecho y su tratamiento, finalmente el 26 de mayo de 2021, la Asamblea Nacional aprobó la ley orgánica de protección de datos personales. (Asamblea Nacional de la República del Ecuador, 2021)

En Ecuador, las amenazas de la era digital se manifiestan en el robo, ataque o divulgación ilegal de bases de datos públicas y privadas, lo que genera numerosas pérdidas económicas y sociales. (Carvajal, 2022) Ante esta realidad, diversos sectores han reclamado un sistema de protección de datos personales que cumpla con los estándares internacionales; proteger los derechos básicos de sus ciudadanos, y así construir un país confiable para transferir este tipo de datos, que hoy es la base de las relaciones comerciales y de cooperación internacional.

1.2. Interrogantes de la investigación

Por lo que las interrogantes son:

- ¿El tratamiento de la información dentro de la La Cooperativa de Ahorro y Crédito Pablo Muñoz Vega, se alinea a la actual ley de protección de datos personales?

- ¿Dará buenos resultados la metodología BPM, en el diseño de proceso de tratamiento de datos personales para dar cumplimiento al registro oficial N° 459, en la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega?

- ¿En la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega, se dará el cumplimiento a las normas utilizadas, a través de capacitaciones de alto nivel al personal de la institución?

- ¿La creación de un puesto de delegado llevará a un mejor cumplimiento de las normas de protección?

1.3. Objetivo de la investigación

1.3.1. Objetivo general

Implementar la Ley Orgánica de Protección de Datos Personales en la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega aplicando estándares ISO/IEC para dar cumplimiento con el registro oficial N° 459.

1.3.2. Objetivos específicos

- Analizar el ciclo actual del tratamiento de la información en la institución.

- Aplicar la metodología BPM, en el diseño de proceso de tratamiento de datos personales para con esto dar cumplimiento al registro oficial N° 459.

- Dar cumplimiento a las normas utilizadas, a través de capacitaciones de alto nivel al personal de la institución.

- Proponer la creación del puesto del delegado de protección de datos personales en Cooperativas de Ahorro y crédito Pablo Muñoz Vega.

1.4. Justificación

El derecho a la protección de datos ha sido objeto de cambios normativos drásticos desde que la Declaración Universal de los Derechos Humanos del 10 de diciembre de 1948, en París, tuviera su primer precursor en el artículo 12. Por lo que ninguna persona

será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, o ataques a su honor o reputación. Por lo que toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques. (Del Valle et al., 2011)

Se debe indicar, además que el Gobierno Nacional, actualmente permite acceder a los ecuatorianos, a servicios digitales con mayor seguridad y fortalecer la protección de sus datos personales, siguiendo las Estrategias Nacionales de Ciberseguridad, en función de seis ejes de acción, los cuales abarcan temas como Gobernanza y coordinación Nacional; Resiliencia cibernética; Lucha contra la ciberdelincuencia; Ciberdefensa nacional y ciberdelincuencia; Habilidades y capacidades de ciberseguridad; y Cooperación internacional (Sistema Nacional de Información, 2022).

En la primera etapa de estipulación, la protección de los datos personales está relacionada con el uso de la informática y "el impacto de muchos datos o el conocimiento preciso enviado al alcance cercano al propietario. Por lo que, este principio es garantizar el control de la información, almacenado en la base de datos y en todos los sitios web que se han registrado (Mayorga et al., 2019).

El impacto de introducir la legislación orgánica en materia de protección de datos, en el régimen ecuatoriano es enorme, especialmente para los responsables del tratamiento de datos de terceros, por lo que el tema de investigación es relevante para las empresas u organizaciones del sector privado, pues es necesario identificar los desafíos asociados, así como establecer los mejores medios y herramientas legales para cumplir con la ley y evitar la sanción.

La línea de investigación en la cual se basará el proyecto es la seguridad informática mediante la aplicación de estándares ISO/IEC 27001:2022, ISO/IEC 27002:2002, ISO/IEC 27701:2019 y SGSI institucional.

CAPITULO II

MARCO REFERENCIAL

2.1. Antecedentes

Como antecedentes se tiene:

Según Godoy (2017), en la Revista de Derecho, con la temática titulada como "El dato personal como presupuesto del derecho a la protección de datos personales y del habeas data en el Ecuador" dice que el artículo 66, con el numeral 19 de la Constitución de la República del Ecuador (CRE), define tanto los datos como la información de una persona natural como requisito previo al derecho a la protección de datos personales. Del mismo modo, el art. 92 de la CRE, relativo al hábeas data, trata de la protección de documentos, datos genéticos, bancos o archivos de datos personales y registros relativos a una persona o su propiedad en forma caso por caso.

En tanto que, Álvarez (2017), en su investigación conocido como Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales, indica que el Ecuador, de emergencia necesita el derecho de proteger los datos personales, de los ciudadanos y promover el desarrollo de sus servicios, que pueden ser tratados con ciudadanos de todo el mundo. Pero desafortunadamente, tiene deficiencias razonables que deben mejorarse en el futuro por las regulaciones del país, que permita superar sus fallas legales, donde los miembros deben comprender la naturaleza superior, de este campo legal, donde la necesidad de obtener asesoramiento completo sobre ese tema.

Mientras que, Gómez y Montoya (2018), en su proyecto con título como Propuesta de implementación y cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), a través de la plataforma de Protección de Datos Personales en Posición de INFOTEC, detallan que la protección de datos personales, es un derecho básico de una persona, por lo que se entiende como un maestro con información sobre el almacenamiento, y opone a su uso y apelación, en contraste con la seguridad, que es el derecho que una persona no debe molestar, el cual está formado por el gobierno apropiado; donde la luz de los criterios debe utilizarse para usar y proteger los datos personales, que permitan alentar el cumplimiento de las reglas aplicadas en este campo, siempre buscando que se las coloque en las reglas.

De acuerdo con Merizalde (2018), en su proyecto titulado como “Protección Legal de Datos Personales y a la Reserva de Información Personal, y su Transferencia sin Consentimiento de su Titular”; dice que en el Ecuador actualmente existe una dispersión jurídica, es decir, una serie de disposiciones constitucionales, penales, administrativas e incluso estatutarias, citadas y analizadas durante la elaboración de esta tesis, encaminadas a que la finalidad de protección de los datos personales se encuentre en las bases de datos de organizaciones, son en su mayoría públicos, pero estas normas no garantizan la protección física y completa de los datos personales, y en este sentido, el derecho a la privacidad del titular de la información. En consecuencia, la mayor parte de la normativa, vigente encaminada a garantizar la protección jurídica de los datos personales es de carácter público, es decir, prácticamente no existe una normativa que regule el tratamiento de datos personales, en las organizaciones de la entidad privada y esto permite que la mitad de la información utilizada para quedar desprotegidos, por lo que se aplica principalmente la normativa en cuanto al manejo de datos personales sensibles.

En tanto, que Castro (2019), en su investigación titulada como Protección de datos personales a través de herramientas de procesamiento automatizado de datos: desafíos y recomendaciones, se refiere a la introducción de la tecnología en muchos aspectos de la vida ha contribuido a cambios en la comprensión del mundo, en las relaciones comerciales, en la dinámica económica y social y, por supuesto, en el derecho. Algunas de estas transformaciones comienzan con la dualidad compatible entre el mundo digital y el físico. Sin embargo, el ciberespacio muestra un gran potencial para conectar a un gran número de personas, influir en ellas y analizar su información. Esto ha creado una nueva economía basada en datos. Por lo que la competencia entre los actores tecnológicos ha amenazado y continúa amenazando la privacidad de las personas cuyos datos se recopilan, almacenan o procesan mediante tecnología informática. Si bien las normas jurídicas han evolucionado como primera solución a los problemas sociales de un momento histórico determinado, su eficacia no radica en su mera existencia.

Ordóñez (2020), en su proyecto titulado como “El derecho fundamental a la protección de datos personales en ecuador. Situación actual y presupuestos para la formulación de un marco jurídico que asegure un nivel adecuado de protección”, indica que, dado que el derecho a la protección de datos es de suma importancia en el sector tecnológico, en una sociedad en red, también requiere una serie de poderes para garantizar el control, la propiedad de los datos personales y la privacidad de las personas. Por ello,

es necesario que la Ley no sea ajena a esta realidad y que, en todos los casos, las personas, organizaciones, organismos y unidades, que tienen contacto directo con menores de edad, sean conscientes de esta realidad y cuenten con un mecanismo de acción para implementarla. Por lo que, en cualquier caso, se reconoce que "esta forma de intimidad no se considera un valor intrínseco, sino auto determinado del sujeto", en las relaciones infantiles debido a la insensibilidad, generada por el intercambio de datos personales, de menores en el entorno digital.

Según Burbano (2021), en su proyecto titulado como “Diseño de un marco de trabajo para el análisis de impacto del proyecto de Ley de protección de datos en el Ecuador en empresas privadas”, especifica que para publicar la Ley Orgánica de Datos Personales de una manera práctica, debe establecer tareas claves, las cuales son atendidas por las empresas privadas y públicas, con lo cual deberán tomar medidas legales, técnicas y organizativas; para proteger los datos proporcionados por los ciudadanos a nivel, junto con el desarrollo del negocio en un plazo de 2 años, en el cual está incluida la recopilación, el procesamiento, el almacenamiento y cualquier forma de procesamiento, que tenga lugar en datos particulares. Por lo que, esta ley plantea grandes desafíos a las empresas privadas y al sector público, ya que deben tomar medidas legales, técnicas y organizativas en un plazo de 2 años, para proteger los datos en poder del público proporcionados, en el proceso de desarrollo comercial, incluyendo la recogida, el tratamiento, el registro y cualquier forma de tratamiento que se realice con determinados datos. Por lo tanto, las empresas necesitan alinear sus iniciativas y objetivos con la estrategia comercial de cada organización para obtener buenos resultados, de modo que en los casos de implementación se puede ver que las empresas, tienden a sobre forzar las políticas, normas y procedimientos de seguridad, a través de estructuras organizativas y de seguridad; buscan mejorar no solo sus políticas y procesos comerciales, sino también la protección de los datos que los clientes confían.

En tanto que Villena (2022), en su investigación doctoral detallada como, Protección de los datos personales e intimidad de las personas trabajadoras: problemática ante el uso de TIC en el trabajo y perspectivas para una defensa efectiva, dice que al considerarse honorables y merecedores de respeto, los empleados son titulares incondicionales de derechos fundamentales e inalienables: derechos personales, incluido el derecho a la privacidad y a la protección de sus datos personales. Por lo que ambos derechos, han estado cubiertos por un único conjunto de leyes que brindan protección a

escala nacional y global durante muchos años. Por lo que, es imposible darse cuenta de la escala específica del impacto y el alcance de la implementación, de la privacidad de los empleados y la protección de datos personales, vinculados con el uso de TI en el lugar de trabajo.

De igual manera, Díaz (2022), en su investigación titulada como La aplicación de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos en el aumento de costos de servicios electrónicos agregados por parte de la operadora telefónica Claro Ecuador en la ciudad de Quito en el año 2020, dice que el Art. 48, el usuario o consumidor, al otorgar o confirmar electrónicamente su consentimiento, debe demostrar razonablemente que puede acceder a la información objeto de su consentimiento las disposiciones son exactas razón por la cual no cabe realizar un análisis pues resalta el objeto y alcance del significado de consentimiento, los mismos que, al no recibir una directriz por parte de los operadores telefónicos generarían una ineficacia del consentimiento y podría este numeral resolver parte de un derecho vulnerado de un usuario/a o consumidor; en el artículo 1, del Reglamento general a la Ley de Comercio Electrónico, Firmas y Mensaje de Datos, Indica que la es responsabilidad del operador telefónico entregar y tener disponible la información de cada consumidor/a cuando éste lo requiera para solventar dudas de la relación contractual.

En tanto que Cano y Jaramillo (2023), en su artículo científico titulado como Análisis sobre el consentimiento del titular bajo la Ley de Protección de Datos Personales, dicen que el derecho a proteger los datos personales se ha convertido no solo en una máxima prioridad, sino también en un problema para los usuarios de todo el mundo. Esto se debe a la globalización y al avance tecnológico diario. Entonces se convierte en una necesidad social porque sin una buena gestión de los datos, se pueden vulnerar los derechos de los propietarios de los datos. Para prevenir la vulneración de derechos, es importante asegurarse de que los datos se recopilan correctamente y, por tanto, establecer un proceso adecuado para otorgar el consentimiento del titular de la información, que debe ser indiscutible. Por lo tanto, el trabajo se centrará en demostrar la importancia del consentimiento en la protección de datos y cómo se maneja en el régimen ecuatoriano.

De igual manera el Banco Bolivariano (2023), referente a las Política para el tratamiento de datos personales del Banco Bolivariano C.A., dice que dicho banco, como responsable del tratamiento, se garantizará la seguridad y calidad del procesamiento de la

información de conformidad con las normas aplicables y demás normas que las modifican, complementándose. Donde sin perjuicio del cumplimiento de las normas sobre secreto bancario o reservas establecidas en el Código Orgánico Monetario y Financiero, Banco Bolivariano C.A., como una institución financiera privada, la cual describe, los principios generales que se implementarán, para proteger los datos personales de los titulares de la información y garantizar el correcto procesamiento de dichos datos. Por lo que se basará en el consentimiento del titular, el cual tendrá finalidades claramente definidas, salvo las excepciones previstas en sus normas.

Mientras que, Guerra y Navarrete (2023), en su proyecto titulado como Propuesta de un plan de cumplimiento del delgado de protección de datos personales en una empresa ecuatoriana de telecomunicaciones, 2022, dicen que el plan de cumplimiento del Delegado de Protección de Datos (DPD), elaborado en este artículo, muestra que la empresa de telecomunicaciones cuenta con dos tipos de medidas macro: una medida preventiva y una medida remedial, siendo la primera parte del despliegue declarado vigente al momento de la publicación, bajo la Ley Orgánica de Protección de Datos Personales (LOPDP); y la segunda macro operación corresponde a acciones y procesos continuos que no se agotan con el primer despliegue, pero que, por la dinámica de los datos, requieren un seguimiento continuo en el tiempo.

Finalmente, Limones y Peralta (2023), en el trabajo titulado como 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, detalla que se puede demostrar que las leyes de Ecuador y Uruguay tienen muchas similitudes y superposiciones. Por lo que es importante señalar que el Reglamento Europeo, también sirve como guía y hoja de ruta para el desarrollo de la legislación en cada país, ya que el continente es pionero en definir e incorporar derechos de privacidad. Aunque este estudio sólo se centró en dos países de América del Sur, por lo que es razonable extenderlo a otras regiones. Donde los altos funcionarios de las organizaciones están cada vez más involucrados, por lo que son más conscientes de la información y los datos de su organización y de las posibles repercusiones legales del incumplimiento. En consecuencia, los métodos de tratamiento que podrán aplicarse a los datos personales; sin embargo, la seguridad de los datos no está garantizada.

2.2. Marco teórico

2.2.1. Estándares ISO

2.2.1.1. Estándar ISO/IEC 27001:2022

Según este estándar, define los requisitos para una gestión eficaz de los riesgos que pueden afectar a la confidencialidad, la integridad y la disponibilidad de la información. (Intedya, 2022)

Este estándar se emplea cuando la PROTECCIÓN DE LA INFORMACIÓN ES CRÍTICA, como en los campos del gobierno, la banca y las finanzas, en el ambiente del derecho, la atención médica, las empresas de servicios de tecnología de la información o las comunicaciones o cualquier otra área donde los activos de información deben protegerse adecuadamente. Intedya, 2022)

Según Intedya (2022), esta norma implica:

- Identificar las responsabilidades para la protección de activos, gestión de riesgos y el cumplimiento de las políticas.
- Mantener el contacto con las autoridades y grupos de interés necesarios.
- Identificar las políticas y medidas de seguridad relacionadas con el uso de dispositivos móviles y el trabajo remoto.
- Gestionar los activos mediante inventario y establecer las reglas de uso adecuadas.
- Clasificar y etiquetar la información, gestionando el transporte y la manipulación de medios móviles.
- Gestionar la vinculación con el departamento de recursos humanos antes, durante y después de establecer relaciones laborales.
- Implementar y probar sistemas de seguridad contra incendio, inundación, corte de energía, acceso no autorizado, etc.
- Definir procedimientos de revisión y gestión de redes y reglas de intercambio de información.
- Gestionar las vulnerabilidades del sistema y de las aplicaciones web con actualizaciones de seguridad.

- Gestionar controles criptográficos como firmas digitales, certificados, marcas de tiempo, entre otros.
- Controlar los procedimientos de acceso e inicio de sesión seguros, así como la autorización de usuarios, pudiendo definir políticas de contraseñas seguras.
- Monitoreo de rendimiento, control de cambios, copias de seguridad, antivirus y sincronización de reloj.
- Ejecutar pruebas de seguridad con evaluación de vulnerabilidad.
- Los mecanismos de planificación y prueba, aseguran la continuidad de sus trabajos, manteniendo reservas de recursos para asegurar la disponibilidad.
- Establecer requisitos con proveedores, incluidos servicios en la nube, asegurando la cadena de suministro de TIC.
- Identificar y gestionar los requisitos legales, con especial énfasis en la protección de datos personales y propiedad intelectual.
- Monitorear eventos e incidentes de seguridad de la información, incluida la comunicación, evaluación, clasificación, respuesta, capacitación y recopilación de evidencia.

2.2.1.2. Estándar ISO/IEC 27002:2002

Se centra en las medidas de seguridad requeridas para proteger la información, cubriendo algunas áreas como la gestión de riesgos, la seguridad física, la seguridad de la red y la seguridad de la información.

La principal diferencia entre ISO 27001 y la ISO 27002 es que ISO 27001 es un estándar riguroso, en tanto que la ISO 27002 es un estándar guía. ISO 27001 especifica los requisitos que un SGSI debe cumplir para ser eficaz, en tanto que el ISO 27002 proporciona orientación sobre la implementación de los controles necesarios para cumplir con estos requisitos. (CYNTHUS, 2023)

Según CYNTHUS (2023), detalla que los nuevos controles de la ISO/IEC 27002:2022 incluyen:

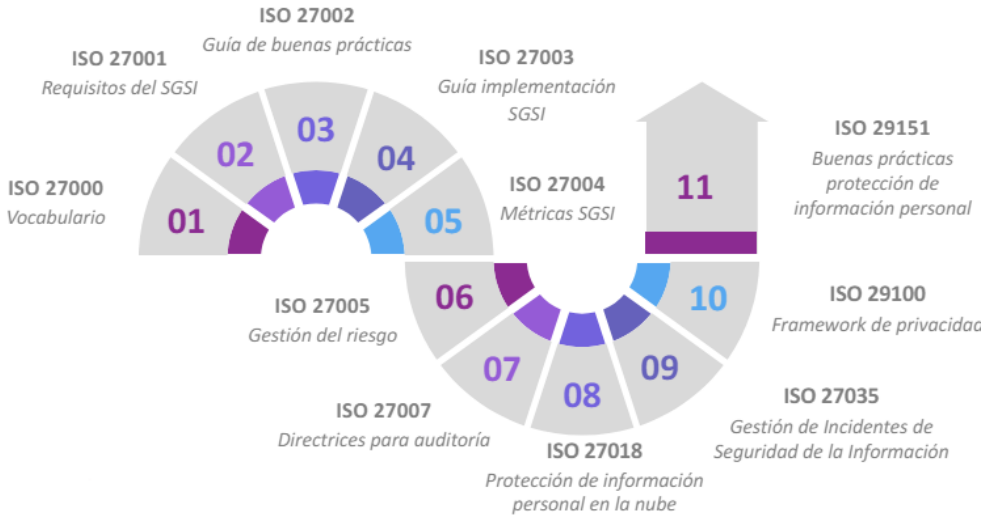
- Información sobre amenazas.
- Seguridad al utilizar servicios en la nube.

- Prepararse para garantizar la continuidad del negocio.
- Monitoreo de seguridad física.
- Gestión de configuración.
- Exclusión de la información.
- Ocultamiento de datos.
- Prevenir fugas de datos.
- Supervisión de las actividades.
- Filtrado web.
- Código de seguridad.

2.2.1.3. Estándar ISO/IEC 27701:2019

El estándar ISO/IEC 27701:2019, como se indica en la figura 1, se proporciona un determinado marco para un Sistema de Gestión de la Seguridad de la Información (SGSI), que sugiere mantener la confidencialidad, integridad y disponibilidad de la información cumpliendo una determinada legislación. (Padilla, 2019)

Figura 1.
Familia de normas 27000



Nota: Tomado de Padilla (2019)

Según Padilla (2019), detalla que los requisitos generales son:

- Estructura del documento, la cual describe la estructura del documento
- Aplicación de los controles, esto detalla que indican controles y objetivos de control de ISO 27002 que sería modificados
- Aplicación, detalla las cláusulas que serán modificadas y ampliadas con elementos

- Cliente; especifica las formas en que debe entenderse el término denominado cliente.

2.2.1.4. SGSI institucional

El tema tradicionalmente conocido como "seguridad informática" se ha desarrollado a un ritmo vertiginoso en 60 años, por agitada historia de las computadoras y la informática. El objetivo original de proteger los costosos equipos de procesamiento de datos de los años 1950 y 1960 contra daños accidentales o intencionados ha quedado obsoleto por muchas razones. La prioridad hoy es proteger la información como un recurso importante de toda organización en muchos aspectos: disponibilidad, integridad, confidencialidad y autenticidad (ACID). (Colegio Oficial de Ingenieros de Telecomunicación, 2009)

Por ello, es necesario desarrollar el concepto de Sistema de Gestión de Seguridad de la Información (SGSI-SGSI = Sistema de Gestión de Seguridad de la Información), que no sólo resuelva problemas (debilidades, amenazas, incidentes, etc.) del componente tecnológico (seguridad TIC), sino que también lo hace adoptando un enfoque global, que también tiene en cuenta otros aspectos: regulatorios, legales, organizativos e incluso (y sobre todo) culturales, y cómo su enfoque parte de una visión de un problema empresarial. (Colegio Oficial de Ingenieros de Telecomunicación, 2009)

2.2.2. Información

La información es una colección organizada de datos relevantes de los cuales uno o más agentes extraen conocimiento. Es decir, es una secuencia de conocimiento que se imparte, comparte o transmite, y por lo tanto constituye una especie de mensaje. Sin embargo, su definición varía según la disciplina o el enfoque del que provenga. (Etecé, 2020)

Según Etecé (2020), los tipos de información son:

- **Información confidencial o clasificada.** Se trata algo a lo que solo tiene acceso un pequeño grupo de personas, debido al carácter confidencial, peligroso, secreto o privado de los datos que contiene.

- **Información pública.** Se trata de que uno permita, compartir contenido con cualquier persona, sin permisos especiales y sin ningún grado de privacidad.

- **Información personal.** Proviene de un individuo en particular, quién puede decidir compartirlo o a quién.

- **Información externa.** Es algo que proviene de una agencia, organización o empresa y los destinatarios, dirigidos a las agencias o personas externas.

- **Información interna.** Coincide con el órgano, la institución o la empresa para que puedan usarse dentro sin un delito fuera de la organización.

2.2.3. Conocimiento

Se trata de la percepción y el comportamiento cognitivo de la realidad corresponden a la actividad humana básica. Por lo que los mecanismos de enseñanza y aprendizaje se construyen en torno a esta capacidad, es decir, la construcción de dicho conocimiento (Güere, 2020).

2.2.3.1. Características del conocimiento

Las características principales del conocimiento, según Güere (2020), son:

a) **Objetiva,** se trata de buscar conocer o revelar toda acción humana de manera coherente con la realidad.

b) **Universal,** es el producto de todo un proceso científico que va de lo particular a lo general o lo universal.

c) **Necesario,** se trata de encargar de contextualizar cada conocimiento en función de las necesidades de cada sociedad, pueblo o grupo de personas.

d) **Fundamentado,** se trata de la ubicación o pre-referenciando diferentes ubicaciones.

2.2.3.2. Niveles de conocimiento

Los niveles de conocimiento según Güere (2020), son:

a) **Empírico,** este es un conocimiento establecido en la experiencia y tiene un grado de ingenuidad. Por lo que este tipo o grado de comprensión se manifiesta, a través de una forma un tanto superficial e ingenua de afrontar y comprender la realidad.

b) **Filosófico,** es el nivel que resume el conocimiento y la experiencia. Corresponde también a la naturaleza de la trascendencia y, sobre todo, permite el desarrollo de preguntas adecuadas para la reflexión, el cuestionamiento o la crítica constantes, así como a los eventos y fenómenos en el nivel del conocimiento filosófico.

c) **Científico,** este es el nivel que favorece la selección metódica y experimental de los análisis en función de la realidad. Así que esto es parte de una serie de estudios objetivos y experimentales. Donde se planifiquen y materialicen métodos y técnicas para codificar la realidad de modo que se puedan demostrar diversas actividades centradas en el conocimiento.

2.2.4. Comparación de la gestión de la información y gestión del conocimiento

La comparación de la gestión de la información y gestión del conocimiento, como se indica en la Tabla 1 es:

Tabla 1.

Comparación de la gestión de la información y del conocimiento

Gestión de la Información	Gestión del Conocimiento
Se enfoca en crear, orquestar, almacenar o asegurar, y recuperar información tanto interna como externa.	Se enfoca en el uso de información y datos creados, o existentes dentro de la organización, incluyendo el conocimiento tácito y explícito.
Su propósito es optimizar la utilidad y la contribución, de las fuentes de información, al logro de los objetivos organizacionales, mediante la creación de canales y medios de transmisión y acceso a la información.	Su objetivo, es desarrollar estrategias, procesos, estructuras y sistemas que permitan a la organización utilizar el conocimiento que poseen sus miembros para crear valor en la gestión de los clientes y la sociedad.

Se enfoca en los procesos de selección, localización, análisis, almacenamiento, búsqueda, recuperación, distribución y mantenimiento de la información, generada dentro de una empresa u organización.	Se centra en la acción y la toma de decisiones.
Garantiza el acceso a la información, para su uso después de pasar por los procesos anteriores.	Aseguran, que la organización retenga el máximo conocimiento, de cada empleado, para que permanezca disponible, después de que se vayan, animando a los miembros de la organización a mejorar y compartir el conocimiento.

Fuente: (CEPAL, 2020)

2.2.5. Ciberseguridad

Se refiere al eliminar las amenazas a la información procesada, almacenada y transportada por sistemas de información interconectados, puede proteger sus recursos de información. (Jaramillo, 2022).

2.2.6. Dato personal

Son los principios, que nos hacen individuos. Por lo que incluye toda la información relevante sobre una persona que permite ser identificada. La información se considera relevante para una persona física, cuando es suficiente para que reconozcamos a la persona física a la que se refieren los datos.

Por lo que se trata del manejo de información empleada sobre personas, independientemente de cómo se recopile, almacene, procese, use, registre o transfiera esa información a otros terceros. Por lo que es el elemento fundamental, para determinar que se trata de datos personales, como la información que, por sí sola o en combinación, hace posible conocer los datos de una persona en particular, al ser directamente identificada con determinados datos o identificable de otra manera. (Cristea, 2018).

2.2.6.1. Clasificación de los datos personales

La clasificación de los datos personales, según Bravo y Pérez (2018) es:

a) Datos personales íntimos.

Se tratan de tener en cuenta, la información relacionada, con la naturaleza interior de una persona (es decir, revelar las emociones, creencias y pensamientos privados de las personas). Por lo tanto, son partes del organismo, que se revelan sólo de manera distinta y específica y rara vez son objeto de circulación pública.

b) Datos personales públicos.

Se trata de información que, como su nombre indica, por lo que incluye información o datos que se encuentran actualmente en circulación o son conocidos, por el público ya que circulan en diversas formas y aparecen en diversos documentos (públicos o privados, en papel y cada vez más populares en formato electrónico y medios de comunicación).

2.2.6.2. Derecho a la intimidad

Este es un derecho fundamental que, en la Constitución en el artículo 66 numeral 20, protege explícitamente. Por lo que se esfuerza por proteger la privacidad humana, así como por garantizar la seguridad de los datos privados. Por lo que la configuración del derecho a la protección, de datos como un derecho fundamental, independiente y autónomo a la intimidad, la cual adopta un enfoque puramente constitucional, incluyendo la protección, del sector, en el que se encuentran sus aspectos singulares y reconocidos, más protectores del desarrollo de la vida humana, como dirección, método de contacto y otros (Díaz & Fonseca, 2019).

2.2.6.3. Datos personales sensibles

Pertenece a una categoría, más estrecha que incluye datos, sobre los aspectos más íntimos de las personas. Según el contexto cultural, social o político, esta categoría puede incluir, por ejemplo, datos sobre salud personal, preferencias o vida sexuales, creencias religiosas, filosofías o ética, afiliación sindical, datos genéticos, datos biométricos para identificar de forma única un cuerpo físico, opiniones políticas u origen racial o étnico, información de cuentas bancarias, documentos oficiales, información obtenida de niños,

o ubicación geográfica personal. En determinados casos, estos datos pueden ser considerados merecedores de una protección especial porque la mala manipulación o divulgación de los datos podría causar un daño grave a una persona o discriminarla de forma ilícita o arbitraria (OEA, 2021).

2.2.6.4. Vulnerabilidad de la seguridad de datos personales

La creciente frecuencia de ataques externos ("violaciones de datos personales"), que implican el acceso no autorizado a datos protegidos, plantea preocupaciones sobre la privacidad e incluso sanciones penales. En tales casos, el Controlador de datos debe notificar a las personas cuyos Datos han sido (o pueden haber sido) comprometidos, así como a las autoridades civiles o penales pertinentes. En muchos países, incluidos los estados miembros de la OEA, la ley exige la notificación en tales casos (OEA, 2021).

2.2.6.5. Datos personales no sensibles

Se refieren a los datos más generales, del titular, más allá de las características físicas del mismo.

Por lo que, según Díaz y Fonseca (2019), estas se dividen en:

- Datos de identificación: se refiere a datos que pueden utilizarse para distinguir a una persona de otra, como nombre, apellido, nacionalidad, DNI, edad, dirección, número de teléfono, dirección de correo electrónico, firma, fecha de nacimiento, etc.

- Datos académicos: esta información se relaciona con la educación que un individuo ha obtenido a lo largo de su vida, como niveles de educación superior, títulos, nombres de centros de capacitación, certificados de seminarios o clases magistrales, etc.

- Datos de movimientos migratorios: se trata de la información sobre entrada y salida del país de origen.

- Datos patrimoniales: son las actividades financieras, cuentas bancarias, bienes muebles e inmuebles a nombre personal, así como otros ingresos y gastos financieros

2.2.6.6. Protecciones de datos personales

El derecho a la protección de datos personales, se establece en la CRE 2008 como un derecho de libertad, ya que incluye un conjunto de derechos que tienen las personas sobre los responsables de sus datos y garantiza que los titulares de sus datos puedan acceder y activar el principio de conocer sus usos y finalidades, para ser utilizado con su consentimiento y difundido legalmente, cuando el propósito principal de su ley de protección de datos en Ecuador, es proteger el derecho de una persona a la autodeterminación de la información (Holguín, 2022).

2.2.6.7. Situación actual de la protección de datos personales en el Ecuador

Según la Ley Orgánica de Protección de Datos Personales, señalada como (LOPDP), detalla los doce capítulos y setenta y siete artículos, los cuales están relacionados con el tema analítico, del título de la obra se encuentra en el capítulo siete, que enumera las funciones del responsable del tratamiento, y en el capítulo seis, que identifica las medidas de seguridad, donde una aplicación desde el punto de vista técnico y legal detallando varios aspectos importantes tanto para el titular como para el responsable, por tal motivo en las siguientes secciones se analizarán los puntos más importantes para entender cómo funciona el sistema de protección de datos en el Ecuador, los roles que cada uno de los miembros cumple, las obligaciones que deben cumplir las empresas como custodio de datos personales, y las sanciones previstas por el incumplimiento de la ley (Holguín, 2022).

2.2.6.8. Derechos del titular de datos personales

Los derechos del titular de datos personales, según Burbano (2021) son:

- Derecho a la lealtad, transparencia e información
- Derechos al acceso
- Derecho a la rectificación y actualización
- Derecho de eliminación
- Derecho al olvido digital
- Derecho de oposición
- Derecho de anulación
- Derecho a restringir el procesamiento
- Derecho a la portabilidad de datos

- Derecho a la limitación del tratamiento
- Derecho a no ser objeto de una decisión basada únicamente en las valoraciones automatizadas.

2.2.7. Metodología BPM

La metodología BPM proviene del término Business Process Management (Gestión de Procesos de Negocio), es un método para diseñar, implementar, analizar y mejorar continuamente cada proceso en una empresa para lograr objetivos específicos.

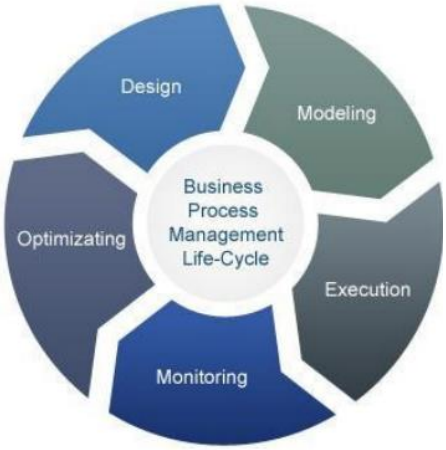
Por lo que según Bustillos y Jáuregui (2018), indican que además del BPM, ya se utilizan otros métodos de trabajo, pero en mayor medida en la industria. Aunque también se supone que se transfieren y combinan conocimientos para mejorar técnicas y métodos.

Según Bustillos y Jáuregui (2018), las características de la Gestión Por Proceso, son:

- Están orientados al cliente.
- Depende de los documentos y la información recibida.
- Cada flujo de trabajo es parte de un procedimiento de nivel superior.
- Cada eslabón de la cadena que identifica adecuadamente sus productos y recursos.
- El proceso puede considerarse como la esencia del negocio.
- Muchos de los aspectos que realmente diferencian a las empresas entre sí residen en sus procesos de trabajo específicos.
- El procedimiento es un parámetro importante que crea una ventaja competitiva.
- Van de principio a fin, es decir, por toda la organización.
- Todos desempeñan diversos roles en el lugar de trabajo: como el proveedor de los materiales necesarios para realizar el servicio; el productor, que realiza las actividades que transforman y agregan valor a dichos recursos para llevar el producto o servicio al cliente, y el cliente, quien primero hace que el proceso funcione en su dirección y segundo es recibir el producto o servicio por el cual tienes que pagar.

El ciclo de la metodología BPM, como se visualiza en la figura 2, son:

Figura 2.
Estructura del Ciclo BPM



Nota: Tomado de Quispe (2018)

Según Quispe (2018), se conceptualiza cada sección de la siguiente manera:

1. **Diseñar.** Durante esta fase, se identifican las características organizacionales existentes, por lo que se debe desarrollar un mapa de procesos. Proporciona una vista del flujo, participantes, alertas y procedimientos y tareas estándar (manuales y automatizados).

2. **Modelar.** Tomar el diseño del paso anterior e ingresar la combinación de variables. Por ejemplo, cambiar los costos de las materias primas para evaluar el desempeño del proceso en situaciones nuevas.

3. **Ejecutar.** Utilizar un sistema informático, donde se automatizan los pasos del proceso. Para ello, primero se debe analizar, diseñar o simular, cada proceso en la etapa anterior, luego se deben asignar tareas a cada jefe de obra, registrando su tiempo de finalización. y todo el proceso; es necesario tener en cuenta los principios organizativos preestablecidos.

4. **Monitorear.** Los procesos de toda organización deben medirse para conocer el nivel de éxito alcanzado con cada automatización. Para hacer esto, se deben rastrear los procesos individuales utilizando la información y estadísticas disponibles, para vincularlos con las estrategias y objetivos de la organización.

5. **Optimizar.** Se debe revisar información relacionada con la ejecución del proceso, identificar cuellos de botella actuales y potenciales, así como posibles reducciones de costos, mejoras de procesos u otras soluciones para aplicar soluciones de diseño de procesos, verificando si se están cumpliendo las expectativas.

2.2.8. Delegado de Protección de Datos (DPD)

Se conceptualiza, al DPD, como un puesto primordial, dentro de una empresa u organización, el cual es el responsable de garantizar, así como proteger adecuadamente la información personal de acuerdo con la ley vigente. Por lo que puede ser, por tanto, una persona natural, encargada de informar al responsable del tratamiento de sus obligaciones legales en materia de protección de datos, así como de velar o controlar el cumplimiento de los requisitos reglamentarios y cooperar con la Autoridad de Protección de Datos Personales, sirviendo de punto de contacto entre éste y el responsable del tratamiento de datos descrito (Guerra & Navarrete, 2023).

Las obligaciones del DPD, según Guerra y Navarrete (2023), son:

a) Informar e instruir al responsable o responsables de su tratamiento y de sus obligaciones.
b) Hacer cumplir o monitorear el cumplimiento.
c) Cooperar con la autoridad de protección de datos, actuando como enlace o canal de comunicación entre la autoridad y el controlador de datos.

2.2.8.1. Principios generales de protección de datos

Según Berroa (2020), los principios generales de protección de datos son:

a) Principio de licitud, se trata del tratamiento de datos personales implica que los fines para los que fueron recabados no deben ser contrarios a la ley o al orden público. El artículo 5, numeral primero de la LDPDP, determina la legitimidad del sistema de almacenamiento de datos personales.

b) Principio de calidad, esencialmente, este principio garantiza que el tratamiento de los datos e información personales se realice de forma fiable, completa y adecuada en relación con el ámbito y los fines para los que fueron recabados.

c) Principio de lealtad, este principio está claramente relacionado con el de legalidad de los datos, mientras que es necesariamente ilegal recopilar y procesar información personal de una manera que implique abuso o fraude.

d) Principio de finalidad, indica que los datos a tratar son parte integrante del contenido de la información que el interesado debe recibir para consentir su tratamiento, en caso de ser necesario. Cuando los datos puedan ser transferidos a

terceros, se debe asegurar que una vez que los datos han sido transferidos, esos datos no pueden ser utilizados para fines distintos a aquellos para los que fueron recopilados.

e) Principio de seguridad, este es uno de los factores que determina el éxito de cualquier sistema de protección de datos personales, el cual estará a cargo de: a) directamente el titular del archivo, registro o banco de datos (es decir, son responsables) y los responsables del propio tratamiento de los datos; b) indirectamente, de expertos autorizados para usarlo" (es decir, personas responsables).

2.2.9. Desafíos y oportunidades de la Ley Orgánica de Protección de Datos Personales (LOPDP)

Los desafíos y oportunidades, según Ramón y Ponce (2021), son:

a) Tratamiento legítimo de datos personales. Para poder ofrecer cualquier tipo de tratamiento, las organizaciones deberán cumplir con los requisitos legales.

b) Derechos de protección. Los titulares de los datos tienen la capacidad de ejercer sus derechos sobre los datos (por ejemplo, acceso, rectificación, conocimiento, transferencia, etc.), en relación con los procesos que deben implementarse declarados para cumplir con sus requisitos.

c) Protección de datos por diseño y por defecto. Las empresas deberán limitar la recopilación y el uso de datos personales, y cumplirán este requisito automáticamente al crear nuevos bienes y servicios.

d) Transferencia de datos personales. Está prohibido enviar información personal a países extranjeros o a terceros.

e) Medidas de seguridad. Es imprescindible la implantación de diversas medidas de seguridad, incluidos análisis de riesgos, análisis de impacto en la protección de datos, procesos de gestión de incidentes, etc.

f) Delegado de protección de datos personales.

g) Dependiendo de la estructura de su empresa, es posible que deba darle un nombre a este nuevo rol.

h) Notificación de vulneraciones de seguridad. Las empresas tendrán sólo cinco días para denunciar una violación de datos personales a los reguladores y, en algunos casos, a las partes afectadas.

i) Multas y sanciones. Las agencias de gestión tienen derecho a multar a las organizaciones que violen el 1% de los ingresos anuales. Por lo que se pueden tomar otras medidas, como restringir (temporalmente) el procesamiento de datos personales

2.2.10. Tratamiento de datos personales

El tratamiento de datos personales en la Administración Pública Central, tiene por objeto proporcionar lineamientos para que las entidades de la Administración Pública Central (APC) mantengan informadas a las personas que acceden a través de sus canales electrónicos, sobre el tratamiento que dan a sus datos personales; y gestionen de manera adecuada los datos personales (Jaramillo, 2022).

2.2.11. Delitos Informáticos

Se conoce como delito informático a la intención, de cometer un delito mientras se utiliza un ordenador, Internet, etc. Por lo que el uso de datos también es un componente del delito informático, que se define como la comisión de actos delictivos, utilizando componentes, medios informáticos o las actividades ilícitas de las que sean parte.

De la definición de delito cibernético, se debe entender que no todos los delitos pueden clasificarse como delitos cibernéticos, simplemente porque se ha utilizado o explotado una computadora u otro dispositivo tecnológico. En este sentido, uno de los estándares utilizados, es que un potencial delito informático debe implicar el uso de tecnologías de la información. Sin embargo, los delitos que impliquen acceso no autorizado a sistemas o destrucción de bases de datos, se clasificarán como delitos de información por su comisión, por lo que no sería posible sin la intervención de la tecnología de la información (Limones & Peralta, 2023).

2.2.12. Principios que deben regir el uso de los datos personales

Los principios que deben regir el uso de los datos personales, según Bravo y Pérez (2018) son:

a) Principios de legalidad

Es aquella, donde se siguen, todos los requisitos legales en el tratamiento de datos personales. Por lo que está prohibida la recopilación fraudulenta, injusta o ilegal de información personal.

b) Principios de consentimiento

Es donde el tratamiento de datos personales sólo se permite con el permiso del titular.

c) Principios de finalidad

Se trata de indicar donde la finalidad se da, para que se recogen los datos personales, los cuales deben ser clara, inequívoca y lícita, excepto en el caso de acciones que tengan valor histórico, estadístico o científico, utilizando el identificador, por lo que el tratamiento de datos personales no debe implicar otros objetivos que no sean evidentes en el momento de su recogida.

d) Principio de proporcionalidad

Se trata, donde para cualquier tratamiento de datos personales, debe ser adecuado, proporcionado y no excesivo, en relación con la finalidad para la que se recogen dichos datos.

e) Principio de calidad

En este punto, el tratamiento de datos personales requiere que la información sea lo más verdadera, exacta y actual posible, así como necesaria, relevante y completa, para los fines que fue obtenida.

f) Principio de seguridad

Es útil para garantizar la seguridad de los datos personales, donde el titular del banco de datos personales y su encargado del tratamiento, están obligados a implementar las medidas técnicas, organizativas y legales apropiadas. Por lo que se debe considerar el tipo de datos personales que se procesan y la idoneidad de las medidas de seguridad.

g) Principio de disposición de recurso

En este ítem, cada titular de datos personales debe tener a su disposición los recursos administrativos o judiciales, necesarios para perseguir y hacer valer sus

derechos, en caso de infracción, como consecuencia de su tratamiento de datos personales.

h) Principio de nivel de protección adecuado

Finalmente, este punto, se da cuando se trata, de datos personales transfronterizos, que deberá garantizarse a los datos personales, tratados un nivel de protección o al menos comparable, al previsto en esta Ley o en las normas internacionales sobre esta materia.

2.2.13. Medidas de seguridad

Según León y Toscano (2020), la Ley Orgánica de Protección de Datos Personales (LPDP), indica que existen dos medidas de seguridad las cuales son:

2.2.13.1. Medidas automatizadas

- **Control de acceso.** Para esta medida, se requiere una identificación apropiada para los empleados que acceden a sistemas que contienen información personal confidencial o de rutina; por lo que esto requiere una gestión de derechos adecuada, supervisión de derechos y gestión de documentos.

- **Trazabilidad.** Mientras que, en este punto, se debe mantener la gestión de seguimiento, así como los registros que deben almacenarse, destruirse, accederse rápidamente, transmitirse y mantenerse, los usuarios, horas de inicio y cierre de sesión, actividades críticas.

- **Gestión de respaldos y conservación**. En condiciones óptimas para el procesamiento y transmisión de datos, es de suma importancia tener en cuenta las pautas de protección física y ambiental contenidas en la norma ISO/IEC 27002:2013. Por lo que esto también significa que se deben verificar las copias de seguridad y las auditorías de dichas copias.

- **Transferencias.** Al enviar datos que contengan datos personales al extranjero; en primer lugar, este debe ser aprobado por el jefe del BDP, para asegurar la transmisión necesaria a utilizar mecanismos, como sumas de verificación, encriptación y otros.

2.2.13.2. Medidas no automatizadas

- **Almacenamiento.** Mientras que, para garantizar la seguridad de los datos, los recursos de almacenamiento deben colocarse en ubicaciones de acceso restringido y protegerse con las medidas de seguridad adecuadas.

- **Copias de Documentos.** La persona autorizada será responsable de copiar los documentos. Por lo que, además, se eliminarán las copias no utilizadas, que contengan datos personales.

- **Acceso a Documentos.** Si varias personas acceden al documento al mismo tiempo, debe existir una grabación. Donde, sólo los usuarios autorizados tienen acceso a los documentos.

- **Traslado de Documentos.** Se deben seguir políticas de seguridad para evitar el acceso no autorizado o la alteración en la transmisión de documentos.

2.2.14. Sanciones o Medidas de Cautelares o Correctivas

Según León y Toscano (2020), la Ley Orgánica de Protección de Datos Personales (LPDP), indica que existen las sanciones o medidas cautelares o correctivas, son:

2.2.14.1. Infracciones Leves

Las infracciones leves, son:

- Procesar datos confidenciales sin el consentimiento del titular.

- Obstruir el ejercicio de los derechos de los titulares de los datos.

2.2.14.2. Infracciones Serias

Las infracciones serias son sancionadas con una multa desde 5 Unidades Impositivas Tributaria (UIT) hasta 50 UIT.

- Gestionar datos sensibles imponiendo opiniones contrarias a los principios establecidos en la Ley de Protección de Datos Personas (LPDP).

- No mantener la seguridad de los datos.

- No registrar la base de datos en Reglamento de Protección de Datos Personales (RPDP).

- Interferir sistemáticamente en el ejercicio de los derechos de los titulares de datos, así como en las actividades realizadas por los organismos de inspección.

2.2.14.3. Infracciones Muy Graves.

Las infracciones graves son sancionadas con una multa desde 50 UIT hasta 100 UIT.

- Tratar datos sensibles imponiendo una postura contraria a los principios establecidos en la LPDP en caso de violación de otros derechos esenciales.

- Recopilar información ilegalmente.

- Proporcionar información falsa

- Continuar procesando datos confidenciales.

- No seguir las pautas establecidas.

2.3. Marco legal

Según la Asamblea Nacional de la República del Ecuador (2021), en la Ley Orgánica de Protección de Datos Personales, detallada en el registro oficial de Suplemento 459 del 26 de mayo del 2021, en el artículo 3, en el numeral 1 del artículo 11 de la Norma Suprema establece que "Los derechos se podrán ejercer, promover y exigir de forma individual o colectiva, ante las autoridades competentes; estas autoridades garantizarán su cumplimiento."

En tanto que en el numeral 2 del artículo 11 de la Norma Suprema prescribe que "Todas las personas son iguales y gozarán de los mismos derechos y oportunidades".

Que, el artículo 277 de la Constitución de la República determina que: "Para la consecución del buen vivir, serán deberes generales del Estado: 1. Garantizar los derechos de las personas, las colectividades y la naturaleza; 2. Dirigir, planificar y regular el proceso de desarrollo; 3. Generar y ejecutar las políticas públicas y controlar y sancionar

su incumplimiento; 4. Producir bienes, crear y mantener infraestructura y proveer servicios públicos; 5. Impulsar el desarrollo de las actividades económicas mediante un orden jurídico e instituciones políticas que las promuevan, fomenten y defiendan mediante el cumplimiento de la Constitución y la ley; 6. Promover e impulsar la ciencia, la tecnología, las artes, los saberes ancestrales y en general las actividades de la iniciativa creativa, comunitaria, asociativa, cooperativa y privada."

Mientras que la Ley Orgánica de Protección de Datos Personales, en el capítulo I, en los ámbitos de aplicación integral dice:

Art. 1.-Objeto y finalidad. -El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección, Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela.

En tanto que en el capítulo V, con referencia a la trasferencia o comunicación y acceso a datos personales por terceros, dice que:

Art. 33.-Transferencia o comunicación de datos personales. -Los datos personales podrán transferirse o comunicarse a terceros cuando se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del responsable y del destinatario, cuando la transferencia se encuentre configurada dentro de una de las causales de legitimidad establecidas en esta Ley, y se cuente, además, con el consentimiento del titular.

Finalmente, en el capítulo VI, referente a seguridad de datos personales dicen en:

Art. 37.-Seguridad de datos personales. -El responsable o encargado del tratamiento de datos personales según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos.

CAPITULO III

MARCO METODOLÓGICO

3.1. Descripción del área de estudio / Descripción del grupo de estudio

El área de estudio fue en el Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega, el cual está conformado por 15 personas.

La Cooperativa de Ahorro y Crédito Pablo Muñoz Vega, como se indica en la figura 3, fue la ubicada en matriz en Tulcán, con dirección en la Colón y el 10 de agosto, con el Acuerdo Ministerial No. 2203, el 29 de julio de 1964, con 47 socios fundadores, desde el mes de enero de 2013 es supervisada por la Superintendencia de Economía Popular y Solidaria. Y desde diciembre del 2022, tiene la calificación de riesgos calificados como "A+". A partir del 28 de febrero del 2023, la institución abre oficinas sucursales en Carchi, Imbabura, Pichincha y Sucumbíos.

Figura 3.
Cooperativa de Ahorro y Crédito Pablo Muñoz Vega - Matriz

Nota: Tomado de Google Maps, 2023

3.2. Enfoque y tipo de investigación.

3.2.1. Enfoque

El enfoque adoptado, fue el del modelo cuantitativo, el cual es empleado para comprobar suposiciones o conjeturas, con base en aproximaciones numéricas y análisis estadísticos, distinguiendo sus patrones de comportamiento, donde hay recursos disponibles, por lo que su objetivo y problema de investigación, se centran en la recopilación de datos, relacionados con la caracterización o prueba real de una hipótesis, incluyendo variables medibles.

3.2.2. Tipo de investigación

Los tipos de investigación utilizados fueron:

3.2.2.1. Investigación bibliográfica

La investigación bibliográfica, puede conceptualizarse como cualquier estudio que involucre la recopilación de información de la literatura publicada. Por lo que estos elementos, pueden incluir fuentes más tradicionales como obras literarias, revistas, periódicos e informes, así como medios electrónicos como grabaciones de audio, video y películas, fuentes en línea como sitios web, blogs y bases de datos de directorios. Por lo que el fácil acceso a computadoras y dispositivos móviles brinda a los investigadores acceso casi instantáneo a una multitud de fuentes de información. La conveniencia de los recursos en línea es una ventaja, pero la velocidad de acceso al material no debe superar la necesidad de calidad o confiabilidad del contenido (Arteaga, 2022a).

Por lo que este tipo de investigación se empleó al utilizar medios de recolección como libros, tesis, revistas, páginas web, entre otras.

3.2.2.2. Investigación de campo

Esta investigación, tiene como objetivo comprender, analizar e interactuar físicamente con las personas en su entorno nativo y recopilar datos. Por lo que, los sociólogos generalmente se refieren al mundo real, donde se estudian las acciones y eventos de la vida cotidiana de las personas (Arteaga, 2022b).

Este tipo de investigación se aplicó en la recopilación de datos obtenidos, de fuentes primarias, para un propósito específico, el cual se encamina a comprender, observar e interactuar con las personas de forma personal.

3.2.2.3. Investigación descriptiva

Este tipo de investigación tiene la tarea de determinar las características de la población de investigación. Por lo que se conceptualiza como "el registro, análisis e interpretación de la naturaleza y composición o proceso real de un fenómeno. Por lo tanto, el enfoque está en la conclusión rectora o cómo una persona, grupo o cosa se comporta u opera en el presente (Guevara et al., 2020).

Este tipo se aplicó al describir el modelo de tesis al aplicar.

3.3. Procedimiento de investigación

El procedimiento de investigación se dará en función de una metodología BPM, la cual se da en las siguientes fases:

3.3.1. Fase 1. Diagnóstico

Este es el primer paso, el cual es responsable de analizar los procesos existentes, conceptualizándolos de acuerdo con metas específicas a alcanzar a través de la gestión de procesos de negocio.

3.3.2. Fase 2. Modelado

En la segunda fase, se debe elegir nuevos procesos, los cuales son descritos de manera individual, según sus propios deseos y conceptualizar los diferentes procesos objetivos sobre dicha base.

3.3.3. Fase 3. Control

En esta etapa, los procesos se monitorean y analizan de manera continua. Por lo que la comparación de los procesos reales con las especificaciones objetivas modeladas está basada en datos, que revela el potencial de optimización; donde sólo aquellos que conocen

exactamente los puntos potenciales y críticos, de sus procesos pueden extraer las soluciones y medidas correctas y aplicarlas de manera efectiva.

3.3.4. Fase 4. Ejecución

A partir del conocimiento adquirido, se toman acciones para mejorar los procesos y utilizar definiciones objetivas. Cuando se utilizan definiciones clásicas de optimización de procesos como Kaizen o Six Sigma, su meta, es monitorear y mejorar continuamente los tiempos de producción, la eficiencia de costos, las tasas de defectos y otras métricas importantes.

3.4. Consideraciones bioéticas

Para realizar, el trabajo presente de investigación, se efectuará un consentimiento informado a las autoridades de la institución, para poder llevar a cabo la propuesta de mejora y así contribuir, con un aporte para que sea un referente de calidad al cliente y un referente en la implementación de tecnología, para el personal deseado.

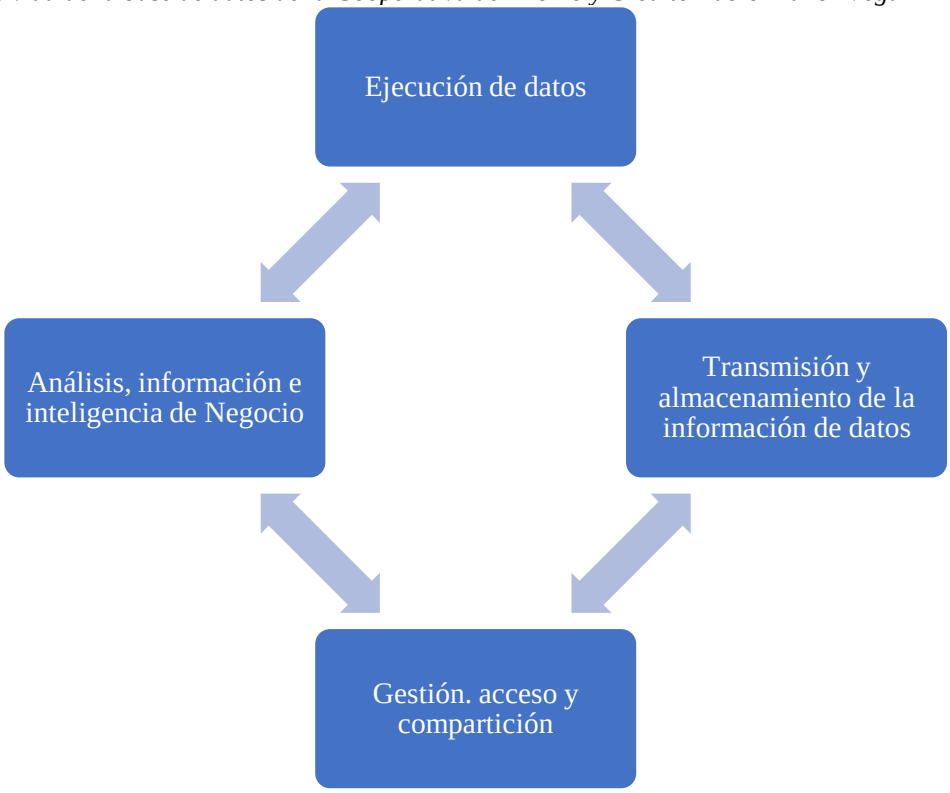
CAPITULO IV

RESULTADO Y DISCUSIÓN

4.1. Análisis de ciclo del tratamiento de la información en la institución

El ciclo de vida de la base de datos de la Institución denominada como Cooperativa de Ahorro y crédito Pablo Muñoz Vega, que se da actualmente, está en la figura 4, esta es:

Figura 4.
Ciclo de vida de la base de datos de la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega



Nota: Tomado de la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega

En la figura 4, se indica el ciclo de vida de la base de datos de la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega, explicando a continuación, como se levantó la información de la siguiente manera:

1. **Ejecución de datos**

En esta etapa, se llevaron a cabo la recolección de datos, identificando las fuentes de información relevantes dentro de la cooperativa, tales como:

- Transacciones financieras.
- Registros de miembros.
- Historial de préstamos y ahorros.
- Información demográfica de los socios.

Para la ejecución de datos, se utilizaron métodos de captura directa como la digitalización de documentos físicos, la entrada de datos manual y la importación de datos desde sistemas de gestión existentes.

2. Transmisión y almacenamiento de datos

Una vez recogidos los datos, se procedió a su transmisión hacia un sistema centralizado de almacenamiento. Este proceso incluyó:

- La utilización de redes seguras para la transferencia de datos desde diferentes sucursales de la cooperativa hacia la sede central.

- La implementación de un sistema de gestión de bases de datos (DBMS) robusto para almacenar la información de manera estructurada.

- Asegurarse de que los datos se almacenaran de forma segura, cumpliendo con las normativas de protección de datos y privacidad.

3. Gestión, acceso y compartición

En esta fase, se organizaron los datos para facilitar su acceso y gestión; por lo que incluyeron las diferentes acciones que son:

- La categorización y etiquetado de los datos para una fácil identificación y recuperación.

- La configuración de permisos de acceso para garantizar que solo el personal autorizado pudiera acceder a información sensible.

- El desarrollo de interfaces de usuario amigables y herramientas de búsqueda para permitir la consulta eficiente de los datos por parte del personal de la cooperativa.

4. **Análisis, información e inteligencia de negocio**

Finalmente, los datos almacenados y gestionados se utilizaron para generar información útil y apoyar la toma de decisiones estratégicas:

- Se emplearon técnicas de análisis de datos como minería de datos, análisis estadístico y modelos predictivos para identificar tendencias y patrones.

- Se elaboraron reportes y dashboards que presentaban la información de manera clara y visualmente comprensible.

- La inteligencia de negocio permitió a la cooperativa entender mejor el comportamiento de los socios, optimizar sus productos y servicios, y mejorar la eficiencia operativa.

Cada una de estas etapas fue crucial para garantizar que la información levantada de la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega no solo fuera precisa y completa, sino también accesible y útil para la toma de decisiones estratégicas.

4.2. Aplicación de la metodología

La metodología por aplicar es la de tipo BPM, quiere decir Business Process Management ósea Gestión por Procesos de Negocio, el cual es un método que permite diseñar, ejecutar, analizar y mejorar de manera continua en cada proceso definido de una organización; porque va a permitir definir el diagnóstico para cumplir el Objetivo I

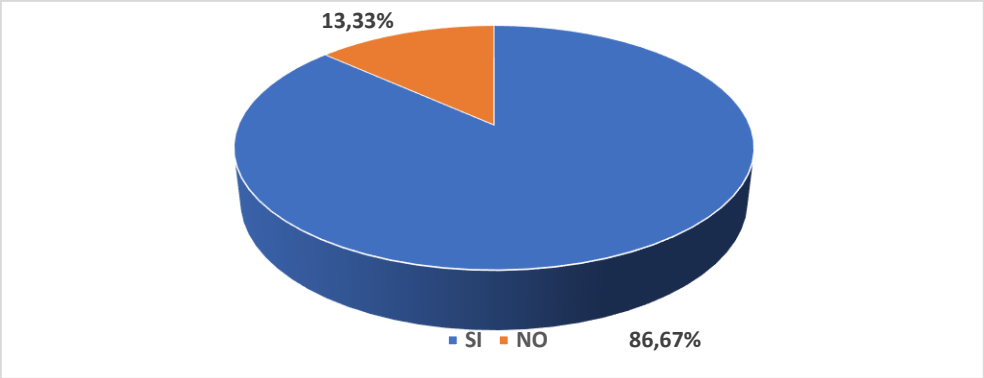
Por lo que estas metodologías cumplen las siguientes fases que son:

4.2.1. Aplicación de la fase 1. Diagnóstico

El diagnóstico se inició con el análisis situacional de la protección de datos en la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega, para lo cual se ejecutó una encuesta para determinar cómo se maneja dicha protección en el Departamento de Tecnología de la Información, en el cual laboran 15 personas.

1. ¿Conoce que es la protección de datos?

Figura 5.
Resultados de la primera pregunta



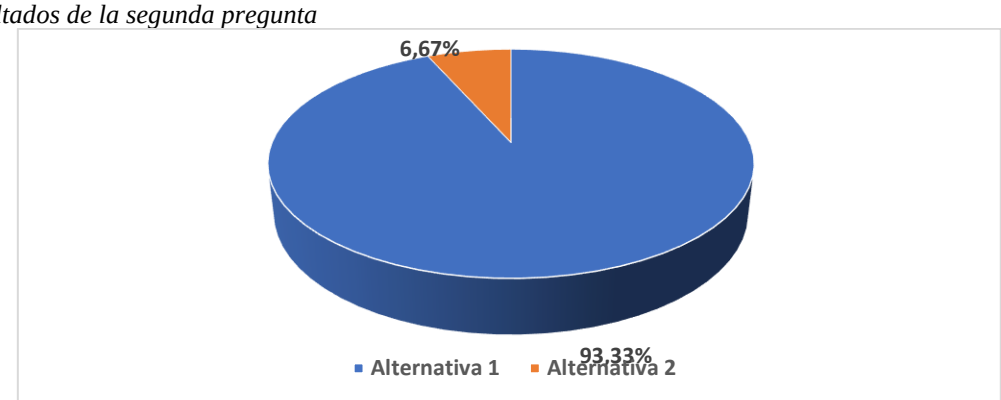
Según la encuesta ejecutada determinada, indica en la figura 5, el 100% que es de 15 encuestados dicen, el 86.67% provenientes de 13 personas, que sí saben o tienen conocimiento de lo que trata la protección de datos, mientras que el 13.33% de 2 encuestados se inclinan por el no tienen conocimiento.

Por lo que se puede decir, que los encuestados Sí conocen que es la protección de datos, los cuales son los derechos de aquellos cuyos datos se recopilan, almacenan y procesan a saber qué datos se están almacenando y utilizando y a corregir cualquier información inexacta.

2. ¿Seleccione un concepto cómo definiría la protección de datos?

- **Alternativa 1.** Es un conjunto de tecnologías informáticas y jurídicas, que se garantizan, que las personas tengan control sobre sus datos personales.
- **Alternativa 2.** Se trata del conjunto de tecnologías para poder bloquear el internet que normalmente se pueden usar, en las cajas de los bancos o cooperativas.

Figura 6.
Resultados de la segunda pregunta

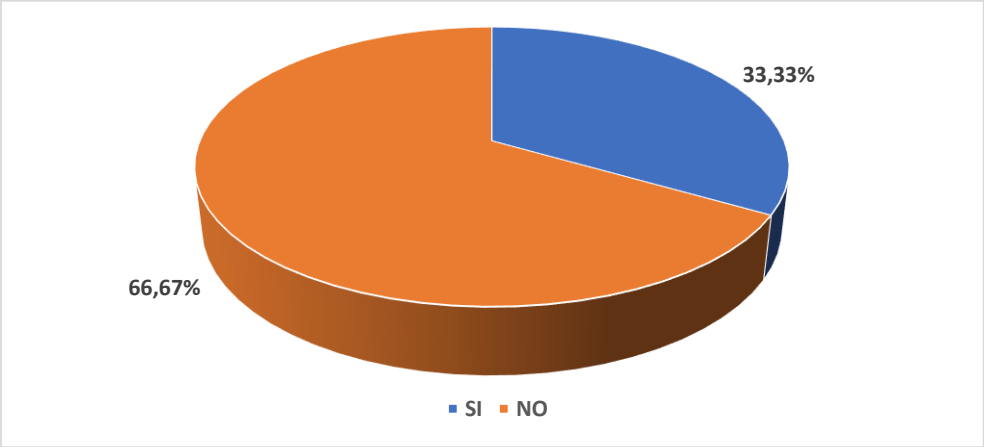


Según la encuesta ejecutada, visualizada en la figura 6, determinada del 100% que es de 15 encuestados, dice el 93.33% provenientes de 14 personas, se inclinan por la alternativa 1, que es un conjunto de tecnologías informáticas y jurídicas, que se garantizan, que las personas tengan control sobre sus datos personales, en tanto que el 6.67% que da de 1 persona encuestada se inclina por la opción 2, que indica que se trata del conjunto de tecnologías para poder bloquear el internet que normalmente se pueden usar.

Por lo que se concluye que la conceptualización de la protección de datos, se trata de un conjunto de tecnologías informáticas y jurídicas, que se garantizan, que las personas tengan control sobre sus datos personales, por lo que se utilizan medidas de seguridad para proteger los datos del acceso no autorizado, manteniendo la confidencialidad, integridad y disponibilidad de la base de datos.

3. ¿Conoce cómo en la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega se aplica la protección de datos?

Figura 7.
Resultados de la tercera pregunta

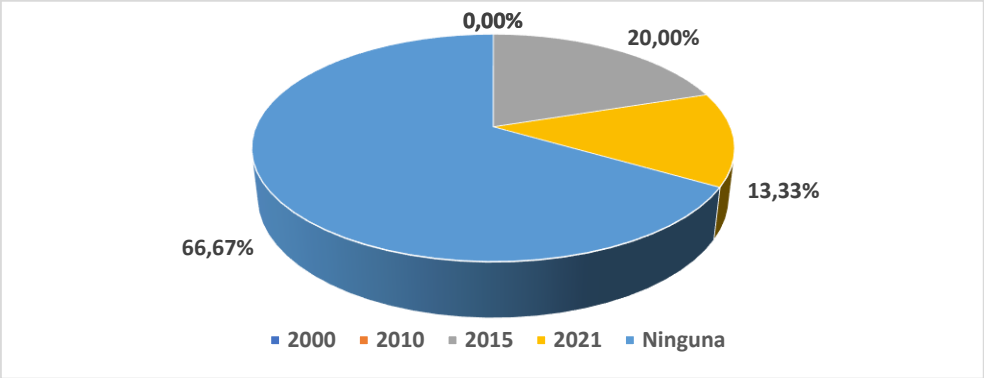


Según en la figura 7, la encuesta ejecutada determinada del 100% que es de 15 encuestados, indican apenas el 33.33% provenientes de 5 personas, que si saben como en la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega se aplica la protección de datos, bajo políticas internas, mientras que el 66.67% que son la mayoría detallan que no saben cómo aplican, o por lo menos que no tienen conocimiento si se aplica o no, dicha protección de datos.

Por lo que se concluye que la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega, no aplica una protección de datos, teniendo presente que como institución financiera son los responsables de brindar una protección de datos.

4. ¿Sabe desde que año está vigente la Ley Orgánica de Protección de Datos en el país?

Figura 8.
Resultados de la cuarta pregunta

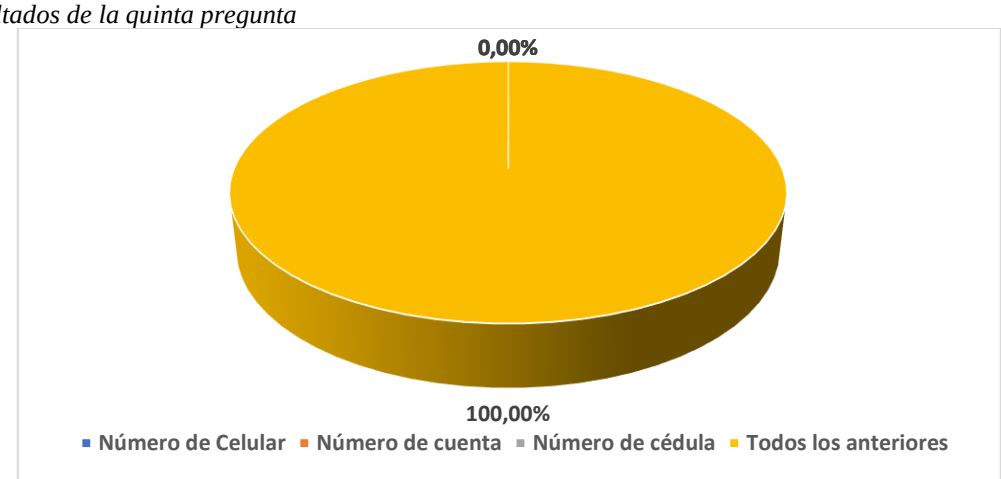


Según la figura 8, la encuesta ejecutada determinada del 100% que es de 15 encuestados, especifican que el 66.67% provenientes de 10 personas, que no saben desde que año está vigente la Ley Orgánica de Protección de Datos en el país, mientras que en menor grado proveniente de 3 encuestados que son el 20% dicen que desde el 2015, por lo que se concluye que les hace falta capacitación sobre esta ley.

Se concluye que no saben que la Ley Orgánica de Protección de Datos en el país, y que está vigente desde el año 2021.

5. ¿Puede indicar que alternativas considera mayormente sensible?

Figura 9.
Resultados de la quinta pregunta

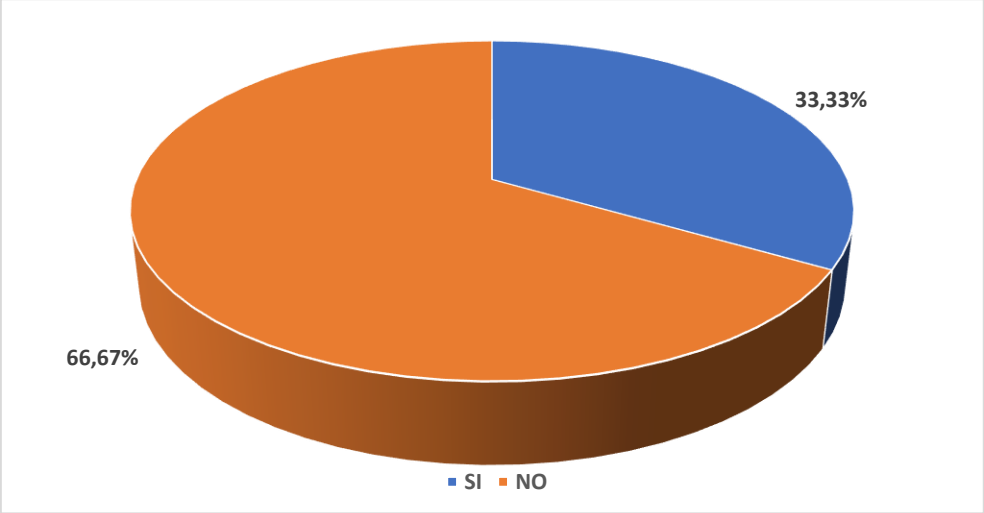


Según la figura 9, la encuesta ejecutada determinada del 100% que es de 15 encuestados, todos coincidieron que la alternativa, mayormente sensible, son todas las alternativas anteriores, las cuales involucran, el número del celular, la cuenta y la cedula.

Se concluye que las alternativas sensibles son el número de cedula, número de cuenta y número de celular.

6. ¿Conoce que tipo de sanciones se da a la persona que falte a la Ley Orgánica de Protección de Datos en el país?

Figura 10.
Resultados de la sexta pregunta

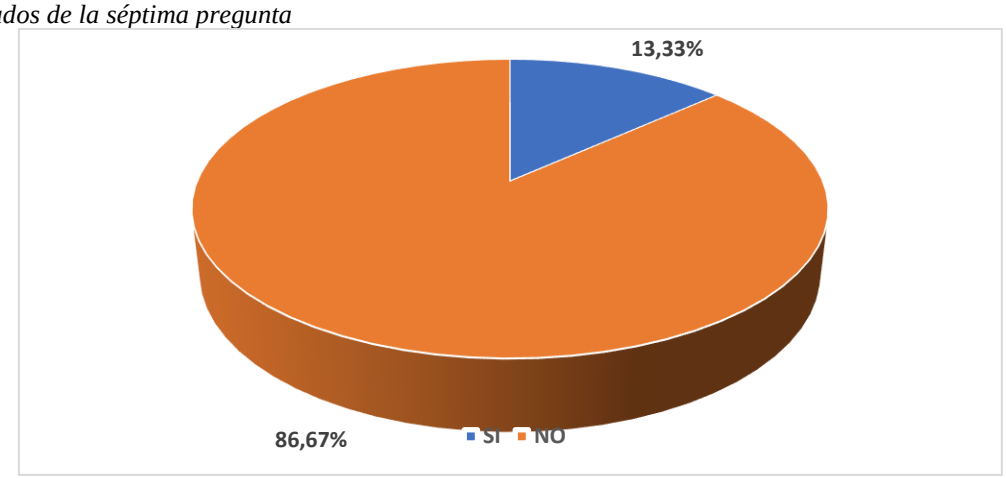


Según la figura 10, la encuesta ejecutada determinada del 100% que es de 15 encuestados, el 66.67%, que representa gran parte del personal encuestado, que es de 10 personas, explican, que no conocen que tipo de sanciones reciben las personas que falte a la Ley Ley Orgánica de Protección de Datos en el país.

Se concluye que no saben los tipos de sanciones por la falta de aplicación a la Ley Orgánica de Protección de Datos, la cual se da en función de diferentes tipos de sanciones, que son infracción leve la cual extiende una multa de hasta el 0,7%, de la facturación de una determinada empresa, o grave con una multa de hasta el 1%, además se podría sancionar hasta con multas de 20 salarios básicos unificados podría ser hasta de 9000$.

7. ¿Sabe de qué se trata el Registro Oficial N° 459?

Figura 11.
Resultados de la séptima pregunta

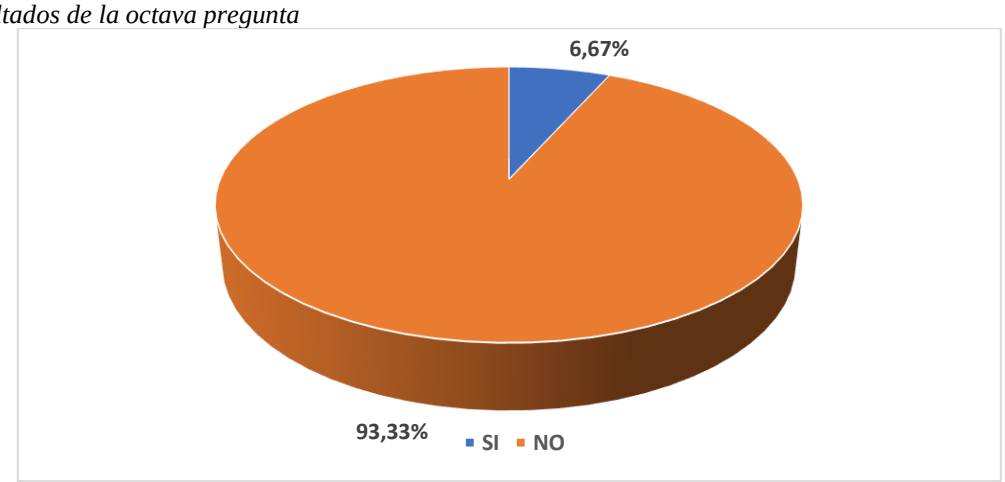


Según la figura 11, la encuesta ejecutada determinada del 100% que es de 15 encuestados, casi todos, representados en el 86.67% que es de 13 encuestados, especifican que no saben de qué se trata el Registro Oficial N° 459, mientras que solo 2 dijeron que si han escuchado.

Se concluye que no saben que el Registro Oficial N° 459, es la Ley Orgánica de Protección de Datos Personales.

8. ¿Conoce de que se trata los estándares ISO/IEC para dar cumplimiento con el Registro Oficial N° 459?

Figura 12.
Resultados de la octava pregunta

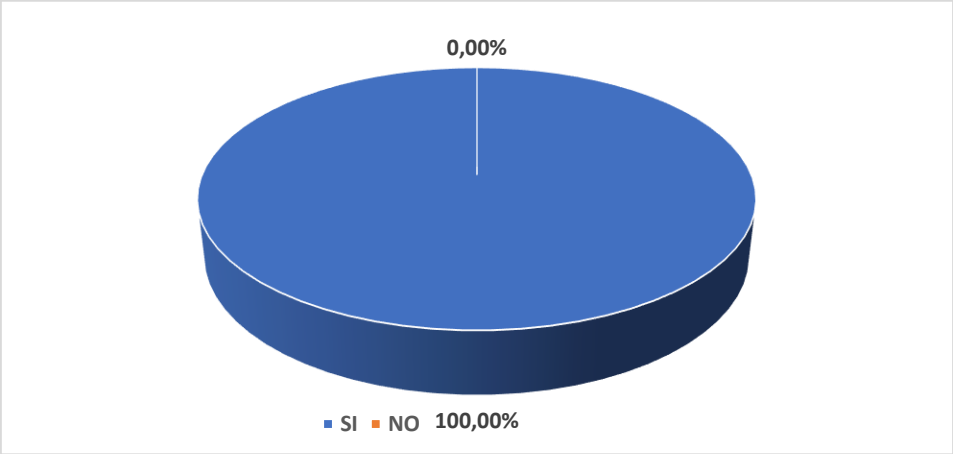


Según la figura 12, la encuesta ejecutada determinada del 100% que es de 15 encuestados, casi todos, representados en el 93.33% que es de 14 encuestados, especifican

que no conocen de cómo se tratan a los estándares ISO/TEC para dar cumplimiento con el Registro Oficial N° 459, mientras que 1, solo dijo que si tenía conocimiento.

9. ¿Piensa que es necesario implementar la Ley Orgánica de Protección de Datos en la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega aplicando estándares ISO/IEC para dar cumplimiento con el Registro Oficial N° 459?

Figura 13.
Resultados de la novena pregunta



Según la figura 13, la encuesta ejecutada determinada del 100% que es de 15 encuestados, todos coincidieron que si piensan que es necesario implementar la Ley Orgánica de Protección de Datos en la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega aplicando estándares ISO/IEC para dar cumplimiento con el Registro Oficial N° 459.

Se concluye que todos coinciden que, si es necesario que se implementará la Ley Orgánica de Protección de Datos en la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega, según los reglamentos vigentes que podrían cumplir con las normativas y así evitar sanciones.

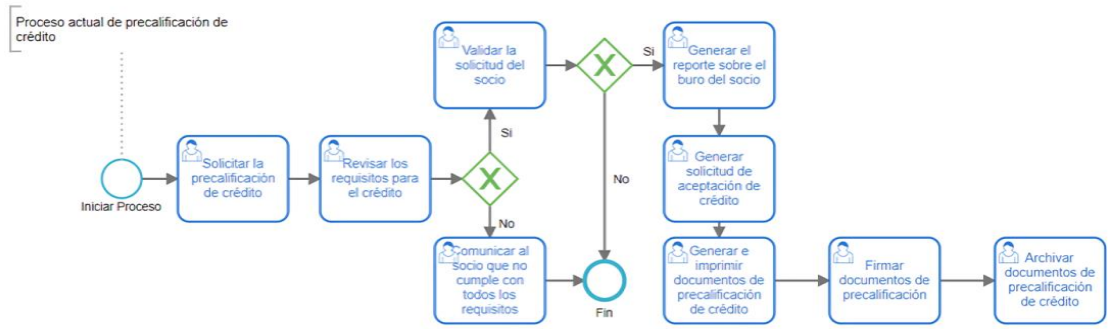
4.2.2. Aplicación de la fase 2. Modelado

El modelado de la implementación de la Ley Orgánica de Protección de Datos Personales en la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega considerando los estándares ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 27001:2019 y el SGSI institucional, debe tener en cuenta:

La meta de la Ley Orgánica de Protección de Datos Personales, la cual es garantizar el derecho a la protección de datos personales, incluido el acceso y decisión sobre la información y datos de este tipo, la cual está constituida por 12 capítulos: Capítulo I: Ámbito de Aplicación Integral; Capítulo II: Principios; Capítulo III: Derechos; Capítulo IV: Categorías Especiales de Datos; Capítulo V: Transferencia o Comunicación y Acceso a Datos Personales por Terceros; Capítulo VI: Seguridad de Datos Personales; Capítulo VII: Del Responsable y del Delegado de Protección de Datos Personales; Capítulo VIII: De la Responsabilidad Proactiva; Capítulo IX: Transferencia o Comunicación Internacional de Datos Personales; Capítulo X: De los Requerimientos Directos y de la Gestión del Procedimiento Administrativo; Capítulo XI: Medidas Correctivas, Infracciones y Régimen Sancionatorio; Capítulo XII: Autoridad de Protección de Datos Personales.

4.2.2.1. Diagrama de proceso actual de precalificación y de liquidación de crédito

Figura 14.
Proceso actual de precalificación de crédito de la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega



Nota: Tomado de la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega

En la figura 14, se detalla el proceso actual de precalificación de crédito de la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega, la cual se da de la siguiente manera:

1. Iniciar Proceso: El proceso comienza cuando un socio inicia la solicitud de precalificación de crédito.
2. El segundo paso es solicitar la precalificación de crédito: El socio presenta una solicitud para la precalificación de crédito.
3. A continuación, se debe revisar los requisitos para el crédito: Donde se revisan los documentos y requisitos presentados por el socio para asegurar que cumplen con los criterios establecidos.
4. Una vez revisado los requisitos para el crédito, se deben validar la solicitud del socio: Donde se evalúa la solicitud del socio. Si la solicitud cumple con todos los

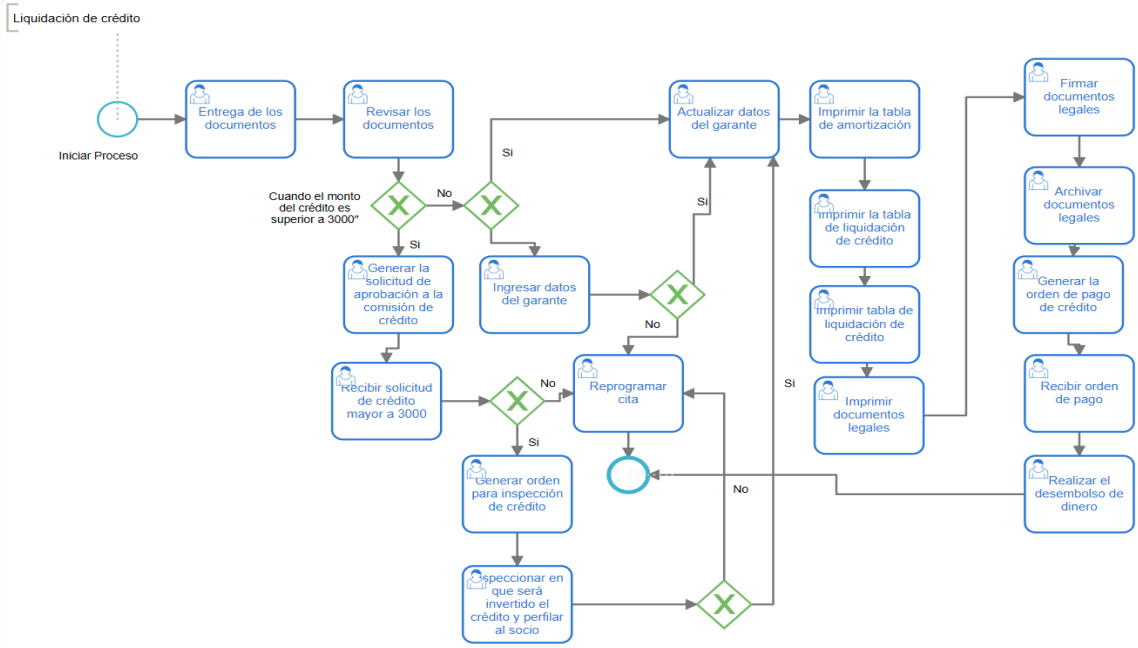
requisitos, se avanza al siguiente paso. Si no cumple, se procede a comunicar al socio la situación, finalizando el proceso para esos casos.

5. Otro paso muy importante es generar el reporte sobre el buró del socio: Si la solicitud es válida, se genera un reporte sobre el buró de crédito del socio.
6. Para generar solicitud de aceptación de crédito: Se procede a crear la solicitud de aceptación de crédito.
7. En tanto que para generar e imprimir documentos de precalificación de crédito: Los documentos necesarios para la precalificación del crédito son generados e impresos.
8. Por consiguiente, se debe firmar documentos de precalificación: Donde el socio y los responsables correspondientes firman los documentos de precalificación.
9. Finalmente se debe archivar documentos de precalificación de crédito: Donde, los documentos firmados se archivan para tener un registro del proceso.

Este flujo garantiza que cada solicitud de precalificación de crédito sea evaluada de manera adecuada y transparente, asegurando que solo aquellos socios que cumplen con todos los requisitos avanzan en el proceso.

Figura 15.

Proceso actual de liquidación de crédito de la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega



Nota: Tomado de la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega

El proceso actual de liquidación de crédito de la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega, como se indica en la figura 15 se divide en varios pasos, que incluyen la entrega y revisión de documentos, la generación de tablas de amortización, la

actualización de datos, la aprobación del crédito por parte de la comisión correspondiente y, finalmente, el desembolso del dinero al socio. Por lo que actualmente se detallada cada paso:

1. Entrega de los documentos:
   - El socio entrega los documentos requeridos para solicitar el crédito a la cooperativa.

2. Revisión de los documentos:
   - Se verifica si los documentos entregados están en orden y cumplen con los requisitos establecidos por la cooperativa.
   - Si los documentos están en orden, se procede con el siguiente paso. De lo contrario, se continua con los pasos 3, 4 o 5, según corresponda.

3. Actualización de datos del garante:
   - Si los documentos están en orden, se actualizan los datos del garante del crédito.
   - Se imprime la tabla de amortización y la tabla de liquidación de crédito, así como los documentos legales pertinentes.
   - Se solicita la firma de dichos documentos y se archivan los documentos legales.

4. Generación del orden de pago de crédito:
   - Se genera el orden de pago del crédito, que incluye la cantidad a desembolsar y los detalles del crédito.
   - Se recibe el orden de pago y se procede con el desembolso del dinero al socio.

5. Verificación y reprogramación:
   - Si los documentos no están en orden, se verifica nuevamente los datos del garante.
   - Si los datos del garante no están en orden, se reprograma la cita para una revisión posterior y se finaliza el proceso.

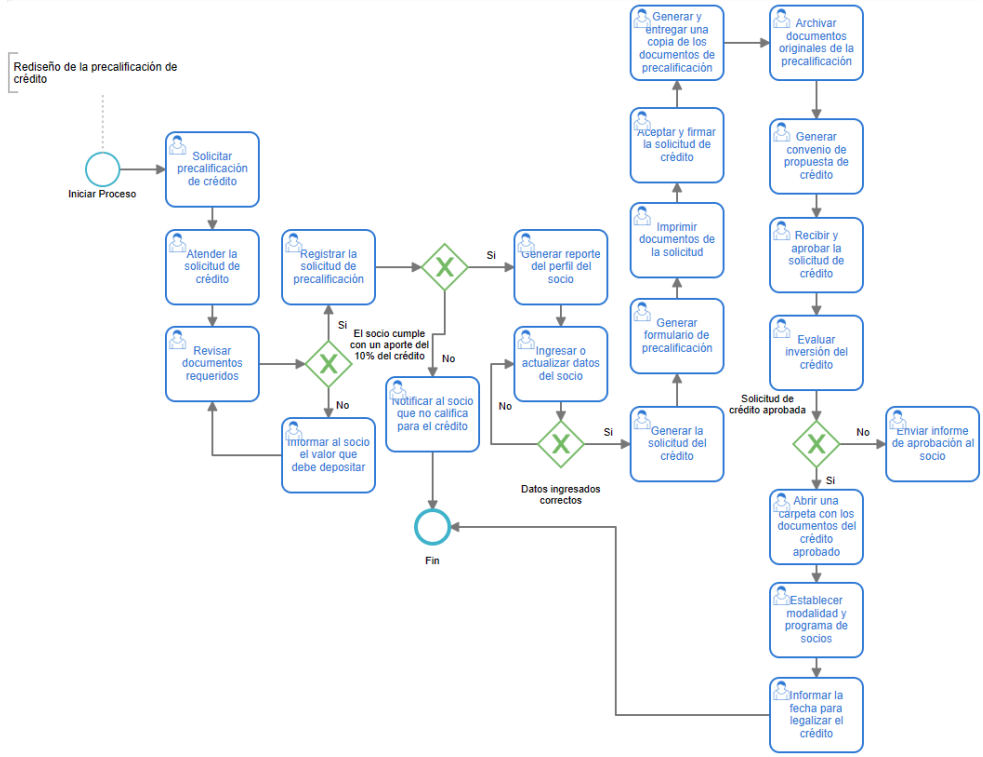
6. Aprobación del crédito por la comisión:
   - Se genera la solicitud de aprobación del crédito y se presenta ante la comisión correspondiente.

- Si el crédito es mayor a 3000 unidades monetarias, se requiere una inspección del destino del crédito.
- Si la solicitud de crédito es aceptable, se procede a la inspección y perfilamiento del socio.
- Se actualizan los datos del garante si es necesario.
- Si no se acepta la solicitud de crédito, se reprograma la cita y se finaliza el proceso.

Este proceso detallado asegura que cada solicitud de crédito sea revisada minuciosamente, que se tomen las decisiones correspondientes y que se realicen los desembolsos de manera adecuada, siguiendo los procedimientos establecidos por la cooperativa.

4.2.2.2. Rediseño del proceso de precalificación de crédito y de liquidación propuesto

Figura 16.
Rediseño del proceso propuesto de precalificación de crédito de la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega



Nota: Adaptado a los Procesos de Precalificación de Crédito que tiene la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega

El rediseño propuesto del proceso de precalificación de crédito de la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega, como se indica en la figura 16, busca mejorar la eficiencia y la claridad en las etapas involucradas. Por lo que los pasos siguientes son:

1. Solicitar precalificación de crédito:
    - El socio inicia el proceso solicitando la precalificación de crédito.

2. Atención de la solicitud de crédito:
    - Se atiende la solicitud y se procede con la revisión de los documentos requeridos.

3. Revisión de documentos y registro de la solicitud:
    - Se verifica si los documentos cumplen con el requisito del 10% de aporte del crédito.
    - Si cumplen, se registra la solicitud de precalificación y se genera el reporte del perfil del socio.
    - Se ingresan o actualizan los datos del socio, y si son correctos, se procede con la generación del formulario de precalificación.
    - Se imprimen los documentos, se acepta y firma la solicitud de crédito.
    - Se entrega una copia de los documentos de precalificación al socio y se archivan los documentos originales.

4. Revisión y aprobación de la solicitud de crédito:
    - Se realiza una nueva revisión de los documentos y se procede si cumplen con el requisito del 10% de aporte del crédito.
    - Si los documentos son adecuados, se genera el convenio de propuesta de crédito y se recibe y aprueba la solicitud de crédito.
    - Se evalúa la inversión del crédito y se procede con la solicitud de crédito aprobado.
    - Si la solicitud es adecuada, se abre una carpeta con los documentos del crédito aprobado, se establece la modalidad y programación de pagos, y se informa al socio la fecha para legalizar el crédito.

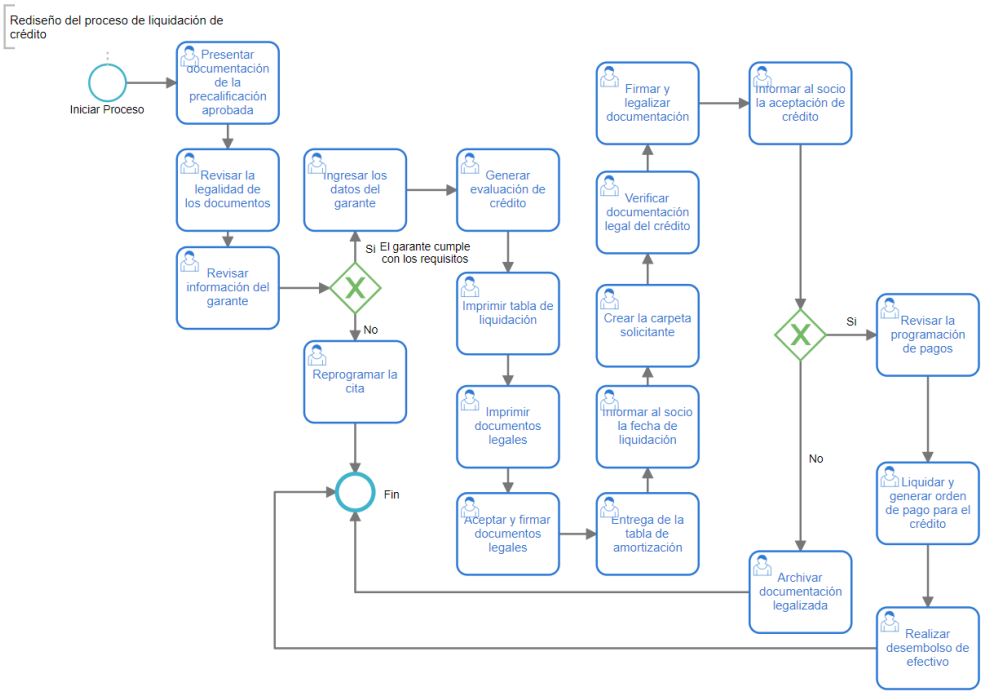
5. Actualización de datos incorrectos:
    - Si se detectan datos incorrectos del socio, se vuelve a ingresar y actualizar la información.

6. Informar al socio sobre el aporte faltante:
    - Si los documentos no cumplen con el requisito del 10% de aporte del crédito, se informa al socio sobre el valor que debe depositar.

- Se procede a revisar nuevamente los documentos requeridos después del depósito.

Este rediseño simplifica el proceso, estableciendo una secuencia clara de pasos y asegurando una atención adecuada a las solicitudes de crédito, lo que puede mejorar la experiencia del socio y la eficiencia operativa de la cooperativa.

Figura 17.
Rediseño del proceso propuesto de liquidación de crédito de la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega



Nota: Adaptado a los Procesos de Liquidación de Crédito que tiene la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega

El rediseño propuesto del proceso de liquidación de crédito de la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega, como se visualiza en la figura 17, busca mejorar la eficiencia y la claridad en las etapas involucradas, donde la explicación es:

1. Presentar documentación de la precalificación aprobada:
   - El socio presenta la documentación de la precalificación aprobada para iniciar el proceso de liquidación del crédito.

2. Revisión de la legalidad de los documentos:
   - Se revisa la legalidad de los documentos presentados por el socio para asegurarse de que estén en orden y cumplan con los requisitos legales establecidos.

3. Revisión de información del garante y generación de evaluación de crédito:
    - Se revisa la información del garante y, si cumple con todos los requisitos, se ingresan los datos del garante.
    - Se genera la evaluación de crédito y se imprime la tabla de liquidación, así como los documentos legales pertinentes.
    - Se aceptan y firman los documentos legales y se entrega la tabla de amortización al socio, informándole sobre la fecha de liquidación.

4. Creación de carpeta solicitante y verificación de documentación legal:
    - Se crea la carpeta del solicitante y se verifica la documentación legal del crédito.
    - Se firman y legalizan los documentos y se informa al socio sobre la aceptación el crédito.
    - Si el crédito es aceptado, se revisa la programación de pagos y se procede con la liquidación y generación del pago para el crédito.
    - Se realiza el desembolso de efectivo al socio, finalizando así el proceso de liquidación del crédito.

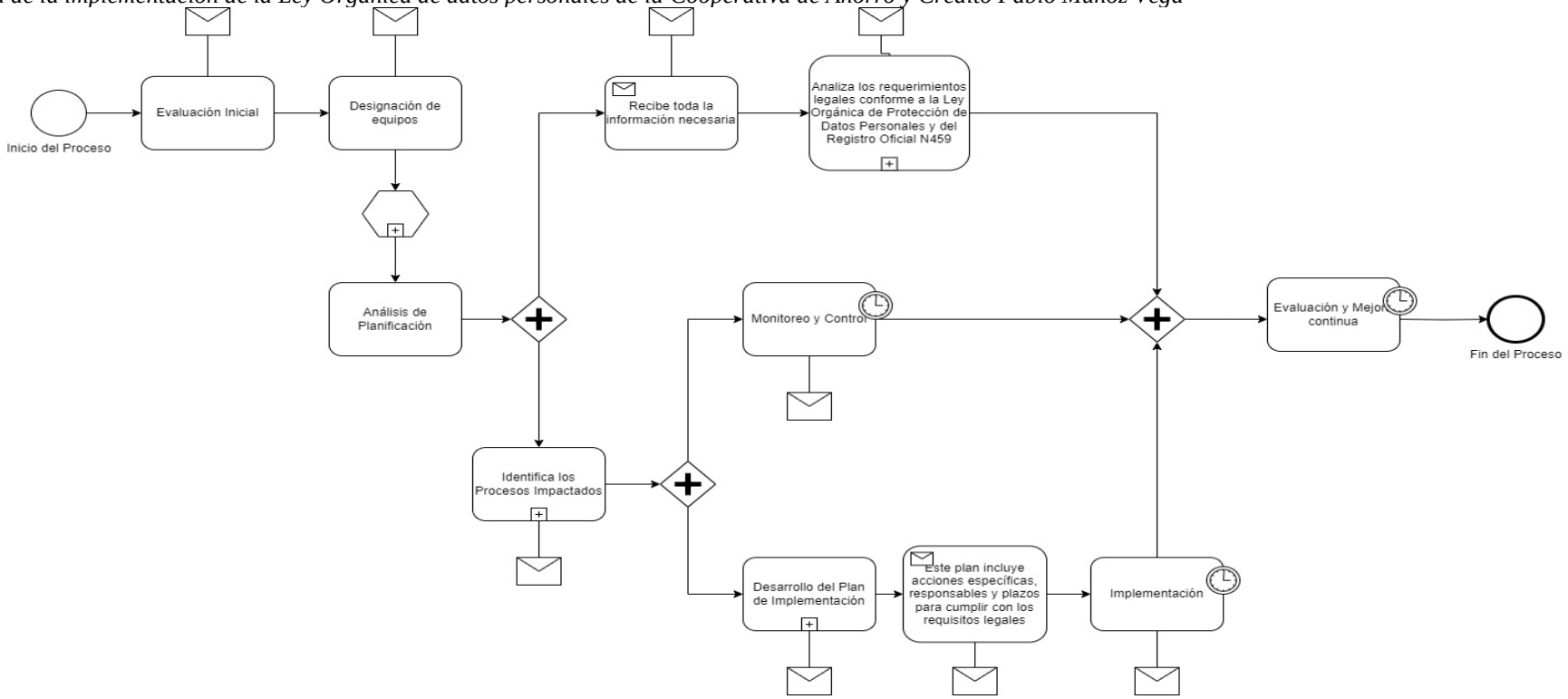
5. Reprogramación de cita en caso de incumplimiento del garante:
    - Si el garante no cumple con todos los requisitos, se reprograma la cita y se finaliza el proceso.

Este rediseño simplifica el proceso, estableciendo una secuencia clara de pasos y asegurando una atención adecuada a las solicitudes de liquidación de crédito, lo que puede mejorar la experiencia del socio y la eficiencia operativa de la cooperativa.

4.2.2.3. Diagrama de la implementación de la ley orgánica de protección de datos personales

Figura 18.

Diagrama de la implementación de la Ley Orgánica de datos personales de la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega



Nota: Adaptado a los Procesos de la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega

Mediante una revisión interna de la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega, referente a la Protección Orgánica de Datos, se observa que se manejan las siguientes políticas, así como cumplimientos:

Por lo que, para dar cumplimiento a las normas relacionadas, a través de capacitaciones de alto nivel al personal de la institución, se dan las siguientes consideraciones, situada en la Tabla 2.

Tabla 2.
Consideraciones para cumplimiento de la Ley Orgánica de Protección de Datos Personales

Ítem	Caracterización	Artículo	Cumplimiento
1	**Seguridad de Datos Personales**	**Art. 37, 38**	
	Las instituciones públicas o financieras, podrán determinar y promulgar, políticas de seguridad más amplias o específicas de conformidad con la Constitución, los estatutos y otras leyes, propias o conexas, así como sus deberes y atribuciones.		La política institucional, requiere de actualizaciones, que permita contener la protección de datos personales.
2	**Organización de la seguridad de la información**	**Art. 11, 37, 38, 39, 41, 55, 56, 57, 59, 60**	
	Una organización debe conceptualizar y asignar todas las responsabilidades de seguridad de la información.		Desarrollar una Política interna de Protección de Datos que detalle las obligaciones y disposiciones de la Ley y su Reglamento.

	Identificar e implementar coordinaciones y controles de seguridad de la información a clientes	Desarrollar procesos de tratamiento de información de datos, de distintos clientes, así como proveedores.
	Establecer las responsabilidades, que deben tener para la seguridad de la información.	Establecer a través de memorandos, las responsabilidades, que permita fijar la seguridad de la información.
	Debe asegurarse de que nadie pueda acceder, modificar o utilizar de forma independiente sin permiso alguno.	Crear una política de acceso a la información, así como a los datos personales.
	Recibir alertas tempranas sobre las vulnerabilidades de una institución financiera y remediación de organizaciones públicas, privadas y académicas reconocidas por sus contribuciones a la gestión de la seguridad de datos personales.	Desarrollar un proceso de consultoría sobre vulnerabilidades al departamento de Tecnología de la información
	Acceder a consejos de expertos en seguridad de la información de agencias que empleen información especializada, sean estas privadas o gubernamentales.	Organizar reuniones con la Dirección Nacional de Datos Públicos, que permita dar soporte a la implementación de la normativa.

Las metas deben darse, en la seguridad de la información, deben ser incluidos entre los objetivos privados de la institución financiera.	En particular, mejorar el tratamiento de datos personales, mediante el compromiso del liderazgo, realizando una integración en la estrategia organizacional, optando por metas medibles, cumpliendo la Normativa Legal.
Identificar los riesgos de seguridad de la información, para poder implementar las medidas de control requerida	Visualizar crecientes amenazas a la seguridad de la información, dando un énfasis especial a la protección de los datos personales.
Establecer requisitos de seguridad, antes de brindar servicios a ciudadanos o clientes de agencias financieras, o gubernamentales que usen o procesen información sobre ellos.	Formular un procedimiento, para el tratamiento de datos personales en los servicios que presta la organización, tanto virtual como presencial.
Proteger los recursos de datos personales.	Agregar políticas de privacidad y seguridad, cifrando datos, realizando un cumplimiento legal y normativo; a través de una revisión continua y mejora.
Establecer políticas de control del acceso	Ampliar el acceso a los datos personales en la política.

Acuerdos útiles que permitan gestionar información inexacta, sobre la seguridad de la información y violaciones de seguridad.	Establecer una Política de Tratamiento de Datos Personales, la cual debe incluir la gestión de los distintos procedimientos administrativos.
Ciudadanía corporativa organizacional y de clientes adecuada. Protección de datos, fundamentada en la Constitución y la normativa nacional, especialmente los datos personales o financieros de la población.	Actualizar políticas de seguridad en los sistemas informáticos de los sitios web, de la institución financiera. Ejecutar, políticas, así como procesos internos relacionados con la protección de datos personales.
Identificar procedimientos de respaldo y continuidad del negocio.	Desarrollar una política de respaldo de información, comprando un software de respaldo automático a la biblioteca de cintas de la institución financiera.
Definir los requisitos necesarios de control y pruebas de seguridad.	Conectarse a través de VPN, que permita registrar, un tiempo definido de conexión, así como al acceso al sistema.

3	**Seguridad de los recursos activos humanos.**	**Art. 7,8,9,12,13,14,15,16,17,18 ,19,26**	
	Realizar verificaciones de antecedentes, así como aquellos que solicitan empleo, así como los que requieren, nombramientos y ascensos de funcionarios de acuerdo con las reglas éticas y regulaciones, los cuales son proporcionales a la naturaleza y a las actividades de agencia financieras, donde dicho control no debe ser discriminatorio en ningún aspecto.		Procedimientos de la Junta Directiva Administrativa que establezcan claramente el procesamiento de la información recopilada en el CV y documentos necesarios.
	Los funcionarios deben aceptar y confirmar los términos de los contratos de trabajo, que establezcan claramente sus deberes y responsabilidades según la ley aplicable vigente.		La actualización del contrato debe ser incluido en el proceso de la Junta Directiva.
	Firmar acuerdos de confidencialidad o no divulgación, antes de que puedan tener acceso a la información. Por lo que el contrato específico debe establecer, claramente los parámetros del contrato,		Procedimientos de la Junta Directiva Administrativa que establezcan claramente, la protección del procesamiento de la información recopilada en los clientes.

	así como la información confidencial relevante, formas de acceso, responsabilidades y funciones algunas.		
	Requerir a los funcionarios o colaboradores, que apliquen medidas de seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la agencia financiera.		Designar un responsable del Departamento de Seguridad de la Información y Tratamiento de Datos, según normativa interna.
	Pactar los términos de empleo, incluida las políticas de seguridad de la información de una determinada organización, con los métodos de trabajo adecuados.		Procesamientos, designados, de la Junta Directiva Administrativa, que establezcan claramente el proceso de procesamiento de la información recopilada.
4	**Gestión de datos sensibles**	**Art. 5,26,40,41**	
	Catalogar, equilibrar y reestablecer, todas las fuentes de información y equipos de procesamiento.		Puede fundamentarse en la orientación de la matriz productiva, pudiendo incluir, los datos personales como otro recurso.
	Determinar, los recursos o soportes de hardware.		Implementar un software de inventario, que permita delimitar varios parámetros establecidos.

Se deben tomar las medidas adecuadas al retirar cuenta alguna de la institución financiera.	Revisar los términos y condiciones, seguido de la liquidación de saldo y transacciones pedantes; actualizar la información de pago automático; retirar fondos y cancelar cheques, seguido de una solicitud del cierre de la cuenta, confirmar el cierre, proteger los datos personales, considerar implicaciones fiscales, comunicar los cambios y finalizar con la mantención de registros.
En el reglamento interno, el responsable de Recursos Activos deberá tener en cuenta las actividades especificadas en los controles correspondientes.	Delimitar la política interna de tratamiento personal, así como los procedimientos de intercambio de información según lo dispuesto en la Ley Orgánica de Protección de Datos Personales.
Todas las comunicaciones, que se den, en el interior de la institución, deben ser rastreadas y almacenadas permanentemente.	Desarrollar una política de respaldo de información, para lo cual se debe comprar un software de respaldo automático a la biblioteca de cintas.
Debe usarse programas que controlen los virus informáticos tanto en los mensajes como en los	Adquisición de soluciones antivirus y anti spam.

	archivos adjuntos antes de dar apertura a los mismos.	
	Debe limitarse a los usuarios el acceso a internet, aplicaciones o servicios en línea, que puedan dañar los intereses o cometer algún paso ilícito en la organización; en particular, el acceso mediante dispositivos fijos y/o móviles a Internet, aplicaciones o servicios en línea que afectan la productividad y las operaciones de la organización.	Adquisición de equipos de protección perimetral de nueva generación (Firewall).
	En el caso de documentos electrónicos, la etiqueta debe estar asociada a metadatos únicos, que pueden ser un código especial.	Aplicar herramientas de cifrado de información libre o gratuita como QuickHash, MultiHasher.
	Los procesos de gestión de medios móviles, deben realizarse de acuerdo con el esquema de clasificación de la organización, y los procedimientos y niveles de autorización documentados.	El proceso de gestión de medios extraíbles, deberá identificar los medios que sujeten datos personales, para lo cual se debe tratarlos adecuadamente.

5	**Control de acceso**	**Art. 34, 37, 38, 41**	**Implementar un sistema de supervisión de acceso con tarjeta magnética para un mejor monitoreo.**
	Mantener registros de control de acceso a la red y a las aplicaciones que indiquen la fecha en que se creó, eliminó, suspendió, activó o canceló el acceso; como todo usuario, asignado a diferentes derechos de acceso.		Implementar módulos de auditoría en el sistema informático de la organización financiera.
	Implementar medidas para controlar los registros de acceso de los usuarios como lectura, escritura, eliminación y ejecución de información, entre otros.		Actualizar el sistema informático, constituido, sobre el software que tiene varios tiempos de uso y actualización de la tecnología, también efectuar el diseño de roles y perfiles de los diferentes colaboradores.
	Usar un administrador de versiones de código fuente, otorgando acceso a los desarrolladores como parte de la autorización.		Implementar un software libre o de código abierto
6	**Criptografía**	**Art. 37, 38, 41**	

	Desarrollar, implementar y publicar una política que regule el uso de medidas de seguridad de la información criptográfica, adecuadas al nivel de protección necesario.		Implementar la utilización de herramientas criptográficas en software libre.
7	**Seguridad física y del entorno**	**Art. 37, 38, 41**	
	Resguardar los equipos de procesamiento, de información sensible para reducir a lo máximo, los riesgos de fuga de información debido a la radiación electromagnética.		Determinar mayor protección del servidor.
	Los equipos deben estar protegidos contra cortes de energía y otras interrupciones debido a fallas de energía principal.		Adquirir un UPS para los equipos, porque no hay energía de emergencia para todas las estaciones de trabajo.
	Los cables eléctricos, así como los de telecomunicaciones que transmiten datos o soportan servicios de información, deben estar protegidos contra bloqueos, interferencias o posibles daños.		Modificación de cableado estructurado.
8	**Seguridad de las operaciones**	**Art. 37,38,39,41,43,46**	

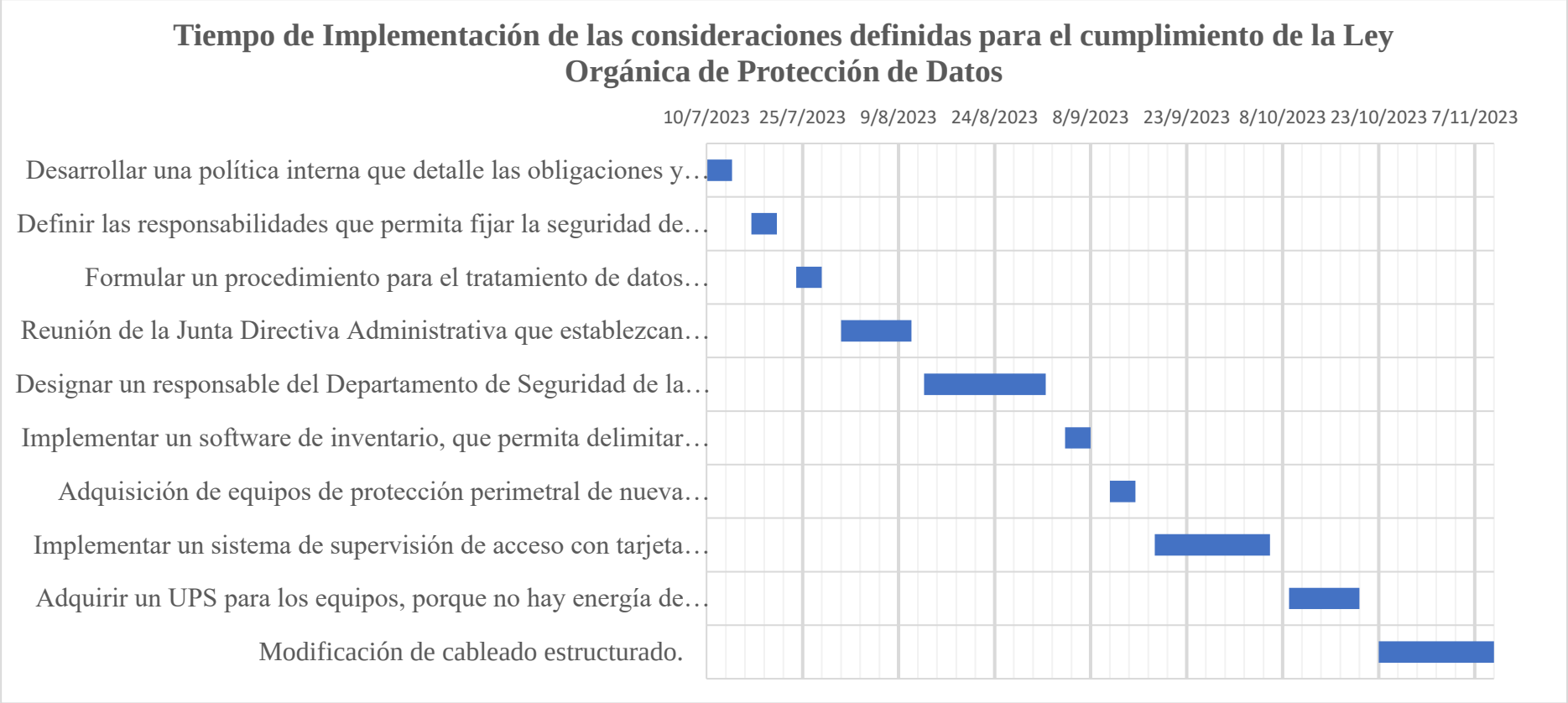
	Entornos separados de desarrollo, prueba y producción alguna.		Legitimación de un segundo centro de datos.
	Sincronización del tiempo.		Implementar servidor NTP.
9	**Seguridad en las comunicaciones**	**Art. 55,56,57,59,60**	
	Implementar tecnologías para proteger los servicios de red, como autenticación, cifrado y control de conexiones de red.		Actualizar y/o cambiar el controlador Wifi, actualmente vía software.
	Preparar, e implementar políticas, procedimientos y controles formales, para proteger la transmisión de información por todo tipo de medios de comunicación.		Implementar WireShark o un software similar.
10	**Adquisición, desarrollo y mantenimiento de los sistemas**	**Art. 39**	
	Determinar los requisitos de seguridad, como la criptografía, gestión de sesiones, entre otros.		Actualizar el sistema o ejecutor del sistema de gestión de seguridad de la información.
11	**Registro de Datos Personales**	**Art. 33, 55,56,57,59,60**	

	La institución deberá registrar los datos personales de todos sus clientes.		Se registraron todos los datos personales de todos sus clientes.
12	**Gestión de incidentes de seguridad de la información**	**Art. 43,46**	
	Se deberá notificar la vulneración de seguridad en caso que exista.		Se resolvieron las notificaciones de las vulneraciones de seguridad.
13	**Aspectos de seguridad de la información para la gestión de la continuidad**	**Art. 61**	
	La organización, debe determinar sus requerimientos de seguridad de la información, así como la continuidad de la gestión de dicha seguridad durante situaciones adversas.		Implementar un centro de datos de reemplazo virtual

El cronograma para la implementación, se visualiza en la figura 19, la cual se dio de la siguiente manera:

Figura 19.

Cronograma de Cumplimiento de la Implementación de las consideraciones definidas por el cumplimiento de la Ley Orgánica de Protección de Datos



4.2.3. Aplicación de la Fase 3. Control

En la tabla 3 se da la clasificación del porcentaje de cumplimiento de la siguiente manera del 0 al 33% tienen una calificación bajo; mientras que del 34 al 66% se da una calificación parcial y del 67 al 100% tiene calificación alto, como se detalla en el Anexo 1, verificando lo que se cumplió en función del porcentaje delimitado

Tabla 3.
Control de las consideraciones planteadas para dar cumplimiento de la Ley Orgánica de Protección de Datos Personales

Ítem	Cumplimiento	Porcentaje de cumplimiento	Validación
1	**Seguridad de Datos Personales**	**Parcial**	**Anexo 1**
	La política institucional, requiere de actualizaciones, que permita contener la protección de datos personales.	Parcial	Check List
2	**Organización de la seguridad de la información**	**Parcial**	**Anexo 1**
	Desarrollar una Política interna de Protección de Datos que detalle las obligaciones y disposiciones de la Ley y su Reglamento.	Parcial	Check List
	Generar procesos de tratamiento de información de datos, de distintos clientes, así como proveedores.	Parcial	Check List
	Establecer a través de memorandos, las responsabilidades, que permita fijar la seguridad de la información.	Parcial	Check List
	Crear una política de acceso a la información, así como a los datos personales.	Parcial	Check List
	Desarrollar un proceso de consultoría sobre vulnerabilidades al departamento de Tecnología de la información	Parcial	Check List

	Organizar reuniones con el Dirección Nacional de Datos Públicos, que permita dar soporte a la implementación de la normativa.	Alto	Check List
	En particular, mejorar el tratamiento de datos personales.	Parcial	Check List
	Visualizar, crecientes amenazas a la seguridad de la información, dando un énfasis, especial a la protección de los datos personales.	Parcial	Check List
	Formular un procedimiento, para el tratamiento de datos personales en los servicios que presta la organización, tanto virtual como presencial.	Parcial	Check List
	Ampliar el acceso a los datos personales en la política.	Alto	Check List
	Establecer una Política de Tratamiento de Datos Personales, la cual debe incluir la gestión de los distintos procedimientos administrativos.	Bajo	Check List
	Actualizar políticas de seguridad en los sistemas informáticos de los sitios web, de la institución financiera.	Bajo	Check List
	Ejecutar, políticas, así como procesos internos relacionados con la protección de datos personales.	Alto	Check List
	Desarrollar una política de respaldo de información, comprando un software de respaldo automático a la biblioteca de cintas de la institución financiera.	Parcial	Check List
	Conectarse a través de VPN, que permita registrar, un tiempo definido de conexión, así como al acceso al sistema.	Parcial	Check List
3	**Seguridad de los recursos activos humanos.**	**Parcial**	**Anexo 1**

	Procedimientos de la Junta Directiva Administrativa que establezcan claramente el procesamiento de la información recopilada en el CV y documentos necesarios.	Parcial	Check List
	La actualización del contrato debe ser incluido en el proceso de la Junta Directiva.	Parcial	Check List
	Procedimientos de la Junta Directiva Administrativa que establezcan claramente, la protección del procesamiento de la información recopilada en los clientes.	Parcial	Check List
	Designar un responsable del Departamento de Seguridad de la Información y Tratamiento de Datos, según normativa interna.	Bajo	Check List
	Procesamientos, designados, de la Junta Directiva Administrativa, que establezcan claramente el proceso de procesamiento de la información recopilada.	Alto	Check List
4	**Gestión de datos sensibles.**	**Parcial**	**Anexo 1**
	Puede fundamentarse en la orientación de la matriz productiva, pudiendo incluir, los datos personales como otro recurso.	Parcial	Check List
	Implementar un software de inventario, que permita delimitar varios parámetros establecidos.	Parcial	Check List
	Eliminar información con software gratuito.	Bajo	Check List
	Delimitar la política interna de tratamiento personal, así como los procedimientos de intercambio de información según lo dispuesto en la Ley Orgánica de Protección de Datos Personales.	Alto	Check List

	Desarrollar una política de respaldo de información, para lo cual se debe comprar un software de respaldo automático a la biblioteca de cintas.	Alto	Check List
	Adquisición de soluciones antivirus y anti spam.	Alto	Check List
	Adquisición de equipos de protección perimetral de nueva generación (Firewall).	Alto	Check List
	Aplicar herramientas de cifrado de información libre o gratuita como QuickHash, MultiHasher.	Bajo	Check List
	El proceso de gestión de medios extraíbles deberá identificar los medios que sujeten datos personales, para lo cual se debe tratarlos adecuadamente.	Parcial	Check List
5	**Control de acceso**	**Parcial**	**Anexo 1**
	Implementar módulos de auditoría en el sistema informático de la organización financiera.	Parcial	Check List
	Actualizar el sistema informático, constituido, sobre el software que tiene varios tiempos de uso y actualización de la tecnología, también efectuar el diseño de roles y perfiles de los diferentes colaboradores.	Alto	Check List
	Implementar un software libre o de código abierto	Parcial	Check List
6	**Criptografía**	**Parcial**	**Anexo 1**
	Implementar la utilización de herramientas criptográficas en software libre alguno.	Parcial	Check List
7	**Seguridad física y del entorno**	**Alto**	**Anexo 1**
	Determinar mayor protección del servidor.	Alto	Check List

	Adquirir un UPS para los equipos, porque no hay energía de emergencia para todas las estaciones de trabajo.	Alto	Check List
	Modificación de cableado estructurado.	Alto	Check List
8	**Seguridad de las operaciones**	**Alto**	**Anexo 1**
	Legitimación de un segundo centro de datos.	Parcial	Check List
	Implementar servidor NTP.	Parcial	Check List
9	**Seguridad en las comunicaciones**	**Parcial**	**Anexo 1**
	Actualizar y/o cambiar el controlador Wifi, actualmente vía software.	Parcial	Check List
	Implementar WireShark o un software similar.	Parcial	Check List
10	**Adquisición, desarrollo y mantenimiento de los sistemas**	**Alto**	**Anexo 1**
	Actualizar el sistema o ejecutor del sistema de gestión de seguridad de la información.	Alto	Check List
11	**Registro de Datos Personales**	**Alto**	**Anexo 1**
	Se registraron todos los datos personales de todos sus clientes.	Alto	Check List
12	**Gestión de incidentes de seguridad de la información**	**Alto**	**Anexo 1**
	Se resolvieron las notificaciones de las vulneraciones de seguridad.	Alto	Check List
13	**Aspectos de seguridad de la información para la gestión de la continuidad**	**Parcial**	**Anexo 1**
	Implementar un centro de datos de reemplazo virtual	Parcial	Check List

El porcentaje de cumplimiento se da en función de las evaluaciones delimitadas las cuales se dan en función de la evaluación de cada ítem determinado, como se indica en la Tabla 4.

Tabla 4.
Control de las consideraciones planteadas para dar cumplimiento de la Ley Orgánica de Protección de Datos Personales

Ítem	Cumplimiento	Calificación
1	Seguridad de Datos Personales	Parcial
2	Organización de la seguridad de la información	Parcial
3	Seguridad de los recursos activos humanos.	Parcial
4	Gestión de datos sensibles	Parcial
5	Control de acceso	Alto
6	Criptografía	Parcial
7	Seguridad física y del entorno	Alto
8	Seguridad de las operaciones	Parcial
9	Seguridad en las comunicaciones	Parcial
10	Adquisición, desarrollo y mantenimiento de los sistemas	Alto
11	Relaciones de Datos Personales	Alto
12	Gestión de incidentes de seguridad de la información	Alto
13	Aspectos de seguridad de la información para la gestión de la continuidad	Parcial
	Cumplimiento	**Alto**

4.2.4. Aplicación de la Fase 4. Ejecución

La aplicación de la fase 4, se dio en función del porcentaje de cumplimiento valorado anteriormente, y por lo que estos son:

4.2.4.1. Seguridad de Datos Personales

Para mejorar la seguridad de los datos personales en la Cooperativa de Ahorro y Crédito “Pablo Muñoz Vega”, puede emplear las siguientes estrategias en función de los estándares, detalladas en la Tabla 5, son:

Tabla 5.
Estrategias para mejorar la seguridad de los datos personales en la Cooperativa de Ahorro y Crédito “Pablo Muñoz Vega”

Estándares	Estrategias	Descripción
SGSI (ISO/IEC 27001:2022)	Evaluación de riesgos	Identificación de activos, amenazas, vulnerabilidades, análisis y tratamiento de riesgos.
	Políticas de seguridad	Desarrollo, documentación, comunicación y entrenamiento en políticas de seguridad de la información.
	Controles de acceso	Implementación de controles de acceso basados en roles y revisión periódica de accesos.
Guías prácticas (ISO/IEC 27002:2022)	Concientización y formación	Programas de formación continua y evaluaciones periódicas para todo el personal.
	Gestión de activos	Inventario actualizado y etiquetado de información sensible con procedimientos de manejo y eliminación segura.
	Cifrado de datos	Utilización de cifrado robusto (TLS/SSL para datos en tránsito, AES-256 para datos en reposo).
Gestión de privacidad (ISO/IEC 27701:2019)	Roles y responsabilidades	Designación de un Oficial de Protección de Datos (DPO) y formación de un equipo de privacidad.
	Políticas de privacidad	Desarrollo y comunicación de políticas de privacidad claras y accesibles.

	Derechos de los titulares de datos	Establecimiento de procedimientos para ejercer derechos, con tiempos de respuesta definidos.
Implementación del SGSI institucional	Evaluación continua	Auditorías internas periódicas y revisiones de la dirección para evaluar y mejorar el SGSI.
	Mejora continua	Aplicación del ciclo PDCA (Plan-Do-Check-Act) y gestión de cambios documentada
	Incidentes de seguridad	Desarrollo y prueba de un plan de respuesta a incidentes, con documentación de lecciones aprendidas.
Medidas adicionales específicas	Autenticación multifactor (MFA)	Implementación de MFA para todas las cuentas que acceden a datos personales.
	Monitoreo y registro	Implementación de sistemas de monitoreo y revisiones regulares de registros de actividades.
	Respaldo y recuperación	Establecimiento de un plan de respaldo y un plan de recuperación ante desastres, con pruebas periódicas.
Cumplimiento normativo	Auditorías externas	Contratación de auditores externos y corrección de deficiencias identificadas.
	Documentación	Mantenimiento y disponibilidad de registros detallados y actualizados de todas las políticas, procedimientos y controles.

Mientras que los mecanismos que pueden implementarse, en la seguridad de los datos personales en la Cooperativa de Ahorro y Crédito “Pablo Muñoz Vega” según la tabla 6, son:

Tabla 6.
Mecanismos a implementar la seguridad de los datos personales en la Cooperativa de Ahorro y Crédito "Pablo Muñoz Vega"

Mecanismo	Pasos	Operaciones	Descripción
1. Cifrado Avanzado	a. Cifrado de datos en tránsito	TLS/SSL	Utilización de protocolos seguros como TLS/SSL para cifrar la comunicación entre servidores y clientes.
		VPN	Implementación de redes privadas virtuales (VPN) para proteger las conexiones remotas.
	b. Cifrado de datos en reposo	AES-256	Uso de algoritmos de cifrado robustos como AES-256 para proteger los datos almacenados.
		Cifrado de discos completos	Implementación de cifrado a nivel de disco para proteger todos los datos en dispositivos de almacenamiento.
2. Control de Acceso Riguroso	a. Autenticación Multifactor (MFA)	MFA para todos los accesos críticos:	Implementación de MFA en todas las cuentas que acceden a datos personales, combinando algo que el usuario sabe (contraseña) con algo que el usuario tiene

			(token, aplicación de autenticación)
	b. Gestión de Identidades y Accesos (IAM)	Políticas de acceso basado en roles (RBAC)	Asignación de permisos basados en el rol del empleado, limitando el acceso solo a la información necesaria para sus funciones.
		Revisiones periódicas de acceso	Realización de revisiones periódicas para asegurar que los accesos otorgados sigan siendo necesarios y adecuados.
3. Monitoreo y Detección de Amenazas	a. Sistemas de Detección y Prevención de Intrusiones (IDS/IPS)	Implementación de IDS/IPS	Implementación de sistemas que detecten y prevengan intrusiones en la red y los sistemas de la organización.
	b. Sistemas de Información y Gestión de Eventos de Seguridad (SIEM)	Implementación de SIEM	Utilización de soluciones SIEM para recopilar, analizar y correlacionar eventos de seguridad, permitiendo una detección y respuesta rápida a incidentes.
4. Gestión de Vulnerabilidades	a. Evaluaciones de Vulnerabilidades	Escaneos de vulnerabilidades	Realización de escaneos de vulnerabilidades regulares para identificar y corregir debilidades en los sistemas y aplicaciones.
	b. Pruebas de Penetración	Pentesting	Contratación de profesionales para realizar pruebas de penetración, simulando ataques reales para identificar y corregir vulnerabilidades.

5. Respaldo y Recuperación	a. Políticas de Respaldo	Respaldo regular	Implementación de políticas de respaldo regular para asegurar que los datos estén protegidos contra pérdida.
		Almacenamiento seguro de respaldos	Almacenamiento de copias de seguridad en ubicaciones seguras y cifradas.
	b. Plan de Recuperación ante Desastres	Desarrollo y prueba del plan de recuperación	Creación y prueba regular de un plan de recuperación ante desastres para asegurar la continuidad de las operaciones.
6. Políticas y Procedimientos de Seguridad	a. Políticas de Seguridad de la Información	Desarrollo y mantenimiento de políticas	Desarrollo de políticas claras y detalladas de seguridad de la información, revisadas y actualizadas regularmente.
	b. Procedimientos de Respuesta a Incidentes	Plan de respuesta a incidentes	Desarrollo y prueba regular de un plan de respuesta a incidentes para manejar de manera efectiva cualquier incidente de seguridad.
7. Concientización y Capacitación	a. Programas de Capacitación	Formación continua	Programas de formación continua para todo el personal sobre prácticas seguras y protección de datos personales.
	b. Simulaciones y Pruebas	Simulaciones de ataques	Realización de simulaciones de ataques de phishing y otros tipos de amenazas para evaluar y mejorar la preparación del personal.
8. Gestión de Proveedores	a. Evaluación de Seguridad de Proveedores	Evaluación y auditoría	Realización de evaluaciones y auditorías de seguridad a los proveedores para asegurar

			que cumplan con las políticas y estándares de seguridad de la organización.
	b. Contratos y Acuerdos	Acuerdos de Nivel de Servicio (SLA)	Establecimiento de SLAs claros que incluyan requisitos de seguridad y privacidad para los proveedores.

En tanto que, para promulgar las políticas de seguridad efectiva de manera esencial, que pueden implementarse, en la seguridad de los datos personales en la Cooperativa de Ahorro y Crédito "Pablo Muñoz Vega" según la tabla 7, son:

Tabla 7.
Operaciones a implementar la seguridad de los datos personales en la Cooperativa de Ahorro y Crédito "Pablo Muñoz Vega"

Operaciones	Acciones	Descripción
Desarrollo y Revisión de Políticas	Redacción clara y comprensible	Escribir políticas en lenguaje accesible y comprensible para todos.
	Revisión colaborativa	Involucrar a diferentes departamentos en la revisión de políticas.
	Aprobación de la alta dirección	Obtener el respaldo de la alta dirección para las políticas.
Comunicación Efectiva	Anuncios formales	Informar a todos los empleados sobre las nuevas políticas a través de diversos canales.
	Documentación accesible	Publicar las políticas en una ubicación accesible y conocida.
	Resumen ejecutivo	Proporcionar resúmenes de las políticas para facilitar su comprensión.
Capacitación y Concientización	Sesiones de capacitación inicial	Organizar sesiones de capacitación para explicar las políticas y su importancia.

	Capacitación continua	Implementar programas de capacitación regular y actualizaciones.
	Simulaciones y ejercicios prácticos	Realizar simulaciones y ejercicios para evaluar la comprensión y respuesta.
Implementación y Monitoreo	Plan de implementación	Desarrollar un plan detallado con responsabilidades y plazos claros.
	Monitoreo y cumplimiento	Establecer sistemas de monitoreo para asegurar el cumplimiento.
	Mecanismos de reporte	Implementar mecanismos de reporte seguro para violaciones de seguridad.
Evaluación y Mejora Continua	Revisiones periódicas	Programar revisiones periódicas de las políticas.
	Recopilación de feedback	Recoger feedback de los empleados sobre la eficacia de las políticas.
	Actualización de políticas	Realizar actualizaciones basadas en evaluaciones y feedback.

4.2.4.2. Organización de la seguridad de la información

Para poder realizar la organización de la seguridad de la información, durante la implementación de la Ley Orgánica de Protección de Datos Personales en la Cooperativa de Ahorro y Crédito “Pablo Muñoz Vega”, es:

1. **Diagnóstico Inicial**

a) **Evaluación de la Situación Actual**

- **Auditoría de Seguridad:** Contratar un equipo de auditoría interna o externa para realizar una evaluación exhaustiva de los sistemas de información y las prácticas actuales de manejo de datos personales.
- **Inventario de Activos:** Crear un inventario detallado de todos los activos de información, incluyendo hardware, software, datos y personas responsables.

b) Identificación de Activos de Información

- **Clasificación de Datos:** Clasificar los datos en función de su sensibilidad y criticidad. Por ejemplo, datos personales sensibles, datos financieros, etc.
- **Mapeo de Flujos de Datos:** Documentar cómo los datos personales se recopilan, almacenan, procesan y transfieren dentro de la organización.

2. Desarrollo del SGSI Basado en ISO/IEC 27001:2022

a) Definición del Alcance

- **Ámbito del SGSI:** Determinar qué partes de la organización y qué tipos de datos estarán cubiertos por el SGSI. Documentar el alcance de manera clara y concisa.

b) Política de Seguridad de la Información

- **Desarrollo de la Política:** Redactar una política de seguridad de la información que incluya objetivos de seguridad, compromisos de la dirección y directrices para la implementación.
- **Aprobación de la Dirección:** Obtener la aprobación formal de la alta dirección para asegurar el compromiso y apoyo necesario.

c) Evaluación de Riesgos

- **Metodología de Evaluación de Riesgos:** Seleccionar y documentar una metodología para la evaluación de riesgos, como ISO 31000.
- **Identificación de Amenazas y Vulnerabilidades: Realizar** talleres con stakeholders para identificar amenazas y vulnerabilidades que puedan afectar a los activos de información.
- **Análisis de Impacto y Probabilidad:** Evaluar el impacto potencial y la probabilidad de ocurrencia de cada riesgo identificado.

d) Control de Riesgos

- **Selección de Controles:** Elegir controles de seguridad adecuados basados en las directrices de ISO/IEC 27002:2022. Por ejemplo, controles de acceso, cifrado, monitoreo de redes, etc.
- **Implementación de Controles:** Implementar los controles seleccionados y documentar los procesos y procedimientos necesarios.

3. Implementación de ISO/IEC 27701:2019

a) Extensión del SGSI a un Sistema de Gestión de la Privacidad (SGP)

- **Integración de ISO/IEC 27701:** Adaptar el SGSI existente para incluir los controles y procesos específicos de ISO/IEC 27701 relacionados con la privacidad.

b) Política de Privacidad

- **Desarrollo de la Política de Privacidad:** Crear una política de privacidad que describa cómo se gestionarán los datos personales conforme a ISO/IEC 27701 y la legislación local.
- **Procedimientos de Gestión de Datos Personales:** Documentar procedimientos específicos para la recolección, almacenamiento, procesamiento y eliminación de datos personales.

c) Roles y Responsabilidades

- **Designación del DPO:** Nombrar un Oficial de Protección de Datos (DPO) que será responsable de supervisar el cumplimiento de las leyes de protección de datos.
- **Asignación de Responsabilidades:** Definir y comunicar claramente las responsabilidades de todos los empleados respecto a la protección de datos personales.

4. Implementación de Controles Técnicos y Organizativos

a) Controles de Acceso

- **Autenticación y Autorización:** Implementar medidas robustas de autenticación (como 2FA) y autorización para asegurar que solo personal autorizado acceda a datos personales.
- **Gestión de Identidades:** Utilizar sistemas de gestión de identidades y accesos (IAM) para gestionar de manera centralizada las identidades de los usuarios y sus permisos.

b) Cifrado y Protección de Datos

- **Cifrado de Datos:** Utilizar cifrado fuerte (AES-256, por ejemplo) para proteger los datos sensibles tanto en tránsito como en reposo.
- **Protección de Bases de Datos:** Implementar medidas de seguridad adicionales para bases de datos, como cifrado de columnas y registros sensibles.

c) Gestión de Incidentes de Seguridad

- **Plan de Respuesta a Incidentes:** Desarrollar y documentar un plan detallado de respuesta a incidentes que incluya procedimientos para la detección, análisis, contención y recuperación de incidentes.
- **Equipo de Respuesta a Incidentes:** Formar un equipo de respuesta a incidentes de seguridad (CSIRT) con roles y responsabilidades claramente definidos.

d) Auditorías y Revisión

- **Auditorías Internas:** Realizar auditorías internas periódicas para evaluar la efectividad del SGSI y el cumplimiento de los controles de seguridad y privacidad.
- **Revisión por la Dirección:** Programar revisiones regulares por la alta dirección para evaluar el desempeño del SGSI y realizar ajustes necesarios.

5. Capacitación y Concienciación

a) Programa de Capacitación

- **Desarrollo de Cursos:** Crear cursos de capacitación sobre seguridad de la información y protección de datos personales para todos los empleados.

- **Frecuencia de la Capacitación:** Programar sesiones de capacitación inicial y continua para asegurar que los empleados estén siempre informados sobre las mejores prácticas y requisitos legales.

b) Concienciación

- **Campañas de Concienciación:** Implementar campañas regulares de concienciación, como boletines informativos, pósteres y seminarios web, para promover una cultura de seguridad de la información.

6. Monitoreo y Mejora Continua

a) Monitoreo y Evaluación Continua

- **Sistemas de Monitoreo:** Implementar sistemas de monitoreo continuo para detectar y responder rápidamente a incidentes de seguridad.
- **Revisión de Controles:** Revisar y evaluar regularmente la efectividad de los controles de seguridad implementados.

b) Revisión de la Dirección

- **Informes Regulares:** Proveer a la alta dirección informes regulares sobre el estado del SGSI, incluyendo métricas de desempeño y hallazgos de auditorías.
- **Reuniones de Revisión:** Realizar reuniones periódicas con la alta dirección para discutir los resultados de las revisiones y planificar mejoras.

c) Mejora Continua

- **Proceso de Mejora Continua (PDCA):** Implementar el ciclo Plan-Do-Check-Act (PDCA) para asegurar la mejora continua del SGSI y la gestión de la privacidad.
- **Retroalimentación y Ajustes:** Utilizar la retroalimentación de auditorías, monitoreo y revisiones para realizar ajustes y mejorar los procesos de seguridad y privacidad.

7. Cumplimiento Legal y Normativo

a) Revisión y Alineación Legal

- **Análisis de Cumplimiento:** Realizar un análisis de cumplimiento para asegurar que todas las políticas y procedimientos estén alineados con la Ley Orgánica de Protección de Datos Personales y otras normativas relevantes.
- **Asesoría Legal:** Consultar con expertos legales para interpretar y aplicar correctamente las leyes y regulaciones de protección de datos.

b) Evaluación de Impacto en la Privacidad (PIA)

- **Realización de PIA:** Llevar a cabo evaluaciones de impacto en la privacidad (PIA) para identificar y mitigar riesgos asociados con el tratamiento de datos personales en nuevos proyectos o cambios significativos.
- **Documentación de PIA:** Documentar los resultados de las PIA y las medidas de mitigación adoptadas.

8. Documentación y Registros

a) Mantener Documentación Completa

- **Políticas y Procedimientos**: Asegurar que todas las políticas, procedimientos y documentos del SGSI estén actualizados y accesibles para el personal autorizado.
- **Manuales y Guías:** Desarrollar manuales y guías detalladas para la implementación y gestión del SGSI y la privacidad.

b) Registros de Actividades

- **Logs y Registros:** Mantener logs y registros detallados de todas las actividades relacionadas con la seguridad de la información y la protección de datos personales.
- **Archivado Seguro:** Asegurar que los registros se almacenen de manera segura y se conserven conforme a las políticas de retención de datos.

Recursos Adicionales

a) Herramientas y Software

- **Gestión de Riesgos:** Utilizar herramientas de gestión de riesgos que cumplan con los estándares ISO para identificar y mitigar riesgos.

- **Cifrado y Seguridad de Datos:** Implementar software de cifrado y soluciones de seguridad de datos que proporcionen protección robusta contra accesos no autorizados.
- **Monitoreo y Detección:** Utilizar sistemas avanzados de monitoreo y detección de intrusos para identificar y responder a amenazas en tiempo real.

4.2.4.3. Control de acceso

La planificación de adquisición para la implementación del sistema de supervisión de acceso con tarjeta magnética en la Cooperativa de Ahorro y Crédito "Pablo Muñoz Vega", se da en función de varias fases que son:

Fase 1: Investigación y Evaluación

1. **Identificación de Requerimientos**

- Definir los requisitos técnicos y funcionales del sistema de supervisión de acceso con tarjeta magnética.
- Determinar las necesidades específicas de cada área y ubicación dentro de la cooperativa.

2. **Investigación de Proveedores y Soluciones**

- Investigar proveedores que ofrecen sistemas de control de acceso compatibles con tarjetas magnéticas.
- Evaluar las soluciones disponibles en el mercado en términos de funcionalidad, seguridad, costos y soporte técnico.

Fase 2: Presupuesto y Planificación Financiera

3. **Establecimiento del Presupuesto**

- Determinar el presupuesto disponible para la adquisición e implementación del sistema.
- Incluir costos de hardware, software, instalación, capacitación y mantenimiento inicial.

4. **Desarrollo de Cronograma y Plazos**

- Establecer un cronograma detallado para la adquisición, instalación y puesta en marcha del sistema.

- Asignar plazos específicos para cada etapa del proyecto, considerando la disponibilidad de recursos y la prioridad de implementación por áreas.

Fase 3: Selección de Proveedores y Negociación

5. **Selección de Proveedor**

- Basado en la investigación previa, seleccionar al proveedor que mejor se ajuste a los requisitos y presupuesto establecidos.
- Considerar la reputación del proveedor, referencias de otros clientes y experiencia en implementaciones similares.

6. **Solicitud de Propuestas (RFP)**

- Preparar y enviar una solicitud de propuestas detallada a los proveedores seleccionados, especificando los requisitos técnicos, funcionales y financieros del proyecto.

7. **Negociación y Contratación**

- Negociar términos contractuales, incluyendo precios, tiempos de entrega, soporte técnico, garantías y condiciones de servicio.
- Formalizar contratos con el proveedor seleccionado, asegurando que todos los aspectos del acuerdo estén documentados y clarificados.

Fase 4: Adquisición e Instalación

8. **Adquisición de Hardware y Software**

- Realizar pedidos de hardware (lectores de tarjetas, tarjetas magnéticas, paneles de control) según lo acordado en el contrato.
- Adquirir licencias de software necesarias para la gestión y monitoreo del sistema de control de acceso.

9. **Instalación y Configuración**

- Coordinar la entrega e instalación del hardware en las ubicaciones designadas dentro de la cooperativa.
- Configurar el software de gestión de acceso de acuerdo con los requisitos específicos y las políticas de seguridad establecidas.

Fase 5: Capacitación y Puesta en Marcha

10. Capacitación del Personal

- Programar sesiones de capacitación para el personal de la cooperativa sobre el uso adecuado del sistema de supervisión de acceso.
- Educar sobre las políticas de seguridad, procedimientos de emergencia y manejo de tarjetas magnéticas.

11. Pruebas de Funcionalidad y Aceptación

- Realizar pruebas exhaustivas del sistema para verificar su funcionamiento correcto y su integración con el SGSI institucional.
- Obtener la aceptación formal del sistema por parte de los responsables designados en la cooperativa.

Fase 6: Monitoreo y Mantenimiento

12. Implementación y Monitoreo Continuo

- Implementar el sistema de supervisión de acceso en todas las áreas de la cooperativa de acuerdo con el plan establecido.
- Establecer procedimientos de monitoreo continuo para supervisar el uso y la efectividad del sistema.

13. Mantenimiento y Actualización

- Programar mantenimientos regulares del hardware y software para garantizar su funcionamiento óptimo.
- Actualizar el sistema conforme a nuevas versiones de software y cambios en los estándares de seguridad.

Fase 7: Evaluación y Mejora Continua

14. Auditorías y Evaluaciones

- Realizar auditorías internas para evaluar el cumplimiento con los estándares ISO/IEC y las políticas establecidas.
- Prepararse para auditorías externas según sea necesario.

15. Mejora Continua del Sistema

- Implementar un proceso formal de mejora continúa basado en retroalimentaciones de usuarios, resultados de auditorías y cambios en el entorno de seguridad.

4.2.4.4. Criptografía

A continuación, se detalla la tabla 8, criptográfica, las cuales son de manera más concisa, proporcionando una referencia útil, para poder aplicar en la Cooperativa de Ahorro y Crédito “Pablo Muñoz Vega” de la siguiente manera:

Tabla 8.
Soluciones criptográficas dadas en la aplicación de la Cooperativa de Ahorro y Crédito “Pablo Muñoz Vega”

Solución Criptográfica	**Descripción**	**Aplicación en la Cooperativa "Pablo Muñoz Vega"**
Encriptación de datos	Utilización de algoritmos criptográficos (como AES) para cifrar datos sensibles almacenados y TLS para asegurar la transmisión segura de datos.	Protección de datos personales almacenados en bases de datos y durante la transmisión entre clientes y servidores.
Tokenización	Sustitución de datos sensibles por tokens no sensibles mediante soluciones de tokenización.	Reducción del riesgo de exposición de datos sensibles al reemplazarlos con tokens en aplicaciones y sistemas de la cooperativa.
Firmas digitales	Empleo de firmas digitales basadas en criptografía de clave pública para verificar la autenticidad y la integridad de los datos.	Verificación y autenticación segura de documentos y transacciones críticas realizadas por la cooperativa.
Gestión de claves	Implementación de políticas y procedimientos para la generación, almacenamiento y gestión segura de claves criptográficas.	Aseguramiento de que las claves criptográficas utilizadas en sistemas y procesos internos estén protegidas y se gestionen de manera segura.

Auditorías criptográficas	Realización de revisiones periódicas para evaluar el cumplimiento de estándares criptográficos y mejorar las prácticas de seguridad.	Evaluación continua de la implementación de soluciones criptográficas para asegurar la conformidad con normativas y estándares internacionales.
Cumplimiento normativo	Aseguramiento de que las soluciones criptográficas implementadas cumplan con las leyes y regulaciones de protección de datos vigentes.	Garantía de conformidad con la Ley Orgánica de Protección de Datos Personales y otras normativas relevantes en el manejo de datos personales.

Los protocolos para poder implementar las soluciones criptográficas indicadas son:

Tabla 9.
Protocolos seguro en función de la aplicación de la Cooperativa de Ahorro y Crédito "Pablo Muñoz Vega"

Protocolo	**Descripción**	**Aplicación en la Cooperativa "Pablo Muñoz Vega"**
TLS (Transport Layer Security)	Protocolo criptográfico que proporciona comunicaciones seguras a través de una red, como Internet.	Uso en todas las transacciones y comunicaciones en línea para asegurar la confidencialidad e integridad de los datos.
IPsec (Internet Protocol Security)	Conjunto de protocolos utilizados para asegurar el intercambio de datos a través de redes IP.	Implementación en redes privadas virtuales (VPN) para proteger el tráfico de datos entre sedes y oficinas remotas de la cooperativa.
SFTP (Secure File Transfer Protocol)	Protocolo de transferencia de archivos que utiliza SSH para	Utilización para la transferencia segura de archivos sensibles entre

	encriptar datos durante la transmisión.	sistemas y con socios comerciales externos.
HTTPS (Hypertext Transfer Protocol Secure)	Versión segura del protocolo HTTP que utiliza TLS para encriptar las comunicaciones web.	Empleo en el sitio web de la cooperativa y aplicaciones en línea para proteger la interacción de los clientes con la institución.
SSH (Secure Shell)	Protocolo de red para operar de manera segura sobre una red insegura utilizando una conexión cifrada.	Acceso seguro a servidores y sistemas críticos de la cooperativa para administración remota y mantenimiento.

4.2.4.5. Seguridad de operaciones

Para cumplir con la seguridad de operaciones durante la implementación de la Ley Orgánica de Protección de Datos Personales en la Cooperativa de Ahorro y Crédito "Pablo Muñoz Vega", considerando los estándares ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 27701:2019 y el SGSI institucional, se puede tener en cuenta:

1. **Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI):**

- Desarrollar e implementar un SGSI que cumpla con los requisitos de ISO/IEC 27001:2022. Esto implica establecer políticas, procedimientos y controles de seguridad de la información adecuados para la cooperativa.

2. **Evaluación de riesgos:**

- Realizar una evaluación de riesgos de seguridad de la información para identificar las amenazas y vulnerabilidades que podrían afectar la protección de los datos personales en la cooperativa.

3. **Controles de seguridad:**

- Implementar controles de seguridad basados en los principios y controles detallados en ISO/IEC 27002:2022. Esto incluye medidas técnicas, organizativas

y físicas para proteger los datos personales contra accesos no autorizados, modificaciones, divulgaciones o destrucciones no autorizadas.

4. **Gestión de accesos:**

- Establecer controles estrictos de gestión de accesos para garantizar que solo las personas autorizadas tengan acceso a los datos personales relevantes. Esto incluye la autenticación sólida y la gestión de privilegios.

5. **Capacitación y concienciación:**

- Realizar programas regulares de capacitación y concienciación en seguridad de la información para todos los empleados de la cooperativa. Esto garantiza que estén al tanto de las políticas de seguridad y de sus responsabilidades individuales para proteger los datos personales.

6. **Monitoreo y auditoría:**

- Implementar sistemas de monitoreo continuo y auditorías periódicas para verificar el cumplimiento de las políticas de seguridad de la información y para identificar posibles problemas de seguridad.

7. **Cumplimiento normativo:**

- Asegurar que todas las actividades de seguridad de la información estén alineadas con los requisitos de la Ley Orgánica de Protección de Datos Personales y otras regulaciones aplicables.

8. **Gestión de incidentes:**

- Establecer procedimientos claros de gestión de incidentes para responder rápidamente a violaciones de seguridad o brechas de datos, minimizando así el impacto potencial en los datos personales de los clientes y empleados.

9. **Mejora continua:**

- Implementar un ciclo de mejora continua para el SGSI, utilizando los principios de la norma ISO/IEC 27001. Esto implica revisar regularmente las políticas y procedimientos de seguridad, así como los controles implementados, para garantizar su eficacia y relevancia continua.

10. **Certificación y auditoría externa:**

- Considerar la posibilidad de obtener la certificación ISO/IEC 27001 para demostrar formalmente el compromiso de la cooperativa con la seguridad de la información. Además, realiza auditorías externas periódicas para validar el cumplimiento con los estándares y regulaciones aplicables.

4.2.4.6. Seguridad en las comunicaciones

La siguiente tabla 10, proporciona una estructura organizada para implementar cada paso de manera efectiva, asegurando las comunicaciones y el cumplimiento de la ley de protección de datos personales en la Cooperativa de Ahorro y Crédito "Pablo Muñoz Vega".

Tabla 10.
Estructura organizada de manera efectiva, asegurando la seguridad en las comunicaciones en la Cooperativa de Ahorro y Crédito "Pablo Muñoz Vega"

Proceso	Medidas y actividades	Detalles
1. Evaluación y Análisis Inicial	Conocimiento de la normativa	Comprender los requisitos específicos de la Ley Orgánica de Protección de Datos Personales aplicables a la cooperativa.
	Análisis de riesgos	Evaluar los riesgos asociados al manejo y transmisión de datos personales en la cooperativa.
2. Diseño de Políticas y Procedimientos	Políticas de seguridad de la información	Desarrollar políticas claras sobre la protección de datos personales y la seguridad en las comunicaciones. Incluir aspectos como clasificación de la información y gestión de accesos.
	Protección de datos en comunicaciones	Definir directrices para asegurar que las comunicaciones que involucren datos personales se realicen de

		manera segura, incluyendo el uso de cifrado y redes privadas virtuales (VPN).
3. Implementación de Medidas Técnicas y Organizativas	Seguridad de red	Implementar firewalls, detección de intrusiones y controles de acceso a la red para proteger la infraestructura de red.
	Cifrado	Utilizar cifrado robusto para proteger la confidencialidad de los datos durante su transmisión.
	Gestión de accesos	Implementar controles para garantizar que solo personas autorizadas accedan a los datos personales.
4. Capacitación y Concienciación	Formación del personal	Capacitar a los empleados sobre políticas de seguridad de la información y buenas prácticas en el manejo de datos personales.
5. Monitoreo y Mejora Continua	Auditorías y revisiones	Realizar auditorías periódicas para evaluar el cumplimiento de las políticas de seguridad y la normativa de protección de datos. Mejorar continuamente el sistema de seguridad según los hallazgos.
	Respuesta a incidentes	Establecer un plan de respuesta a incidentes para actuar rápidamente en caso de brechas de seguridad o violaciones de datos.
6. Cumplimiento Normativo	Seguimiento de normativas	Mantenerse al tanto de los cambios en la normativa de protección de datos y ajustar políticas y procedimientos en consecuencia.

CAPITULO V

PROPUESTA

Ficha Informativa	
Fecha de elaboración	10 de Julio del 2023
Realizado por:	Ing. Gerzon Vladimir Fuel Rodríguez
Revisado por:	Ing. Marcelo Caicedo
Aprobado por:	

La implementación de la Ley Orgánica de Protección de Datos Personales en la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega considerando los estándares ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 27001:2019 y el SGSI institucional, para dar cumplimiento de la siguiente manera:

5.1. Delimitación de políticas para el tratamiento de datos personales

5.1.1. Base legal

En función de lo establecido en la Constitución de la República del Ecuador y en la Ley Orgánica de Protección de Datos Personales publicada el 21 de mayo del 2021, por el Ingeniero Hugo del Pozo Barrezueta, quien es el Director del Registro Oficial, remitido con oficio del número PAN-CLC-2021-0384 del 11 de mayo del 2021; delimitada por información titulada en diferentes capítulos como son: el ámbito de aplicación integral; principios, derechos, especiales de datos, transferencia o comunicación y acceso a datos

personales por terceros, seguridad de datos personales, del responsable y del delegado de protección de datos personales, de la responsabilidad proactiva, transferencia o comunicación internacional de datos personales, de los requerimientos directos y de la gestión del procedimiento administrativo, medidas correctivas, infracciones y régimen sancionatorio, autoridad de protección de datos personales.

5.1.2. Responsable del Tratamiento de Datos Personales

Cooperativa de Ahorro y Crédito Pablo Muñoz Vega, ubicada en matriz en Tulcán, con dirección en la Colón y el 10 de agosto, con el Acuerdo Ministerial No. 2203, el 29 de julio de 1964; permitirá recolectar, almacenar y tratar datos personales, según la Ley Orgánica de Protección de Datos Personales (LOPDP).

5.1.3. Destinatarios

Esta política se aplica a todos los clientes, usuarios, colaboradores, proveedores, accionistas y en general, para todos aquellos, que presentan interés y tratamientos de datos personales. Incluyendo también a todas las personas naturales, que solicitan información sobre productos y/o servicios a través de sitios web, bancos móviles, agencias nacionales, y agentes no bancarios; por lo que también incluyen a cualquier persona para completar la transacción relacionada con el producto o servicio proporcionado.

5.1.4. Base de datos personales

Los datos podrán almacenarse en las bases de datos personales, que será inscrita en el Registro Nacional de Protección de Datos Personales.

5.1.5. Finalidades del Tratamiento de Datos Personales

Las finalidades del tratamiento de datos personales, según la Ley Orgánica de Protección de Datos Personales en la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega aplicando estándares ISO/IEC para dar cumplimiento con el registro oficial N° 459, son:

5.1.5.1. Clientes o usuarios

- Saber su comportamiento financiero, transaccional y crediticio, pudiendo cumplir con sus obligaciones legales.

- Completar los pasos necesarios para confirmar y actualizar la información del usuario

- Confirmar y verificar, las identidades de los diferentes usuarios, que permita proporcionar y gestionar productos, así como servicios e intercambiar información con diversos participantes del mercado local, nacional e internacional.

- Definir, mantener y finalizar relaciones contractuales.

- Grabar llamadas, que registren las interacciones de la Cooperativa con usuarios a través de los call center.

- Tomar comunicaciones relativas a la gestión de cobranzas y adquisición de cartera, ya sea directamente o a través de un tercero contratado para esta función.

- Garantizar prestaciones y gestiones adecuadas de los servicios financieros, abarcando la gestión de cobranza.

- Proporcionar información comercial, legal, de servicios u otra información de seguridad.

- Saber la ubicación del cliente, geolocalización e información de contacto para recibir notificaciones de seguridad y brindar beneficios e incentivos comerciales.

- Saber el estado de las operaciones activas, pasivas o de cualquier naturaleza o las que el cliente posee con la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega, así como con otras instituciones sean estas públicas, privadas o financieras.

- Prevenir el lavado de activos, así como la financiación del terrorismo, la detección del fraude, entre otras actividades ilegales, mediante la verificación de la información proporcionada por el cliente mediante fuentes públicas y privadas.

- Ejecutar, verificar o autorizar transacciones, pudiendo copiar datos confidenciales como huellas dactilares, imágenes o voz, si es necesario; tendiéndoles como registros únicos.

- Efectuar encuestas de satisfacción, a los clientes, por los servicios ofertados.

- Examinar con los distintos organismos administrativos y judiciales, las bases de datos públicas encargadas de gestionar este tipo de datos sobre multas y sanciones.

5.1.5.2. Proveedores

- La información requerida por el proveedor, cuando corresponda, puede incluir información sobre un individuo o entidad. Asimismo, es posible que dicha información pueda ser solicitada a empleados del proveedor que desempeñen alguna función o tengan algún vínculo con la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega.

- Implementar un procedimiento de intercambio de información entre proveedores y la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega, ejecutando procesos internos, influyendo relaciones contables, financieras, comerciales, logísticas, etc.

- Gestionar y fortalecer las vinculaciones comerciales con proveedores, contribuyendo a un mejor monitoreo.

- Analizar y evaluar el desempeño de proveedores para mejorar el proceso de contratación en la Cooperativa de Ahorro y Crédito.

- Realizar, así como analizar investigaciones comerciales, estadísticas, de riesgo, de mercado, interbancarias y financieras en base a resultados de proveedores.

- Gracias a convenios con sus proveedores, la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega, define que, como parte de su plan de continuidad comercial, puede realizar una copia de seguridad de toda la información en la que se almacenan datos personales utilizando cualquier almacenaje en la nube, donde se pueden transferir información a servidores internacionales para su almacenamiento.

5.1.5.3. Colaboradores

- Cumplir con las obligaciones y derechos procedentes de sus actividades, así como de las actividades propias de los fines principales de su institución financiera, que podrán realizar directamente o con la asistencia de terceros a quienes se transferirán sus datos para fines vinculados con la organización.

- Transferir sus datos personales a autoridades nacionales o extranjeras, las cuales puede ser judiciales o administrativas, si así lo requieren, algunas razones legales, procesales y/o fiscales.

- Acceder y autorizar los beneficios definidos por el empleador, según se requiera.

- Verificar sus datos contra listas, de control interno de acuerdo a las regulaciones nacionales y políticas internas, sobre todo aquellas que puedan estar vinculadas con los riesgos de lavado de dinero y financiamiento del terrorismo.

5.1.5.4. Accionistas

- Proporcionar información sobre procedimientos y requisitos de los accionistas.

- Proporcionar acceso a información a autoridades judiciales o administrativas que requieran datos para el desempeño de sus funciones.

- Gestionar los riesgos de blanqueo de capitales, financiación del terrorismo y corrupción.

5.1.5.5. Permitir, monitorear y proteger a instalaciones de la institución financiera

- Tener acceso a la información sobre empleados individuales y de empresas proveedoras que trabajan para la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega, pudiendo ingresar a sus instalaciones.

- Inspeccionar y determinar, aquel personal que tienen derechos de acceso a la instalación de la Cooperativa.

- Conservar la seguridad y supervisar, los accesos a los departamentos diferentes de la instalación de la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega.

- Supervisar los sistemas CCTV y respaldo de video para gestionar cualquier riesgo y cumplir con requisitos legales.

5.2. Delegado de protección de datos personales en Cooperativas de Ahorro y crédito Pablo Muñoz Vega

5.2.1. Perfil del delegado de protección de datos personales

El delegado de Protección de Datos es el responsable de detallar el significado y alcance, de los términos relevantes para la regulación, tales como datos personales, tratamientos, ficheros, responsable del tratamiento, encargado del tratamiento, etc., así como los estudios artísticos en general. 37, 38 y 39.

Las destrezas que se deben reunir el delegado de Protección de Datos (PDP), según normativa son:

- **Especializado en Protección de Datos Personales,** es una persona encargada, la cual tendrá amplios conocimientos y capacidades para administrar las leyes nacionales. Por lo que deberá conocer las actividades de procesamiento específicos que se llevan a cabo dentro de la institución financiera, donde se trate o supongan un riesgo para los derechos y libertades de los interesados.

- **Cualidades profesionales,** debe poseer conocimientos del Derecho y la práctica en materia de protección de datos.

- **Habilidades para su desempeño,** las habilidades que deben tener son, iniciativa propia, deben ser creativos, tener una visión global, debe tener un aprendizaje continuo, trabajar en equipo, poseer una capacidad de enfoque, empatía y capacidad de comunicación.

5.2.2. Posición del delegado de Protección de Datos

La posición del delegado de protección de datos es:

- **Participación necesaria,** el delegado de Protección de Datos (DPD) deberá intervenir con prontitud y su implicación será la adecuada en todo lo relativo a la protección de datos personales.

- **Recursos necesarios,** deberá estar basado en un presupuesto suficiente y acorde al ejercicio de su función, tanto para la obtención de servicios, medios

tecnológicos, humanos, en formación y cualquier otro recurso requerido para su correcta operación.

- **Reporte a la dirección,** el delegado de Protección de Datos (DPD), es la principal persona, en la rendición de cuentas, ya que se fundamenta de manera directa, la cual debe ser superior en la jerarquía.

- **Independencia,** es importante, darle independencia para el ejercicio de su labor, visualizando que pueda ejercer sus funciones con un manto de protección, libre de injerencias e instrucciones, tanto sobre cómo debe orientar su trabajo o como debe proceder y sin que pueda ser sancionado o despedido por ello, salvo que incurriera en alguna negligencia grave.

- **Conflictos e intereses,** es otro elemento importante tiene que ver con la necesidad de que el delegado de Protección de Datos (DPD) no tenga un conflicto de intereses.

- **Accesibilidad,** igualmente se requiere que el delegado de Protección de Datos (DPD), sea accesible y fácilmente contactable, por cualquier interés en el ejercicio de sus derechos.

5.2.3. Funciones del delegado de Protección de Datos

Las funciones del delegado son:

- **Funciones organizativas,** el delegado de Protección de Datos (DPD), deberá implantar y mantener un registro de operaciones de tratamiento de datos personales, donde se detallen las diferentes operaciones.

- **Funciones de Supervisión,** el DPD deberá encargarse de las violaciones a la seguridad de datos personales, debiendo notificar a la gerencia.

- **Funciones consultivas,** se le pedirá que asesore y monitoree el cumplimiento de las políticas de protección de datos vigentes, a la cual se le pedirá que revise los documentos y contratos, pudiendo proponer los cambios necesarios, que garanticen el cumplimiento con todos los requisitos legales.

- **Nexo de contacto,** en este caso, el DPD, debe cooperar con las autoridades supervisoras para responder a las solicitudes realizadas cuando se necesita información o para facilitar el acceso a los documentos o la información solicitada.

- **Funciones de información y sensibilización,** se trata de una cuestión de cumplimiento de la normativa vinculada a la protección de datos, que debe hacerse de forma integral, implicando a todos los empleados y, por tanto, es su responsabilidad concienciar y formar al personal

5.2.4. Responsabilidades del delegado de Protección de Datos

Entre sus responsabilidades están:

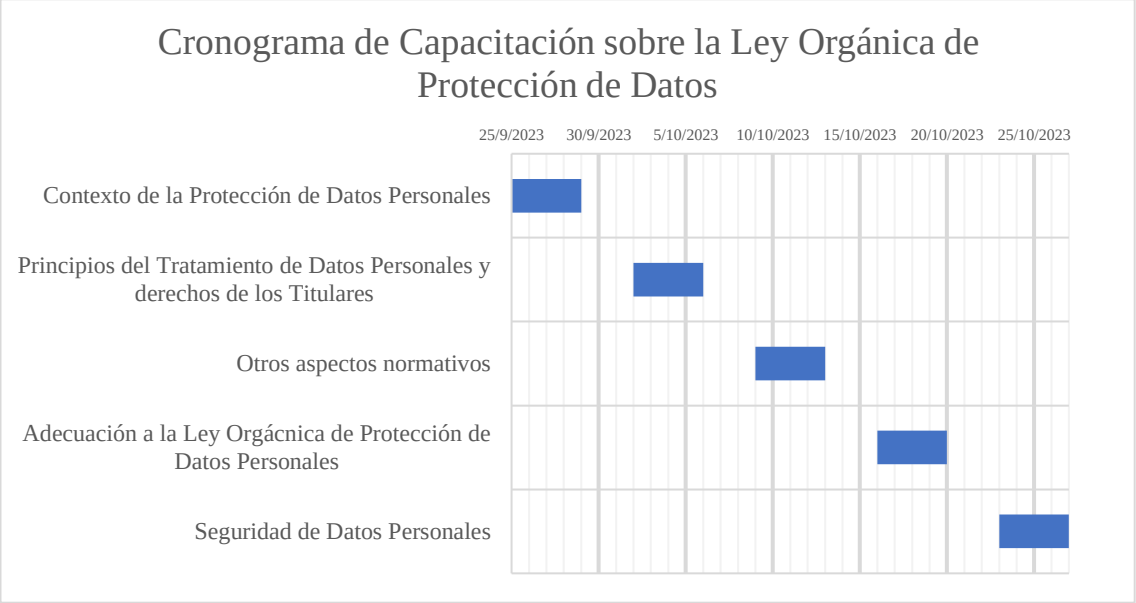
- **Responsabilidad Penal,** el delegado de Protección de Datos (DPD), será penalmente responsable, al llegar a incurrir en un ilícito tipificado penalmente

- **Responsabilidad Administrativa,** como sanción, las medidas adicionales deberían incluir la suspensión o revocación de los certificados emitidos como DPD. Aclarando que, según la normativa, no será personalmente, el responsable si incumple las obligaciones establecidas, las cuales pueden entenderse como normas destinadas a proteger el establecimiento del DPD eximiéndolo de responsabilidad.

5.3. Cronograma de capacitaciones al personal de la Cooperativas de Ahorro y crédito Pablo Muñoz Vega

El cronograma de capacitación, según la figura 26 es:

Figura 20.
Cronograma de Capacitación sobre la Protección de Datos basado en la Ley Orgánica de Protección de Datos



CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

- Se analizó el ciclo que se da a la información de datos iniciando con la ejecución de datos, seguido con la transmisión y almacenamiento de la información de datos, sigue la gestión, el acceso y la compartición de datos, finalizando con el análisis, la información e inteligencia de negocio; obteniendo como consecuencias la eficiencia operativa, la toma de decisiones informadas, así como la seguridad de la información, continuando con la colaboración efectiva y finalizando con la mejora continua en la institución.

- Se aplicó la metodología Business Process Management (BPM), iniciando con un diagnóstico actual de la protección de datos, mediante una encuesta elaborada a los colaboradores del Departamento de Tecnología de la Información, obteniéndose datos que necesitan implementar la Ley Orgánica de Protección de Datos aplicando estándares ISO/IEC para dar cumplimiento con el Registro N° 459, seguido por el modelado verificando qué se debe cumplir en cada

caracterización, continuando con la aplicación del control, y finalizando con la implementación, ejecución y optimización; obteniendo datos afirmativos; por lo que como consecuencia se tienen positivamente en términos de cumplimiento normativo; así como la mejora en la gestión de datos; continuando con la optimización de procesos, finalizando con la garantía de calidad y seguridad de datos.

- Se dio cumplimiento a las Normas y Regulaciones Relevantes, donde se puede definir los objetivos de capacitación; creando un Plan de Capacitación Estructurado, involucrando a expertos y formadores calificados, utilizando múltiples métodos de aprendizaje; fomentando una cultura de cumplimiento, documentando y manteniendo registros, la cual se da en función de la implementación de mejora continua en la Cooperativa de Ahorro y crédito Pablo Muñoz Vega.

- Se cumple con todo el proceso de creación del delegado de protección de datos personales, en la Cooperativa de Ahorro y crédito Pablo Muñoz Vega, detallando el perfil, su posición, funciones y responsabilidades de la persona que cubriría el puesto, completándose con éxito el cumplimiento de todo el proceso requerido para la creación del puesto presentada a los directivos, para su posterior revisión y consideración, quedando en manos de los directivos, para poder implementarlas; dando como consecuencia el inicio de la fase en la que los directivos tomarán las decisiones finales.

6.2. Recomendaciones

- Se recomienda que el plan de respuestas de incidentes debe darse en función de la evaluación de riesgos de datos, seguido de la recopilación y almacenamiento seguro de datos de incidentes, continuándose con el análisis de datos de incidentes, así como con la comunicación y colaboración, dándose además con la toma de decisiones informadas, y finalizando con la mejora continua.

- Se recomienda emplear la metodología BPM, en los siguientes procesos de la Cooperativa de Ahorro y crédito Pablo Muñoz Vega, que son identificación y documentación de procesos, en la optimización de la eficiencia y de la reducción de costos; en la mejora de la experiencia del cliente; así como en la gestión de

riesgos y cumplimiento, continuando con la capacitación del personal y finalizando en la evaluación y mejora continua.

- Se recomienda dar cumplimiento a las normas empleadas a través de capacitaciones de alto nivel, para lo cual se debe identificar las Normas y Regulaciones Aplicables, desarrollando un Plan de Capacitación Estructurado, involucrando a expertos en la materia, para lo cual se debe personalizar el contenido para diferentes roles, estableciendo un calendario de capacitación regular, fomentando una cultura de cumplimiento, incluyendo un escenario de riesgo y respuesta a incidentes, documentando y manteniendo registros, llegando a promover la Mejora Continua.

REFERENCIAS

ACNUR. (2015). Política sobre la Protección de Datos personales de interés del ACNUR. *UNHCR*, *1*(1), 48.

Alonso, C. (2023). *Claves de la Ley Orgánica de Protección de Datos Personales de Ecuador*. GlobalSuite. https://www.globalsuitesolutions.com/es/claves-proyecto-ley-organica-proteccion-de-datos-personales-ecuador/

Álvarez, L. (2017). Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de la Ley Orgánica de Protección a los Derechos a la Intimidad y la Privacidad sobre los Datos Personales. *Revista de Derecho FORO*, *27*(27), 43–61. file:///C:/Users/Core i7-Home/Downloads/1924.pdf

Arteaga, G. (2022a). *Investigación bibliográfica – Cómo llevar a cabo una*. Testisiteforme. https://www.testsiteforme.com/investigacion-bibliografica/

Arteaga, G. (2022b). *Qué es la investigación de campo: Definición, métodos, ejemplos y ventajas*. Testsiteforme. https://www.testsiteforme.com/investigacion-de-campo/

Asamblea Nacional de la República del Ecuador. (2021). Ley Organica De Proteccion De Datos Personales. *Registro Oficial Órgano de La República Del Ecuador*, 1–70.

Banco Bolivariano. (2023). *Política para el tratamiento de datos personales del Banco Bolivariano C.A.* 1–11.

Berroa, R. (2020). *Configuración jurídica del derecho fundamental a la protección de los datos personales en República Dominicana. Especial referencia a la tutela de los datos en el ámbito de las sociedades de información crediticia*. Universidad Castilla - La Mancha.

Blake, M. (2019). Data protection: a legal comparative study of 9 countries. *REUTERS*, 32.

Bravo, K., & Pérez, Y. (2018). *Nivel de cumplimiento de la Ley de Protección de Datos Personales por parte de las Entidades Bancarias en el Distrito de Chiclayo, periodo 2016*. Universidad Señor de Sipán.

Burbano, M. (2021). *Diseño de un marco de trabajo para el análisis de impacto del proyecto de Ley de protección de datos en el Ecuador en empresas privadas*. Escuela Politécnica Nacional.

Bustillos, L., & Jáuregui, J. (2018). *Propuesta de un modelo de Gestión por Procesos BPM para el área de distribución de productos terminados*. Universidad Tecnológica del Perú.

Cano, N., & Jaramillo, D. (2023). *Análisis sobre el consentimiento del titular bajo la Ley de Protección de Datos Personales*. *459*, 19–21.

Carvajal, V. (2022). *HACKTIVISMO DE ANONYMOUS EN EL ECUADOR: ANÁLISIS REALISTA DE LAS ESTRATEGIAS Y CONSECUENCIAS DE LOS ACTORES NO ESTATALES TRANSNACIONALES EN EL MODELO ECUATORIANO DE CIBERSEGURIDAD (2011-2020)*. PUCE.

Castro, M. (2019). *Protección de datos personales a través de herramientas de procesamiento automatizado de datos: desafíos y recomendaciones*. INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación.

CEPAL. (2020). *Gestión del Conocimiento (GDC)*. *1*(1), 1.

Convenio de Ciberdelincuencia del Consejo de Europa. (2014). Convenio N ° 185 , del Consejo de Europa , sobre la Ciberdelincuencia (Convenio de Budapest). *Biblioteca Del Congreso Nacional de Chile*, 1–3.

Cristea, L. (2018). *La protección de datos de carácter sensible en el ámbito europeo. Historia clínica digital y big data en salud* [Universitat Abat Oliba CEU].

https://www.educacion.gob.es/teseo/mostrarRef.do?ref=1563228

Del Valle, D., Morales, C., & Montúfar, J. (2011). Declaración Universal. *Copredeh*, 47. https://www.corteidh.or.cr/tablas/28141.pdf

Díaz, G., & Fonseca, M. (2019). *Vulneración al derecho de la intimidad y privacidad por el indebido tratamiento de datos personales en el Ecuador*. UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL.

Díaz, L. (2022). *La aplicación de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos en el aumento de costos de servicios electrónicos agregados por parte de la operadora telefónica Claro Ecuador en la ciudad de Quito en el año 2020*. Universidad Central del Ecuador.

Etecé. (2020). *Información*. Concepto. https://concepto.de/informacion/

Godoy, L. (2017). El dato personal como presupuesto del derecho a la protección de datos personales y del habeas data en el Ecuador. *Revista de Derecho*, *27*, 1–20. https://revistas.uasb.edu.ec/index.php/foro/article/view/501/488%0Ahttps://revistas.uasb.edu.ec/index.php/foro/article/view/501

Gómez, I., & Montoya, N. (2018). *Propuesta de implementación y cumplimiento de la LGPDPPSO a través de la plataforma de Protección de Datos Personales en Posición de INFOTEC*. INFOTEC.

Güere, J. (2020). *Teoría del conocimiento virtual* [Univercidad Nacional del Centro del Peru]. https://repositorio.uncp.edu.pe/handle/20.500.12894/6845%0Ahttps://repositorio.uncp.edu.pe/bitstream/handle/20.500.12894/6845/T010_70454682_M.pdf?sequence=1&isAllowed=y

Guerra, M., & Navarrete, A. (2023). *Propuesta de un plan de cumplimiento del delgado de protección de datos personales en una empresa ecuatoriana de telecomunicaciones, 2022*. UDLA.

Guevara, G., Verdesoto, A., & Castro, N. (2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción). *RECIMUNDO*, *1*(1), 163–173.

Holguín, J. (2022). *Incidencia de nuevos retos para el tratamiento de datos personales y su regulación en el Ecuador*. Universidad de Guayaquil.

Jaramillo, J. (2022). *Consideraciones para la Implementación del Esquema Gubernamental de Seguridad de la Información basado en la Ley de Protección de Datos Personales caso de estudio: Instituto Nacional de Patrimonio Cultural*. Universidad Tecnológica Israel.

León, O., & Toscano, G. (2020). *Propuesta de Evaluación del Tratamiento de los Datos Personales para medir el nivel de cumplimiento de la Ley N° 29733 en Jadal Software S.A.C.* Universidad Tecnológica del Perú.

Limones, J., & Peralta, J. (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*. Universidad Politécnica Salesiana – Sede Cuenca.

Mayorga, T., García, M., Duret, J., Carrión, J., & Yarad, P. (2019). Legislación y Leyes Nacionales Articulo Original Historia de la normativa reguladora de la Protección de Datos de carácter personal en distintos países Latinoamericanos History of the regulating norm of the protection of personal data in the different Lat. *Revista Cientifica Dominio de Las Ciencias*, *5*(1), 518–537.

Merizalde, A. (2014). *Protección Legal de Datos Personales y a la Reserva de Información Personal, y su transferencia sin consentimiento de su titular*. Pontificia Universidad Católica del Ecuador.

OEA. (2021). *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales* (Comité Jur). https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

Ordóñez, L. (2020). *El derecho fundamental a la protección de datos personales en ecuador. Situación actual y presupuestos para la formulación de un marco jurídico que asegure un nivel adecuado de protección*. Universidad de Cádiz.

Pascual, E., Genoud, J., Aramburu, G., & Pontaquarto, M. (2000). PROTECCION DE LOS DATOS PERSONALES Ley 25.326. *Encyclopedia of Volcanoes.*, 15.

Quispe, C. (2018). *Metodología BPM para mejorar la productividad en el área de legalización en una notaría* [UNIVERSIDAD PERUANA LOS ANDES]. http://repositorio.upla.edu.pe/handle/UPLA/957

Ramón, P., & Ponce, L. (2021). Preparando a su organización para la protección de datos

personales. *Pwc*, 1–2. https://www.pwc.ec/es/publicaciones/lopd-pwc-ecuador.pdf

Sistema Nacional de Información. (2022). *El Gobierno Nacional presentó la Estrategia Nacional de Ciberseguridad*. Ministerio de Telecomunicaciones y de La Sociedad de La Información. https://www.telecomunicaciones.gob.ec/el-gobierno-nacional-presento-la-estrategia-nacional-de-ciberseguridad/

Villena, K. (2022). *Protección de los datos personales e intimidad de las personas trabajadoras: problemática ante el uso de TIC en el trabajo y perspectivas para una defensa efectiva* [Universidad del País Vasco]. http://hdl.handle.net/10810/57267

Zavala, D. (2021). *La base de datos personales y el derecho a la protección*. Universidad Regional Autónoma de los Andes.

ANEXO

Anexo 1. Validación del control de las consideraciones planteadas para dar cumplimiento de la Ley Orgánica de Protección de Datos Personales

N	**Cumplimiento**	**Caracterización**	**Evaluación**	
	Seguridad de Datos Personales		**Porcentaje a cumplir**	**Porcentaje cumplido**
1			**Alto**	**Parcial**
	La política institucional, requiere de actualizaciones, que permita contener la protección de datos personales.	Determinar Políticas de Seguridad	Bajo	Bajo
		Creación de estrategias en función de estándares	Bajo	Bajo
		Promulgar las Políticas de Seguridad	Parcial	
			Alto	Parcial
2	**Organización de la seguridad de la información**		**Alto**	**Parcial**
	Desarrollar una Política interna de Protección de Datos que detalle las obligaciones y disposiciones de la Ley y su Reglamento.	Conceptualizar	Bajo	Bajo
		Diagnóstico	Bajo	Bajo
		Asignar responsabilidades	Parcial	
			Alto	Parcial

	Generar procesos de tratamiento de información de datos, de distintos clientes, así como proveedores.	Identificar coordinaciones	Parcial	Parcial
		Implementar controles de seguridad	Parcial	
			Alto	Parcial
	Establecer a través de memorandos, las responsabilidades, que permita fijar la seguridad de la información.	Definir las responsabilidades	Parcial	Parcial
		Establecer responsabilidades	Parcial	
			Alto	Parcial
	Crear una política de acceso a la información, así como a los datos personales.	Determinar las seguridades a aplicar	Parcial	Parcial
		Modificar o utilizar de forma independiente	Parcial	
			Alto	Parcial
	Desarrollar un proceso de consultoría sobre vulnerabilidades al departamento de Tecnología de la información	Definir alertas vulnerables	Parcial	Parcial
		Remediar organizaciones	Parcial	
			Alto	Parcial
	Organizar reuniones con el Dirección Nacional de Datos Públicos, que permita dar soporte a la implementación de la normativa.	Acceder a consejos de expertos de seguridad	Alto	Alto
			Alto	Alto
	En particular, mejorar el tratamiento de datos personales.	Objetivo General	Parcial	Parcial
		Objetivos específicos	Parcial	
			Alto	Parcial
	Visualizar, crecientes amenazas a la seguridad de la información, dando un énfasis, especial a la protección de los datos personales.	Identificar los riesgos de seguridad	Parcial	Parcial
		Implementar medidas de control	Parcial	
			Alto	Parcial
	Formular un procedimiento, para el tratamiento de datos personales en los servicios que presta la organización, tanto virtual como presencial.	Establecer requisitos	Parcial	Parcial
		Procesado de información	Parcial	

			Alto	Parcial
	Ampliar el acceso a los datos personales en la política.	Definir políticas de control	Alto	Alto
			Alto	Alto
	Establecer una Política de Tratamiento de Datos Personales, la cual debe incluir la gestión de los distintos procedimientos administrativos.	Acuerdos útiles que permiten gestionar información	Alto	
			Alto	Bajo
	Actualizar políticas de seguridad en los sistemas informáticos de los sitios web, de la institución financiera.	Actualización de acuerdos	Alto	
			Alto	Bajo
	Ejecutar, políticas, así como procesos internos relacionados con la protección de datos personales.	Protección de datos	Parcial	Parcial
		Fundamentar la normativa	Parcial	Parcial
			Alto	Alto
	Desarrollar una política de respaldo de información, comprando un software de respaldo automático a la biblioteca de cintas de la institución financiera.	Identificar procedimientos de respaldo	Parcial	Parcial
		Continuidad del negocio	Parcial	
			Alto	Parcial
	Conectarse a través de VPN, que permita registrar, un tiempo definido de conexión, así como al acceso al sistema.	Definir requisitos de control	Parcial	Parcial
		Ejecutar pruebas de seguridad	Parcial	
			Alto	Parcial
3	**Seguridad de los recursos activos humanos.**		**Alto**	**Parcial**
	Procedimientos de la Junta Directiva Administrativa que establezcan claramente el procesamiento de la información recopilada en el CV y documentos necesarios.	Realizar verificaciones de antecedentes	Parcial	Parcial
		Verificación de nombramientos de funcionarios	Bajo	
		Verificación de ascensos de funcionarios	Bajo	

			Alto	Parcial
	La actualización del contrato debe ser incluido en el proceso de la Junta Directiva.	Establecer los deberes de los funcionarios	Bajo	Bajo
		Responsabilidades de los funcionarios	Bajo	Bajo
		Aceptar y confirmación de funcionarios	Parcial	
			Alto	Parcial
	Procedimientos de la Junta Directiva Administrativa que establezcan claramente, la protección del procesamiento de la información recopilada en los clientes.	Definir los parámetros que debe tener el contrato	Bajo	Bajo
		Establecer responsabilidades y funciones	Bajo	Bajo
		Firmar acuerdos de confidencialidad	Parcial	
			Alto	Parcial
	Designar un responsable del Departamento de Seguridad de la Información y Tratamiento de Datos, según normativa interna.	Requerimiento a los funcionarios que apliquen medidas de seguridad	Alto	
			Alto	Bajo
	Procesamientos, designados, de la Junta Directiva Administrativa, que establezcan claramente el proceso de procesamiento de la información recopilada.	Pactar los términos de empleo, incluida las políticas de seguridad de la información	Alto	Alto
			Alto	Alto
4	**Gestión de activos**		**Alto**	**Parcial**
	Puede fundamentarse en la orientación de la matriz productiva, pudiendo incluir, los datos personales como otro recurso.	Catalogar las fuentes de información	Bajo	Bajo
		Equilibrar las fuentes de información	Bajo	Bajo
		Reestablecer las fuentes de información	Parcial	
			Alto	Parcial
	Implementar un software de inventario, que permita delimitar varios parámetros establecidos.	Determinar los soportes de hardware	Parcial	Parcial
		Implementar los recursos de hardware	Parcial	
			Alto	Parcial
	Eliminar información con software gratuito.	Tomar medidas adecuadas al retirar cuenta alguna	Alto	

			Alto	0,00%
	Delimitar la política interna de tratamiento personal, así como los procedimientos de intercambio de información según lo dispuesto en la Ley Orgánica de Protección de Datos Personales.	Tener en cuenta las actividades en los controles	Alto	Alto
			Alto	Alto
	Desarrollar una política de respaldo de información, para lo cual se debe comprar un software de respaldo automático a la biblioteca de cintas.	Rastrear todas las comunicaciones que se den en la institución	Alto	Alto
			Alto	Alto
	Adquisición de soluciones antivirus y anti spam.	Adquirir antivirus	Alto	Alto
			Alto	Alto
	Adquisición de equipos de protección perimetral de nueva generación (Firewall).	Adquirir equipos de protección perimetral	Alto	Alto
			Alto	Alto
	Aplicar herramientas de cifrado de información libre o gratuita como QuickHash, MultiHasher.	Asociar etiquetas a metadatos	Alto	
			Alto	Bajo
	El proceso de gestión de medios extraíbles, deberá identificar los medios que sujeten datos personales, para lo cual se debe tratarlos adecuadamente.	Acuerdos con el esquema de clasificación	Parcial	Parcial
		Procedimientos de gestión de medios móviles	Parcial	
			Alto	Parcial
5	**Control de acceso**		**Alto**	**Alto**
	Implementar módulos de auditoría en el sistema informático de la organización financiera.	Planificación de la mantención de registros	Parcial	Parcial
		Mantención de registros de control	Parcial	
			Alto	Parcial

	Actualizar el sistema informático, constituido, sobre el software que tiene varios tiempos de uso y actualización de la tecnología, también efectuar el diseño de roles y perfiles de los diferentes colaboradores.	Implementar medidas para controlar los registros	Parcial	Parcial
		Ejecución de información	Parcial	Parcial
			Alto	Alto
	Implementar un software libre o de código abierto	Planificación para la implementación del sistema	Parcial	Parcial
		Adquirir un administrador de versiones de código	Parcial	
			Alto	Parcial
6	**Criptografía**		**Alto**	**Parcial**
	Implementar la utilización de herramientas criptográficas en software libre alguno.	Desarrollar una política que regule el uso de medidas de seguridad	Bajo	Bajo
		Plan de aplicación	Bajo	Bajo
		Implementar una política de uso de medidas de seguridad	Parcial	
			Alto	Parcial
7	**Seguridad física y del entorno**		**Alto**	**Alto**
	Determinar mayor protección del servidor.	Adquirir protección de servidores	Alto	Alto
			Alto	Alto
	Adquirir un UPS para los equipos, porque no hay energía de emergencia para todas las estaciones de trabajo.	Adquisición de equipos de protección	Alto	Alto
			Alto	Alto
	Modificación de cableado estructurado.	Adquisición de cables eléctricos	Parcial	Parcial
		Modificación de cables eléctricos	Parcial	Parcial
			Alto	Alto
8	**Seguridad de las operaciones**		**Alto**	Parcial
	Legitimación de un segundo centro de datos.	Adquisición de entornos separados	Bajo	Bajo
		Plan de implementación	Bajo	Bajo
		Realización de pruebas	Parcial	

			Alto	Parcial
	Implementar servidor NTP.	Plan de adquisición	Parcial	Parcial
		Adquisición de servidor NTP	Parcial	
			Alto	Parcial
9	**Seguridad en las comunicaciones**		**Alto**	**Parcial**
	Actualizar y/o cambiar el controlador WiFi, actualmente vía software.	Adquirir tecnología para proteger los servicios de red	Bajo	Bajo
		Estructura la seguridad de la comunicación	Bajo	Bajo
		Implementar tecnologías	Bajo	
			Alto	Parcial
	Implementar WireShark o un software similar	Preparar procedimiento de controles formales	Parcial	Parcial
		Implementar políticas y procedimientos	Parcial	
			Alto	Parcial
10	**Adquisición, desarrollo y mantenimiento de los sistemas**		**Alto**	**Alto**
	Actualizar el sistema o ejecutor del sistema de gestión de seguridad de la información.	Determinar los requisitos de seguridad	Alto	Alto
			Alto	Alto
11	**Relaciones con provisores y clientes**		**Alto**	**Alto**
	Relaciones con provisores y clientes	Relacionarse con proveedores	Parcial	Parcial
		Relaciones con clientes	Parcial	Parcial
			Alto	Alto
12	**Gestión de incidentes de seguridad de la información**		Alto	Alto
			Alto	Alto
13	**Aspectos de seguridad de la información para la gestión de la continuidad**		**Alto**	**Parcial**
	Implementar un centro de datos de reemplazo virtual	Determinar requerimientos de seguridad	Bajo	Bajo
		Plan de implementación	Bajo	Bajo
		Continuar con la gestión de seguridad	Parcial	
			Alto	Parcial
Porcentaje de Cumplimiento				**71.82%**

Facultad de Posgrado
IBARRA - ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE
RESOLUCIÓN 173-SE-33-CACES 2020
26 de octubre del 2020
FACULTAD DE POSGRADO

Tulcán, 17 de mayo de 2024

ACTA DE ENTREGA RECEPCION DEL PROYECTO DE GRADO IMPLEMENTACIÓN DE LA LEY ORGANICA DE PROTECCIÓN DE DATOS PERSONALES EN LA COOPERATIVA DE AHORRO Y CRÉDITO "PABLO MUÑOZ VEGA" CONSIDERANDO LOS ESTÁNDARES ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 27701:2019 Y EL SGSI INSTITUCIONAL

En la ciudad de Tulcán, el día 19 correspondiente al mes de mayo de 2024 comparecen: el Ing. Gerson Fuel R. estudiante de Maestría en Computación con Mención en Seguridad informática, Cohorte I, quien ENTREGA el proyecto de tesis de maestría realizado para la obtención del título de magister en la Universiada Técnica del Norte al Ing. Marcelo Caicedo Oficial de Seguridad de la Información de la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega, para que sea utilizado como referente en la creación del puesto del delegado de protección de datos personales y en la implementación de la ley orgánica de protección de datos personales en la institución.

Para constancia de lo actuado, firman el Ing. Marcelo Caicedo oficial de seguridades y el Ing. Gerzon Fuel estudiante de maestría.

Anexo 2. Acta entrega recepción de proyecto al oficial de seguridades de la institución

Ing. Gerzon Fuel R.
ESTUDIANTE DE MAESTRIA
UNIVERSIDAD TÉCNICA DEL NORTE
(Entrega)

Ing. Marcelo Caicedo
OFICIAL DE SEGURIDAD DE LA INFORMACIÓN
COAC. PABLO MUÑOZ VEGA
(Recibe)

Anexo 3. Validación de la revisión de los artículos de la Ley Orgánica de Protección de Datos Personales con respecto a la situación actual de la seguridad de la información de la institución, estas actividades se realizaron a lo largo del desarrollo del proyecto con el jefe de seguridades Ing. Marcelo Caicedo y el personal de TI quien hizo el acompañamiento hasta la finalización del proyecto.

CRONOGRAMA PARA LA REVISIÓN DE LOS ARTÍCULOS DE LA LEY ORGANIGA DE PROTECCIÓN DE DATOS PERSONALES Y SU APLICACIÓN EN COMPARACIÓN CON LA NORMATIVA DE LA INSTITUCIÓN.

Se realiza el análisis de la normativa vigente en la institución y su mejoramiento aplicando la ley orgánica de protección de datos personales

		2023				2024																
	Actividades/semana	Noviembre			Di	Enero				Febrero			Marzo			Abril				Mayo		Aprobado por
		2	3	4	1	1	2	3	4	1	3	4	1	2	3	1	2	3	4	1	2	
1	Seguridad de Datos Personales Art. 37, 38																					
2	Organización de la seguridad de la información Art. 11, 37, 38, 39, 41, 55, 56, 57, 59, 60																					
3	Seguridad de los recursos activos humanos. Art. 7,8,9,12,13,14,15,16,17,18,19,26																					
4	Gestión de datos sensibles Art. 5,26,40,41																					
5	Control de acceso Art. 34, 37, 38, 41																					
6	Criptografía Art. 37, 38, 41																					
7	Seguridad física y del entorno Art. 37, 38, 41																					

8	Seguridad de las operaciones Art. 37,38,39,41,43,46																				
9	Seguridad en las comunicaciones Art. 55,56,57,59,60																				
10	Adquisición, desarrollo y mantenimiento de los sistemas Art. 39																				
11	Registro de Datos Personales Art. 33, 55,56,57,59,60																				
12	Gestión de incidentes de seguridad de la información Art. 43,46																				
13	Aspectos de seguridad de la información para la gestión de la continuidad Art. 61																				