# UNIVERSIDAD TECNOLÓGICA ISRAEL

## ESCUELA DE POSGRADOS "ESPOG"

## MAESTRÍA EN SEGURIDAD INFORMÁTICA

*Resolución: RPC-SO-02-No.053-2021*

**PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER**

| **Título del artículo** |
| --- |
| Propuesta de Política interna alineada a la Ley de Protección de Datos Personales mediante estándar NIST para Cooperativas de Ahorro y Crédito. |
| **Línea de Investigación:** |
| Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo Sustentable |
| **Campo amplio de conocimiento:** |
| Tecnologías de la información y Comunicación |
| **Autora:** |
| Encalada Aguiar Diana Marisol |
| **Tutor:** |
| Mg. Toasa Guachi Renato Mauricio<br>PhD. Urdaneta Herrera Maryory |

**Quito – Ecuador**

**2024**

**APROBACIÓN DEL TUTOR**

Yo, Toasa Guachi Renato Mauricio, con C.I: 1804724167 en calidad de Tutor del proyecto de investigación titulado: **Propuesta de Política interna alineada a la Ley de Protección de Datos Personales mediante estándar NIST para Cooperativas de Ahorro y Crédito.**

Elaborado por: Diana Marisol Encalada Aguiar, de C.I: 1803549763, estudiante de la Maestría de Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2024

Firmado electrónicamente por:
RENATO MAURICIO
TOASA GUACHI

_____

**Mg. Toasa Guachi Renato Mauricio**

**APROBACIÓN DEL TUTOR**

Yo, Urdaneta Herrera Maryory, con C.I: 1759316126 en calidad de Tutor del proyecto de investigación titulado: **Propuesta de Política interna alineada a la Ley de Protección de Datos Personales mediante estándar NIST para Cooperativas de Ahorro y Crédito.**

Elaborado por: Diana Marisol Encalada Aguiar, de C.I: 1803549763, estudiante de la Maestría de Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2024

Firmado electrónicamente por:
MARYORY URDANETA HERRERA

_____

**PhD. Urdaneta Herrera Maryory**

**DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE**

Yo, Diana Marisol Encalada Aguiar con C.I: 1803549763, autora del proyecto de titulación denominado **Propuesta de Política interna alineada a la Ley de Protección de Datos Personales mediante estándar NIST para Cooperativas de Ahorro y Crédito**. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., marzo de 2023

Firmado electrónicamente por:
DIANA MARISOL
ENCALADA AGUIAR

_____

**Firma**

**https://orcid.org/0009-0008-1967-3738**

**Tabla de contenidos**

**Índice de tablas**

**Índice de figuras**

## INFORMACIÓN GENERAL

### Contextualización del tema

La protección de datos personales cada vez tiene mayor importancia y relevancia en la era digital, la información personal se ha convertido en un recurso muy valioso tanto para las empresas como para los cibercriminales debido a ello los dos sectores cada vez se preparan de mejor forma por esta razón se ha incrementado la necesidad de salvaguardarla y garantizar la privacidad de los usuarios para proteger sus datos. (Ángel, 2023)

En Ecuador el artículo 66, numeral 19 de la Constitución de la República (2021), establece: "el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley" la (DINARP) elaboró la propuesta del proyecto de Ley de Protección de Datos Personales que busca cuidar a las personas titulares de los datos, para que puedan decidir a quién entregar su información personal de cuerdo a la confianza que tengan. (Dirección Nacional de Registros Públicos, 2021)

Esta ley se ha tornado importante para grandes como pequeñas empresas de diferentes sectores donde el sector financiero no es la excepción debido a la gran cantidad de datos que trata, ya que su objetivo fundamental es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos personales, así como su correspondiente protección.

Cada vez las empresas van tomando conciencia sobre la importancia que tiene el tratamiento de los datos personales que poseen y recolectan a diario en su modelo de negocio.

### Problema de investigación

De acuerdo con la resolución No SEPS-IGT-IGDO-IGJ-IGS-SG-DNSI-2023-017 de la Superintendencia de Economía Popular y Solidaria (SEPS) indica que las Cooperativas de Ahorro y crédito de los diferentes segmentos deben crear políticas alineadas la Ley de Protección de Datos Personales que resguarde los activos de datos de las cooperativas de ahorro y crédito, ente esta resolución las Cooperativas de Ahorro y Crédito al igual que todas las empresas debe crear políticas y procedimientos para el tratamiento de los Datos personales para realizar un mejor resguardo de los datos personales que poseen y recolectan. (SEPS, 2023)

En base a lo anterior se puede decir que las Cooperativas deben implementar el tratamiento de datos de los titulares que interactúan en estas organizaciones, sin embargo la mayor parte de cooperativas aún no han realizado esta implementación, debido a ello se propone crear políticas y procedimientos claros en cada institución y que estén alineados a la Ley orgánica de Protección de datos personales y se apoyen por un estándar de calidad, en este caso se utilizará el estándar NIST para la protección de datos personales puesto que proporciona un marco reconocido internacionalmente, está basado en riesgos, es flexible, integral y alineado con estándares y regulaciones, lo que ayuda a las organizaciones a proteger de manera efectiva la información personal de sus clientes y usuarios.

**Objetivo general**

Elaborar una propuesta de políticas internas bajo el estándar NIST alineadas a la Ley Orgánica de Protección de Datos Personales para Cooperativas de Ahorro y Crédito.

**Objetivos específicos**

- Contextualizar los fundamentos sobre la Ley Orgánica de Protección de Datos personales y el estándar NIST para desarrollar políticas internas de protección de datos Personales en Cooperativas de Ahorro y Crédito.
- Determinar la situación actual de las Cooperativas de Ahorro y Crédito sobre el tratamiento de los datos personales para dar cumplimiento normativo.
- Elaborar políticas y procedimientos que aseguren el cumplimiento de las leyes y regulaciones de protección de datos personales en Cooperativas de ahorro y crédito.
- Validar el impacto de la aplicación de un marco de referencia mediante el estándar NIST para el tratamiento de datos personales en Cooperativas de Ahorro y Crédito.

**Vinculación con la sociedad y beneficiarios directos:**

La implementación de una propuesta de políticas internas alineadas con la Ley de Protección de Datos Personales para Cooperativas de Ahorro y Crédito bajo el estándar NIST aporta diversos beneficios a la sociedad y beneficia directamente a los titulares de datos que se tratan en las cooperativas por lo que se puede vincular con el ODS Industria Innovación y Estructura, debido a que el diseño de políticas ayudará a garantizar que la información personal se maneje de manera ética y segura, y brindando protección contra el uso indebido de datos personales.

Mediante esta propuesta se establecen restricciones y sanciones para el uso no autorizado de datos personales, lo que reduce el riesgo de abuso, robo de identidad y fraude, aumentan la confianza de las personas en las Cooperativas de Ahorro y Crédito y en la forma en que se manejan sus datos. Esto es especialmente importante en la era de la información, donde la confianza es fundamental para

el comercio electrónico y las transacciones en línea. Las instituciones deben ser transparentes en su manejo de datos personales y rendir cuentas por cualquier incumplimiento de las leyes de protección de datos. Esto promueve la responsabilidad y la ética en el tratamiento de datos personales.

Al establecer reglas claras sobre cómo se deben manejar los datos personales, se fomenta la innovación en la tecnología y los servicios que respetan la privacidad de los individuos, las políticas están relacionadas con la protección de los derechos humanos fundamentales, como el derecho a la privacidad y la no discriminación por lo que se relaciona con el ODS Paz y Justicia en Instituciones Sólidas. Al cumplir con las regulaciones de protección de datos, las organizaciones pueden participar en el comercio internacional con mayor facilidad, ya que muchas jurisdicciones exigen el cumplimiento de normas de privacidad para la transferencia de datos transfronteriza.

Estas leyes pueden ayudar a prevenir el acoso y la discriminación al establecer límites en la recopilación y el uso de datos personales con fines discriminatorios o acosadores y de esta forma contribuyen a una sociedad más justa y segura al proteger los derechos y la privacidad de las personas, alentar la confianza en la tecnología y promover la responsabilidad en el manejo de datos personales. Estas leyes son esenciales en la era digital y desempeñan un papel importante en el equilibrio entre la innovación tecnológica y la protección de los derechos individuales.

## CAPÍTULO I: DESCRIPCIÓN DEL ARTÍCULO PROFESIONAL

### 1.1. Contextualización general del estado del arte

#### 1.1.1. Ley Orgánica de Protección de Datos personales Ecuador

Según la RESOLUCIÓN No SEPS-IGT-IGDO-IGJ-IGS-SG-DNSI-2023-017 (2023), en su artículo 4 define al Dato Personal como "Dato que identifica o hace identificable a una persona natural, directa o indirectamente"; en el artículo 10, literales g y literal j, menciona que la Confidencialidad indica el tratamiento de datos personales debe concebirse sobre la base del debido sigilo y secreto, es decir, no se debe tratar para cualquier fin solo para lo que fueron recogidos, a menos que se dé una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en esta ley. (Moncayo, 2021)

Es importante mencionar que según la Ley Orgánica de Protección de Datos Personales debe existir en la un responsable del Tratamiento de Datos quién será el que controla, decide y se responsabiliza de los datos. Por su parte, el encargado del tratamiento es quien almacena los datos personales, pero no decide sobre ellos. Toda empresa o entidad, sea pública o privada, domiciliada en Ecuador, que tenga y maneje datos personales debe cumplir esta normativa. (Dinarp, 2021)

La protección de datos personales surgió como un mecanismo para cuidar el derecho a la privacidad a partir de finales de la década de 1970 en países europeos como Francia y Alemania. La Unión Europea se convirtió en un referente en este ámbito con la directiva 95/46/CE. No obstante, debido a problemas de homogeneización entre los países miembros y la falta de mecanismos que aseguraran su cumplimiento, se promulgó el Reglamento General de Protección de Datos, el cual comenzó a aplicarse el 25 de mayo de 2018. (Universidad Andina Simón Bolívar, 2021).

Según Serrano (2023), indica que la Ley de Protección de Datos es aplicable a empresas de todos los sectores y tamaños, así como a personas naturales. En ese sentido, algunas de las acciones a tomar para la aplicación de la ley son:

- Realizar capacitaciones a todo el personal de la institución.
- Establecer las bases de datos, abarcando todas las áreas de la empresa y determinando cómo se obtienen y utilizan los datos.
- Identificar los proveedores que manejan datos personales, considerando que no todos los proveedores requieren un acuerdo de tratamiento de datos.
- Revisar los contratos con clientes que sean personas naturales, especificando los datos necesarios para el propósito del contrato.

- Identificar las políticas pertinentes relacionadas con la privacidad, gestión de derechos y seguridad de la información.
- Evaluar los riesgos asociados.
- Implementar medidas de seguridad técnicas, físicas y legales.
- Proporcionar capacitación adicional al personal para verificar la implementación y asegurar el correcto funcionamiento de los procesos.

### 1.1.2. Normas y Estándares para la protección de datos personales

En cada país y región se crear sus propias leyes y reglamentaciones en protección de datos personales estas van de acuerdo con la realidad de cada uno. De esta forma se hace fundamental que las organizaciones conozcan las legislaciones que aplican en los lugares donde operan. Ecuador desde el 2021 cuenta con la Ley Orgánica de Protección de datos Personales a la que se ha hecho referencia en el presente documento sin embargo es importante mencionar las siguientes normas y estándares para conocer un poco más de ellos.

#### 1.1.2.1. RGPD De La Unión Europea

Según la Comisión Europea (2021), en el Reglamento Oficial de Protección de datos (RGPG), establece los siguientes parámetros:

**Ámbito de aplicación:** dirigida para instituciones que se encuentran dentro y fuera de la Unión Europea que tratan datos personales.

**Principios:** establece ocho principios: licitud, lealtad, transparencia, limitación de la finalidad, minimización de los datos, exactitud, limitación del almacenamiento y la integridad y confidencialidad.

**Consentimiento:** exige el consentimiento explícito e informado de los individuos antes de tratar sus datos personales.

**Derechos de los individuos:** derechos en relación con sus datos personales, como el acceso, rectificación, supresión (derecho al olvido), oposición, limitación del tratamiento y portabilidad de los datos.

**Responsabilidad y gobernanza:** se debe demostrar que cumple con la normativa implementando políticas, procesos y tecnologías adecuadas.

### 1.1.2.2. Marco de privacidad NIST

Conjunto de prácticas, directrices y herramientas desarrolladas por el Instituto Nacional de Estándares y tecnología (NIST, por sus siglas en ingles) de los Estados Unidos para ayudar a las organizaciones a gestionar y proteger la privacidad de los datos personales y cumplir con las regulaciones y estándares aplicables. (Ángel, 2023)

**Estructura del marco:** tiene cinco funciones principales: identificar, gobernar, controlar, comunicar y proteger. Cada función se divide en categorías y subcategorías que describen prácticas y actividades específicas relacionadas con la gestión de la privacidad de los datos personales.

**Enfoque basado en riesgos:** para la gestión de la privacidad de los datos personales, permite organizaciones identificar y abordar de manera efectiva los riesgos de privacidad asociados con el tratamiento de los datos personales.

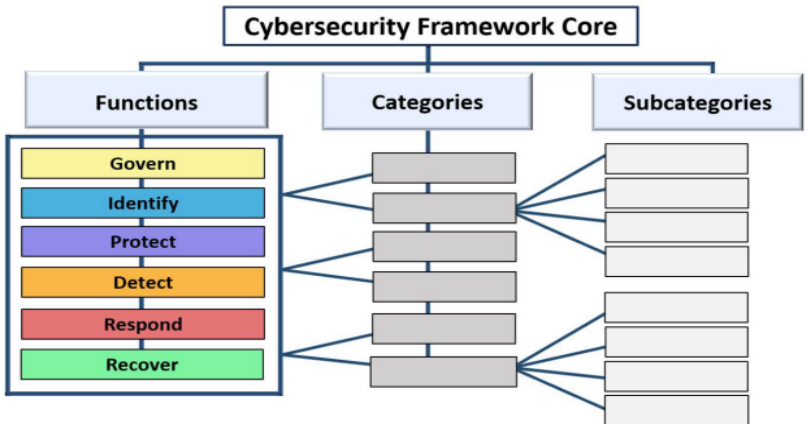
**Flexibilidad y adaptabilidad:** es flexible y adaptable, por lo que las organizaciones pueden ajustar sus prácticas de privacidad de datos personales en función de sus necesidades específicas, el contexto y los requisitos legales y normativos aplicables.

**Integración con el Marco de Ciberseguridad NIST:** el Marco de Privacidad NIST se puede integrar con el Marco de Ciberseguridad NIST, permitiendo a las organizaciones a gestionar de manera holística tanto la privacidad como la ciberseguridad de los datos personales.

**Funciones, categorías y subcategorías**

**Figura 1**

*CSF Core Structure*




Nota: la figura muestra cómo se debe organizar las funciones, categorías y subcategorías básicas del marco NIST. (NIST, 2024)

Las funciones básicas del marco son las siguientes:

**GOBERNAR (GV):** Dirigir el establecimiento de la estrategia de ciberseguridad, gestión de riesgos de la cadena de suministro; funciones, responsabilidades y autoridades; políticas, procesos y trámites. (Espinoza,2023).

**PROTEGER (PR):** Implementar medidas de protección con el fin de prevenir o disminuir el riesgo de ciberseguridad implica identificar y clasificar los riesgos. Los resultados de esta función incluyen la sensibilización y la formación; seguridad de datos; identidad, gestión, autenticación y control de acceso; seguridad de la plataforma (es decir, asegurar el hardware, software y servicios de plataformas físicas y virtuales); y la resiliencia de la infraestructura tecnológica. (Espinoza, 2023).

**DETECTAR (DE):** Analizar posibles ataques y compromisos de ciberseguridad, descubre de manera oportuna anomalías, indicadores de compromiso y otros eventos de seguridad cibernética potencialmente adversos que pueden indicar que se están produciendo ataques e incidentes. (Espinoza, 2023)

**RESPONDER (RS):** Implementar acciones frente a un incidente de ciberseguridad detectado implica tener la capacidad de controlar el impacto de dichos incidentes. Esta función abarca la gestión, análisis, mitigación, notificación y comunicación de estos. (Espinoza, 2023)

**RECUPERAR (RC):** Restaurar activos y operaciones afectados por un incidente es fundamental para restablecer las operaciones normales de manera oportuna y mitigar el impacto de los incidentes de ciberseguridad. Esto permite una comunicación adecuada durante los esfuerzos de recuperación. Las funciones del CSF interactúan entre sí, formando un ciclo integrado donde cada una se relaciona con las demás. (Espinoza, 2023)

**Figura 2**

*CSF Funciones*


Nota: La figura 2 muestra una rueda, haciendo referencia a las funciones de CSF ya que todas ellas se relacionan entre sí, tomado de (NIST C. F., 2024)

Según El Marco de Ciberseguridad (CSF) 2.0 del NIST (2024), una organización puede optar por utilizar los niveles para informar a sus perfiles actuales y de destino. Los niveles caracterizan el rigor de las prácticas de gobernanza y gestión de riesgos de ciberseguridad de una organización, y proporcionan contexto sobre cómo una organización ve los riesgos de ciberseguridad y los procesos implementados para administrar esos riesgos. Los niveles, como se muestra en la siguiente figura se cómo: Parcial (Nivel 1), Informada sobre el riesgo (Nivel 2), Repetible (Nivel 3) y Adaptable (Nivel 4)

Los niveles describen una progresión desde respuestas informales y ad hoc a enfoques ágiles, informados sobre el riesgo y mejorando continuamente. La selección de niveles ayuda a establecer el tono general de cómo una organización gestionará sus riesgos de ciberseguridad.

**Figura 3**

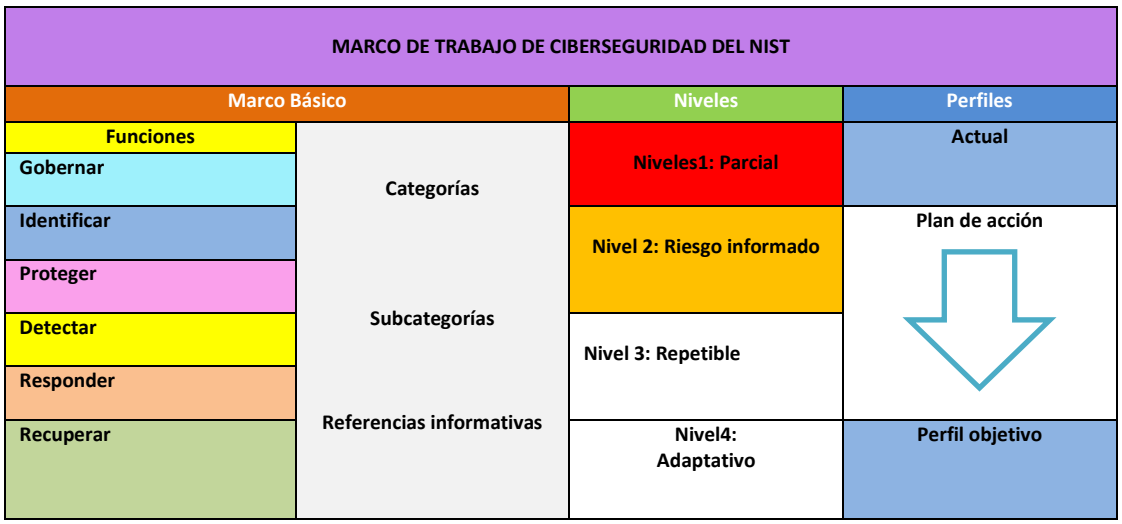
*CSF Niveles de riego de ciberseguridad*


Nota: Se muestran los niveles que describen una progresión desde respuestas informales y ad hoc a enfoques ágiles, informados sobre el riesgo y la mejora continua. (NIST C. F., 2024)

De acuerdo con las descripciones anteriores, la arquitectura global del marco de trabajo NIST quedaría de la siguiente manera:

**Figura 4**

*Marco de trabajo NIST*



Nota: La figura muestra la Arquitectura del marco de trabajo de ciberseguridad del NIST (CSF) que se aplica en este estándar.

### 1.1.3. ISO 27001

La norma ISO 27001:2022 es un estándar internacional diseñado para garantizar la seguridad, confidencialidad e integridad de los datos, la información y los sistemas que los procesan. Permite a las organizaciones evaluar los riesgos y aplicar los controles necesarios para mitigarlos o eliminarlos. La adopción de la norma ISO 27001 proporciona a las organizaciones una ventaja competitiva y mejora su imagen, ya que demuestra un compromiso con la seguridad de la información. Además, la Gestión de la Seguridad de la Información se complementa con las buenas prácticas y controles establecidos en la norma ISO 27002. (Isotools, 2022)

### 1.1.4. Similitudes entre ISO 27001 y NIST

Según Untiveros (2023), ambos marcos comparten algunas similitudes clave:

**Enfoque en la gestión de riesgos:** Tanto ISO 27001 como NIST ponen énfasis en la identificación y gestión de riesgos de seguridad. Ambos contribuyen a que las organizaciones evalúen y aborden de forma proactiva las amenazas cibernéticas y los posibles incidentes de seguridad.

**Enfoque basado en procesos:** ISO 27001 y NIST adoptan un enfoque basado en procesos para la seguridad de la información y la ciberseguridad. ISO 27001 utiliza el ciclo PDCA para gestionar los riesgos, mientras que NIST se organiza en torno a cinco funciones clave.

**Personalización:** Ambos marcos permiten a las organizaciones adaptar sus directrices a sus necesidades específicas. Esto les brinda la flexibilidad necesaria para implementar medidas de seguridad que se ajusten a su entorno y riesgos particulares ( (Untiveros, 2023).

### 1.1.5. Diferencias entre ISO 27001 y NIST

A pesar de sus similitudes Untiveros, (2023) menciona que existen diferencias importantes entre ISO 27001 y NIST:

**Cobertura:** ISO 27001 se centra en la seguridad de la información, mientras que NIST abarca un espectro más amplio de ciberseguridad, incluyendo aspectos como la privacidad, la gestión de amenazas, la respuesta a incidentes y la recuperación.

**Contexto geográfico:** La ISO 27001 es una norma internacional ampliamente adoptada en todo el mundo, mientras que NIST se originó en los Estados Unidos. Sin embargo, el Marco de Ciberseguridad de NIST ha sido ampliamente adoptado globalmente.

**Profundidad y detalle:** NIST proporciona detalles técnicos específicos en muchas áreas, lo que puede ser especialmente útil para organizaciones que requieren una orientación técnica detallada. En contraste, ISO 27001 tiende a ofrecer una orientación más general.

### 1.1.6. Protección de Datos y Seguridad de la Información

Dentro de la seguridad de la información se analiza la protección de datos personales para luego establecer procesos que deben estar disponibles permanente mente e implementados en las instituciones permitiendo garantizar los derechos de los titulares, responder a los incidentes de protección de datos, se hace necesario crear un Sistema de protección de datos personales para resolver problemas que pueden darse en este tratamiento. (Isotools, 2022)

## 1.2. Proceso investigativo metodológico

Para la investigación del tema planteado se ha seleccionado el siguiente método:

### 1.2.1. Investigación Cualitativa

Se puede utilizar en varios campos, aplican técnicas como la observación, entrevistas, es importante que al momento de seleccionar la técnica a utilizar el investigador debe tener en cuenta el escenario o contexto en el que se desarrolla la investigación, las limitaciones de tiempo y recursos que puedan existir y las características de las personas involucradas. (Bobadilla,2021)

### 1.2.2. La observación

La observación cualitativa no se limita a la simple observación de eventos; ya que, requiere una inmersión completa en el entorno y las circunstancias que se están investigando, con el observador desempeñando un papel activo y reflexionando constantemente sobre lo que está observando. Se ha realizado una observación directa para esta investigación debido a que el observador forma parte de la vida del grupo observado. (Bobadilla, 2021).

Para la presenta investigación se ha realizado una observación presencial llevada a cabo en el entorno de la Cooperativa que se tomó de muestra, esta observación se realizó durante las horas laborales por ser parte del equipo de esta institución. Se ha utilizado un enfoque participante y estructurado, ya que el investigador ha estado presente y ha interactuado directamente con los participantes. Se ha registrado las interacciones de los procesos que la Cooperativa realiza mediante la entrevista que se realizó al responsable de Seguridad de la Información y conversaciones y observaciones directas a los miembros de la Unidad de Sistemas, Unidad de Procesos equipo Legal, también se ha tomado notas detalladas en un de la estructura de la cooperativa con todo este material se realizará un análisis para identificar patrones de comportamiento y temas necesarios para este trabajo.

### 1.2.3. La entrevista

Según Bobadilla (2021), la entrevista cualitativa se caracteriza por ser más personal, manejable y flexible, representando un intercambio de información entre dos individuos. Se pueden clasificar en tres tipos principales: las entrevistas estructuradas, donde el entrevistador sigue un conjunto específico de preguntas predefinidas; las entrevistas semiestructuradas, donde el investigador tiene cierta libertad para decidir el contenido, orden, profundidad y formulación de las preguntas, pudiendo agregar otras según sea necesario; y finalmente, las entrevistas abiertas, que se centran en el tema de investigación pero no siguen una guía de preguntas específica, permitiendo al entrevistador hacer las preguntas que considere pertinentes en el momento.

## 1.3. Análisis de resultados

Luego de realizar la entrevista para obtener una muestra sobre el estado de las Cooperativas en cuanto al tratamiento de datos personales, se puede evidenciar que las Cooperativas de Ahorro y Crédito utilizan varios datos personales de todas las personas que intervienen en las actividades del negocio, estos datos se utilizan en las transacciones financieras de las Cooperativas de manera digital o presencial y en todas las actividades que los funcionarios realizan en su día a día.

Los datos recolectados de los Miembros de la Asamblea General, Consejo de Administración los respectivos Comités, Colaboradores, Proveedores, Visitantes, Socios, Clientes y Prospectos que manejan las cooperativas son: Datos de Identificación, Datos de Contacto, Datos Laborales, Datos Financieros, Datos Comerciales (Referencias), Datos Biométricos, Datos de Genero, Datos Médicos.

En cuanto a los datos del personal de la cooperativa se puede observar que existe datos de estado de salud de los empleados, también se manejan datos de menores de edad por los productos que poseen, estos datos de acuerdo con la ley orgánica de Datos Personales se clasifican como datos sensibles por lo que se le debe dar el tratamiento adecuado alineándose a lo que establece la ley.

Hay varias Cooperativas de Ahorro y Crédito que aún no han iniciado con el tratamiento de datos personales como lo establece la ley, esto puede ser debido a que al ser un tema nuevo hay desconocimiento causando demora en su implementación, existen otras Cooperativas que ya han iniciado este proceso con la designación de los responsables de este tratamiento, ubicando ciertas políticas en sus portales web pero no tienen un sistema establecido de protección de datos personales para tener una mejor organización ya que muchas veces se confunde cual debe ser el procedimiento a seguir. Para solventar esta situación se ha alineado el estándar NIST en el tratamiento de los datos personales mediante su marco de trabajo de ciberseguridad y mediante la creación de una propuesta de políticas que abarque lo requerido por la ley.

## CAPÍTULO II: ARTÍCULO PROFESIONAL

### 2.1. Resumen problema propuesta y resultado

La Ley Orgánica de Protección de Datos Personales debe ser aplicada por todas las organizaciones que realicen tratamiento de datos, las Cooperativas de Ahorro y Crédito para cumplir con esta normativa deben crear políticas claras sobre el tratamiento de datos personales y considerar apoyarse en un estándar de calidad que ayude a mejorar este proceso, para esta investigación se utilizará el estándar NIST puesto que proporciona un marco reconocido internacionalmente, está basado en riesgos, es flexible, integral y alineado con estándares y regulaciones.

Con políticas de protección de datos personales se permitirá garantizar el cumplimiento de las disposiciones legales de protección de datos personales, así como fortalecer la postura de seguridad de los datos en las Cooperativas de Ahorro y Crédito frente a las amenazas cibernéticas y los riesgos asociados con el tratamiento de información sensible. Alinearse al estándar NIST ayudará a obtener una estructura para la gestión de la seguridad de los datos, creando confianza en la institución, abordando aspectos clave como la identificación y clasificación de datos, el control de acceso, la gestión de riesgos, la respuesta a incidentes, por otro lado, también la capacitación del personal es de gran importancia ya que permitirá establecer una cultura organizacional centrada en la seguridad y la protección de datos personales.

**a. Palabras clave:**

Datos personales, NIST, política, Cooperativas de ahorro y crédito, tratamiento

### 2.2. Abstract

The Organic Law on the Protection of Personal Data establishes that all organizations that carry out data processing must apply it, Savings and Credit Cooperatives are not exempt, for this they must create clear policies in the processing of personal data, it is necessary to rely on a quality standard, in this case the NIST standard will be used since it provides an internationally recognized framework, it is risk-based, flexible, comprehensive, and aligned with standards and regulations.

In this way, it will be possible to guarantee compliance with the legal provisions on the protection of personal data, as well as to strengthen the security posture of Savings and Credit Unions against cyber threats and the risks associated with the processing of sensitive information, and with the NIST standard, it will be possible to obtain a structure for the management of data security. Creating trust in the institution, addressing key aspects such as data identification and classification, access control, risk management, incident response and staff training to establish an organizational culture focused on security and personal data protection.

## 1. Keywords

Personal data, nist, policy, Cooperativas de Ahorro y Crédito, treatment

## 2.3. Introducción

En la actualidad con la era digital se ha evidenciado que la información se ha convertido en uno de los activos más valiosos, la protección de datos cada vez más es una prioridad tanto para las personas como para instituciones de todos los ámbitos. La creación de leyes de protección de datos, como el Reglamento de Protección de Datos va marcando un hito en la forma en que se aborda la privacidad y seguridad de la información, para que pueda darse la privacidad de datos personales se deben complementar con el apoyo de seguridad informática en varios aspectos como herramientas necesarias para proteger los datos personales, las metodologías que pueden aplicarse y que son muy importantes al momento de realizar este tratamiento, también es muy importante tener en cuenta estándares que ayudan a mejorar los procedimientos al momento de realizar la protección de datos y que cada vez son de más ayuda. (Ángel, 2023)

Las Cooperativas de Ahorro y Crédito no están alejadas de cumplir con la protección de datos puesto que al ser instituciones financieras manejan grandes cantidades de datos personales de sus clientes , socios, personal, tercero entre otros, en muchos casos estos datos que se utilizan se consideran datos sensibles por lo que deben ser tratados de acuerdo a lo que la Ley Orgánica de Datos Personales conjuntamente con el Reglamento vigentes en Ecuador, en estos documentos se puede evidenciar varios aspectos que las Cooperativas de Ahorro y Crédito deben tener en consideración al momento de realizar el tratamiento de los datos personales, de esta forma se podrán crear políticas y procedimientos claros que sean aplicadas internamente por cada uno de los miembros de la institución. (Dinarp, 2021)

El uso de las NIST permitirá conseguir un enfoque proactivo y más estructurado para la gestión de la seguridad de los datos personales con sus mejores prácticas, abordando aspectos clave como la identificación y clasificación de datos, el control de acceso, la gestión de riesgos, la respuesta a incidentes y la capacitación del personal de esta forma si se logra realizar un buen tratamiento de datos se promoverá la confianza en las Cooperativas de Ahorro y Crédito por parte de sus socios y clientes y creando una mejor cultura centrada en la seguridad de la información que se maneja. (NIST C. F., 2024)

En el presente trabajo se utilizará la Ley Orgánica de Protección de Datos Personales, el Reglamento de protección de datos personales y el estándar NIST por lo que se hace necesario mencionar algunas definiciones que se tratarán más adelante:

### 2.3.1. Ley de Protección de Datos Personales

Según Registro Oficial Suplemento 459 (2021), afirma:

### 2.3.2. Marco de Privacidad del NIST

Con el propósito de establecer un recurso opcional para la privacidad, el Instituto Nacional de Normas y Tecnología (NIST) introduce el Marco de Privacidad, una herramienta destinada a fortalecer la privacidad a través de la gestión de riesgos empresariales. Su objetivo es fomentar prácticas óptimas que se alineen con los principios de privacidad desde el diseño, asistiendo a las organizaciones en la protección de la privacidad de las personas. Esto se logra generando confianza en la organización, mejorando la toma de decisiones éticas en el diseño o la implementación de productos y servicios que optimicen la utilización beneficios de los datos, y reduzcan al mínimo las repercusiones negativas en la privacidad de las personas y la sociedad en su conjunto. (NIST, 2020)

Por otro lado, también se busca el cumplimiento de las obligaciones sobre la protección de productos y servicios contra la obsolescencia para cumplir con estas obligaciones en un entorno tecnológico y normativo en constante evolución. Asimismo, se busca mejorar la comunicación sobre las prácticas de privacidad entre todos los miembros involucrados en las organizaciones. (NIST, 2020)

### 2.3.3. Gestión de los riesgos a la privacidad y la ciberseguridad

El método del Marco de privacidad para los riesgos a la privacidad considera eventos de privacidad como posibles problemas de las operaciones de sistemas, productos o servicios con datos en formato digital o no digital desde la recolección de los datos hasta su eliminación. (NIST, 2020)

Para gestionar los riesgos de privacidad se usan las funciones Identificar, Gobernar, Controlar, Comunicar y Proteger.

**Figura 5**

*Uso de funciones para gestionar los riesgos a la ciberseguridad y privacidad*

Nota: Tomado de Marco de Privacidad para los riesgos a la privacidad (NIST, 2020)

Para ayudar a las instituciones a crear o mejorar un programa de privacidad se puede usar el Marco de privacidad de NIST. La gestión de riesgo de privacidad ayuda a crear confianza en los productos y servicios, comunicar mejor sobre las prácticas de privacidad y cumplir obligaciones de cumplimiento.

Se puede empezar la protección de datos personales utilizando el marco de privacidad siguiendo el modelo sencillo con las fases identificación, gobernanza, control, comunicación y protección que se muestra en la siguiente tabla:

**Tabla 1**

*Gestión de Riesgos de privacidad*

| | | | |
|---|---|---|---|
| **Identificación:** | Identificar los datos que se procesan en la cooperativa (como recolección, uso, intercambio, almacenamiento) y mapear su flujo a través de los sistemas en todo el ciclo de vida de los datos, desde la recolección a la eliminación. | Evaluación de riesgos de privacidad utilizando un mapa de datos para evaluar cómo las actividades de procesamiento de datos pueden crear problemas para los titulares (como vergüenza, discriminación o pérdidas económicas). Evaluar el efecto a la Cooperativa si esos problemas ocurrieran (como pérdida de la confianza del cliente o daños de imagen/reputación) que pudieran afectar su rentabilidad. | Solicitar información sobre opciones para contratos, productos y servicios que utiliza para operar la Cooperativa para garantizar que estén configurados y reflejar sus prioridades de privacidad. |
| **Gobernanza:** | Conectar los valores y políticas de privacidad de la Cooperativa con su evaluación de riesgos de privacidad para lograr fomentar la confianza en sus productos y servicios, estar al día con el conocimiento de sus obligaciones legales. | Fortalecer el conocimiento de roles y responsabilidades de los empleados de la cooperativa para que puedan tomar mejores decisiones sobre cómo gestionar riesgos de privacidad efectivamente en la presentación de productos y servicios. | Reevaluar periódicamente y verificar si los riesgos de privacidad han cambiado debido a cualquier circunstancia o en obligaciones legales para cambiar procesamientos de datos. |
| **Control:** | ¿Está adquiriendo, intercambiando o conservando información que resulta innecesaria? Evalúe cómo sus políticas contribuyen a mantener un control efectivo sobre los datos. | Considerar las responsabilidades legales y los riesgos de privacidad al tomar decisiones sobre la funcionalidad de servicios, productos, sistemas o procesamiento de datos. Contemplar un diseño adaptable | ¿Qué clases de tratamiento de datos realiza? Evaluar cómo diferentes estrategias técnicas, como la desidentificación o la descentralización del procesamiento de datos, entre otras técnicas, pueden facilitar la |

| | | | |
|---|---|---|---|
| | | para adaptarse de manera más eficiente a las preferencias cambiantes de privacidad de los clientes y a un entorno legal en constante evolución. | consecución de metas empresariales o de agencia, al mismo tiempo que se garantiza la protección de la privacidad. |
| **Protección:** | Administrar el acceso a la red de la Cooperativa, así como el uso de computadoras y otros dispositivos, regulando quiénes pueden iniciar sesión. | Cifrar los datos sensibles, en reposo y en tránsito.<br>Realizar respaldos periódicos de datos. Utilizar software de seguridad para proteger los datos. | Mantener una práctica regular de actualización de software de seguridad, automatizando este proceso.<br>Establecer políticas oficializadas para gestionar de manera segura la disposición de datos. |
| **Comunicación:** | Establecer políticas claras para comunicar tanto interna como externamente las actividades de procesamiento de datos. Mejorar la transparencia mediante la presentación de avisos e informes claros y accesibles, así como la implementación de alertas, notificaciones u otras señales para informar a los titulares sobre las actividades de procesamiento de datos y sus derechos correspondientes. | Incluir la privacidad en la Cooperativa para estar más familiarizados y aprender sobre las preferencias de privacidad de los titulares. | Tener en cuenta que acciones se realizarán en caso de una violación a los datos. |

Nota: Tomado de Pasos del Marco de privacidad de NIST. (NIST, 2022)

De acuerdo con el objetivo establecido en el presente trabajo nos centraremos en la propuesta de políticas internas bajo el estándar NIST alineadas a la Ley Orgánica de Protección de Datos Personales para Cooperativas de Ahorro y Crédito, donde podemos indicar las actividades que se deben realizar en las funciones del Marco de Privacidad NIST con sus respectivas categorías y subcategorías que han seleccionadas debidamente, esta información se muestra en la tabla del Anexo 2 donde se ha añadido una columna de entregables para complementar e indicar los aspectos que se deben tomar en cuenta por las Cooperativas para crear las políticas internas de protección de datos personales.

### 2.4. Metodología

La metodología empleada para la realización de la presente investigación es de tipo cualitativa ya que se ha empleado una entrevista estructurada a la persona encargada de la Seguridad de la Información en la Cooperativa que se tomó de muestra, la entrevista se puede encontrar en el ANEXO 2, la misma que fue realizada mediante un banco de preguntas para obtener información y analizar el estado de

la Cooperativa en el tratamiento de datos, los procedimientos que llevan, los datos que manejan y como lo han ido abordando la implementación del Sistema de Protección de Datos Personales.

Con la información obtenida se pudo conocer los procedimientos que utilizan a diario en esta institución y como se pueden relacionar con los procedimientos que se realizarán para el tratamiento de Datos Personales.

En esta investigación se involucra el uso y recolección de materiales, investigaciones, observaciones propias de experiencia laboral, artículos legales y normativas, que describen de forma real el tema propuesto. (Mena, 2022)

Mediante el estándar NIST se ha complementado este trabajo con ayuda de su Framework y Marco de Privacidad, de modo que se ha podido lograr comprender la importancia de la herramienta en relación con el tratamiento de datos personales y así poder establecer políticas que ayuden a las Cooperativas de Ahorro y Crédito en la protección de datos personales. (NIST C. F., 2024)

### 2.4.1. Caso de Estudio

Según Mohan (2021), indica que los detalles de un caso de estudio pueden ser los siguientes que han sido alineados a la investigación propuesta en el presente trabajo:

- **Contexto:** Las cooperativas de ahorro y crédito son instituciones financieras que gestionan una gran cantidad de datos personales de sus miembros, incluyendo información financiera, datos de identificación personal y otra información sensible, por lo que es de suma importancia crear políticas internas sólidas para proteger la información personal.
- **Participantes:** Dentro de los participantes se puede encontrar a las Cooperativas de ahorro y crédito quiénes establecerán políticas internas de protección de datos, otro de los participantes son los individuos cuyos datos personales serán tratados y protegidos por estas políticas.
- **Eventos y acciones:** Se propone que las cooperativas deben llevar a cabo un análisis detallado de los riesgos asociados con la gestión de datos personales mediante el Marco de privacidad NIST, identificando posibles amenazas y vulnerabilidades para poder realizar políticas y procedimientos para tratar datos.
- **Selección del estándar NIST:** Luego de realiza de una revisión detallada de los estándares de seguridad de la información, se ha decidido utilizar el marco de seguridad y privacidad del NIST como base para sus políticas internas.
- **Desarrollo de políticas internas:** Se considera que al desarrollar políticas internas es importante que cumplan con los requisitos del NIST, incluyendo controles de seguridad, procedimientos de gestión de riesgos y medidas de cumplimiento. (Mohan, 2021)

## 2.5. Resultados – Discusión

Las Cooperativas de Ahorro y Crédito con el fin de dar cumplimiento a la Ley Orgánica de Protección de Datos Personales, se han encontrado con varias dificultades en el proceso de adaptar sus políticas a esta ley, debido a ello en esta investigación se ha propuesto una alternativa de mejoras utilizando las NIST mediante su Marco de Privacidad para la creación de políticas internas que ayudarán a los procesos de implementación del tratamiento de Protección de Datos Personales, por lo que se ha obtenido los siguientes resultados:

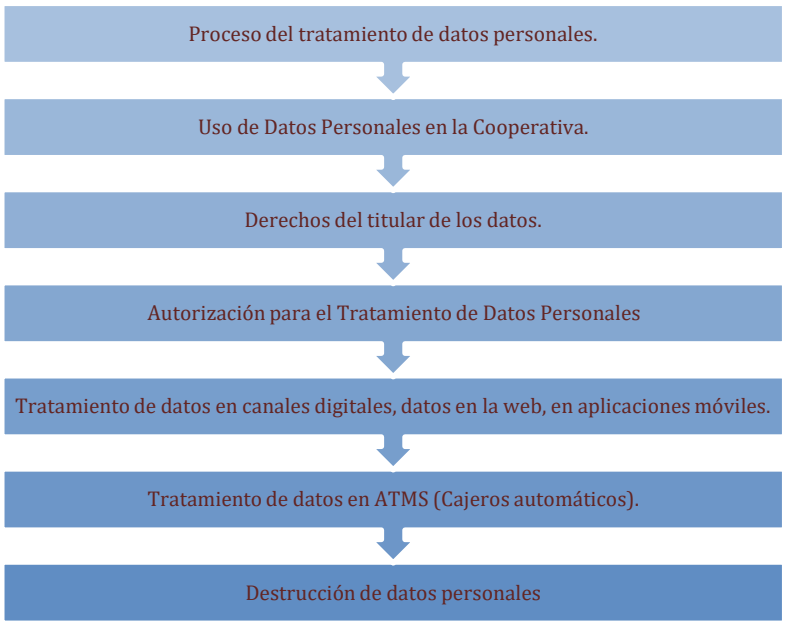
**Política de Tratamiento de datos personales**

Se ha llevado a cabo un análisis exhaustivo de la Ley Orgánica de Protección de Datos Personales y del estándar NIST para orientar la elaboración de las políticas internas de protección de datos personales, para Cooperativas de Ahorro y Crédito, para ello como punto de partida se debe identificar los tipos de datos que son procesados (en la recolección, uso, intercambio y almacenamiento) para hacer un seguimiento de cómo fluyen a través de los sistemas de la institución durante todo el ciclo de vida de los datos, desde su recolección hasta su eliminación, luego de ello se ha realizado la política teniendo en cuenta los aspectos mencionados en las tablas 1 y en el ANEXO 2 Núcleo del Marco de Privacidad NIST de este documento.

La política completa se muestra en el ANEXO 3: Propuesta de Política Interna de Protección de Datos Personales para Cooperativas de Ahorro y Crédito, a continuación, se presenta la estructura de la política.

**Figura 6**

*Estructura de Política interna de Protección de datos personales*



**Datos que se tratan**

Mediante la entrevista realizada al Oficial de Seguridad de la Información de la Cooperativa que se tomó de muestra, se pudo conocer sobre los datos que administran, los procedimientos que mantienen y los procesos se han ido implementando para cumplir con la normativa por lo que es indispensable que las Cooperativas generen políticas acordes a su realidad que se adapten a su necesidad.

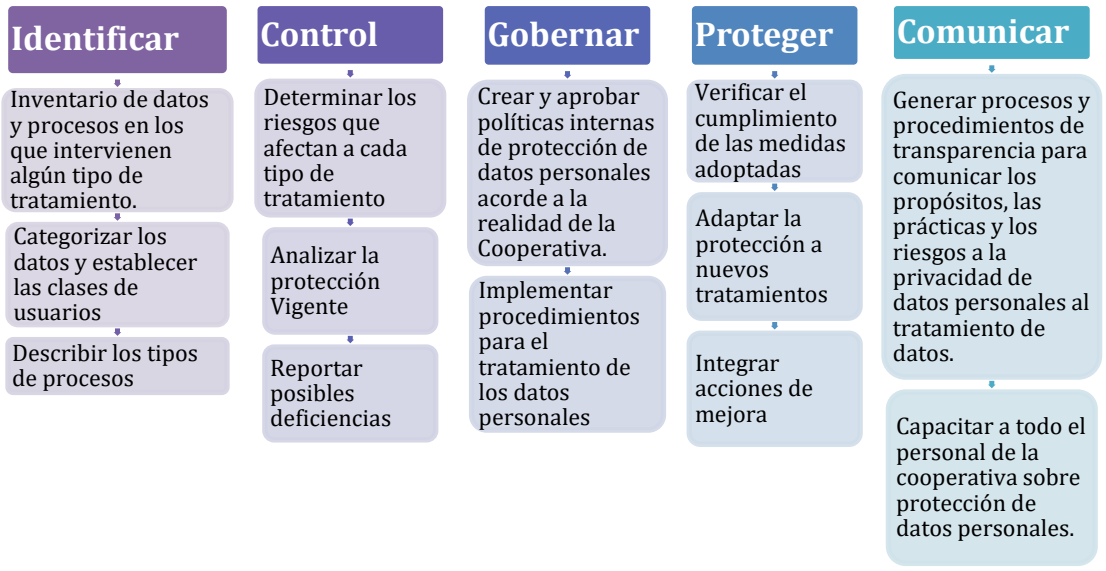
Por otro lado, se pudo conocer que se manejan datos que pueden considerarse sensibles, como es el caso de estado de salud de personal de la Cooperativa, números de cuentas, números de tarjetas de crédito, números de identificación, direcciones domiciliarias, datos de menores de edad debido a los productos y servicios que ofrece la institución, entre otros datos que por su valor se pueden considerar sensibles haciéndose necesario hacer un tratamiento adecuado para garantizar la confidencialidad, integridad y disponibilidad de los datos.

**Procesos de Protección de Datos Personales**

Los procedimientos para la Protección de Datos Personales pudieron alinearse a las NIST para obtener un plan más dinámico y eficaz que las Cooperativas de Ahorro y Crédito pueden adaptar con de elaboración de políticas para que pueda realizase todos los procesos que sean pertinentes.

**Figura 7**

*Marco de trabajo para implementar la protección de datos personales*

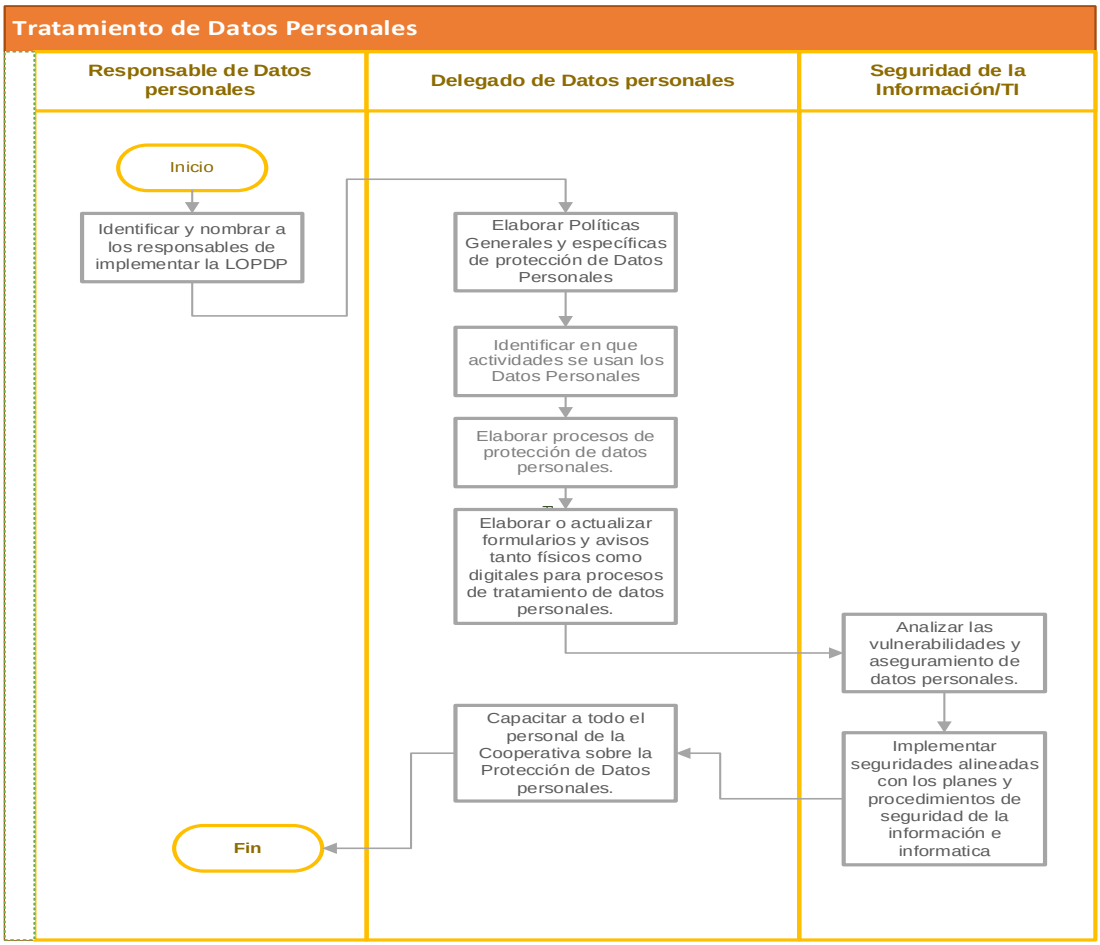



Nota: La figura muestra un Marco de trabajo alineado a las NIST para crear procesos de Protección de datos personales.

En la siguiente figura se muestra un diagrama del Proceso de Tratamiento de Protección de Datos Personales con sus respectivos procedimientos, que fue creado como una muestra general que incluye a los responsables de los procedimientos y que puede ser adaptado a la realidad de cada Cooperativa.

**Figura 8**

*Flujo de proceso de tratamiento de protección de datos personales*




Nota: En este proceso es una muestra de manera general de cómo se podría realizar el tratamiento de protección de datos personales.

En la tabla 1 se muestran los pasos del Marco de Privacidad de NIST el mismo que es una herramienta que hemos podido usar para mantener la privacidad de datos personales incluso cuando no podemos contar con un gran equipo de privacidad.

En la tabla del Anexo 2 de acuerdo con la propuesta de políticas internas bajo el estándar NIST alineadas a la Ley Orgánica de Protección de Datos Personales para Cooperativas de Ahorro y Crédito se muestran la estructura de los identificadores de la Funciones del Marco de privacidad NIST que se pueden utilizar para la creación de políticas y procedimientos para la protección de datos personales.

## CONCLUSIONES

En base a la ley Orgánica de protección de datos personales y a su reglamento se puede establecer políticas y procedimientos para garantizar un acceso seguro a los sistemas y datos, con los debidos controles para garantizar la confidencialidad, integridad y disponibilidad de los datos.

Combinar la Ley Orgánica de Protección de Datos Personales y el Marco de privacidad de la NIST permitirá a las Cooperativa identificar, evaluar y mitigar los riesgos asociados con el tratamiento de datos de manera más efectiva mediante sus políticas y procedimientos.

En ciertas Cooperativas puede darse una falta de conciencia sobre la importancia del cumplimiento normativo relacionado al tratamiento de datos personales debido a varios factores como falta de recursos, capacitación o comprensión sobre las implicaciones legales y de seguridad asociadas con el manejo de información sensible.

NIST es un estándar muy adaptable y flexible permitiendo a las cooperativas de ahorro y crédito personalizar sus políticas y procedimientos de acuerdo con sus necesidades específicas y su entorno operativo.

Mediante el estándar NIST las cooperativas de ahorro y crédito pueden fomentar la mejora continua en la gestión de datos personales, revisar y actualizar regularmente sus prácticas de seguridad y cumplimiento.

Mediante la creación de políticas y procedimientos en el cumplimiento de las leyes y regulaciones de protección de datos personales en cooperativas de ahorro y crédito es esencial para proteger la privacidad de los clientes, reducir los riesgos legales, construir confianza, mantener estándares éticos, mejorar la reputación y promover la eficiencia operativa.

## RECOMENDACIONES

Es importante tomar en cuenta que la protección de datos personales es responsabilidad de cada institución que trata datos personales por lo que es importante que se desarrolle un plan de respuesta a incidentes que defina los procedimientos para manejar y notificar las brechas de seguridad de datos, en cumplimiento con las regulaciones vigentes.

Realizar un inventario de los datos que se manejan en cada Cooperativa será de gran ayuda para tener mayor claridad a ciencia cierta sobre los datos que realmente se están usando y cuáles no, puesto a que suele existir varios datos de titulares que ya no están activos.

Realizar capacitaciones de manera regular a todo el personal de las Cooperativas sobre las políticas y procedimientos de protección de datos, así como sobre las amenazas de seguridad cibernética y las mejores prácticas de seguridad ayudarán a crear una cultura de seguridad para protección de Datos personales.

**BIBLIOGRAFÍA**


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

Medellín, C. d. (2023). GUÍA DE BUENAS PRÁCTICAS EN PROTECCIÓN. Medellin, Medellín, Antioquia.

Mena, H. A. (2022). ANÁLISIS DE USO DE SOLUCIONES DATA LOSS PREVENTION PARA INSTITUCIONES FINANCIERAS COMO MECANISMO PARA EL CUMPLIMIENTO DE NORMATIVA PCI-DSS. . *ANÁLISIS DE USO DE SOLUCIONES DATA LOSS PREVENTION PARA INSTITUCIONES FINANCIERAS COMO MECANISMO PARA EL CUMPLIMIENTO DE NORMATIVA PCI-DSS.* . Quito, Pichincha, Ecuador: http://repositorio.uisrael.edu.ec/handle/47000/3362.

NIST. (2020). *Marco para la mejora de la seguridad cibernética en infraestructuras críticas, versión 1.1.* Instituto Nacional de Normas y Tecnología NIST: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020es.pdf

NIST. (2022). *Primeros pasos del Marco de privacidad de NIST*. ¿Qué es el Marco de privacidad de NIST y cómo lo puede usar mi organización?: https://www.nist.gov/privacy-framework

NIST, C. F. (2024). *NIST National Institute of Standards and Technology.* NIST National Institute of Standards and Technology: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Pichincha, B. (2022). *Banco Pichincha.* https://www.pichincha.com/blog/ley-proteccion-datos-ecuador-que-es

Untiveros, S. (2023). *AprendaRedes.* Título: ISO 27001 vs. NIST: Un Análisis Comparativo y su Complementariedad: https://www.aprendaredes.com/titulo-iso-27001-vs-nist-un-analisis-comparativo-y-su-complementariedad/

Finder Loyal. (2021). *Ley Orgánica de Protección de Datos Personales*. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Comisión Europea. (2021). *Normas sobre protección de datos personales dentro y fuera de la UE*. https://commission.europa.eu/law/law-topic/data-protection_es

Universidad Andina Simón Bolívar. (2020). *Protección de datos personales.* https://www.uasb.edu.ec/ciberderechos/proteccion-de-datos/

Serrano, J., & Chávez, D. (2021). *Protección de datos personales en Ecuador: Análisis de la Ley Orgánica de Protección de Datos Personales y su reglamento. Actualidad Jurídica, 9(15), 63-79.*

Sandoval, Y. (2022). *ISO 27001: De qué se trata y cómo implementarla*. https://www.piranirisk.com/es/academia/especiales/iso-27001-que-es-y-como-implementarla

Moncayo, J. (07 de agosto de2023). RESOLUCIÓN N° SEPS-IGT-IGDO-IGJ-IGS-SG-DNSI-2023-017. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.seps.gob.ec/wp-content/uploads/SEPS-IGT-IGDO-IGJ-IGS-SG-DNSI-2023-017-002_firmado.pdf

Isotools. (2022). Iso 27001. https://www.isotools.us/normas/riesgos-y-seguridad/iso-27001/

Comisión Europea. Retrieved February 24, 2024. La protección de datos en la UE. (n.d.). https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_es

**ANEXOS**

**ANEXO 1**

**FORMATO DE ENTREVISTA**

| **Cooperativa de Ahorro y Crédito de muestra** | | |
|---|---|---|
| **Fecha de realización de la entrevista** | **17-01-2024** | **Entrevista realizada al Responsable de Seguridad de la Información** |

**Preguntas**

**1. ¿La Institución realiza algún tratamiento de datos personales?**

La Institución realiza varios tratamientos, ya que al ser una institución financiera constantemente se usan estos datos personales en los procesos que se realizan con nuestros socios.

2. **¿Sus avisos de privacidad contienen todos los elementos señalados en la Ley Orgánica de Datos Personales?**

Tenemos avisos para la aplicación móvil pero aun nos falta en la web transaccional que se lo va a ir implementando en los procesos de tratamiento de datos personales

3. **¿Cómo se realizará la recolección de los datos personales (encuesta, entrevista, grabación, formulario, fotografías, directamente del sujeto o de un tercero)?**

En la Institución ya tenemos datos recolectados como es el caso de nuestros socios, personal de la Cooperativa, Proveedores. Para continuar con la recolección de datos se realiza cuando los potenciales clientes solicitan servicios financieros, para ello deben abrir una cuenta de ahorros, esto se lo realiza de manera presencial, también se realiza la captación de clientes por nuestras redes sociales o página web, asesores de captaciones,

4. **¿Se ha pedido el consentimiento a los sujetos que se recogen los datos personales? ¿Cómo se ha realizado? ¿Tiene alguna evidencia?**

Hemos realizado un procedimiento inicial que se lo irá mejorando con el tiempo puesto que tenemos un formulario de consentimiento de consulta al buró de crédito en el que se ha adicionado un texto que indica sobre el consentimiento de uso de datos personales de los socios y clientes.

En el área de Talento humano se tiene un formulario de consentimiento de uso de datos personales de los empleados de la cooperativa, esperamos ir mejorando los procesos por lo que ubicaremos en la web de la Cooperativa un consentimiento que sea aprobado por los socios y clientes para el tratamiento de datos personales de forma digital.

5. **¿Se ha informado a los sujetos de que tratamiento se va a realizar con los datos personales cuando se hace la recolección de ellos? ¿De qué y cómo se les ha informado?**

Si, mediante los formularios mencionados en la pregunta anterior

**6. ¿Cómo se garantiza la seguridad de la información manejada?**

En la Cooperativa tenemos algunas medidas de seguridad necesarias para garantizar la protección de la información del titular, a fin de evitar su alteración, pérdida, tratamiento o acceso no autorizado, garantizando la integridad, confidencialidad y disponibilidad de esta estas medidas son:

• Uso de antivirus.

• Firewall.

• Copias de seguridad.

• Mantenimiento y actualización continua de software y equipos de seguridad.

**7. ¿Se ha evaluado los riesgos y el impacto en la privacidad?**

Sabemos que hay muchos riesgos en la privacidad de los datos que somos custodios y de lo que recolectamos, sin embargo, no hemos evaluado estos riesgos de manera formal.

**8. ¿Dónde se guarda la información? ¿Quién tiene acceso a esta información?**

Esta información se guarda en nuestras bases de datos del Core Financiero, además se guarda de manera física donde hay un responsable de cada área que usa varios datos de los clientes acorde a su cargo, el área se TI tiene acceso a todo el Core Financiero donde están todos los datos de clientes, talento humano tiene acceso a datos de empleados, el área financiera también tiene acceso a estos datos por cuestiones financieras, y seguridad de la información también posee acceso.

**9. ¿Se comparte o publica los datos personales de los sujetos de la institución a terceros?**

Tenemos algunos terceros que nos ayudan en las cobranzas con ellos compartimos esta información, en los casos de los empleados también se comparte para temas de seguros de vida.

**10. ¿Se ha establecido el tiempo de conservación de los datos personales?**

No tenemos un tiempo de conservación, lo estamos revisando para aplicarlo en las políticas del tratamiento de datos.

**11. ¿Cómo se tiene previsto destruir los datos luego del tiempo de conservación?**

Debemos establecer el procedimiento más adecuado acorde a las normativas vigentes y también con ayuda de buenas prácticas que lo iremos implementando.

**12. ¿Qué le ha limitado para realizar el tratamiento de datos personales en la Cooperativa?**

Realmente si se torna complicado entender la ley en primer lugar ya que es extensa y engloba varios puntos, ponerse de acuerdo con todas las partes involucradas también suele ser un limitante ya que toda normativa y documentación debe ser aprobado por el Consejo de Administración se pasan los tiempos eso causa limitantes, sin embargo, estamos encaminados para realizar el tratamiento de datos.

## ANEXO 2

## NÚCLEO DEL MARCO DE PRIVACIDAD NIST

| Función | Categoría | Subcategoría | Entregables |
|---|---|---|---|
| **GOBERNAR-P (GV-P):** Define e implementa la estructura de gobernanza organizativa para facilitar el conocimiento continuo de las prioridades de gestión de riesgos de la Cooperativa basadas en el riesgo a la privacidad. | Políticas, procesos y procedimientos de la gobernanza (GV.PO-P): Se conocen las políticas, los procesos y los procedimientos para gestionar y vigilar los requisitos normativos, legales, de riesgo. | GV.PO-P1: Se establecen y comunican los valores y las políticas de la privacidad de la organización (por ejemplo, las condiciones sobre el tratamiento de datos, como los usos o los períodos de retención de datos, y las prerrogativas de las personas con respecto al tratamiento de estos).<br>GV.PO-P2: Se establecen e implementan procesos para infundir los valores de la privacidad de la organización a la elaboración y las operaciones del sistema, producto o servicio.<br>GV.PO-P3: Se establecen las funciones y las responsabilidades del personal con respecto a la privacidad.<br>GV.PO-P4: Se coordinan las funciones y las responsabilidades de la privacidad, y se alinean con los terceros que tengan un interés (por ejemplo, proveedores de servicios, clientes y socios).<br>GV.PO-P5: Se conocen y gestionan los requisitos legales, normativos y contractuales relativos a la privacidad.<br>GV.PO-P6: Las políticas, los procesos y los procedimientos de la gestión de riesgos y la gobernanza abordan los riesgos a la privacidad. | Políticas internas que deben referirse a los siguientes aspectos:<br>Proceso del tratamiento de datos personales.<br>Uso de Datos Personales en la Cooperativa.<br>Cumplimiento de la legislación vigente en la protección y seguridad de la información y de los sistemas de información, aplicable a todos sus procesos de negocio<br>Procedimientos de Seguridad de la Información que aplicaren, a fin de proteger y garantizar los niveles de confidencialidad,<br>integridad y disponibilidad de la información y los recursos para proteger los datos personales.<br>Derechos del titular de los datos.<br>Autorización para el Tratamiento de Datos Personales<br>Tratamiento de datos en canales digitales, datos en la web, en aplicaciones móviles.<br>Uso de cookies en plataformas digitales<br>Tratamiento de datos en ATMS (Cajeros automáticos). |

| | | | |
|---|---|---|---|
| | | | Tratamiento de datos mediante videovigilancia<br>Tratamiento de datos en canales presenciales<br>Cambios en las políticas o en el aviso de privacidad |
| **CONTROL-P (CT-P):** Desarrolla e implementa actividades adecuadas para que las Cooperativas puedan aplicar los datos con detalle suficiente y gestionar los riesgos a la privacidad. | Políticas, procesos y procedimientos del tratamiento de datos (CT.PO-P): Se establecen y emplean políticas, procesos y procedimientos para gestionar el tratamiento de datos. | CT.PO-P1: Se establecen e implementan políticas, procesos y procedimientos para autorizar el tratamiento de datos (por ejemplo, decisiones organizativas, consentimiento de las personas), y la revocación y conservación de autorizaciones. | Planes de implementación de Control de Políticas, procesos y procedimientos del tratamiento de datos |
| | | CT.PO-P2: Se establecen e implementan políticas, procesos y procedimientos para habilitar la revisión, transferencia, uso compartido, revelación, modificación y eliminación de datos (por ejemplo, para mantener la calidad de los datos y gestionar la retención de estos). | |
| **COMUNICAR-P (CM-P):** Desarrolla e implementa actividades adecuadas por medio de las cuales las Cooperativas y las personas pueden obtener un conocimiento confiable y participar en un diálogo acerca de la manera en que se procesan los datos y los riesgos a la privacidad conexos. | Políticas, procesos y procedimientos de la comunicación (CM.PO-P): Se establecen y emplean políticas, procesos y procedimientos para aumentar la transparencia de las prácticas del tratamiento de datos de la organización (por ejemplo, el propósito, el alcance, las funciones y las | CM.PO-P1: Se establecen e implementan políticas, procesos y procedimientos de transparencia para comunicar los propósitos, las prácticas y los riesgos a la privacidad conexos relativos al tratamiento de datos. | Plan de comunicación y capacitación sobre Políticas, procesos y procedimientos de la comunicación |

| | | | |
|---|---|---|---|
| | responsabilidades en el ecosistema de tratamiento de datos, y el compromiso de la gestión), y los riesgos a la privacidad conexos. | | |
| **PROTEGER-P (PR-P): Establece e implementa salvaguardias adecuadas para proteger los datos personales en las Cooperativas de Ahorro y crédito.** | Políticas, procesos y procedimientos de la protección de datos (PR.PO-P): Se establecen y emplean políticas (por ejemplo, el propósito, el alcance, las funciones y las responsabilidades en el ecosistema de tratamiento de datos, y el compromiso de gestión), procesos y procedimientos de seguridad y privacidad para gestionar la protección de datos. | PR.PO-P1: Se crea y mantiene una configuración básica de la tecnología de la información que incorpora principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).<br>PR.PO-P2: Se establecen e implementan los procesos de control de cambios de configuración.<br>PR.PO-P3: Se hacen, conservan y prueban copias de seguridad de la información.<br>PR.PO-P5: Se mejoran los procesos de protección.<br>PR.PO-P7: Se establecen, implementan y gestionan los planes de respuesta (de respuesta a incidentes y de continuidad de la empresa) y los planes de recuperación (de recuperación de incidentes y de recuperación de desastres).<br>PR.PO-P10: Se elabora e implementa un plan de gestión de vulnerabilidades. | Hoja de ruta de salvaguardas para proteger los datos personales. |

Nota: Adaptado del "*Identificadores únicos de las Funciones y las Categorías del Marco de privacidad" tomado de* (NIST, 2020)

## ANEXO 3

## DEFINICIONES DE TÉRMINOS LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES

**Art. 4.-Términos y definiciones. -**Para los efectos de la aplicación de la presente Ley se establecen las siguientes definiciones:

**Anonimización:** La aplicación de medidas dirigidas a impedir la identificación o reidentificación de una persona natural, sin esfuerzos desproporcionados.

**Consentimiento**: Manifestación de la voluntad libre, específica, informada e inequívoca, por el que el titular de los datos personales autoriza al responsable del tratamiento de los datos personales a tratar los mismos.

**Dato biométrico:** Dato personal único, relativo a las características físicas o fisiológicas, o conductas de una persona natural que permita o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos, entre otros.

**Dato personal:** Dato que identifica o hace identificable a una persona natural, directa o indirectamente.

**Datos personales crediticios:** Datos que integran el comportamiento económico de personas naturales, para analizar su capacidad financiera.

**Datos relativos a la salud:** datos personales relativos a la salud física o mental de una persona, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

**Datos sensibles:** Datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.

**Titular:** Persona natural cuyos datos son objeto de tratamiento.

**Transferencia o comunicación:** Manifestación, declaración, entrega, consulta, interconexión, cesión, transmisión, difusión, divulgación o cualquier forma de revelación de datos personales realizada a una persona distinta al titular, responsable o encargado del tratamiento de datos personales. Los datos personales que comuniquen deben ser exactos, completos y actualizados.

**Tratamiento:** Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recogida, recopilación, obtención, registro, organización, estructuración,

conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión, comunicación o transferencia, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales.

**Vulneración de la seguridad de los datos personales:** Incidente de seguridad que afecta la confidencialidad, disponibilidad o integridad de los datos personales.

**ANEXO 4**

**PROPUESTA DE POLÍTICA INTERNA DE PROTECCIÓN DE DATOS PERSONALES**

**PARA COOPERATIVAS DE AHORRO Y CRÉDITO**

**OBJETIVO:** Garantizar el derecho constitucional que tienen todas las personas de conocer, actualizar, rectificar, revocar, suprimir, eliminar o Inactivar la información con datos personales que se hayan recopilado sobre ellas en las bases de datos o archivos de la Cooperativa.

**DATOS INFORMATIVOS DE LA COOPERATIVA**

**Dirección:**

**Teléfono:**

**Correo:**

**Finalidad del tratamiento:** La Cooperativa utilizará sus datos personales para la realización de actividades de intermediación financiera.

**Destinatarios.** La Cooperativa no compartirá los datos personales de sus socios y clientes con terceros, salvo autorización del titular o requerimiento de autoridad competente.

**Derechos:** El titular de los datos en cualquier momento podrá ejercer sus derechos respecto a la protección de estos, ello conforme lo prescribe la Ley Orgánica de Protección de Datos, es decir, podrá solicitar el acceso, modificación, suspensión o eliminación de los datos personales, además de otros derechos.

**1. INFORMACIÓN DEL USO DE DATOS PERSONALES**

- La Cooperativa en cumplimiento de la Ley Orgánica de Protección de Datos, informa a sus socios sobre el tratamiento de datos personales que se realiza durante el ejercicio de actividades de intermediación financiera (prestación de productos y servicios financieros), dicho tratamiento se lo realizará de acuerdo con a las disposiciones de la Ley Orgánica de protección de datos personales y su Reglamento.
- La Cooperativa de ha implementado medidas técnicas y organizativas para garantizar al usuario un alto nivel de seguridad y privacidad al momento de tratar sus datos personales, evitando de esta manera el mal uso, perdida, filtración, alteración, o acceso no autorizado de la información facilitada por el titular.

## 2. POLÍTICAS PARA EL TRATAMIENTO DE LOS DATOS PERSONALES

### 2.1. FINALIDAD DEL TRATAMIENTO

1. Los usuarios de Información de la Cooperativa deberán cumplir con las políticas, procesos y procedimientos de Seguridad de la Información que se apliquen, a fin de proteger y garantizar los niveles de confidencialidad, integridad y disponibilidad de la información y los recursos que soportan la misma.
2. La Cooperativa informa a sus socios y clientes que sus datos personales y el tratamiento de estos serán utilizados para:
    - Ofrecer de manera individual o en conjunto productos o servicios financieros brindados por la Cooperativa a través de cualquier medio, ya sea digital o físico, incluyendo la posibilidad de contactar al titular para dichos propósitos.
    - Contratación de servicios o productos financieros entre el titular y la Cooperativa.
    - Validación de información o confirmación de transacciones realizadas por el titular en las cuales pueda intervenir datos personales.
    - Para gestionar, en caso de incumplimiento, de cualquiera de las obligaciones que el titular adquiere a favor de la Cooperativa.
    - Cumplimiento de la normativa vigente.
    - Análisis estadístico y encuestas de satisfacción acerca de productos financieros ofertados por la Cooperativa.
    - Verificación de capacidad de endeudamiento, capacidad crediticia y demás información que la Cooperativa requiera para otorgar sus servicios o productos.
    - Garantizar la seguridad de las personas, así como de los bienes e instalaciones físicas de la entidad.
    - Facturación de productos ofertados por la institución.

### 2.2. DERECHOS DEL TITULAR DE LOS DATOS

En cualquier momento el titular de los datos podrá hacer uso de sus derechos prescritos en la Ley Orgánica de Protección de Datos:

- Conocer, actualizar o rectificar sus datos personales.
- Ser informado, previa solicitud, sobre el uso y tratamiento que la Cooperativa realiza con sus datos personales.
- Revocar la autorización y solicitar la suspensión del tratamiento cuando el tratamiento no respete los principios, derechos y garantías legales, siempre y cuando esta solicitud no interfiera con las obligaciones adquiridas con la Cooperativa por parte del titular y con exigencias normativas y legales.

## 2.3. DESTINATARIOS DE LA INFORMACIÓN

- La Cooperativa pone en conocimiento que, para brindar ciertos servicios, cuenta con el apoyo de terceros (proveedores), los cuales podrían acceder a datos personales de socios y clientes si fuera necesario.
- La Cooperativa maneja estrictos criterios de selección de proveedores con la finalidad de conocer de manera más excautiva a los mismos y dar cumplimiento a las obligaciones establecidas en la normativa.

## 2.4. CONSENTIMIENTO PARA TRATAR DATOS PERSONALES

- La Cooperativa solicitará el consentimiento del titular para el tratamiento de sus datos personales. Este consentimiento puede otorgarse durante la recolección inicial de los datos o al inicio de un contrato de servicio o producto.
- La solicitud de consentimiento se realizará a través de los canales oficiales de la Institución, ya sea de forma física o digital.
- La autorización del titular no será necesaria cuando se trate de información requerida por un ente legal o por orden de autoridad competente.
- Cada área de la Cooperativa que realice un tratamiento activo de datos personales debe garantizar la custodia y almacenamiento de la autorización para el tratamiento de los datos ya se de manera física como digital.

## 2.5. TRATAMIENTO DE DATOS PERSONALES

- La Cooperativa utiliza los datos del titular únicamente para fines específicos, explícitos y exactos. Durante el tratamiento de datos, se garantiza que la información empleada sea adecuada, relevante y limitada a las actividades específicas internas de la Cooperativa.
- En el tratamiento de datos personales se implementarán medidas técnicas, físicas y organizativas apropiadas para proteger los datos personales contra actividades ilícitas, o cualquier forma de vulneración de la información del titular, utilizando medidas de protección como cifrado de los datos o seudonimización de la información para garantizar la confidencialidad, integridad, y disponibilidad de los datos personales.
- Se tomarán medidas razonables para garantizar que los datos personales sean precisos, completos y actualizados, y se proporcionarán mecanismos para que los miembros corrijan cualquier inexactitud.
- Se realizará de manera permanente capacitaciones sobre el tratamiento de los datos Personales con la finalidad de establecer una cultura de conocimiento sobre el tema.
- Las aplicaciones desarrolladas por la Cooperativa deben contar con los estándares necesarios de seguridad para resguardar la información de los usuarios.

## 2.6. CANALES DIGITALES

- La Cooperativa ofrece a sus socios y clientes el uso de aplicaciones web y móviles, a través de terceros por lo que deberá verificar que estas aplicaciones cuenten con la debida protección y seguridad de la información que se maneje.
- La Cooperativa ofrece a sus socios y clientes acceso a una red de cajeros automáticos ATMS a nivel nacional, operados por un tercero, los que permiten realizar retiros y otros servicios proporcionados por la institución de esta forma procesan información personal del usuario con el propósito de validar tanto su información personal como financiera antes de iniciar cualquier transacción, el tercero deberá garantizar la seguridad de estos datos de acuerdo a lo que la ley establece y ajustado a buenas prácticas de los estándares NIST.
  Para cumplir con las normativas, la Cooperativa emplea una variedad de sistemas de videovigilancia colocados en sus instalaciones, cajeros automáticos y ubicaciones externas a la institución. La información recopilada a través de estos dispositivos se utiliza para asegurar la seguridad de las personas, así como de los activos y las instalaciones de la institución. Además, previa solicitud, dicha información puede ser utilizada por autoridades judiciales, administrativas, fiscales, entre otras, o por la propia institución.
- Existirá leyendas informativas colocadas en las oficinas o instalaciones de la Cooperativa indicando que se usa videovigilancia teniendo en cuenta que al momento de ingresar a nuestros establecimientos se interpretará como una acción de autorización expresa e informada para llevar a cabo el tratamiento de estas imágenes, amparados en la ley.
- En las agencias de La Cooperativa se encuentran las áreas operativas de cajas, servicio al cliente, inversiones, créditos y tarjetas para poder brindar productos o servicios, se solicitan datos personales a los socios y clientes para gestionar los servicios financieros que la Institución, esta información será tratada bajo los mismos procedimientos de seguridad y protección que se han detallado anteriormente y con la finalidad de brindar un entorno financiero seguro al usuario.

## 2.7. DATOS DE MENORES DE EDAD

- En caso del tratamiento de datos personales de niñas, niños o personas de edad menor a 15 años es necesario el consentimiento expreso de su representante legal. Los adolescentes mayores de 15 años pueden proporcionar su consentimiento de forma directa.

## 2.8. DESTRUCCIÓN DE DATOS PERSONALES

- La Cooperativa seleccionará los métodos adecuados de destrucción de datos, teniendo en cuenta el tipo de medio de almacenamiento (por ejemplo, discos duros, papel impreso, dispositivos de almacenamiento móvil, etc.), incluyendo la utilización de herramientas y técnicas específicas para garantizar que la información no pueda ser recuperada de manera indebida.

- Se proporcionará capacitación periódica al personal involucrado en el manejo y la destrucción de datos personales, con el fin de garantizar el cumplimiento adecuado de los procedimientos establecidos.

## ANEXO 5

## VALIDACIÓN DE ESPECIALISTAS

**RESUMEN**

Se solicitó a dos especialistas para evaluar la propuesta del proyecto de titulación, los dos son especializados en Ingeniería en Sistemas en campos de Desarrollo de Software y Ciberseguridad respectivamente, en su validación de obtiene calificaciones de 35 puntos y 33 puntos, los dos especialistas coinciden que el alcance que tendrá la propuesta y su representatividad es de gran valor, que cumple con los requisitos de Impacto, Aplicabilidad, Conceptualización, Actualidad, Calidad Técnica, Factibilidad, Pertinencia debido a que es un tema que puede ser aplicado por Cooperativas de Ahorro y crédito y otras instituciones puesto que es un tema actual y de gran explotación más adelante.

**INSTRUMENTO DE VALIDACIÓN**

**UNIVERSIDAD TECNOLÓGICA ISRAEL**

**ESCUELA DE POSGRADOS "ESPOG"**

**MAESTRÍA EN SEGURIDAD INFORMÁTICA**

**INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA**

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: **Propuesta de política interna alineada a la Ley de Protección de Datos Personales mediante estándar NIST para Cooperativas de Ahorro y Crédito.**

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por:

| **Título obtenido** |
| --- |
| Magister en Ciberseguridad |
| **Cédula de Identidad** |
| 1719596874 |
| **E- mail** |
| mario.congo@tipti.market |
| **Institución de Trabajo** |
| TIPTI S.A. |
| **Cargo** |
| CISO |
| **Años de experiencia en el área** |
| 2 años |

1

**Instructivo:**

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque **una X** en cada indicador, tomando en cuenta que Muy adecuado equivale a 5,
  Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuadoequivale a 2 e Inadecuado equivale a 1.

**Tema:** Propuesta de política interna alineada a la Ley de Protección de Datos Personales mediante estándar NIST para Cooperativas de Ahorro y Crédito.

| *Indicador* | *Descripción* | Muy adecuado | Bastante Adecuado | Adecuado | Poco adecuado | Inadecuado |
|---|---|---|---|---|---|---|
| ***Impacto*** | *El alcance que tendrá la propuesta y su representatividaden la generación de valor* | 5 | | | | |
| ***Aplicabilidad*** | *La capacidad de implementaciónde la propuesta considerando que los contenidos sean aplicables* | | 4 | | | |
| ***Conceptualización*** | *La base de conceptos y teoríaspropias de la propuesta de manera sistémica y articulada* | 5 | | | | |
| ***Actualidad*** | *Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta* | 5 | | | | |
| ***Calidad Técnica*** | *Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de susbeneficiarios* | 5 | | | | |
| ***Factibilidad*** | *El nivel de utilización de lapropuesta por parte de la organización acorde a los recursos disponibles* | | 4 | | | |
| ***Pertinencia*** | *La contundencia y conveniencia de la propuesta para solucionar el problema planteado.* | 5 | | | | |
| | ***Total*** | 25 | 8 | | | |

**Observaciones:**

El estándar NIST es un buen marco de referencia para aplicar políticas y controles de seguridad dentro de una empresa por lo que puedo mencionar que este trabajo está muy bien enfocado y alineadocon dicho estándar, comprender cada uno de los planteamientos, es de vital importancia, para brindar seguridad y alinearse con la ley de protección de datos, personales. El uso de la Inteligencia Artificial (IA) en la seguridad informática está creciendo exponencialmente, con el potencial de revolucionar la forma en que se protegen los sistemas y ahora los datos personales.

La protección de datos personales supone un alto esfuerzo en procesos de tratamiento, monitoreo,

gestión de riesgos entre otros, lo que implica un equipo que alto conocimiento y dedicación en cada una de las aristas que representa, ya que en estos procesos se debe analizar grandes volúmenes de datos de forma rápida y eficiente para identificar patrones y anomalías que podrían indicar un ataque.

**Recomendaciones**

Es importante que en este trabajo se tome en cuenta con mucha claridad que el tratamiento de datos no solo depende de la creación de políticas internas, si bien es una gran herramienta es necesario siempre contar con talento humano para crear una cultura de protección de datos personales para que se haga un seguimiento continuo del tratamiento de Datos Personales para evitar ser vulnerables a ataques, lo que podría tener graves consecuencias para la seguridad de los sistemas y datos.

Finalmente, como cualquier otro aspecto de seguridad, se necesita personal capacitado para desarrollar, implementar y administrar la seguridad de datos, por lo indicado considero que es muy importante establecer lineamientos en las empresas tales como políticas y procedimientos como se muestran en el documento partiendo de ello en todo este gran proceso que ahora las normativas nos exigen.

Como aporte adicional, quiero felicitar a la autora de esta propuesta, por el gran trabajo y esfuerzo que ha plasmado en su proyecto ya que se ha enfocado en un tema de alto impacto que en la actualidad no solo es importante, sino que es el pilar dentro del desarrollo empresarial y la continuidad de negocio, si bien es cierto muchas empresas aún se resisten en invertir en seguridad y protección de datos personales, con el criterio de que "nunca nos va a pasar" o "no nos ha pasado", trabajos como este demuestran que hay preocupación por el futuro empresarial y que la seguridad es de vital importancia para su desarrollo y protección de datos.

**Lugar, fecha de validación**: Quito 9 de marzo 2024


Firma del especialista

**INSTRUMENTO DE VALIDACIÓN**

**UNIVERSIDAD TECNOLÓGICA ISRAEL**

**ESCUELA DE POSGRADOS "ESPOG"**

**MAESTRÍA EN SEGURIDAD INFORMÁTICA**

**INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA**

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: Propuesta de política interna alineada a la Ley de Protección de Datos Personales mediante estándar NIST para Cooperativas de Ahorro y Crédito.

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Ing. Daniel Arcentales

| **Título obtenido** |
| --- |
| **Ingeniero en Sistemas e Informática** |
| **Cédula de Identidad** |
| **1721594446** |
| **E- mail** |
| **daniel.arcentales1994@gmail.com** |
| **Institución de Trabajo** |
| **Banco Internacional** |
| **Cargo** |
| **Analista de Desarrollo** |
| **Años de experiencia en el área** |
| **6** |

1

**Instructivo:**

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque **una X** en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

**Tema:** Propuesta de política interna alineada a la Ley de Protección de Datos Personales mediante estándar NIST para Cooperativas de Ahorro y Crédito.

| *Indicador* | *Descripción* | Muy adecuado | Bastante Adecuado | Adecuado | Poco adecuado | Inadecuado |
|---|---|---|---|---|---|---|
| ***Impacto*** | *El alcance que tendrá la propuesta y su representatividad en la generación de valor* | x | | | | |
| ***Aplicabilidad*** | *La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables* | x | | | | |
| ***Conceptualización*** | *La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada* | x | | | | |
| ***Actualidad*** | *Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta* | x | | | | |
| ***Calidad Técnica*** | *Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios* | x | | | | |
| ***Factibilidad*** | *El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles* | x | | | | |
| ***Pertinencia*** | *La contundencia y conveniencia de la propuesta para solucionar el problema planteado.* | x | | | | |
| *Total* | | 35 | | | | |

**Observaciones:** Considero que esta propuesta es de mucho valor debido a que, en la actualidad por normativa se solicita realizar tratamiento de datos personales por lo que esta propuesta es muy factible para poderla desarrollar.

**Recomendaciones**

Sería muy importante que se dé seguimiento a esta propuesta ya que podría ayudar a las cooperativas a cumplir con la ley orgánica de protección de datos personales.

**Lugar, fecha de validación**: Quito 9 de marzo 2023

**Firma del especialista**

2