**UNIVERSIDAD TÉCNICA DEL NORTE**

**FACULTAD DE POSGRADO**

**MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA**

**TEMA:**

# "IMPLEMENTACIÓN DE UNA APLICACIÓN WEB PARA EVALUAR LOS CONOCIMIENTOS EN SEGURIDAD DE LA INFORMACIÓN DEL PERSONAL DE LAS INSTITUCIONES FINANCIERAS DEL SECTOR POPULAR Y SOLIDARIO UNO, BASÁNDOSE EN LA NORMATIVA DE SEGURIDAD DE LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA (SEPS)"

**Trabajo de Titulación previo a la obtención del Título de Magíster en Computación con Mención en Seguridad Informática**


**AUTOR:**

Marco Vinicio Terán Tabango

**DIRECTOR:**

PH. D QUIÑA MERA JOSÉ ANTONIO

**ASESOR:**

MSC. SALAZAR FIERRO FAUSTO ALBERTO



IBARRA - ECUADOR

2025

**APROBACIÓN DEL TUTOR**

En calidad de Tutor del Trabajo de Investigación con el tema: "IMPLEMENTACIÓN DE UNA APLICACIÓN WEB PARA EVALUAR LOS CONOCIMIENTOS EN SEGURIDAD DE LA INFORMACIÓN DEL PERSONAL DE LAS INSTITUCIONES FINANCIERAS DEL SECTOR POPULAR Y SOLIDARIO UNO, BASÁNDOSE EN LA NORMATIVA DE SEGURIDAD DE LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA (SEPS)." De auditoria de Terán Tabango Marco Vinicio, para obtener el Titulo de Magister en Computación con mención en Seguridad Informática, doy fe que dicho trabajo reúne los requisitos y méritos suficientes para ser sometidos a presentación y evaluación por parte del jurado examinador que se designe.

En la ciudad de Ibarra, a los 13 días del mes de marzo de 2025

JOSE ANTONIO QUIÑA MERA

Firmado digitalmente por JOSE ANTONIO QUIÑA MERA
Nombre de reconocimiento (DN): c=EC, sn=QUIÑA MERA, givenName=JOSE ANTONIO, serialNumber=IDCEC-1002322384, cn=JOSE ANTONIO QUIÑA MERA, 2.5.4.97=TINEC-1002322384001

PhD. Antonio Quiña

Tutor.

**UNIVERSIDAD TÉCNICA DEL NORTE**

**BIBLIOTECA UNIVERSITARIA**

**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 del presente trabajo a la UniversidadTécnica 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** | 1003853965 | | |
| **APELLIDOS Y NOMBRES** | Terán Tabango Marco Vinicio | | |
| **DIRECCIÓN** | Juan Rojas y Vicente Zamora, Otavalo | | |
| **EMAIL** | marquin.90@gmail.com | | |
| **TELÉFONO FIJO** | | **TELÉFONO MÓVIL:** | 0983736641 |

| **DATOS DE LA OBRA** | |
|---|---|
| **TÍTULO:** | IMPLEMENTACIÓN DE UNA APLICACIÓN WEB PARA EVALUAR LOS CONOCIMIENTOS EN SEGURIDAD DE LA INFORMACIÓN DEL PERSONAL DE LAS INSTITUCIONES FINANCIERAS DEL SECTOR POPULAR Y SOLIDARIO UNO, BASÁNDOSE EN LA NORMATIVA DE SEGURIDAD DE LA |

| | |
|---|---|
| | SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA (SEPS) |
| **AUTOR (ES):** | Terán Tabango Marco Vinicio |
| **FECHA: DD/MM/AAAA** | 18/03/2025 |
| **PROGRAMA DE POSGRADO** | Maestría en Computación con mención en Seguridad Informática |
| **TITULO POR EL QUE OPTA** | Magíster en Computación con mención en Seguridad Informática |
| **TUTOR** | PH. D QUIÑA MERA ANTONIO |

## 2. CONSTANCIAS

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

Ibarra, a los 20 días del mes de mayo del año 2025

**EL AUTOR:**


Firma _____

Nombre: Marco Vinicio Terán Tabango

## DEDICATORIA

A mi esposa y a mi hijo, por su amor constante y por la paciencia que me brindaron a lo largo de este proceso de estudios. Gracias por ser mi apoyo incondicional y por motivarme siempre a crecer tanto personal como profesionalmente.

A mi madre, por su amor profundo y por su entrega inquebrantable en cada etapa de nuestras vidas. Por cuidarnos, educarnos y darnos los valores que me han guiado a lo largo de mi camino.

A mis hermanas, por enseñarme lo que realmente significa la perseverancia, el esfuerzo y el cariño familiar. Gracias por estar a mi lado y apoyarme para lograr alcanzar una de las metas más importantes de mi vida.

## AGRADECIMIENTO

A Dios, por brindarme la oportunidad de cumplir todas las metas que me he propuesto y por las que seguiré alcanzando en el futuro, con su guía y bendición constante.

A mi tutor, el Ph.D. Antonio Quiña Mera, y a mi asesor, el Msc. Fausto Salazar Fierro, por su dedicación, tiempo y conocimientos. Gracias por orientarme con paciencia y por compartir su experiencia en cada etapa de este trabajo de investigación.

A todos los docentes de la Maestría, por compartir sus saberes y por brindarme las herramientas necesarias para expandir mi campo profesional.

# ÍNDICE DE CONTENIDOS

# ÍNDICE DE TABLAS

# ÍNDICE DE FIGURAS

**UNIVERSIDAD TÉCNICA DEL NORTE**

**INSTITUTO DE POSGRADOS**

**PROGRAMA DE MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA**

# IMPLEMENTACIÓN DE UNA APLICACIÓN WEB PARA EVALUAR LOS CONOCIMIENTOS EN SEGURIDAD DE LA INFORMACIÓN DEL PERSONAL DE LAS INSTITUCIONES FINANCIERAS DEL SECTOR POPULAR Y SOLIDARIO SEGMENTO UNO, BASÁNDOSE EN LA NORMATIVA DE SEGURIDAD DE LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA (SEPS)

**Autor**: Marco Vinicio Terán Tabango

**Tutor**: Quiña Mera José Antonio

**Año**: 2025

## RESUMEN

La presente investigación se basa principalmente en la implementación de una herramienta que nos permitió evaluar la eficacia de la formación del personal de las diferentes instituciones pertenecientes al sector popular y solidario para determinar el nivel de concienciación y aplicabilidad respecto a la seguridad y privacidad de la información, logrando así determinar si es necesario fortalecer los conocimientos en el personal, a la vez permitan a las instituciones cumplir con las leyes respecto a la protección de datos y alinearse a las directivas y políticas emitidas por los organismos de control, evitando así sanciones que afecten la reputación institucional.

La investigación se llevó a cabo en varias fases con el propósito de recopilar datos sobre el nivel de comprensión o retención de conocimiento de las capacitaciones

normativas en seguridad y privacidad de la información dentro de una institución financiera perteneciente al sector popular y solidario, específicamente en el segmento uno de la provincia de Imbabura. Posteriormente, se procedió con la implementación de una herramienta web que facilita una capacitación interactiva a través de cuestionarios y videos respecto a la seguridad y privacidad de la información, la misma que a la vez permite se autoevalúen respecto a los conocimientos adquiridos y finalmente se emiten los resultados tanto para el personal responsable de la Seguridad de la Información, como para el nivel Directivo y puedan generar una toma de decisiones oportunas en la formación del personal a cargo.

**Palabras clave:** Seguridad de la Información, Privacidad, Protección de Datos, Economia Popular y Solidaria.

## ABSTRACT

This research primarily focuses on the implementation of a tool designed to assess the effectiveness of training for staff in institutions belonging to the popular and solidarity sector. The goal was to determine the level of awareness and the applicability of information security and privacy practices, thereby identifying whether it is necessary to strengthen the staff's knowledge. This would also enable institutions to comply with data protection laws and align with the guidelines and policies issued by regulatory bodies, thus avoiding sanctions that could damage the institution's reputation.

The research was conducted in multiple phases, allowing the collection of data to assess the level of training in information security and privacy within a financial institution in the popular and solidarity sector, specifically in segment one of the Imbabura province. Following this, a web-based tool was implemented to provide interactive training through quizzes and videos on information security and privacy. The tool also allows individuals to self-assess their knowledge and generates results for both the Information Security personnel and the management team, enabling timely decisions regarding further staff training.



**Keywords:** Information Security, Privacy, Data Protection, Popular and Solidarity Economy.

# CAPITULO I
# EL PROBLEMA

## 1.1. Introducción

Hoy en día, la tecnología desempeña un rol crucial en una sociedad que se digitaliza progresivamente, impactando desde la forma en que nos comunicamos hasta la operatividad de las organizaciones. No obstante, este avance también ha traído consigo nuevos retos en cuanto a la protección y privacidad de la información. El progreso continuo de las amenazas informáticas y el aumento de los riesgos asociados han convertido la gestión de la seguridad informática en un tema prioritario a nivel mundial. El Departamento de Seguridad Nacional de los Estados Unidos indica que: "Nuestra vida cotidiana, la economía y la seguridad nacional dependen de un espacio digital estable." (Gutiérrez, 2022).

En Ecuador, las instituciones financieras del sector popular y solidario enfrentan retos similares. La Superintendencia de Economía Popular y Solidaria (SEPS) establece normativas específicas para garantizar la protección de la información de los socios de las entidades y organizaciones sobre las que ejercen supervisión y control, pero su implementación efectiva se ve limitada por la falta de herramientas que evalúen el nivel de conocimiento del personal responsable. Este proyecto busca resolver esta problemática mediante el diseño e implementación de una herramienta web que permita identificar brechas en los conocimientos de seguridad, fortalecer el cumplimiento de la normativa de la SEPS y fomentar una cultura de seguridad en el sector.

## 1.2. Problema de investigación

Los ciberataques han tenido un incremento exponencial a escala mundial, adquiriendo una mayor sofisticación y peligrosidad. Estos ataques utilizan diversas tácticas, que abarcan desde la aplicación de varias técnicas combinadas hasta la diversificación de sus orígenes geográficos y el apoyo de organizaciones delictivas con un elevado grado de especialización tecnológica. (Castillo, 2020)

Entre los métodos más habituales se incluyen el Phishing, que implica la suplantación de identidad a través de emails; el Smishing, que emplea mensajes de texto para engañar a las víctimas; el Vishing, fundamentado en llamadas telefónicas engañosas; y el Ransomware Targeted, destinado específicamente a compañías para el secuestro de datos. Igualmente, sobresalen las noticias falsas, que intentan desinformar, los ataques a

infraestructuras vitales y la difusión de malware para móviles y otras variantes de software malintencionado. (Castillo, 2020)

En este escenario, las compañías en Ecuador han lidiado con varios incidentes de seguridad, ocasionando grandes pérdidas debido a la insuficiente preparación para manejar los riesgos vinculados a la implementación de tecnologías emergentes y el proceso de digitalización.

En Ecuador, pocas son las entidades que han destinado recursos humanos, tecnológicos y económicos para fortalecer sus seguridades, resistir ataques cibernéticos, salvaguardar los recursos económicos y la información sensible de la empresa y la de sus clientes.

El control no solo se basa en la adquisición e implementación de tecnología de seguridad. Utilizando un arma muy antigua y efectiva —la Ingeniería Social—, los ataques de los hackers llegan a tener éxito porque atacan el punto más estratégico de toda empresa, el recurso humano (Navarrete, 2020).

En el ámbito específico de las empresas financieras y las fintech, los riesgos son aún más acuciantes. Estas empresas manejan grandes volúmenes de datos financieros y personales, lo que las convierte en objetivos atractivos para los ciberdelincuentes. Los ataques cibernéticos pueden tener repercusiones devastadoras, incluyendo la pérdida de activos, daños en la imagen corporativa y penalizaciones jurídicas.

América Latina y, en particular, Ecuador no son inmunes a estos desafíos. Las empresas financieras y las fintech de la zona se hallan en una etapa de crecimiento y transformación digital, lo que implica una mayor exposición a las amenazas cibernéticas. La falta de conocimiento y recursos adecuados puede ser un obstáculo significativo para la ejecución de medidas sólidas de seguridad y privacidad en estas organizaciones.

De acuerdo con la evaluación realizada por la Policía Nacional de Ecuador, la ausencia de educación digital y la baja sensibilización acerca de la ciberseguridad hacen que la población sea susceptible a la delincuencia cibernética. Numerosas víctimas no identifican oportunamente que sus bienes han sido afectados y, incluso si lo hacen, hay un desconocimiento generalizado sobre cómo reportar estos crímenes. La falta de confianza en la habilidad de las autoridades para indagar y castigar estos delitos, junto con las restricciones en los medios para su solución, causa que numerosos casos no se registren. Por lo tanto, una considerable proporción de los crímenes cibernéticos

permanecen sin castigo. Además, de acuerdo con información del Ministerio de Gobierno, los delitos informáticos más habituales en Ecuador abarcan el fraude en línea, el hurto de identidad y la infracción de información personal, impactando de manera considerable a los ciudadanos ( Ministerio de Telecomunicaciones y Sociedad de la Información, 2022).

A eso se suma la falta de herramientas tecnológicas que permitan evaluar de manera sistemática y objetiva el nivel de conocimiento del personal de las instituciones financieras del sector popular y solidario sobre seguridad de la información, que generan el incumplimiento de las normativas de seguridad establecidas por la SEPS, riesgos elevados de brechas de seguridad debido a la falta de capacitación adecuada y falta de información precisa para implementar estrategias de mejora en la gestión de la seguridad de la información.

### 1.3. Interrogantes de la investigación

- ¿Cuáles son los requerimientos de evaluación en seguridad y privacidad tomando como referencia la normativa vigente y los controles definidos en la ISO 27002-2022?
- ¿Qué herramientas existen para evaluar la eficacia de formación en seguridad y privacidad de la información al personal en las Instituciones financieras?
- ¿Cómo se puede mejorar el conocimiento en seguridad y privacidad de la información en el personal que conforman las instituciones financieras del segmento uno de la provincia de Imbabura?

### 1.4. Objetivos de la investigación

**Implementación de una aplicación web para evaluar los conocimientos en Seguridad de la Información del personal de las instituciones financieras del sector popular y solidario del segmento uno, basándose en la normativa de seguridad de la información de la Superintendencia de Economía Popular y solidaria (SEPS): Un caso de estudio.**

#### 1.4.1. Objetivo general

Implementar una aplicación web para evaluar los conocimientos en Seguridad de la Información del personal de las instituciones financieras del sector popular y solidario del segmento uno, basándose en la normativa de seguridad de la información de la Superintendencia de Economía Popular y solidaria (SEPS).

### 1.4.2. Objetivos específicos

- Establecer un marco conceptual y tecnológico acerca de la seguridad de la información basado la normativa de la SEPS.
- Implementar una aplicación web aplicando las buenas prácticas para evaluar los conocimientos de la seguridad de la información basado la normativa de la SEPS.
- Evaluar la mejora de los conocimientos del personal de una Cooperativa (caso de estudio), acerca de la seguridad de la información utilizando la aplicación implementada.

## 1.5. Justificación

Para reducir los peligros vinculados con la ciberdelincuencia, Ecuador instauró la Política Nacional de Ciberseguridad mediante el Acuerdo Ministerial N°. 006-2021, publicado el 23 de junio de 2021 en la Edición Especial del Registro Oficial 479. El objetivo de esta política es potenciar las habilidades del país en términos de seguridad digital, garantizando libertades de los ciudadanos y la protección de los derechos, además de la protección de los bienes legales del Estado en el ámbito digital. Además, define una serie de medidas estratégicas orientadas a fomentar un entorno cibernético más seguro y fiable ( Ministerio de Telecomunicaciones y Sociedad de la Información, 2022).

Basada en el acuerdo ministerial algunas instituciones han optado por brindar capacitación como por ejemplo la SEPS en la implementación de la ISO 27001 en el sector cooperativo, además de la difusión de la estrategia nacional de ciberseguridad del Ecuador propuesto por el Ministerio de Telecomunicaciones y Sociedad de la Información, razones por la cual el presente proyecto de investigación pretende determinar las acciones que han tomado las instituciones financieras que pertenecen al segmento uno de la provincia de Imbabura y el nivel de formación que han brindado al talento humano de cada una de ellas, para evaluar la eficacia respecto a la seguridad y privacidad de la información.

# CAPITULO II
# MARCO REFERENCIAL

Este capítulo presenta un análisis detallado de los conceptos fundamentales que sustentan la temática de la seguridad y privacidad de la información en el contexto de las instituciones del sector popular y solidario. A lo largo de este capítulo, se aborda la normativa emitida por ente de control de Ecuador SEPS que regulan la gestión de la seguridad de la información en las cooperativas y otras entidades financieras de este sector. Además, se exploran los principios y mejores prácticas para la protección de datos, así como las herramientas tecnológicas necesarias para implementar una cultura de seguridad dentro de estas instituciones. Este marco teórico y normativo servirá de base para el desarrollo de la herramienta web propuesta, que tiene como objetivo evaluar y mejorar los conocimientos de los funcionarios en relación con la seguridad de la información.

## 2.1.Antecedentes

Las instituciones financieras tienen la responsabilidad de proteger la información de sus usuarios, especialmente la relacionada con las cuentas ahorristas, conforme a los lineamientos establecidos por la SEPS. Según las normativas de estas entidades, es imperativo que las instituciones financieras implementen políticas de seguridad para la protección de datos personales y financieros, a fin de evitar vulneraciones de privacidad o fraudes. En este contexto, (Solidaria, 2022),se destaca la importancia de que el personal esté capacitado y sea consciente de las normativas vigentes para cumplir con los estándares requeridos.

Es fundamental evaluar el nivel de conocimiento que el personal tiene sobre estas regulaciones, para garantizar que estén preparados para gestionar la información de manera segura y conforme a los requisitos legales establecidos. Por ello, el objetivo de la presente investigación es diseñar una herramienta web para evaluar esos conocimientos, permitiendo detectar posibles brechas y establecer estrategias de capacitación en seguridad de la información.

### Antecedentes de las Evaluaciones

Diversas investigaciones previas han resaltado la importancia de evaluar el nivel de conocimiento del personal en materia de seguridad de la información. Para ello, distintas instituciones han implementado herramientas y metodologías de evaluación, aunque la mayoría de los sistemas actuales están enfocados en la gestión de información financiera y contable. A nivel nacional, no se han identificado estudios relevantes en este campo; sin embargo, a nivel internacional, se ha documentado una investigación destinada a medir el grado de comprensión y aplicación de las normativas de seguridad.

- EVALUACIÓN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LOS SISTEMAS DE INFORMACIÓN GERENCIAL COMO HERRAMIENTA DE COMPETITIVIDAD EN EMPRESAS DE SERVICIOS DE ENSAYOS NO DESTRUCTIVOS EN LA CIUDAD DE LIMA – PERÚ (Juan J. Lugo Marín, 2020)

**Antecedentes de la Institución en donde se Implementará la Herramienta**

La Cooperativa de Ahorro y Crédito Pilahuin Tio Ltda., nace por la iniciativa de un grupo de jóvenes idealistas del sector indígena de la Sierra Centro - Norte del Ecuador dirigida a atender a todos los sectores, sin discriminación de etnia, condición social o religión. Así nació PILAHUIN TIO Ltda., que significa "Pilar de desarrollo de los pueblos del país". Con este propósito y la obligación de fomentar una ideología de desarrollo personal y democrático comunitario, se oficializó la creación del sistema cooperativo en beneficio de socios, clientes y la comunidad en su conjunto. De esta forma lograron ofrecer oportunidades de ahorro, operaciones de crédito y fuentes de trabajo. Atendiendo a todos los sectores como: el agricultor, campesino, artesano, comerciante y microempresarios.

Es así que, el seis de noviembre del año 2006 se marcó un día histórico y especial para toda la ciudadanía Imbabureña, porque se abrieron las puertas de la Cooperativa de Ahorro y Crédito Pilahuin Tio Ltda., administrada netamente por indígenas kichwa hablantes, para el servicio y atención de los sectores indígenas y rurales de la zona central y norte del país. (Pilahuin Tio, 2020)

Al ser una institución con gran trayectoria y de gran aceptación por miles de socios y clientes, fue seleccionada para la implementación de la herramienta web propuesta, considerando que es parte del sector popular y solidario, además pertenece a las

cooperativas de ahorro y crédito segmento uno, misma que está sujeta a las normativas emitidas por la SEPS.

Sin embargo, existen desafíos relacionados con la capacitación continua del personal en temas de seguridad y privacidad de la información. A través de la evaluación de sus conocimientos, se busca fortalecer la comprensión y aplicar prácticas seguras en el manejo de datos sensibles.

## 2.2.Marco Teórico

### 2.2.1. Seguridad de la información

**Concepto**

La seguridad de la información es la protección de la integridad, disponibilidad y confidencialidad de la información, según el nivel requerido para los objetivos de negocio de la empresa (SEPS S. d., 2022).

**Conceptos generales**

En la seguridad de la información existen tres conceptos principales: la privacidad, la integridad y la disponibilidad, a menudo denominadas la tríada de la seguridad de los datos o la tríada de la protección de la información. Esta triada que ha sido utilizada por más de 20 años, brinda un modelo mediante el cual podemos pensar y discutir conceptos de seguridad, y tiende a centrarse mucho en la seguridad de los datos (Vega Briceño, 2021).

**Tabla 1**
*Tríada de seguridad de la información.*

| Confidencialidad | Integridad | Disponibilidad |
|---|---|---|
| Se refiere a nuestra capacidad de proteger nuestros datos de aquellos que no están autorizados para verlos. | Se refiere a la capacidad de evitar que nuestros datos se modifiquen de manera no autorizada o indeseable. | Se refiere a la capacidad de acceder a nuestros datos cuando los necesitamos. |

**Sistema de Gestión de la seguridad de la información (SGSI)**

Frente a la dependencia de los sistemas de información y al crecimiento de las amenazas existentes, se hace necesario para las organizaciones establecer un Sistema de gestión de Seguridad de la Información, considerando que la seguridad no es un producto, es un proceso; por tanto, la seguridad no puede comprarse, pero puede gestionarse (SEPS S. d., 2022).

**Tabla 2**
*Beneficios Sistema Gestión Seguridad de la Información*

| | |
|---|---|
| Beneficios del SGSI | Mitigación de riesgos debido a la implementación y seguimiento de los controles. |
| | Mitigación de amenazas hasta alcanzar un nivel asumible. |
| | Aseguramiento de la continuidad del negocio. |
| | Cumplimiento de la normativa legal vigente por los entes de control. |
| | Incremento reputación cuando se obtiene la certificación SGSI. |

### 2.2.2. Regulación establecida por la SEPS

Actualmente se establece la "Norma de control respecto a la seguridad de la Información en las entidades del sector financiero popular y solidario bajo el control de la Superintendencia de Economía Popular y Solidaria", la misma que fue aprobada mediante RESOLUCIÓN NO. SEPS-IGS-IGT-IGJ-INGINT-INTICINSESF-INR-DNSI-2022-002 (SEPS S. d., 2022).

Las instituciones serán controladas dependiendo del régimen al que pertenecen y se utilizará los siguientes criterios:

- **Régimen General:** Cooperativas de ahorro y crédito pertenecientes a los segmentos 1 y 2, así como asociaciones mutualistas de ahorro y crédito para vivienda y la CONAFIPS.
    - Aplicaciones informáticas para gestión financiera y sistemas computacionales
    - Transaccionales y de pago
    - Red de cajeros automáticos
    - Generadoras de cartera
    - Administradoras de tarjetas
- **Régimen Especial:** Cooperativas de ahorro y crédito del segmento 3.
    - Transporte de especies monetarias y de valores
    - Cobranzas
- **Régimen Simplificado:** Cooperativas de ahorro y crédito clasificadas en los segmentos 4 y 5.
    - Giro inmobiliario
    - Servicios contables

El presente documento se elaboró con las políticas definidas para el REGIMEN GENERAL, el mismo que establece los siguientes requisitos obligatorios:

Las organizaciones y empresas sujetas a este régimen deberán disponer, como mínimo, de los siguientes elementos:

- Comité de Seguridad de la Información (CSI)
- Normativas, directrices, metodologías, funciones y obligaciones para la administración de la seguridad de la información.
- Distribución de recursos humanos, tecnológicos y financieros destinados a la seguridad de la información.
- Actividades de concienciación y formación en temas concernientes en seguridad de la información.
- Los requisitos establecidos en el Anexo 1 de esta resolución, aplicables al Régimen General.
- Documentación de incidentes de seguridad de la información en la "Bitácora de Eventos de Riesgos", utilizando como referencia la metodología de gestión de riesgos detallada en el Anexo 2.

### 2.2.3. ISO/IEC 27001 Seguridad de la información

La norma ISO/IEC 27001 es un estándar global que establece las exigencias para crear, poner en marcha, conservar y perfeccionar de manera constante un Sistema de Gestión de Seguridad de la Información (SGSI). Su implementación facilita a las entidades la administración sistemática de los riesgos vinculados a la seguridad de la información, asegurando la privacidad, integridad y accesibilidad de los datos. En el escenario ecuatoriano, la aplicación de la ISO/IEC 27001 ha ganado una importancia cada vez mayor, motivada por la digitalización y la exigencia de robustecer la salvaguarda de la información en un ambiente cada vez más interrelacionado y regulado. Este estándar no solo contribuye al cumplimiento de normativas locales e internacionales, sino que también mejora la confianza de clientes y socios estratégicos en la gestión de la seguridad de la información dentro de las organizaciones. (NQA, 2023)

**ISO 27001 en Ecuador:**

La adopción de ISO 27001 en Ecuador se alinea con la necesidad de garantizar la confidencialidad, integridad y disponibilidad de la información, especialmente en sectores como el financiero, gubernamental y de salud. La norma proporciona un marco sólido para la identificación y gestión de riesgos de seguridad de la información, promoviendo buenas prácticas y medidas preventivas. (SEPS, 2021)

**Requisitos de ISO 27001:**

- Contexto Organizacional: La organización debe comprender su contexto y las expectativas de las partes interesadas para establecer un SGSI efectivo (ISO, 2013).
- Liderazgo y Compromiso: El liderazgo de la alta dirección es esencial para establecer la dirección y el compromiso con la seguridad de la información (ISO, 2013).
- Planificación de la Seguridad de la Información: Identificación de riesgos, evaluación de impacto y establecimiento de objetivos de seguridad (ISO, 2013).
- Soporte Organizacional: Recursos, competencia, conciencia y comunicación son esenciales para el funcionamiento efectivo del SGSI (ISO, 2013).
- Operación: Implementación y gestión de controles de seguridad de la información (ISO, 2013).

- Evaluación del Desempeño: Monitoreo, medición, análisis y evaluación para garantizar la mejora continua (ISO, 2013).

**Beneficios en el Contexto Ecuatoriano:**

- Adherencia a normativas: La norma ISO 27001 permite a las organizaciones en Ecuador alinearse con las regulaciones y leyes vigentes en materia de protección de datos.
- Credibilidad ante las partes interesadas: Obtener la certificación ISO 27001 refleja el compromiso de una organización con la protección de la información, fortaleciendo la confianza de clientes y socios comerciales.
- Mitigación de Riesgos: Ecuador, al ser parte de un entorno digital en constante evolución, se beneficia al implementar medidas proactivas para mitigar riesgos de seguridad.

### 2.2.4. Ley de protección de datos

La Ley Orgánica de Protección de Datos Personales (LOPDP) tiene como objetivo garantizar y regular el derecho fundamental de toda persona natural en Ecuador a la protección de sus datos personales. Esta normativa establece los principios, derechos, obligaciones y mecanismos de tutela necesarios para asegurar el adecuado tratamiento de la información personal, otorgando a los ciudadanos el control sobre sus datos y la facultad de acceder, rectificar, actualizar y suprimirlos cuando corresponda. La ley no es aplicable a personas jurídicas, empresas o compañías en lo que respecta a su información corporativa, pero sí impone responsabilidades a las entidades que gestionan datos personales, promoviendo un tratamiento seguro y conforme a estándares internacionales de protección de la privacidad. (Corporación Nacional de Finanzas Populares y Solidarias, 2021)

**Conceptos básicos:**

- **Dato personal:** se refiere a todos los datos que permiten identificar de forma directa o indirecta a un individuo (no empresa), como, por ejemplo: Nombres, Identificación Personal, Teléfono, IP (Cidhpda, 2023).
- **Titular**: es cualquier individuo (no empresa) con información susceptible a tratamiento (Cidhpda, 2023)

- **Tratamiento**: se refiere al empleo de datos de individuos de cualquier manera, ya sea automatizada, semiautomática o no automatizada, que conlleva la recolección, registro, organización, preservación, custodia, adaptación, modificación, supresión, indexación, extracción, consulta, elaboración, uso, propiedad, aprovechamiento, distribución, cesión, comunicación o eliminación de dicha información (Cidhpda, 2023).
- **Consentimiento**: es cuando el propietario (individuo) expresa de manera libre e informada su consentimiento para que sus datos sean gestionados por un responsable (Cidhpda, 2023).

## Ley de Protección de Datos en Instituciones Financieras del Ecuador

La protección de datos en instituciones financieras es una preocupación clave en la actualidad, y en Ecuador, se rige principalmente por la Ley Orgánica de Protección de Datos Personales (LOPD) y su reglamento. La implementación de esta legislación es esencial para garantizar la privacidad y seguridad de la información personal de los clientes. (Corporación Nacional de Finanzas Populares y Solidarias, 2021)

## Ley Orgánica de Protección de Datos en Ecuador

La Ley Orgánica de Protección de Datos Personales (LOPD) en Ecuador, aprobada en 2018, establece los principios, derechos y deberes para el tratamiento de datos personales en todas las instituciones, incluyendo las financieras (Asamblea Nacional del Ecuador, 2018).

## Aspectos de la LOPD

- Consentimiento: La ley destaca la importancia del consentimiento informado como base para el tratamiento de datos personales (Asamblea Nacional del Ecuador, 2018).
- Principios de Tratamiento: Establece principios como la finalidad legítima, proporcionalidad, calidad, transparencia, seguridad, confidencialidad y temporalidad en el tratamiento de datos (Asamblea Nacional del Ecuador, 2018).
- Derechos de los Titulares: Reconoce derechos como el acceso, rectificación, cancelación, oposición, portabilidad y olvido (Asamblea Nacional del Ecuador, 2018).

- Seguridad y Confidencialidad: Instituciones financieras deben implementar medidas de seguridad técnicas y organizativas para proteger la integridad y confidencialidad de los datos personales (Asamblea Nacional del Ecuador, 2018).

**Impacto en las Instituciones Financieras:**

- **Gestión Responsable de Datos:** La LOPD exige que las entidades financieras administren los datos personales de forma responsable, asegurando su privacidad y protección.
- **Reputación y Confianza:** El cumplimiento de la legislación fortalece la reputación de las instituciones financieras, generando confianza entre los clientes y el público en general.
- **Sanciones por Incumplimiento:** La ley establece sanciones por el tratamiento indebido de datos, lo que incentiva a las instituciones financieras a cumplir rigurosamente con las disposiciones legales (Asamblea Nacional del Ecuador, 2018).

## 2.3.Herramientas y métodos tecnológicos

El desarrollo de la aplicación web para evaluar los conocimientos en seguridad y privacidad de la información se basa en el uso de herramientas tecnológicas que cumplen con los requisitos específicos establecidos por la institución en la que se implementará la solución. La elección de estas herramientas responde tanto a las necesidades funcionales del sistema como a los recursos técnicos y capacidades disponibles dentro del entorno institucional. Además, se ha considerado la facilidad de integración, escalabilidad, rendimiento y seguridad que ofrecen las tecnologías seleccionadas, aspectos esenciales para garantizar que la aplicación sea eficiente, robusta y fácil de mantener. La combinación de frameworks como CodeIgniter y sistemas de gestión de bases de datos como MariaDB asegura una implementación óptima y un desarrollo ágil, que cumple con los estándares modernos de desarrollo de software.

### 2.3.1. Codenigter (PHP)

“CodeIgniter es un framework basado en el patrón de arquitectura de software MVC (Model-View-Controller), que organiza la aplicación en tres partes fundamentales. Este enfoque facilita la separación de responsabilidades, lo que contribuye a una estructura más clara y ordenada del código. La implementación de MVC en CodeIgniter mejora la

eficiencia en el desarrollo y mantenimiento de aplicaciones web, permitiendo un desarrollo ágil, modular y fácil de escalar. A continuación, se detallan sus componentes:

- **Controlador**: se ocupa de la lógica de negocio de la aplicación.
- **Vista**: relacionada con la presentación de páginas web al usuario, es decir es la interfaz que visualiza el usuario.
- **Modelo**: se ocupa de modelar los datos (la representación de la información) e acceder a la base de datos." (Bandiera, 2019)

**Figura 1**

*Patrón arquitectura de software MVC*

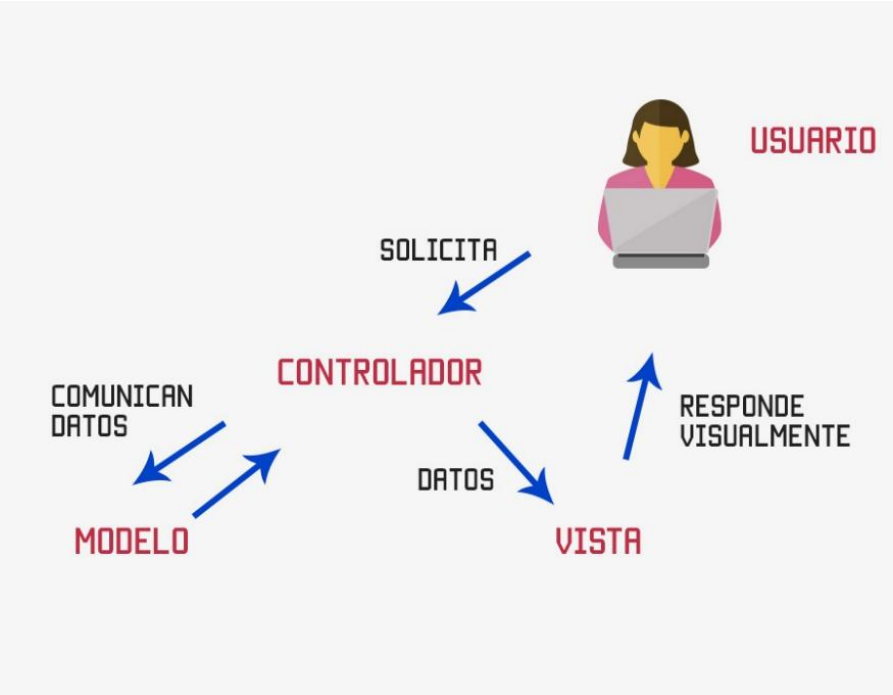
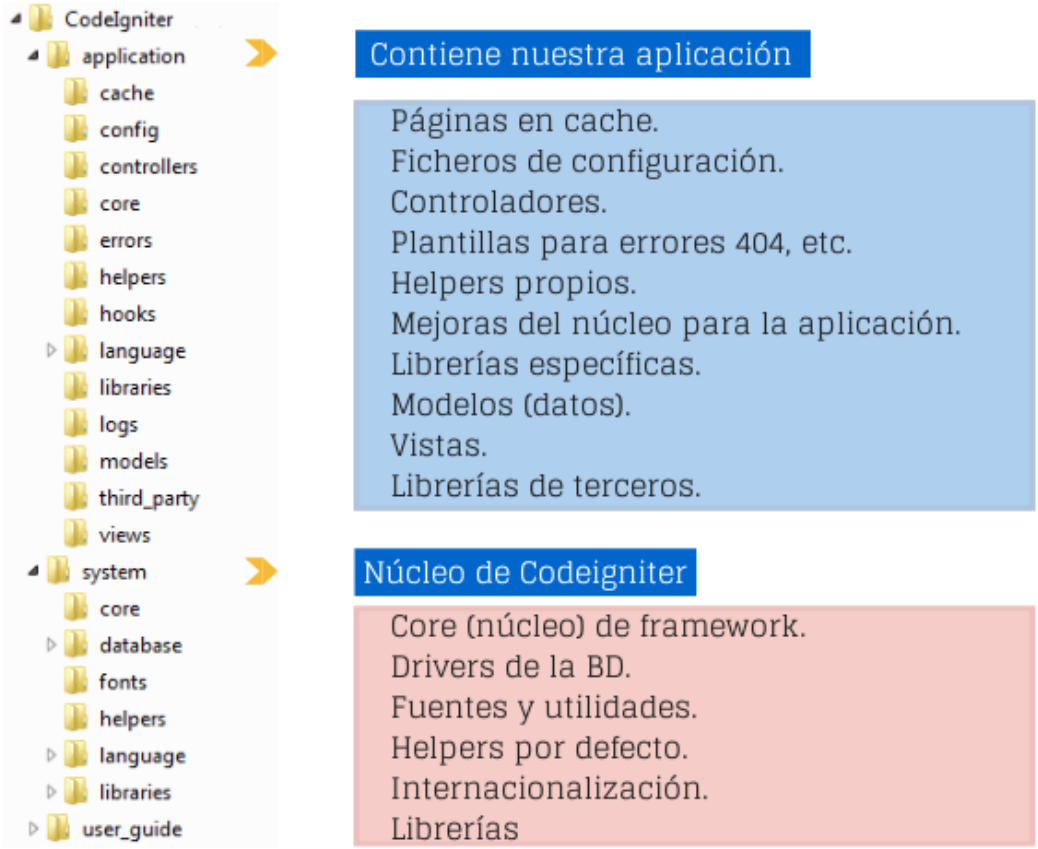


**Figura 2**
*Estructura de carpetas y archivos Codeigniter.*




### 2.3.2. Maria DB

“MariaDB es un motor de base de datos relacional de código abierto que nace a partir de un fork de MySQL.

Esta creado por algunos de los creadores originales de MySQL para asegurar que la comunidad podía seguir disfrutando de un "MySQL" de código abierto. Uno de sus creadores es Michael "Monty" Widenius, uno de los fundadores de MySQL. De hecho, MariaDB tiene el nombre por la hija pequeña de Monty, María.

Mantiene una gran compatibilidad con MySQL. Realmente se puede utilizar en cualquier proyecto para sustituir a MySQL.

Su primer release salió en 2009. Sus primeros números de versión son parejos a los de MySQL. Por ejemplo, MariaDB 5.5 es similar a MySQL 5.5. Después de esa versión algunos cambios implementados en MariaDB hacen que los desarrolladores decidan cambiar el versionado y pase de la versión 5.5 a la 10.0

En la gran mayoría de sistemas Linux actuales es el tipo de base de datos que vienen por defecto cuando quieres instalar una base de datos para proyectos que usen MySQL.” (Urtiaga, (n.d))

### 2.3.3. Metodología de desarrollo

#### 2.3.3.1. Metodología de Desarrollo SCRUM

La metodología SCRUM es una estrategia ágil empleada en el desarrollo de software, que valora la cooperación, la flexibilidad y la entrega gradual de productos. Este modelo organizado simplifica la administración de proyectos complejos, posibilitando que los grupos de trabajo se adapten de forma rápida a las variaciones en las necesidades del usuario. SCRUM se cimenta en principios esenciales como la transparencia, la inspección y la adaptabilidad, utilizando roles concretos, eventos organizados y artefactos que guían el proceso de desarrollo. La Figura 3 muestra una ilustración visual de este método.

**Los roles en SCRUM:**

1. **Product Owner:** Este rol representa los intereses del cliente y es responsable de definir y priorizar los elementos del producto. (Schwaber & Sutherland, 2017)
2. **Scrum Master:** Encargado de facilitar el proceso SCRUM, eliminando obstáculos y asegurando que el equipo siga las prácticas y reglas establecidas. (Schwaber & Sutherland, 2017)
3. **Equipo de Desarrollo:** Un grupo autoorganizado de profesionales que realizan el trabajo real de construcción del producto. (Schwaber & Sutherland, 2017)

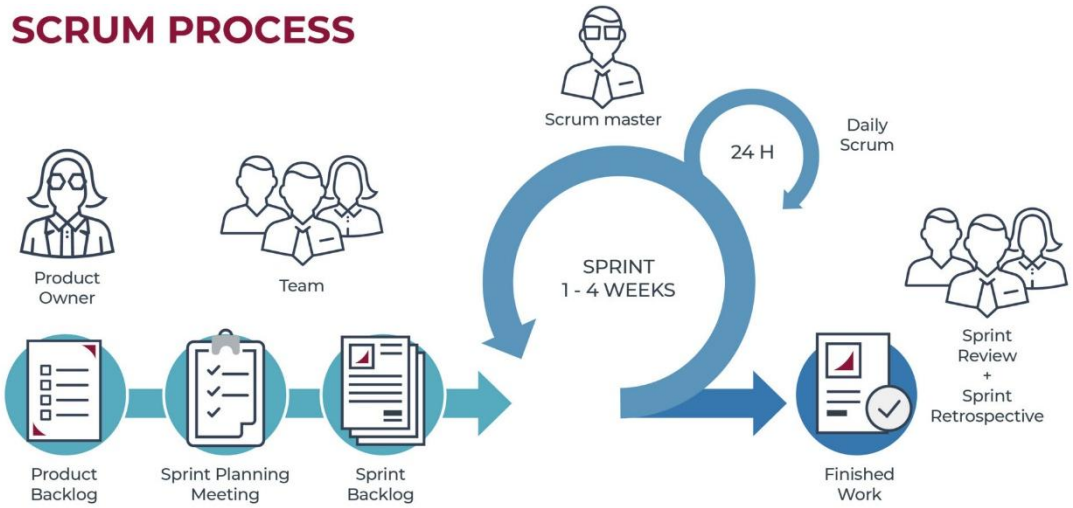
**Eventos en SCRUM:**

1. **Sprint**: Periodo de tiempo fijo (generalmente 2-4 semanas) en el que se desarrolla un incremento potencialmente entregable del producto. (Schwaber & Sutherland, 2017)
2. **Reunión de Planificación del Sprint:** Evento en el que el equipo selecciona elementos del Backlog del Producto que se compromete a entregar al final del Sprint. (Schwaber & Sutherland, 2017)
3. **Revisión del Sprint:** Sesión en la que el equipo presenta el trabajo completado al Product Owner y otros stakeholders, obteniendo retroalimentación (Schwaber & Sutherland, 2017).

**Artefactos en SCRUM:**

1. **Product Backlog**: Lista priorizada de todos los elementos que podrían ser necesarios en el producto, gestionada por el Product Owner (Schwaber & Sutherland, 2017).
2. **Sprint Backlog**: Conjunto de elementos del Product Backlog seleccionados para el Sprint, junto con el plan para entregarlos (Schwaber & Sutherland, 2017).

**Figura 3**
*Proceso Scrum*




## 2.4.Marco legal

A partir del año 2008, La Constitución de Ecuador otorga el derecho a la protección de la información personal. En años recientes, esta protección se ha expandido y regulado con la emisión de la Ley Orgánica de Protección de Datos Personales (LOPDP), emitida el 6 de mayo de 2021. Esta regulación impone responsabilidades que deben ser respetadas tanto por entidades privadas como por organismos e instituciones del sector público para asegurar el correcto manejo y protección de la información personal.

Desde el 26 de mayo de 2023, entran en vigor las disposiciones que establecen la implementación del sistema de sanciones y acciones correctivas si se viola la Ley de Protección de Datos Personales (LOPDP). Este sistema distingue entre infracciones leves y graves, determinando que las faltas leves serán sancionadas con multas que oscilan entre el 0.1% y el 0.7% del volumen de actividad correspondiente al ejercicio económico previo a la imposición de la sanción, según lo estipulado en el Artículo 73 de la LOPDP.

La Ley Orgánica de Protección de Datos personales concede a los ciudadanos los derechos necesarios para garantizar la seguridad de su información personal y demandar que sus datos se guarden con principios de transparencia, confidencialidad y consentimiento, esto apoyado con la Ley de comercio electrónico, firmas y mensajes de datos, que en el Art. 58 textualmente indica “A continuación del artículo 202, inclúyanse los siguientes artículos innumerados (Asamblea Nacional del Ecuador, 2012): "Art. ..- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica. Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica. La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica. Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica. Art. ..- Obtención y utilización no autorizada de información. - La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica”.

**Normativa de la SEPS y su Impacto en el Sector Popular y Solidario**

La SEPS, que regula y supervisa las instituciones del sector financiero popular y solidario en Ecuador, ha establecido una normativa específica que obliga a las entidades del segmento 1 (las más grandes en términos de activos y operaciones) a implementar medidas de seguridad de la información. El propósito de esta regulación es salvaguardar la información delicada de los usuarios y asegurar la estabilidad del sistema financiero solidario.

La SEPS ha sido clara en cuanto a la necesidad de que las instituciones financieras del sector solidario adopten estándares internacionales de seguridad de la información, como la ISO 27001, y cuenten con un Sistema de Gestión de Seguridad de la Información (SGSI) adecuado. El cumplimiento de estas regulaciones es obligatorio y forma parte de los requisitos de supervisión y auditoría de las cooperativas y otras entidades del sector. De no cumplir con las disposiciones de la SEPS, las instituciones pueden enfrentar sanciones, que incluyen desde multas hasta la pérdida de su habilitación para operar.

Además, la SEPS ha orientado sus esfuerzos hacia la protección de datos personales en el ámbito financiero, lo que implica una estrecha vinculación con la Ley Orgánica de Protección de Datos Personales (LOPDP). Las cooperativas de ahorro y crédito, especialmente aquellas pertenecientes al segmento 1, deben implementar prácticas de seguridad que aseguren la confidencialidad y protección de la información de sus socios y clientes, así como alinearse con los principios establecidos por la LOPDP.

# CAPITULO III
# MARCO METODOLÓGICO

La provincia de Imbabura está situada en la región norte de Ecuador y tiene como capital administrativa a la ciudad de Ibarra. La conforman un total de seis cantones, los cuales son: Antonio Ante, Cotacachi, Ibarra, Otavalo, Pimampiro y Urcuquí. Se caracteriza por su diversidad geográfica, que incluye montañas, lagos y valles fértiles, así como por su riqueza cultural, influenciada por comunidades indígenas y mestizas. Además, su economía se sustenta en diversas actividades como la agricultura, el comercio, el turismo y la industria textil, lo que la convierte en una provincia con un importante desarrollo económico y social dentro del país.

**Figura 4**

*Provincia de Imbabura*

El cantón Otavalo, ubicado en la provincia de Imbabura, es nombrado a nivel nacional e internacional por su riqueza y diversidad cultural, así como su tradicional mercado artesanal, considerado uno de los más importantes de América Latina. La principal actividad se basa en el comercio, la artesanía, el turismo y la agricultura, con una fuerte presencia de comunidades indígenas kichwas que han conservado sus costumbres y saberes ancestrales. La ciudad de Otavalo, cabecera cantonal, es un centro económico y comercial clave en la región, con una infraestructura en crecimiento que facilita el desarrollo de diversas actividades productivas y financieras, incluyendo el sector cooperativo. (Ortiz, 2024)

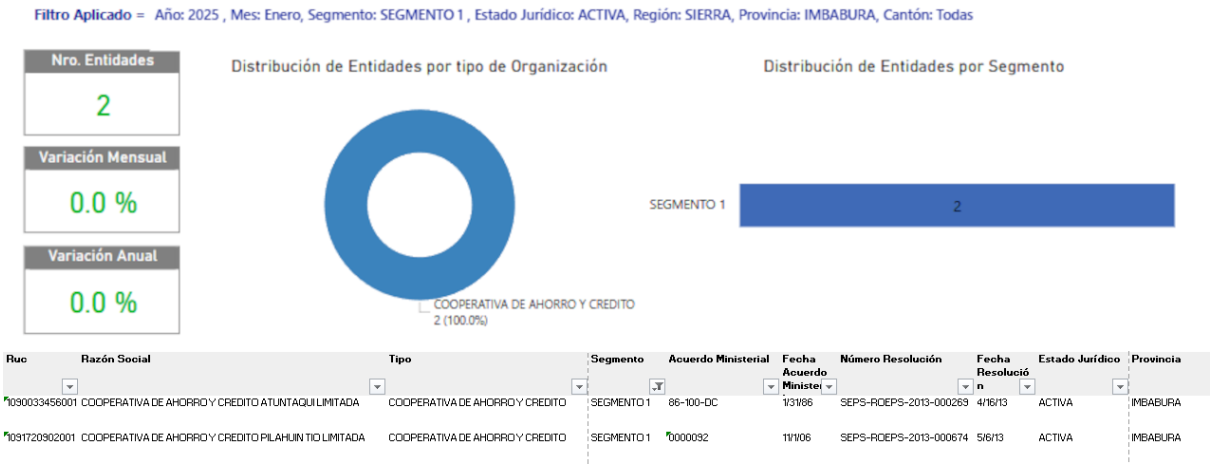
**Figura 5**

Cantones de la provincia de Imbabura


Según el catastro de organizaciones activas publicadas en la página de la Superintendencia de Economía Popular y Solidaria, actualmente en la provincia de Imbabura existen 20 instituciones registradas y avaladas por las SEPS, de las cuales 2 pertenecen al segmento 1 (SEPS S. D., 2023).

**Figura 6**

Catastro SEPS




***Nota.*** Adaptado de Superintendencia de Economía Popular y Solidaria (SEPS). (s.f.). *Plataforma de datos abiertos.* SEPS. https://data.seps.gob.ec/#/dashboards/analytics/0/1

### 3.1.Descripción del área de estudio

De acuerdo con la SEPS, las cooperativas de ahorro y crédito, mutualistas y financieras en Ecuador se dividen en cinco segmentos, del 1 al 5, tomando como criterio el saldo de sus activos. (Superintendencia de Economía Popular y Solidaria, s.f.)

**Tabla 3**

Instituciones activas de Imbabura en el catastro SEPS

| Segmento | Número de Instituciones |
|---|---|
| Segmento 1 | 2 |
| **TOTAL** | **2** |

***Nota.*** Esta tabla muestra las instituciones de segmento 1 en la provincia de Imbabura.

**Tabla 4**

*Cantidad de instituciones segmento 1 por cantón de Imbabura*

| Cantón | Instituciones |
|---|---|
| Atuntaqui | 1 |
| Otavalo | 1 |
| **TOTAL** | **2** |

*Nota.* Cantidad de instituciones que se encuentran por cada cantón de la provincia de Imbabura.

**Tabla 5**

*Talento humano por institución financiera segmento 1*

| Razón Social (Cooperativa de Ahorro y Crédito) | Segmento | Provincia | Cantón | Agencia | Personal Estimado |
|---|---|---|---|---|---|
| COAC ATUNTAQUI LTDA. | UNO | IMBABURA | ATUNTAQUI | 13 | 135 |
| COAC PILAHUIN TIO LTDA. | UNO | IMBABURA | OTAVALO | 13 | 143 |

***Nota.*** Talento Humano por institución financiera y su segmentación.

Dentro del segmento uno, de las cooperativas, se estableció colaboración con la Cooperativa Pilahuin Tio como caso de estudio, en función de su nivel de asociabilidad y el contexto coyuntural. Esta cooperativa fue seleccionada debido a su mayor disponibilidad de talento humano, así como a la accesibilidad del personal tanto en la agencia matriz como en sus sucursales, lo que facilita el desarrollo de la investigación.

**MUESTRA:** La muestra del estudio está conformada por la totalidad del personal que labora en la Cooperativa Pilahuin Tio, perteneciente al segmento uno. Dado que el proyecto involucra el uso de una herramienta web y abarca aspectos relacionados con la Seguridad de la Información, se determinó que todos los empleados de la institución debían participar en el estudio. Esta decisión garantiza una representación completa de la organización y permite evaluar el impacto del proyecto en todas las áreas y niveles de la cooperativa. En total, se trabajará con 143 personas, quienes desempeñan funciones en la agencia matriz y en sus sucursales.

### 3.2.Enfoque y tipo de investigación

Esta investigación se estableció en un enfoque cuantitativo. Según Sampieri (Sampier, 2014), una investigación bajo el enfoque cuantitativo busca escribir, explicar, comprobar y predecir los fenómenos (causalidad), generar y probar teorías. Razón suficiente por la que, se recopilan datos utilizando herramientas estandarizadas y validadas, para evidenciar su fiabilidad; de esta forma, se asigna intencionalmente la información, midiendo con exactitud las variables en estudio.

### CARACTERÍSTICAS DEL ENFOQUE CUANTITATIVO

De acuerdo a Aguilera & Blanco (Aguilera & Blanco, 1987) y Hernández, Fernández, & Baptista (Hernández, Fernández, & & Baptista, 2014) la investigación cuantitativa se distingue por diversas características, entre ellas:

- Enfocarse en alcanzar la objetividad en el estudio.
- El investigador se mantiene distante de los datos recopilados.
- Se prioriza el uso de métodos experimentales aleatorios, cuasi-experimentales y estudios estadísticos.
- Los datos se obtienen a través de instrucciones estandarizados, validados por la comunidad científica.
- Para el análisis de la información, se emplean técnicas estadísticas.
- La formulación del problema de estudio es precisa y bien delimitada, aunque puede ajustarse a lo largo de la investigación.
- Se busca ejercer un control riguroso sobre las variables y los grupos experimentales, con el objetivo de minimizar la incertidumbre y reducir posibles errores.

**VENTAJAS DE LA INVESTIGACIÓN CUANTITATIVA** (Santa Gadea, Gadea, & Vera - Quiñonez, 2018)

Por medio de ella, es posible realizar análisis estadísticos de los resultados, llegando a una respuesta abstractiva del cual se desarrollan discusiones y publicaciones legítimas. En los estudios cuantitativos, si se estructuran adecuadamente, es posible minimizar la influencia de factores externos, lo que permite que los resultados obtenidos sean más objetivos y confiables. Este enfoque es especialmente útil para validar descubrimientos previos en investigaciones cualitativas, facilitando la obtención de conclusiones más sólidas y delimitando el alcance de futuras exploraciones dentro del estudio.
En este escenario, el enfoque de la investigación cuantitativa ofrece beneficios:

- La aplicación de este tipo de técnicas facilita la generalización.
- Es posible obtener datos de un número relativamente amplio de personas.
- Proporciona información numérica o de calificación para la investigación.
- Ofrece datos cuantitativos o de evaluación para la investigación. (Santa Gadea, Gadea, & Vera - Quiñonez, 2018)

Las investigaciones cuantitativas se llevan a cabo principalmente a través de encuestas, las cuales facilitan la obtención organizada de datos a partir de una muestra representativa de una población más extensa. Para ello, se emplea un cuestionario previamente diseñado, compuesto por preguntas estandarizadas que tienen como objetivo analizar la distribución del grupo en función de distintas características. La información recogida podrá emplearse en análisis cuantitativos para identificar y conocer la magnitud de los problemas que se suponen o se conocen en forma parcial; también puede utilizarse para un análisis de correlación para probar hipótesis descriptivas (Rojas, 2013). Se utilizan cuando se busca alcanzar resultados proyectables a un objetivo específico.

Estas técnicas facilitan la respuesta exacta a preguntas como “cuántos”, “quiénes”, “con qué frecuencia”, “dónde”, o “cuándo”, y se enfocan en conseguir acciones y medidas. datos cuantitativos y objetivos de hechos, costumbres, conductas u opiniones.

Los cuestionarios deben ser elaborados con meticulosidad, para evitar preguntas ambiguas o prejuiciadas, que sean de fácil comprensión para cualquier miembro de la muestra, y que incluyan todos los propósitos de la investigación, con el objetivo de facilitar su cuantificación y tratamiento estadístico.

Los enfoques de investigación cuantitativa, como las encuestas, tienen como objetivo medir y clasificar distintos fenómenos, además de analizar su magnitud. Asimismo, permiten extrapolar los resultados a una población más amplia a partir del estudio de una muestra representativa, tomando en cuenta márgenes de error y niveles de confianza previamente establecidos.

Tomando como referencia estos conceptos se ha definido que la mejor técnica para el presente proyecto es la utilización de las ENCUESTAS.

### 3.3.Procedimiento de investigación

Para la presente investigación el procedimiento se llevó a cabo mediante tres fases:

**FASE 1:** Diagnosticar los conocimientos de los funcionarios de la Cooperativa PILAHUIN TIO, acerca de la seguridad de la información basándose en la normativa de la seguridad de la SEPS.

Para lo cual, se aplicará la técnica de encuesta tipo cuestionario con información inherente de la institución del caso de estudio y basado en la normativa de la seguridad de la SEPS. (Tamayo y Tamayo, EL PROCESO DE LA INVESTIGACIÓN CIENTÍFICA, 2003), destacan que la encuesta "es aquella que permite dar respuestas a problemas en términos descriptivos como de relación de variables, tras la recogida sistemática de información según un diseño previamente establecido que asegure el rigor de la información obtenida". Y el cuestionario según Tamayo y Tamayo (Tamayo y Tamayo, EL PROCESO DE LA INVESTIGACIÓN CIENTÍFICA, 2008), señala que "el cuestionario contiene los aspectos del fenómeno que se consideran esenciales; permite, además, aislar ciertos problemas que nos interesan principalmente; reduce la realidad a cierto número de datos esenciales y precisa el objeto de estudio".

Por lo que el cuestionario se aplicó al personal de la entidad financiera para evaluar el conocimiento de seguridad de la información y protección de datos, para lo cual se realizó mediante el uso de herramientas informáticas, posterior a la recogida de información se realizó la tabulación respectiva, al ser una encuesta online se facilitó el procesamiento de datos y la visualización de resultados.

**FASE 2:** Implementar una herramienta web que permite tener acceso a capacitación interactiva acerca de la seguridad y privacidad de la información, para lo cual se

desarrolló una aplicación web la cual automatiza de una manera didáctica las características y conceptos que se manejan en seguridad de la información y protección de datos personales, además de términos principales establecidos en la normativa de la SEPS, posterior la herramienta permite realizar la evaluación de los conocimientos adquiridos y emite un certificado si cumple con el puntaje mínimo establecido para las calificaciones, el mismo que se enfocó en todo el personal de la cooperativa Pilahuin Tío, perteneciente al sector popular y solidario dentro del segmento uno en la Provincia de Imbabura.

**FASE 3:** Se evalúa la mejora en los conocimientos adquiridos por el personal de la Cooperativa Pilahuin Tio a través del uso de la aplicación web. Como parte del proceso de evaluación, el aplicativo genera un certificado de conocimiento, el cual sirve como evidencia del cumplimiento de la normativa establecida por la SEPS. Esta normativa hace referencia a la ISO 27001, con un enfoque específico en los principios de liderazgo y compromiso que la norma establece en materia de Seguridad de la Información.

### 3.4.Consideraciones bioéticas

Para efectuar el trabajo de investigación se realizó un consentimiento informado a las autoridades pertinentes de la institución, adicional se suscribieron los respectivos acuerdos de confidencialidad y protección de datos con el fin de que la institución pueda ser evaluada de manera integral y sin temor de repercusiones por parte de los empleadores, sino más bien que se tome como una herramienta para generar conciencia y pueda ayudar en la mejora del manejo de la seguridad y privacidad de la información que manejan en cada uno de sus puestos laborales y sean tomados como referentes siendo las Instituciones que gestionan la Seguridad y Privacidad de la información de los clientes de la provincia de Imbabura.

# CAPITULO IV
# RESULTADOS Y DISCUSIÓN

En el estudio se analizaron los datos recopilados de 143 personas, las mismas que laboran la COOPERATIVA DE AHORRO Y CRÉDITO PILAHUIN TIO perteneciente al sector popular y solidario dentro del segmento uno de la provincia de Imbabura, con el fin de evaluar los conocimientos del personal respecto a la Norma de Cumplimiento establecido por la SEPS.

## 4.1 Diagnóstico de conocimientos sobre Seguridad de la Información basada en la Normativa establecida por la SEPS

Se realizará un diagnóstico sobre el nivel de conocimientos de los funcionarios de la Cooperativa Pilahuin Tio LTDA., en materia de seguridad y privacidad de la información, basándose en la normativa y principios establecidos por el ente de control denominado SEPS. La importancia de este diagnóstico radica en la necesidad de medir la conciencia y la comprensión de las normativas de seguridad de la información por parte del personal, en particular las regulaciones que afectan al sector financiero del segmento 1.

Para lograr este diagnóstico, se empleó la técnica de encuesta tipo cuestionario, que se diseñará específicamente para evaluar los conocimientos relacionados con los principios de seguridad de la información y la protección de datos personales, según la normativa establecida por la SEPS. La encuesta estará compuesta por preguntas clave relacionadas con los siguientes temas:

- Conceptos Básicos de Seguridad de la Información
- Protección de Datos Personales
- Seguridad en la Nube
- Cumplimiento Normativo y Legislación
- Buenas Prácticas de Seguridad

Cada sección del cuestionario está alineada con los temas clave de la normativa de la SEPS, permitiendo evaluar el grado de conocimiento de los empleados sobre los principios fundamentales de seguridad y privacidad de la información. La encuesta fue revisada y validada por un experto en Seguridad de la Información, garantizando su coherencia y pertinencia con los objetivos del estudio. En los anexos se adjunta el cuestionario junto con el instrumento de validación correspondiente.

Los resultados obtenidos en este diagnóstico servirán como una línea base que permitirá medir el nivel inicial de conocimiento de los empleados antes del uso de la herramienta de capacitación interactiva. Esta evaluación preliminar permitirá identificar con precisión las áreas que necesitan ser reforzadas, y una vez implementada la herramienta de capacitación, los resultados se compararán para evaluar el progreso y la mejora en los conocimientos del personal. De este modo, se podrá cuantificar el impacto de la herramienta en la mejora del conocimiento y conciencia en torno a las normativas de seguridad de la información, lo que contribuirá a un entorno más seguro y conforme a la normativa de la SEPS.

### 4.1.1 Descripción de la Encuesta

Para el presente proyecto se estableció la siguiente encuesta web, la misma que abarca los dos ejes principales como son Seguridad de la Información y Protección de datos personales y fue aplicada a los funcionarios que laboran para la cooperativa Pilahuin Tio, institución que fue establecida para el muestreo de nuestro estudio.

**Encuesta de Evaluación de Conocimientos en Seguridad de la Información y Protección de Datos**

Instrucciones: Marque la respuesta que considere correcta.

**a) Tema 1: Conceptos Básicos de Seguridad de la Información**

1. ¿Qué significa el término "ciberseguridad"?
    a. La protección física de los datos en una empresa.
    b. ✓ La protección de los sistemas informáticos contra amenazas cibernéticas.
    c. El almacenamiento seguro de información en la nube.
    d. La protección contra incendios en centros de datos
    e. Desconozco el tema.
2. ¿Qué es un "ataque de fuerza bruta" en el contexto de la seguridad informática?
    a. Un ataque que utiliza la ingeniería social para engañar a los usuarios.
    b. ✓ Un ataque que intenta adivinar contraseñas probando todas las combinaciones posibles.
    c. Un ataque que utiliza software malicioso para robar información.
    d. Un ataque que busca sobrecargar un servidor con tráfico malicioso.

e. Desconozco el tema.

3. ¿Cuál de las siguientes opciones describe el concepto de "phishing"?
    a. Un intento de bloquear el acceso a un sitio web.
    b. ✓ Un ataque que intenta engañar a las personas para que revelen información confidencial.
    c. Un método para proteger correos electrónicos contra el spam.
    d. Una práctica para enviar mensajes publicitarios no deseados.
    e. Desconozco el tema.
4. ¿Qué es un "antivirus" y cuál es su función principal?
    a. Un programa para crear contraseñas seguras.
    b. ✓ Una herramienta para proteger contra virus y malware.
    c. Un sistema de autenticación de dos factores.
    d. Una plataforma para almacenar datos en la nube.
    e. Desconozco el tema.

**b) Tema 2: Protección de Datos Personales**

5. ¿Qué es la "Ley Orgánica de Protección de Datos Personales" en Ecuador y cuál es su propósito?
    a. Una legislación que regula el uso de dispositivos electrónicos personales.
    b. ✓ Una regulación que protege los datos personales y garantiza los derechos de privacidad de las personas.
    c. Un conjunto de pautas para proteger la propiedad intelectual en línea.
    d. Un protocolo para el manejo seguro de información financiera en instituciones bancarias.
    e. Desconozco el tema.
6. ¿Qué se considera un dato confidencial en el contexto de la protección de datos personales?
    a. ✓ Información que puede identificar directa o indirectamente a una persona.
    b. Datos que están disponibles públicamente en internet.
    c. Documentos impresos almacenados en una oficina.
    d. Información sobre productos o servicios de una empresa.
    e. Desconozco el tema.

**c) Tema 3: Seguridad en la Nube**

7. ¿Qué es la "autenticación multifactor" y por qué es importante en la seguridad de la información en la nube?
    a. Un método para proteger las contraseñas de las cuentas de usuario.
    b. ✓ Un proceso que requiere múltiples formas de verificación de identidad para acceder a una cuenta.
    c. Una técnica para cifrar datos almacenados en la nube.
    d. Un estándar de seguridad para proteger servidores de bases de datos.
    e. Desconozco el tema.
8. ¿Cuál de las siguientes afirmaciones describe el concepto de "privacidad de la información" en la nube?
    a. El control total de los datos por parte del proveedor de servicios en la nube.
    b. ✓ La protección de los datos contra el acceso no autorizado y su uso indebido.
    c. La capacidad de acceder a los datos desde cualquier ubicación sin restricciones.
    d. La práctica de compartir datos personales en redes sociales sin restricciones.
    e. Desconozco el tema.

**d) Tema 4: Cumplimiento Normativo y Legislación**

9. ¿Qué es un registro de actividades de tratamiento de datos personales?
    a. ✓ Un documento donde se registra y documenta el procesamiento de datos personales, incluyendo detalles como quién accede a los datos, cuándo y con qué propósito.
    b. Una herramienta para cifrar datos sensibles almacenados en servidores.
    c. Un protocolo para la destrucción segura de datos obsoletos.
    d. Una política para el uso adecuado de contraseñas en una organización.
    e. Desconozco el tema.
10. ¿Qué significa el término "cumplimiento normativo" en el contexto de la seguridad de la información?
    a. ✓ El cumplimiento de las leyes y regulaciones relacionadas con la protección de datos.

b. La implementación de medidas de seguridad para proteger la información confidencial.
c. La capacidad de una empresa para recuperarse de un incidente de seguridad.
d. La protección de los datos contra el acceso no autorizado y su uso indebido.
e. Desconozco el tema.

**e) Tema 5: Buenas Prácticas de Seguridad**

11. ¿Cuál de las siguientes acciones ayuda a proteger la privacidad de los datos personales?
    a. Compartir datos personales en redes sociales.
    b. Almacenar contraseñas en un archivo de texto sin cifrar.
    c. ✓ Utilizar conexiones seguras (HTTPS) al enviar información confidencial.
    d. Compartir información personal con desconocidos.
    e. Desconozco el tema.
12. ¿Qué es una "cookie" en el contexto de la seguridad de la información en línea?
    a. Un tipo de virus informático.
    b. ✓ Un archivo que almacena información sobre la actividad del usuario en un sitio web.
    c. Una técnica para cifrar mensajes de correo electrónico.
    d. Un software para proteger la privacidad en línea.
    e. Desconozco el tema.
13. ¿Qué es un "ataque de ingeniería social"?
    a. Un ataque que utiliza la fuerza bruta para acceder a contraseñas.
    b. ✓ Un ataque que intenta engañar a las personas para que revelen información confidencial.
    c. Un ataque que utiliza malware para robar datos.
    d. Un ataque que utiliza redes sociales para difundir spam.
    e. Desconozco el tema.
14. ¿Qué es la seguridad de la red?
    a. Un programa de ejercicios físicos en el lugar de trabajo.

b. ✓ Un conjunto de medidas para proteger los datos y los sistemas informáticos contra amenazas cibernéticas.
c. Un método para protegerse contra incendios en el lugar de trabajo.
d. Un protocolo para enviar correos electrónicos cifrados.
e. Desconozco el tema.

15. ¿Por qué es importante mantener el software actualizado en un dispositivo?
    a. Para reducir el espacio de almacenamiento.
    b. Para mejorar el rendimiento del dispositivo.
    c. ✓ Para corregir vulnerabilidades de seguridad.
    d. Para aumentar la velocidad de conexión a internet.
    e. Desconozco el tema.
16. ¿Cuál es una medida para proteger una contraseña?
    a. Compartirla con amigos y familiares.
    b. Utilizar la misma contraseña para múltiples cuentas.
    c. Mantenerla en un archivo de texto en el escritorio.
    d. ✓ Crear una contraseña única y compleja.
    e. Desconozco el tema.
17. ¿Por qué es importante no hacer clic en enlaces sospechosos en correos electrónicos?
    a. ✓ Porque pueden contener virus o malware.
    b. Para aumentar el tráfico en el sitio web.
    c. Porque pueden proporcionar acceso a descuentos exclusivos.
    d. Para mejorar la seguridad de la cuenta de correo electrónico.
    e. Desconozco el tema.
18. ¿Cuál de las siguientes acciones pone en riesgo la privacidad de los datos personales?
    a. ✓ Compartir datos personales en redes sociales.
    b. Utilizar conexiones seguras (HTTPS) al enviar información confidencial.
    c. Proteger el acceso a cuentas con autenticación multifactor.
    d. Usar una VPN para conexiones en redes públicas.
    e. Desconozco el tema.

### 4.1.2 Resultado de la evaluación diagnóstica

En esta etapa del diagnóstico, se evaluó el nivel de conocimientos de los funcionarios de la Cooperativa Pilahuin Tio LTDA. sobre los principios de seguridad de la información y la protección de datos personales, basados en la normativa establecida por ente de control de las Economías Populares y Solidarias de Ecuador (SEPS).

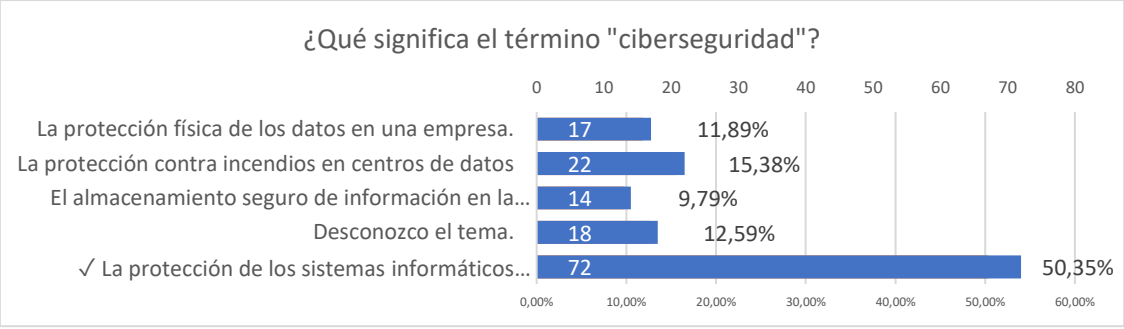
Todo resultado obtenido de la encuesta permite identificar las áreas en las que los funcionarios poseen un conocimiento adecuado y aquellas en las que se requieren mejoras significativas. Estos resultados constituyen la línea base para evaluar la efectividad de la herramienta de capacitación web que se implementará en la siguiente fase, la cual tiene como objetivo mejorar los conocimientos de los empleados en los aspectos más deficientes.

De esta manera, se pudo medir el impacto de la herramienta web, comparando el nivel de conocimientos antes y después de su uso, permitiendo así un análisis detallado sobre las mejoras alcanzadas en materia de la seguridad de la información dentro de la cooperativa.

#### 4.1.2.1 Tema: Conceptos básicos de la seguridad de la información

En la pregunta uno referente a ¿Qué significa el término "ciberseguridad"?, se puede evidenciar que el 50.35% del personal está familiarizado con el concepto, mientras que el 49.65% no asocia correctamente, por lo que el índice de desconocimiento es alto dentro de la institución, considerando que la SEPS establece que todo el personal o en su mayoría debe estar familiarizado respecto a la Seguridad de la Información y Protección de Datos.

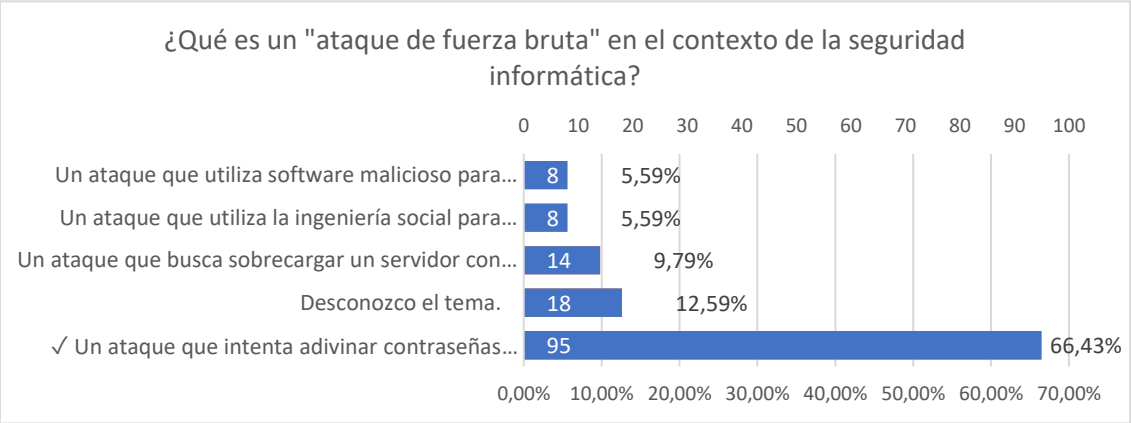
**Figura 7**
*Resultados encuesta - Pregunta 1*



En la pregunta dos referentes a ¿Qué es un "ataque de fuerza bruta" en el contexto de la seguridad informática?, se puede evidenciar que el 66.43% del personal conoce o ha escuchado del tema, mientras que el 33.57% no asocia correctamente, pero dentro de este porcentaje el 12.59% desconoce totalmente del tema.

**Figura 8**

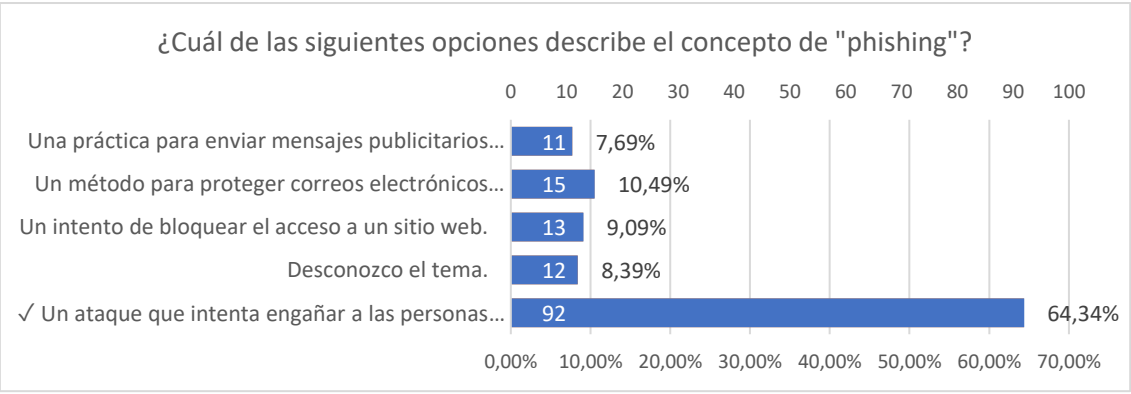
*Resultados encuesta - Pregunta 2*




En la pregunta tres referentes a ¿Cuál de las siguientes opciones describe el concepto de "phishing"?, se puede evidenciar que el 64.34% del personal conoce acerca del phishing, mientras que el 35.66% desconoce el tema, en teoría es un porcentaje alto de conocimiento, pero al ser un tema de gran importancia se considera que, si tan solo una persona cae en este tipo de ingeniería social, puede hacer que se afecte toda la institución al dejar expuesta la información y dejar abierta una puerta de entrada a ciberdelincuentes.

**Figura 9**

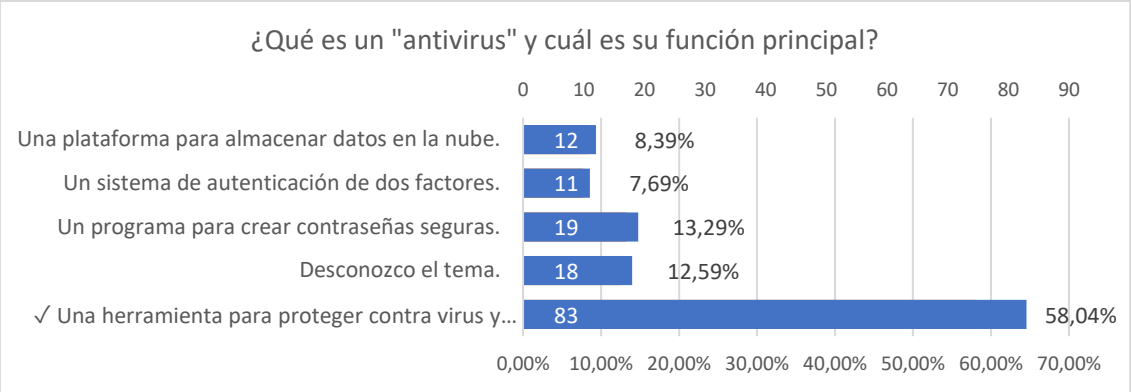
*Resultados encuesta - Pregunta 3*




En la pregunta cuatro referentes a ¿Qué es un "antivirus" y cuál es su función principal?, se puede evidenciar que el 58.04% del personal está familiarizado con el

concepto, mientras que el 41.96% desconoce del tema, como es de conocimiento el manejo de conceptos y conocimiento de antivirus es fundamental para evitar intrusiones, perdidas de información o ataques maliciosos, por lo que también el índice de desconocimiento es representativo y puede causar afectaciones a nivel institucional.

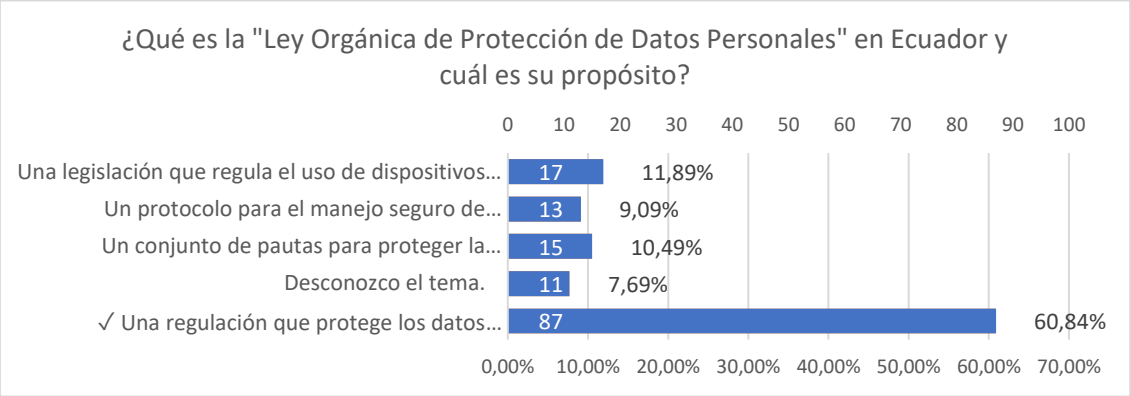
**Figura 10**
*Resultados encuesta - Pregunta 4*




### 4.1.2.2 Tema: Protección de Datos Personales

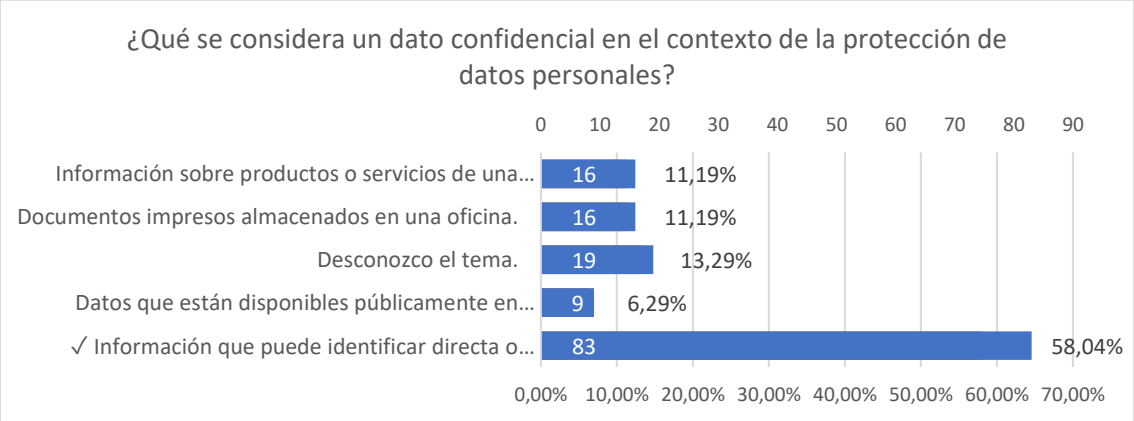
En la pregunta cinco referente a ¿Qué es la "Ley Orgánica de Protección de Datos Personales" en Ecuador y cuál es su propósito?, se puede evidenciar que el 60.84% del personal conoce del tema, mientras que el 39.16% tiene desconocimiento, pese a que la Ley ha sido difundida en la institución y por los diferentes medios de comunicación apenas se promulgo la misma al ser de interés social, además bajo la política que establece la SEPS en su Resolución No. SEPSIGT-IGPJISTI-2015-10 (05 de marzo de 2015) Art. 1.- “Son objetivos de la SEPS en cuanto a Seguridad de la Información: a) Minimizar los riesgos mediante la prevención de los incidentes de seguridad, reducir su potencial impacto. b) Adoptar controles dentro de la Institución, para que la información esté protegida contra: divulgación a usuarios no autorizados (confidencialidad) modificación inadecuada (integridad) y su falta de acceso cuando se la necesita (disponibilidad)”, por lo que es relevante que todo el personal esté capacitado y tenga conocimientos del tema.

**Figura 11**
*Resultados encuesta - Pregunta 5*




En la pregunta seis, referente a ¿Qué se considera un dato confidencial en el hilo de la protección de datos personales?, se puede evidenciar que el 58.04% del personal tiene claros los conceptos de protección de datos, mientras que el 41.96% desconoce del tema o lo asocia de manera incorrecta, con el antecedente expuesto en la pregunta cinco, es obligatorio que el todo personal conozca y maneje los términos relacionados a la protección de datos.

**Figura 12**
*Resultados encuesta - Pregunta 6*

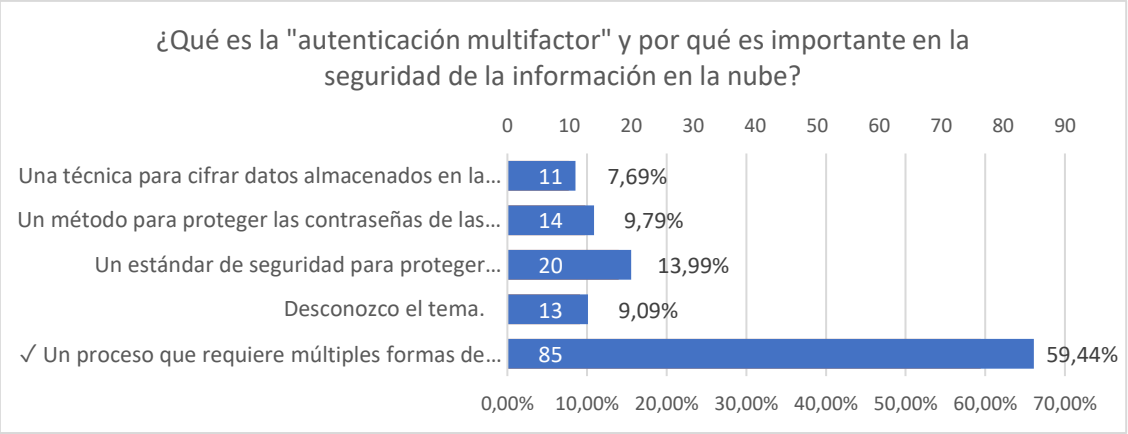



### 4.1.2.3 Tema: Seguridad en la Nube

En la pregunta siete referente a ¿Qué es la "autenticación multifactor" y por qué es transcendental en la seguridad de la información en la nube?, se puede evidenciar que el 59.44% del personal conoce los términos relacionados a seguridad de la información, mientras que el 40.56% no asocia los conceptos correctamente, por lo que es importante

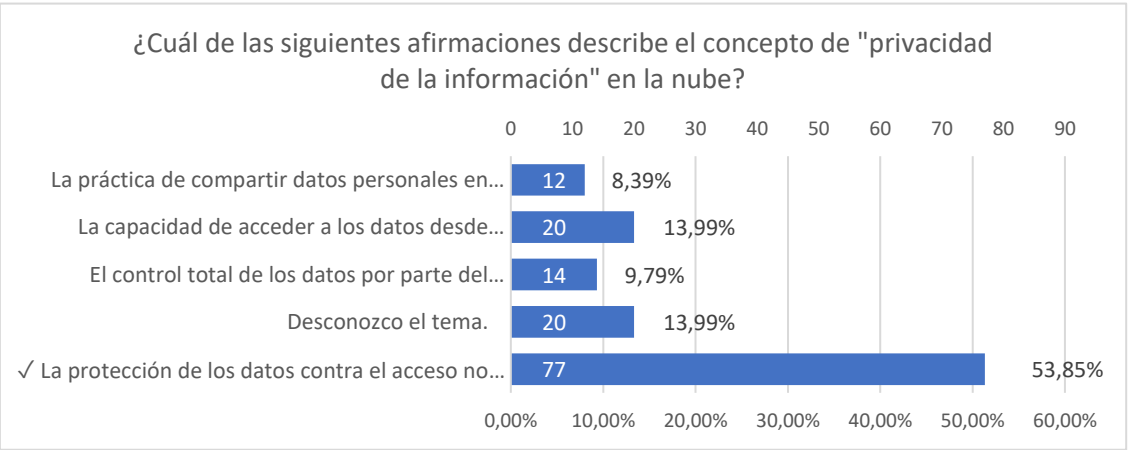
se realice una capacitación para que todo el personal tenga el conocimiento que rige las políticas establecidas por la SEPS.

**Figura 13**
*Resultados encuesta - Pregunta 7*




En la pregunta ocho referente a ¿Cuál de las siguientes afirmaciones describe el concepto de "privacidad de la información" en la nube?, se puede evidenciar que el 53.85% tiene conocimiento de privacidad de la información y sus conceptos, mientras que el 46.15% no tiene conocimientos del tema, en este caso al ser una pregunta solamente de conocimiento no afectaría el desconocimiento a nivel operativo en la institución, más bien la afectación es a nivel reputacional por incumplimiento de la Normativa

**Figura 14**
*Resultados encuesta - Pregunta 8*

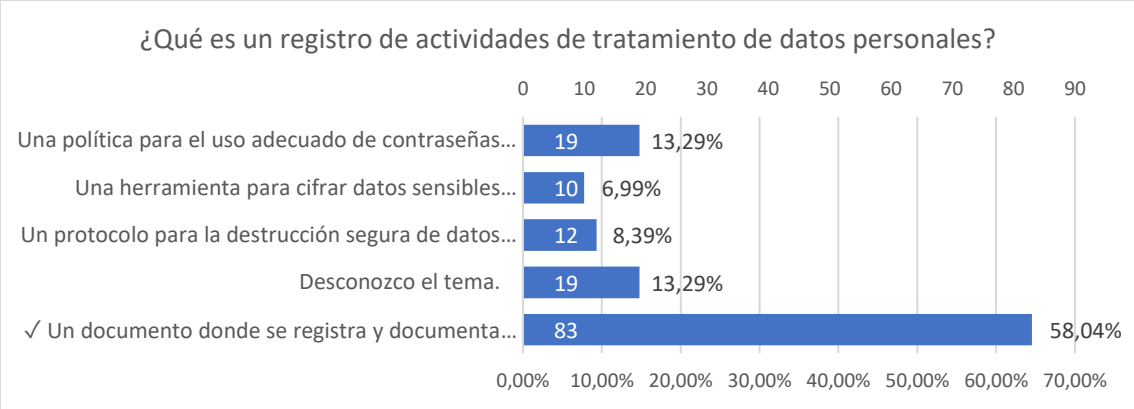



### 4.1.2.4 Tema: Cumplimiento Normativo y Legislación

En la pregunta nueve, referente a ¿Qué es un registro de actividades de tratamiento de datos personales?, se puede evidenciar que el 58.04% conoce el tratamiento de datos

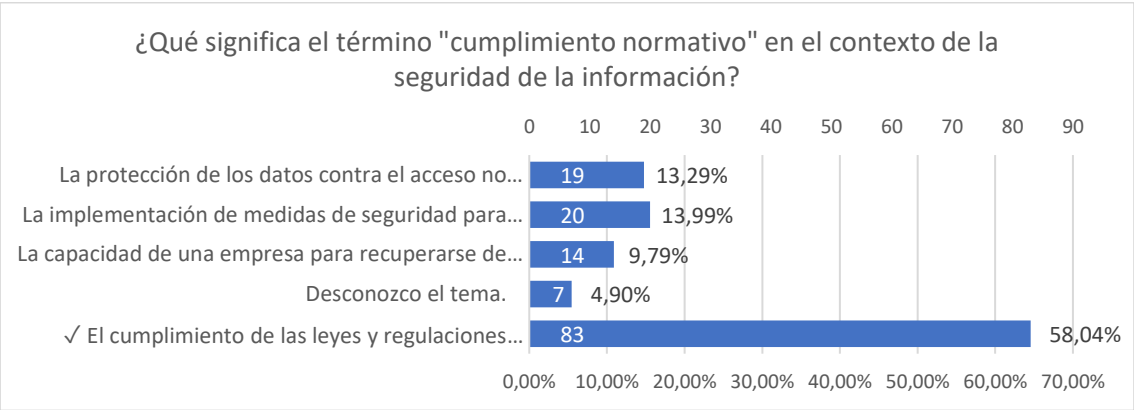
personales, mientras que el 41.96% desconocen el tema lo que puede ocasionar que por mal manejo de la información relativa a los datos personales se genere una sanción a la institución, por parte del organismo de control.

**Figura 15**
*Resultados encuesta - Pregunta 9*




En la pregunta diez ¿Qué significa el término "cumplimiento normativo" en el tema de la seguridad de la información?, se puede evidenciar que el 58.04% del personal conoce de normativa, por lo que está familiarizado con los procesos relacionados a seguridad de la información, a la vez aporta con el valor agregado a la institución al cumplir con las Normas establecidas, mientras que el 41.96% no tiene el conocimiento suficiente.

**Figura 16**
*Resultados encuesta - Pregunta 10*

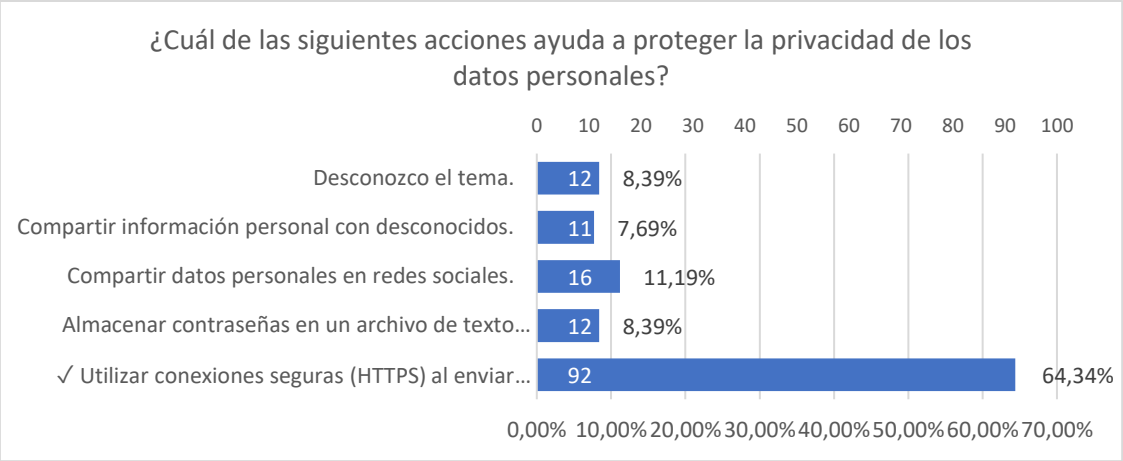



### 4.1.2.5 Tema: Buenas Prácticas de Seguridad

En la pregunta once, referente a ¿Cuál de las siguientes acciones ayuda a proteger la privacidad de los datos personales?, se puede evidenciar que el 64.34% del personal

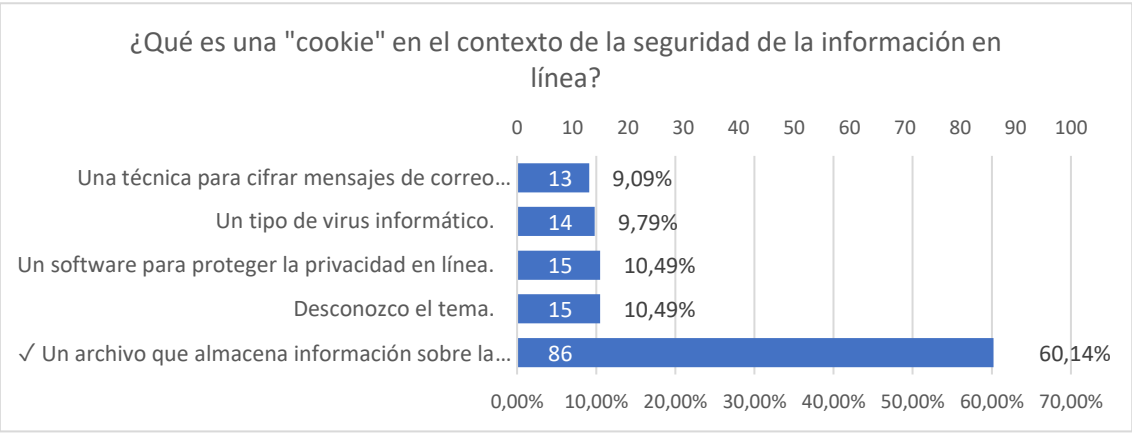
asocia correctamente los términos relacionados a datos personales, mientras que el 35.66% desconocen completamente del tema, considerando las opciones que se presentan en las respuestas se puede validar que el personal que se encuentra dentro de este porcentaje es fácilmente vulnerable.

**Figura 17**
*Resultados encuesta - Pregunta 11*




En la pregunta doce, referente a ¿Qué es una "cookie" en el hilo de la seguridad de la información en línea?, se puede evidenciar que el 60.14% del personal está familiarizado con el concepto, mientras que el 39.86% desconoce del tema, al ser un concepto de conocimiento general no tiene implicación o afectación en la Institución.

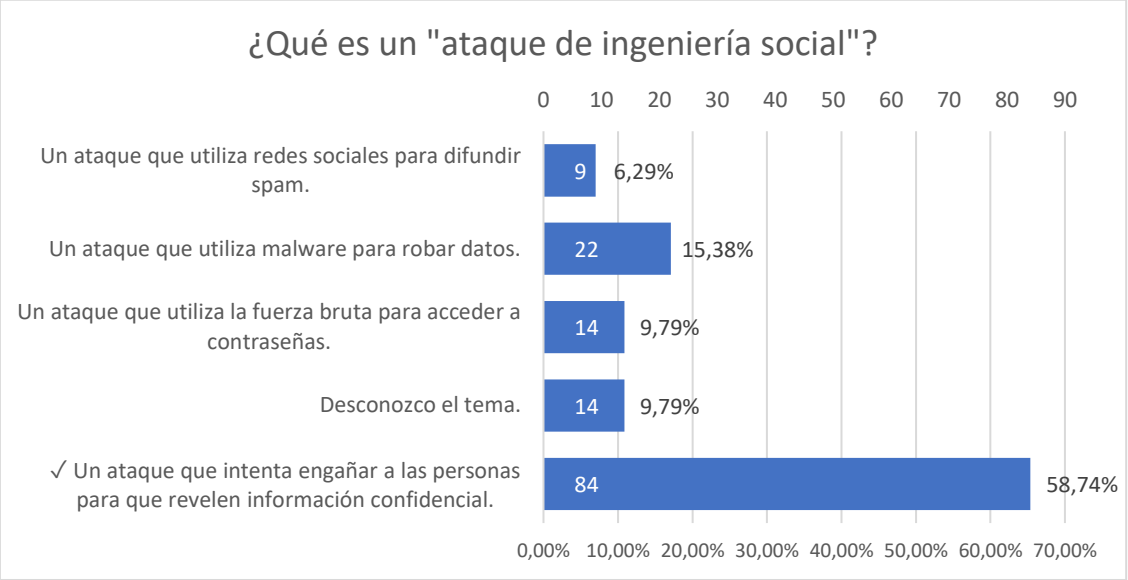
**Figura 18**
*Resultados encuesta - Pregunta 12*




En la pregunta trece, referente a ¿Qué es un "ataque de ingeniería social"?, se puede evidenciar que el 58.74% del personal está capacitado en los temas relacionados a seguridad de la información, mientras que el 41.96% desconoce del tema, siendo esta

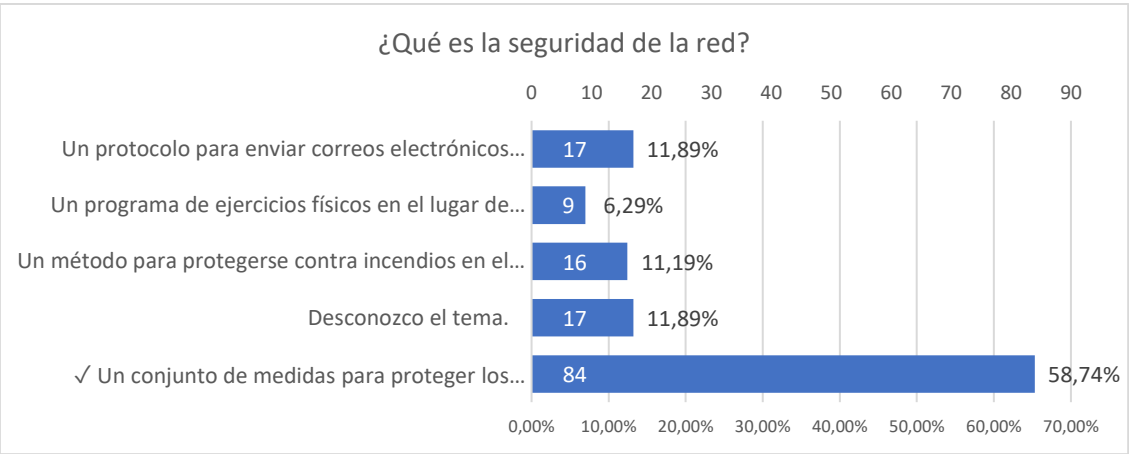
población la más vulnerable y que puede caer en este tipo de técnicas que utilizan los ciberdelincuentes, provocando así un impacto significativo en la disponibilidad y confidencialidad de la información que maneja la institución.

**Figura 19**
*Resultados encuesta - Pregunta 13*




En la pregunta catorce, referente a ¿Qué es la seguridad de la red?, se puede evidenciar que el 58.74% del personal está familiarizado con el concepto, mientras que el 41.26% no asocia correctamente, por lo que el índice de desconocimiento es alto dentro de la institución, considerando que la SEPS establece que todo el personal o en su mayoría debe estar familiarizado respecto a la Seguridad de la Información y Protección de Datos.

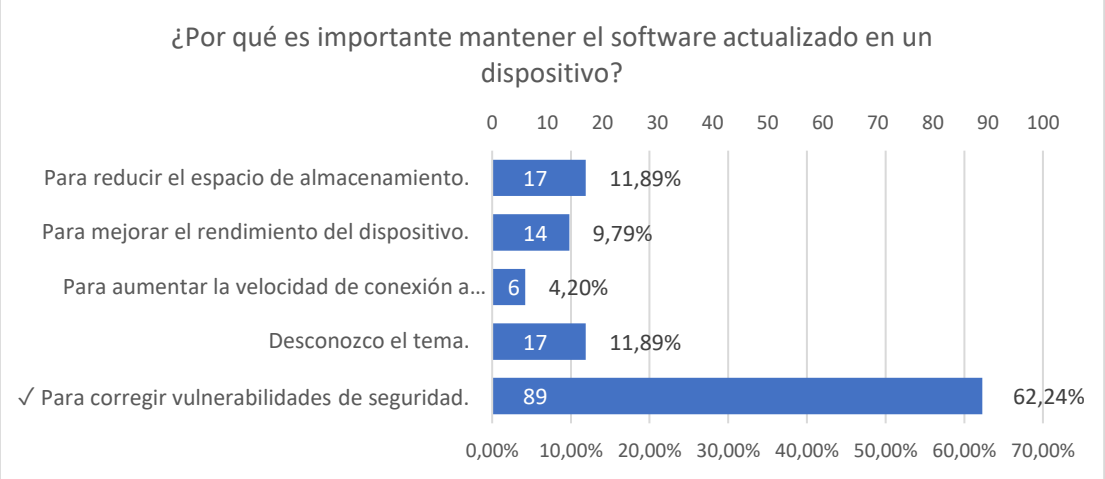
**Figura 20**
*Resultados encuesta - Pregunta 14*



En la pregunta 15, referente a "¿Por qué es importante mantener el software actualizado en un dispositivo?", se evidencia que el 62.24% del personal reconoce que la actualización del software es clave para corregir vulnerabilidades de seguridad. Sin embargo, un 37.76% asocia las actualizaciones con otros factores como el rendimiento del dispositivo (11.89%), la velocidad de conexión a internet (9.79%) o el espacio de almacenamiento (4.20%), e incluso un 11.89% desconoce la importancia de este proceso. Esto sugiere que, aunque la mayoría comprende la relación entre actualizaciones y seguridad, existe una brecha de conocimiento que podría abordarse con capacitaciones enfocadas en la mitigación de riesgos y la protección de la información.

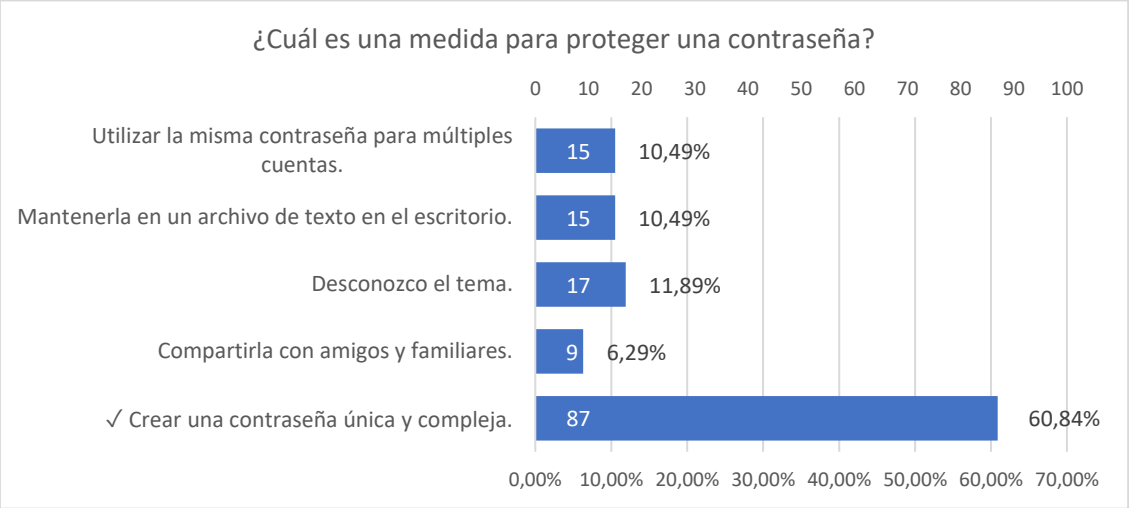
**Figura 21**

*Resultados encuesta - Pregunta 15*



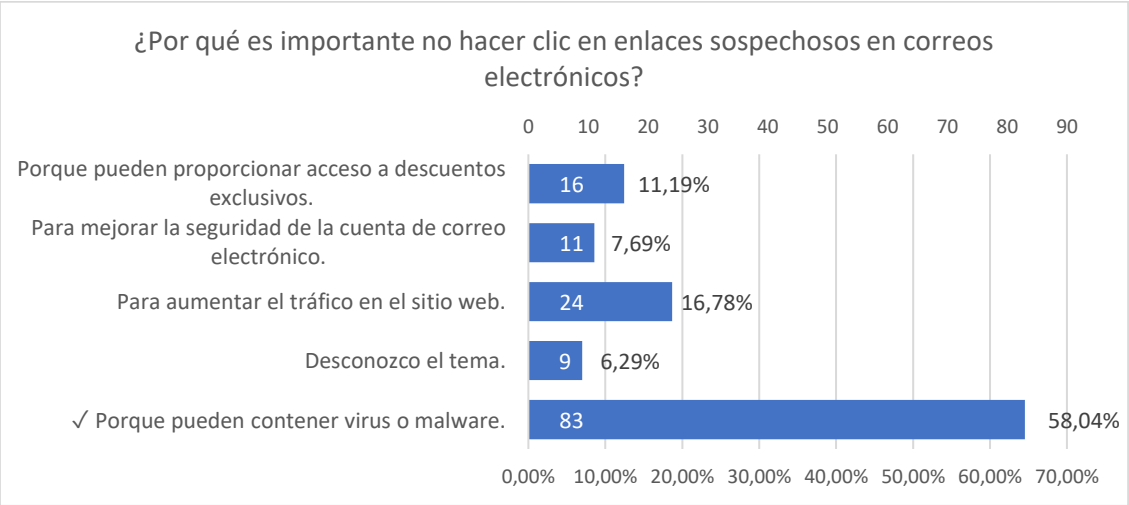

En la pregunta 16, referente a "¿Cuál es una medida para proteger una contraseña?", se evidencia que el 60.84% del personal identifica correctamente que una contraseña segura debe ser única y compleja. No obstante, el 39.16% tiene concepciones erróneas sobre la gestión de contraseñas, ya que el 6.29% cree que compartirla con amigos y familiares es una medida adecuada, el 11.89% considera seguro reutilizar la misma contraseña en múltiples cuentas, y el 10.49% almacena, contraseñas en archivos de texto en el escritorio. Además, un 10.49% desconoce el tema. Estos resultados reflejan una brecha de conocimiento significativa en la institución, lo que resalta la necesidad de capacitaciones en buenas prácticas de seguridad para reforzar la protección de credenciales y minimizar riesgos de acceso no autorizado.

**Figura 22**
*Resultados encuesta - Pregunta 16*



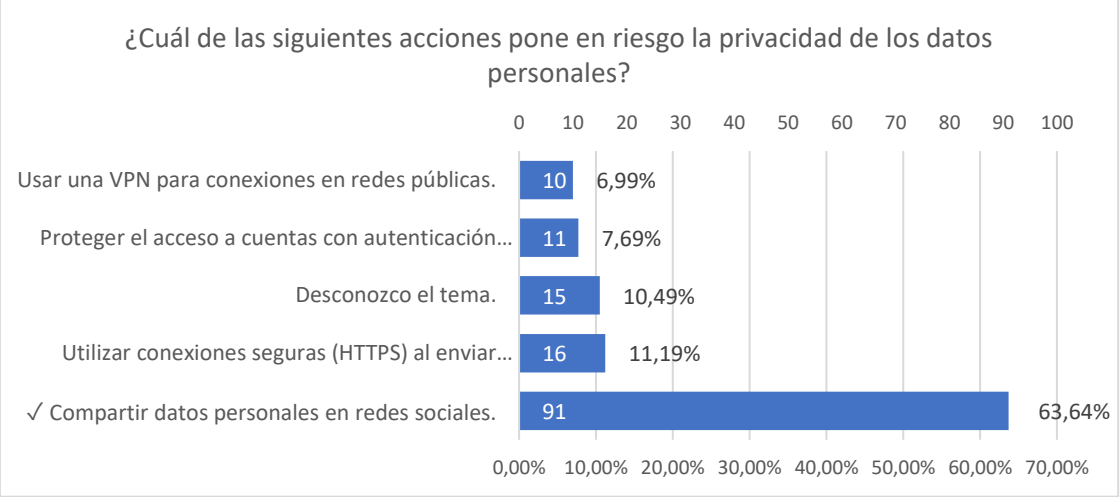

En la pregunta 17, referente a "¿Por qué es importante no hacer clic en enlaces sospechosos en correos electrónicos?", se evidencia que el 58,04% del personal reconoce correctamente que dichos enlaces pueden contener virus o malware. Sin embargo, un 41,96% del personal eligió respuestas equivocadas o manifestó desconocimiento: un 6,29% asocia erróneamente esta acción con el aumento del tráfico en un sitio web, un 16,78% piensa que estos enlaces pueden proporcionar descuentos exclusivos, un 7,69% cree que al hacer clic se mejora la seguridad de la cuenta de correo electrónico, y un 11,19% desconoce el tema. Estos resultados indican la existencia de brechas en el conocimiento sobre los riesgos asociados a los enlaces sospechosos, lo cual subraya la necesidad de reforzar la capacitación en seguridad informática.

**Figura 23**
*Resultados encuesta - Pregunta 17*



En la pregunta 18, referente a "¿Cuál de las siguientes acciones pone en riesgo la privacidad de los datos personales?", se evidencia que el 63,64% del personal identifica correctamente que compartir datos personales en redes sociales es un riesgo para la privacidad. Sin embargo, un 36,36% tiene percepciones incorrectas o desconoce el tema: el 11,19% cree que utilizar conexiones seguras (HTTPS) es una acción riesgosa, el 10,49% considera que la autenticación multifactor afecta la privacidad, y el 7,69% piensa que el uso de una VPN en redes públicas representa un peligro. Además, un 6,99% manifiesta desconocimiento sobre el tema. Estos resultados indican la necesidad de fortalecer la capacitación en privacidad y protección de datos personales, ya que aún persisten conceptos erróneos que pueden llevar a prácticas inseguras dentro de la institución.

**Figura 24**
*Resultados encuesta - Pregunta 18*




## 4.2 Implementación de una herramienta web: Capacitación interactiva

En esta sección se detalla el diseño y la implementación de una herramienta web diseñada para facilitar el acceso a un curso interactivo, adaptado a las demandas identificadas durante la fase de diagnóstico. La herramienta abarca principios básicos de Seguridad de la Información, Protección de Datos y Legislación en vigor, permitiendo a los trabajadores de la Cooperativa Pilahuin Tio LTDA. mejorar sus competencias en estos ámbitos.

Mediante esta plataforma, el objetivo es automatizar el proceso de socialización de la normativa actual, ofreciendo un ambiente activo para la formación y evaluación

subsiguiente del personal. A continuación, se detallan las etapas del desarrollo de la herramienta, su puesta en práctica y los logros alcanzados después de su uso.

### 4.2.1 Desarrollo de la herramienta web

Esta herramienta web se creó con el objetivo de valorar los conocimientos en Seguridad de la Información de los empleados de las instituciones financieras del sector popular y solidario del segmento 1. Su evolución se fundamentó en las regulaciones de seguridad de la información dictadas por el ente controlador de Economías Populares y Solidarias (SEPS), haciendo uso de un caso de estudio particular como punto de referencia.

Para alcanzar esta meta, se estableció una plataforma que facilita la evaluación de los empleados a través de exámenes estructurados y dinámicos, garantizando que el grado de conocimiento obtenido se adecue a los lineamientos exigidos por la SEPS. La herramienta no solo simplifica la gestión de las pruebas, sino que también posibilita un monitoreo del rendimiento individual y a nivel institucional.

Para mejorar el desarrollo y asegurar la entrega eficaz de un producto operativo, se empleó la metodología SCRUM, la cual posibilitó una administración ágil e iterativa del proyecto, segmentando la labor en ciclos de desarrollo graduales conocidos como sprint.

El desarrollo de la herramienta web se estructuró en las siguientes fases:

**Tabla 6**
*Fases del desarrollo*

| Fase | Descripción |
|---|---|
| **1. Levantamiento de Requerimientos** | Se identificaron las necesidades de la aplicación y se definieron los roles de usuario (Administrador, Instructor y Estudiante). Se establecieron las funcionalidades clave y los requisitos técnicos. |
| **2. Diseño del Sistema** | Se presentan los prototipos de la interfaz y la arquitectura del sistema. Se definieron los flujos de navegación y la experiencia de usuario. |

| | |
|---|---|
| **3. Desarrollo del Módulo Administrador** | Se implementaron las funciones de gestión de usuarios, cursos y evaluaciones, así como la configuración de la plataforma. |
| **4. Desarrollo del Módulo Instructor** | Se crearon herramientas para que los instructores puedan diseñar cursos, subir materiales (videos, PDFs, encuestas) y configurar criterios de certificación. |
| **5. Desarrollo del Módulo Estudiante** | Se habilitó el acceso a los cursos, la visualización de materiales, la rendición de evaluaciones y la generación de certificados tras la aprobación. |
| **6. Pruebas y Validación** | Se realizaron pruebas funcionales, de integración y usabilidad para garantizar la estabilidad del sistema. Se incluyeron pruebas con usuarios finales. |
| **7. Despliegue e Implementación** | Se puso en marcha la herramienta web en un entorno real, acompañado de una capacitación a los usuarios y un seguimiento inicial para garantizar su correcta adopción. |

Para la recopilación y definición de requisitos en el desarrollo del proyecto, se empleó la técnica de historias de usuario. Este enfoque permitió capturar de manera estructurada tanto los requisitos funcionales como los no funcionales, facilitando una comprensión clara de las necesidades de la herramienta web y orientando el desarrollo hacia una solución alineada con los objetivos del presente proyecto.

**Tabla 7**
*Historia de Usuario N.º 1*

| | |
|---|---|
| **Nombre:** Iniciar Sesión | **Identificador:** PTIO-HU-01 |
| **Usuario:** Cualquier usuario registrado (Administrador, Instructor, Estudiante) | |
| **Valor para la organización:** Alta | **Estimación:** 5 |
| **Descripción:** Como usuario registrado quiero iniciar sesión con mis credenciales corporativas para acceder a la plataforma según mi rol. | |

| |
|---|
| **Criterios de aceptación:**<br>- Permitir inicio de sesión solo a usuarios registrados.<br>- Validar credenciales con autenticación segura.<br>- Redirigir a la pantalla principal correspondiente según el rol.<br>- Mostrar mensaje de error si las credenciales son incorrectas. |
| **Dependencias:** No tiene |

***Nota.*** Inicio de sesión con usuarios corporativos.

**Tabla 8**

*Historia de Usuario N.º 2*

| | |
|---|---|
| **Nombre:** Configurar Pantalla Principal | **Identificador:** PTIO-HU-02 |
| **Usuario:** Administrador, Instructor, Estudiante | |
| **Valor para la organización:** Alta | **Estimación:** 4 |
| **Descripción:** Como usuario quiero acceder a una pantalla principal adaptada a mi rol para visualizar solo las opciones relevantes. | |
| **Criterios de aceptación:**<br>- Mostrar opciones de cursos según el rol del usuario.<br>- Para estudiantes: Mostrar cursos en progreso y cursos finalizados.<br>- Para instructores: Mostrar panel de cursos activos y panel de instructor.<br>- Para administradores: Mostrar opciones de gestión (usuarios, roles, cursos, parámetros). | |
| **Dependencias:** PTIO-HU-01 (Inicio de sesión) | |

***Nota.*** Administración de pantalla principal según el rol.

**Tabla 9**

*Historia de Usuario N.º 3*

| | |
|---|---|
| **Nombre:** Ver Cursos Estudiante | **Identificador: PTIO-HU-03** |
| **Usuario:** Estudiante | |
| **Valor para la organización:** Alta | **Estimación:** 3 |
| **Descripción:** Como estudiante quiero visualizar los cursos en los que estoy inscrito para poder continuar con mi formación. | |
| **Criterios de aceptación:**<br>- Mostrar lista de cursos en progreso.<br>- Mostrar cursos finalizados con su estado (Aprobado/Reprobado).<br>- Permitir acceso a detalles de cada curso. | |

| |
|---|
| **Dependencias:** PTIO-HU-02 (Pantalla Principal) |

***Nota.*** Visualización de cursos para estudiantes.

**Tabla 10**
*Historia de Usuario N.º 4*

| | |
|---|---|
| **Nombre:** Gestionar Cursos Instructor | **Identificador:** PTIO-HU-04 |
| **Usuario:** Instructor | |
| **Valor para la organización:** Alta | **Estimación:** 4 |
| **Descripción:** Como instructor, necesito acceder y gestionar los cursos asignados para monitorear el avance de los estudiantes. | |
| **Criterios de aceptación:**<br>- Mostrar lista de cursos activos.<br>- Permitir visualización de estudiantes inscritos.<br>- Permitir marcar y actualizar estado de avances en el curso.<br>- Acceso al panel de instructor para gestión de materiales y evaluaciones. | |
| **Dependencias:** PTIO-HU-02 (Pantalla Principal) | |

***Nota.*** Panel de cursos para instructores.

**Tabla 11**
*Historia de Usuario N.º 5*

| | |
|---|---|
| **Nombre:** Administrar Usuarios | **Identificador:** PTIO-HU-05 |
| **Usuario:** Administrador | |
| **Valor para la organización:** Alta | **Estimación:** 5 |
| **Descripción:** Como administrador quiero gestionar los usuarios de la plataforma para administrar roles y permisos. | |
| **Criterios de aceptación:**<br>- Crear, editar y eliminar usuarios.<br>- Asignar y modificar roles de usuario (Administrador, Instructor, Estudiante).<br>- Filtrar y buscar usuarios registrados. | |
| **Dependencias:** PTIO-HU-01 (Inicio de sesión) | |

***Nota.*** Gestión de usuarios por el administrador.

**Tabla 12**
*Historia de Usuario N.º 6*

| | |
|---|---|
| **Nombre:** Administrar Cursos | **Identificador:** PTIO-HU-06 |
| **Usuario:** Administrador | |
| **Valor para la organización:** Alta | **Estimación:** 5 |
| **Descripción:** Como administrador quiero gestionar los cursos de la plataforma para organizar el contenido disponible. | |
| **Criterios de aceptación:**<br>- Crear, editar y eliminar cursos.<br>- Asignar instructores a los cursos.<br>- Definir parámetros como fechas de inicio y finalización. | |
| **Dependencias:** PTIO-HU-05 (Administración de Usuarios) | |

***Nota.*** Gestión de cursos por el administrador.

**Tabla 13**
*Historia de Usuario N.º 7*

| | |
|---|---|
| **Nombre:** Inscripción en Cursos | **Identificador:** PTIO-HU-07 |
| **Usuario:** Estudiante | |
| **Valor para la organización:** Alta | **Estimación:** 4 |
| **Descripción:** Como estudiante quiero inscribirme en cursos disponibles para poder iniciar mi aprendizaje. | |
| **Criterios de aceptación:**<br>- Permitir a los estudiantes inscribirse en los cursos activos.<br>- Validar si el curso tiene cupo disponible antes de inscribirse.<br>- Confirmación de inscripción y acceso a los materiales. | |
| **Dependencias:** PTIO-HU-06 (Administración de Cursos) | |

***Nota.*** Inscripción en cursos.

**Tabla 14**
*Historia de Usuario N.º 8*

| | |
|---|---|
| **Nombre:** Gestión de Materiales de Curso | **Identificador: PTIO-HU-08** |
| **Usuario:** Instructor | |

| | |
|---|---|
| **Valor para la organización:** Alta | **Estimación:** 5 |
| **Descripción:** Como instructor quiero subir y gestionar materiales de curso para proporcionar contenido a los estudiantes. | |
| **Criterios de aceptación:**<br>- Subir archivos PDF, videos y enlaces externos.<br>- Organizar los materiales por módulos o temas.<br>- Controlar acceso solo a estudiantes inscritos. | |
| **Dependencias:** PTIO-HU-07 (Inscripción en Cursos) | |

***Nota.*** Gestión de materiales de curso.

**Tabla 15**

*Historia de Usuario N.º 9*

| | |
|---|---|
| **Nombre:** Evaluaciones y Exámenes | **Identificador:** PTIO-HU-09 |
| **Usuario:** Instructor | |
| **Valor para la organización:** Alta | **Estimación:** 6 |
| **Descripción:** Como instructor quiero crear evaluaciones para medir el aprendizaje de los estudiantes. | |
| **Criterios de aceptación:**<br>- Crear preguntas tipo test, abiertas o de selección múltiple.<br>- Definir fechas de apertura y cierre de exámenes.<br>- Mostrar resultados automáticamente o permitir calificación manual. | |
| **Dependencias: PTIO-HU-08 (Gestión de Materiales de Curso)** | |

***Nota.*** Evaluaciones y exámenes.

**Tabla 16**

*Historia de Usuario N.º 10*

| | |
|---|---|
| **Nombre:** Reportes y Progreso del Estudiante | **Identificador:** PTIO-HU-10 |
| **Usuario:** Estudiante | |
| **Valor para la organización:** Alta | **Estimación:** 4 |
| **Descripción:** Como estudiante quiero ver mi progreso en los cursos para conocer mi rendimiento. | |
| **Criterios de aceptación:**<br>- Mostrar el porcentaje de avance en cada curso. | |

| |
|---|
| - Mostrar notas de evaluaciones.<br>- Generar reportes de desempeño. |
| **Dependencias:** PTIO-HU-09 (Evaluaciones y Exámenes) |

***Nota.*** Reportes y progreso del estudiante.

Tras establecer cada historia de usuario, se creó el Product Backlog, un listado organizado de funcionalidades y requerimientos fundamentales para el desarrollo de la plataforma. Este backlog abarcó tanto aspectos clave como la autenticación, gestión de cursos y usuarios, inscripción de estudiantes, administración de materiales, evaluaciones y reportes.

La Tabla 17 muestra el Product Backlog, en el cual se especifican las historias de usuario junto con su respectiva estimación de esfuerzo, permitiendo visualizar de manera estructurada el trabajo necesario para la implementación de cada funcionalidad en el sistema.

**Tabla 17**
*Product Backlog*

| Orden | Código HU | Nombre | Estimación |
|---|---|---|---|
| **1** | PTIO-HU-01 | Iniciar Sesión | 5 |
| **2** | PTIO-HU-02 | Configurar Pantalla Principal | 4 |
| **3** | PTIO-HU-03 | Ver Cursos Estudiante | 3 |
| **4** | PTIO-HU-04 | Gestionar Cursos Instructor | 4 |
| **5** | PTIO-HU-05 | Administrar Usuarios | 5 |
| **6** | PTIO-HU-06 | Administrar Cursos | 5 |
| **7** | PTIO-HU-07 | Inscripción en Cursos | 4 |
| **8** | PTIO-HU-08 | Gestión de Materiales de Curso | 5 |
| **9** | PTIO-HU-09 | Evaluaciones y Exámenes | 6 |
| **10** | PTIO-HU-10 | Reportes y Progreso del Estudiante | 4 |

#### 4.2.1.1 Planificación e implementación de Sprints

El proceso de desarrollo de la herramienta web destinada a evaluar los conocimientos en seguridad y privacidad de la información se estructuró en siete sprints. Cada iteración

tuvo una duración de dos semanas, salvo las fases tres y cinco, las cuales se extendieron a tres semanas debido a la complejidad de las funcionalidades a implementar.

A lo largo de la mayor parte del desarrollo, se destinaron 30 horas por sprint para la construcción de módulos y ejecución de tareas asignadas. No obstante, en los sprints 3 y 5, la asignación de tiempo se amplió a 35 horas, ya que en estas etapas se abordaron aspectos clave como la gestión de cursos, el proceso de inscripción de estudiantes y la administración de materiales de aprendizaje.

Para el sprint final, se contemplaron 20 horas de trabajo, enfocadas exclusivamente en ajustes finales, corrección de detalles y la documentación necesaria antes del despliegue definitivo de la plataforma.

En la Tabla 18, se brinda una visión resumida del esquema de sprints, incluyendo su duración y la carga horaria prevista en cada fase.

**Tabla 18**
*Sprints del desarrollo de la herramienta web.*

| Sprint | Fecha inicio | Fecha fin | Horas |
|---|---|---|---|
| Sprint #0 | 05-Jun-2023 | 12-Jun-2023 | 15 |
| Sprint #1 | 13-Jun-2023 | 27-Jun-2023 | 30 |
| Sprint #2 | 28-Jun-2023 | 12-Jul-2023 | 30 |
| Sprint #3 | 13-Jul-2023 | 03-Aug-2023 | 35 |
| Sprint #4 | 04-Aug-2023 | 18-Aug-2023 | 30 |
| Sprint #5 | 19-Aug-2023 | 09-Sep-2023 | 35 |
| Sprint #6 | 10-Sep-2023 | 24-Sep-2023 | 30 |
| Sprint #7 | 25-Sep-2023 | 09-Oct-2023 | 20 |

#### 4.2.1.1.1 Sprint 0 - Arquitectura Tecnológica

**Planificación**

**Objetivo:** Definir la arquitectura tecnológica, establecer la estructura del sistema y los roles de usuario.

**Asistentes:** Product Owner, Scrum Master, Development Team

**Tabla 19**
*Tareas del Sprint 0*

| Proceso de Desarrollo | Tarea | Duración (Horas) |
|---|---|---|
| **Diseño** | Analizar y seleccionar las herramientas tecnológicas óptimas para el desarrollo del proyecto. | 3 |
| **Diseño** | Diseño y armado de la arquitectura tecnológica. | 4 |
| **Diseño** | Diseñar la arquitectura de la base de datos. | 6 |
| **Diseño** | Establecer roles y permisos en la plataforma. | 4 |
| **Planificación** | Crear el backlog inicial y planificación de sprints. | 2 |
| **Revisión** | Evaluar la arquitectura y realizar ajustes. | 2 |

**Revisión del Sprint 0**

Durante el Sprint 0, se definió la arquitectura tecnológica y se estableció la estructura de la plataforma. Se revisaron herramientas clave, se diseñó la base de datos y se determinaron los roles y permisos.

#### 4.2.1.1.2 Sprint 1 - Inicio de Sesión y Gestión de Usuarios

**Planificación**

**Objetivo:** Implementar el sistema de autenticación y gestión de usuarios para garantizar el acceso seguro.

**Asistentes:** Product Owner, Scrum Master, Development Team

**Tabla 20**
*Tareas del Sprint 1*

| Historia de Usuario | Proceso de Desarrollo | Tarea | Duración (Horas) |
|---|---|---|---|
| **PTIO-HU-01** | Análisis | Revisar requerimientos de autenticación. | 4 |

| | | | |
|---|---|---|---|
| | Diseño | Diseñar el flujo de inicio de sesión. | 3 |
| | Desarrollo | Implementar autenticación y sesiones de usuario. | 6 |
| | Desarrollo | Configurar permisos y seguridad de acceso. | 5 |
| | Pruebas | Validar credenciales y medidas de seguridad. | 3 |
| **PTIO-HU-05** | Análisis | Revisar requisitos de gestión de usuarios. | 3 |
| | Desarrollo | Implementar CRUD de usuarios y asignación de roles. | 6 |
| | Pruebas | Validar creación y edición de usuarios. | 3 |

**Revisión del Sprint 1**

Se implementó el sistema de autenticación y la gestión de usuarios, asegurando que cada usuario pueda iniciar sesión y se le asignen permisos correctamente.

**Figura 25**

*Pantalla ingreso de usuario.*

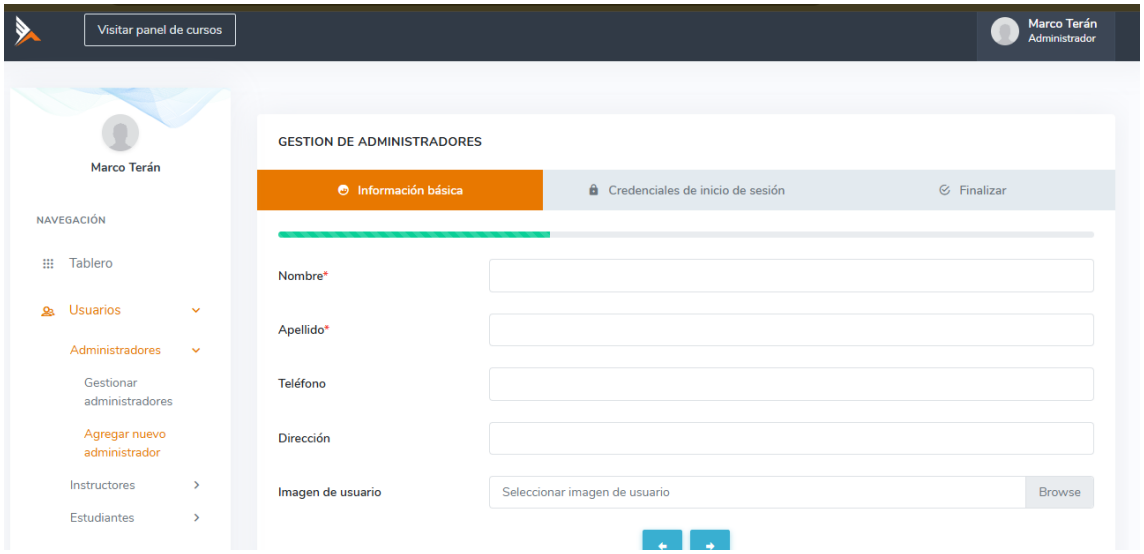
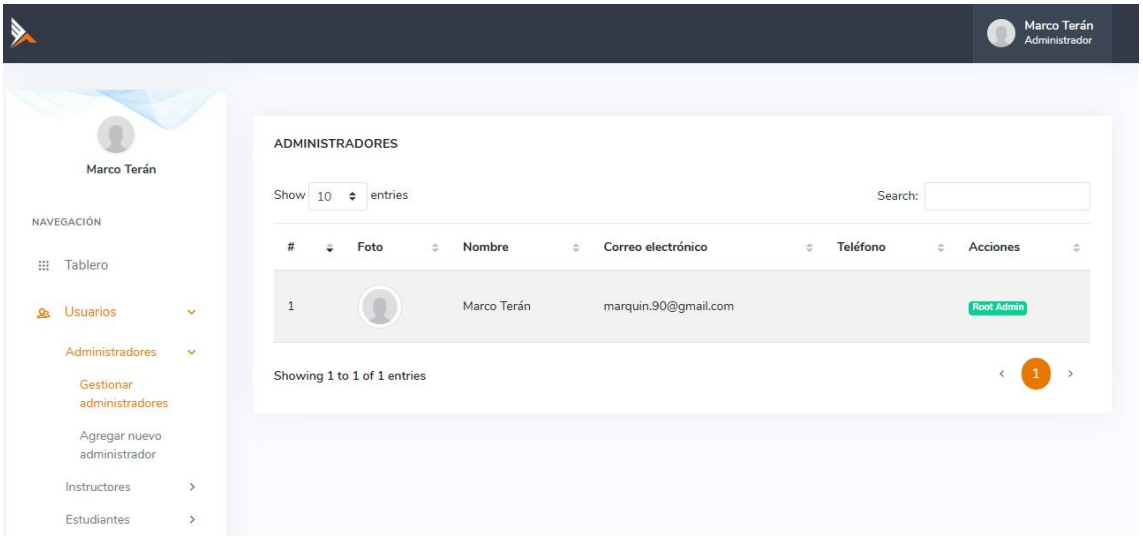


**Figura 26**
*Pantalla para gestión de usuarios.*




#### 4.2.1.1.3 Sprint 2 - Configuración de la Pantalla Principal

**Planificación**

**Objetivo:** Implementar la pantalla principal y personalizarla según el rol del usuario.

**Asistentes:** Product Owner, Scrum Master, Development Team

**Tabla 21**
*Tareas del Sprint 2*

| Historia de Usuario | Proceso de Desarrollo | Tarea | Duración (Horas) |
|---|---|---|---|
| **PTIO-HU-02** | Análisis | Definir estructura y funcionalidades de la pantalla principal. | 3 |
| | Diseño | Diseñar la interfaz de usuario según cada rol. | 3 |
| | Desarrollo | Implementar pantalla principal con opciones dinámicas. | 6 |
| | Desarrollo | Configurar accesos y permisos por rol. | 5 |
| | Pruebas | Validar navegación y accesibilidad. | 3 |

**Revisión del Sprint 2**

Se completó la pantalla principal con visualización personalizada para estudiantes, instructores y administradores.

#### 4.2.1.1.4 Sprint 3 - Gestión de Cursos

**Planificación**

**Objetivo:** Implementar la funcionalidad de administración de cursos y el flujo de inscripción.

**Tabla 22**
*Tareas del Sprint 3*

| Historia de Usuario | Proceso de Desarrollo | Tarea | Duración (Horas) |
|---|---|---|---|
| **PTIO-HU-06** | Análisis | Revisar estructura de los cursos en la base de datos. | 3 |
| | Diseño | Crear interfaz para gestión de cursos. | 3 |
| | Desarrollo | Implementar CRUD de cursos. | 6 |
| | Pruebas | Validar funcionalidad de administración de cursos. | 3 |
| **PTIO-HU-07** | Análisis | Revisar flujo de inscripción de estudiantes. | 3 |
| | Desarrollo | Implementar funcionalidad de inscripción en cursos. | 5 |

**Figura 27**
*Pantalla de gestión de cursos.*


#### 4.2.1.1.5 Sprint 4 - Funcionalidades para Estudiantes e Instructores

**Planificación**

**Objetivo:** Implementar las vistas y paneles específicos para estudiantes e instructores.

**Tabla 23**
*Tareas del Sprint 4*

| Historia de Usuario | Proceso de Desarrollo | Tarea | Duración (Horas) |
|---|---|---|---|
| **PTIO-HU-03** | Desarrollo | Implementar vista de cursos en progreso para estudiantes. | 5 |
| **PTIO-HU-04** | Desarrollo | Implementar gestión de cursos para instructores. | 6 |

#### 4.2.1.1.6 Sprint 5 - Materiales y Evaluaciones

**Planificación**

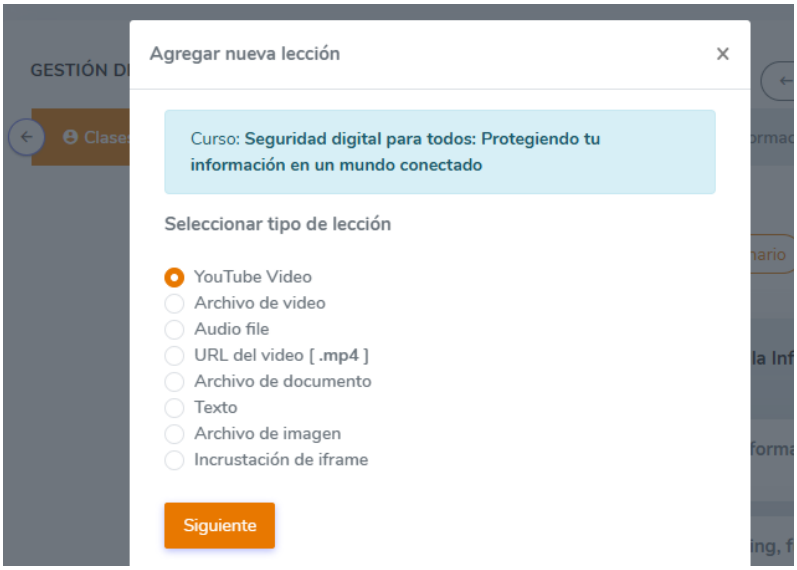
**Objetivo:** Implementar carga de materiales y evaluaciones para cursos.

**Tabla 24**
*Tareas del Sprint 5*

| Historia de Usuario | Proceso de Desarrollo | Tarea | Duración (Horas) |
|---|---|---|---|
| **PTIO-HU-08** | Desarrollo | Implementar carga y gestión de materiales de curso. | 5 |
| **PTIO-HU-09** | Desarrollo | Implementar módulo de evaluaciones y exámenes. | 6 |

**Figura 28**
*Pantalla gestión de curso.*


**Figura 29**
*Pantalla tipo de contenido curso.*




#### 4.2.1.1.7 Sprint 6 - Reportes y Optimización

**Planificación**

**Objetivo:** Implementar reportes de progreso y realizar optimizaciones finales.

**Tabla 25**
*Tareas del Sprint 6*

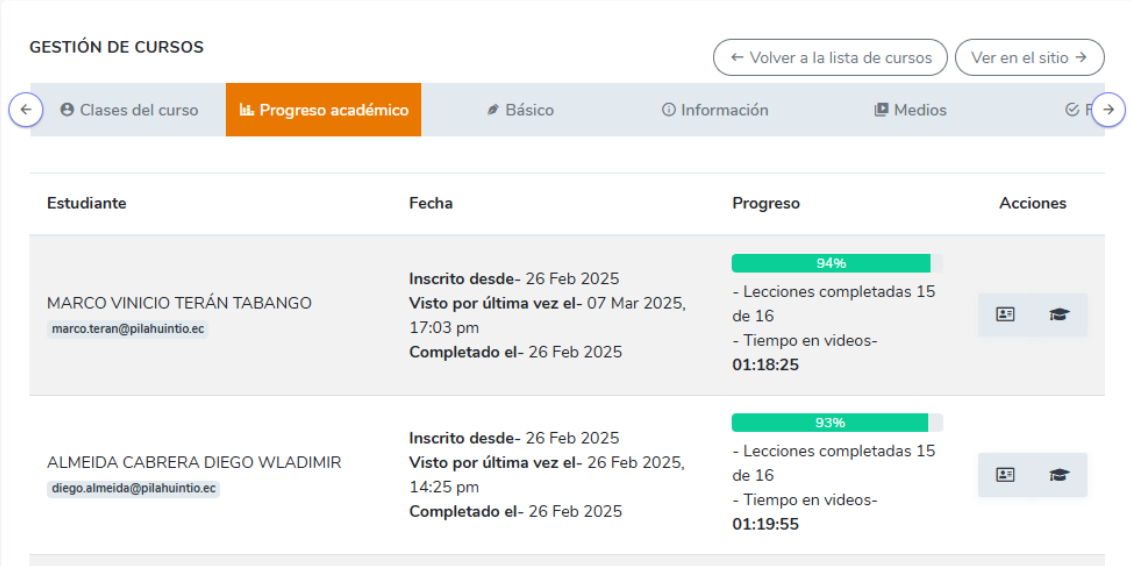
| Historia de Usuario | Proceso de Desarrollo | Tarea | Duración (Horas) |
|---|---|---|---|

| | | | |
|---|---|---|---|
| **PTIO-HU-10** | Desarrollo | Implementar reportes de progreso y métricas. | 4 |

**Revisión del Sprint 6**

Se completó la funcionalidad de reportes y se realizaron optimizaciones en la plataforma.

**Figura 30**
*Pantalla de métricas y progreso de curso por estudiante.*




#### 4.2.1.1.8 Sprint 7 - Despliegue y Documentación

**Planificación**

**Objetivo:** Desplegar la aplicación y generar documentación final.

**Tabla 26**
*Tareas del Sprint 7*

| Proceso de Desarrollo | Tarea | Duración (Horas) |
|---|---|---|
| **Despliegue** | Configurar entorno de producción. | 4 |
| **Documentación** | Redactar manual de usuario. | 4 |
| **Revisión** | Validación final y puesta en marcha. | 2 |

### 4.2.2 Implementación y uso de la herramienta web

La herramienta web desarrollada fue aplicada en la Cooperativa Pilahuin Tio LTDA, con el propósito de evaluar los conocimientos en Seguridad de la Información y Protección de Datos Personales del personal. Para implementar, se llevó a cabo una

campaña de socialización y evaluación dirigida a los empleados de la institución, con el fin de asegurar la participación y el adecuado uso de la plataforma. En la Tabla 27, se presentan detalles del curso, incluyendo el temario, la fecha de aplicación, el público objetivo y evidencia fotográfica del proceso.

La campaña de socialización incluyó la difusión de información sobre la herramienta, beneficios y la debida explicación sobre la obligatoriedad de la evaluación de conocimientos en seguridad y privacidad de la información. Se emplearon correos electrónicos institucionales, reuniones informativas y materiales de apoyo, tales como charlas en video, para guiar a los empleados en el acceso y uso de la plataforma.

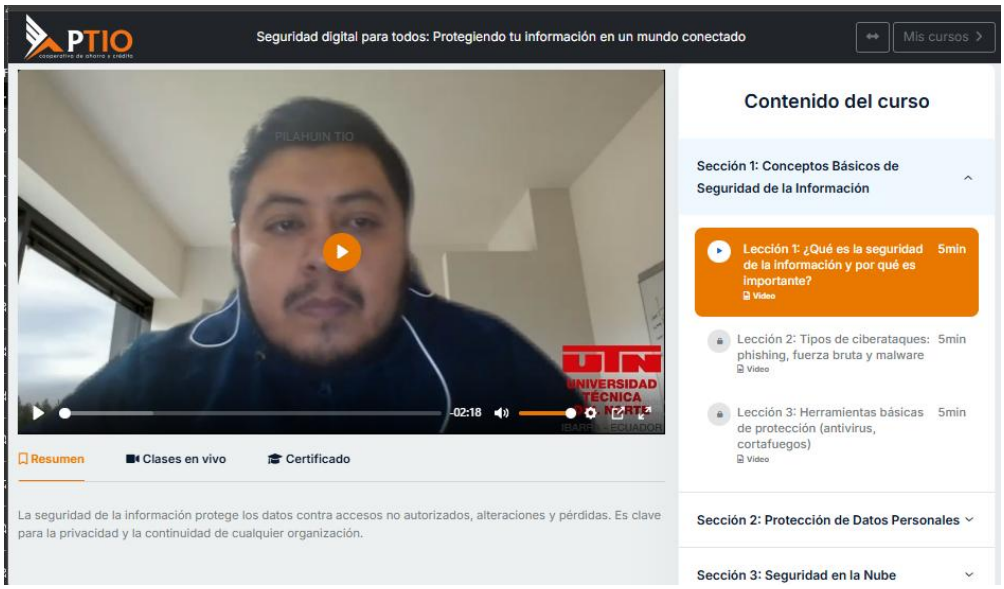
**Figura 31**
*Entrenamiento en el uso de la herramienta web*


***Nota.*** Tomada de la plataforma Teams Institucional, se dejó grabada la introducción y se explicó obligatoriedad del uso de la herramienta web.

Posteriormente, los empleados accedieron a la herramienta web a través de sus credenciales institucionales y participaron en las actividades dispuestas dentro del sistema, las cuales incluyeron:

- Capacitación interactiva: Acceso a cursos estructurados con contenido en diversos formatos (videos, textos, documentos PDF, entre otros).

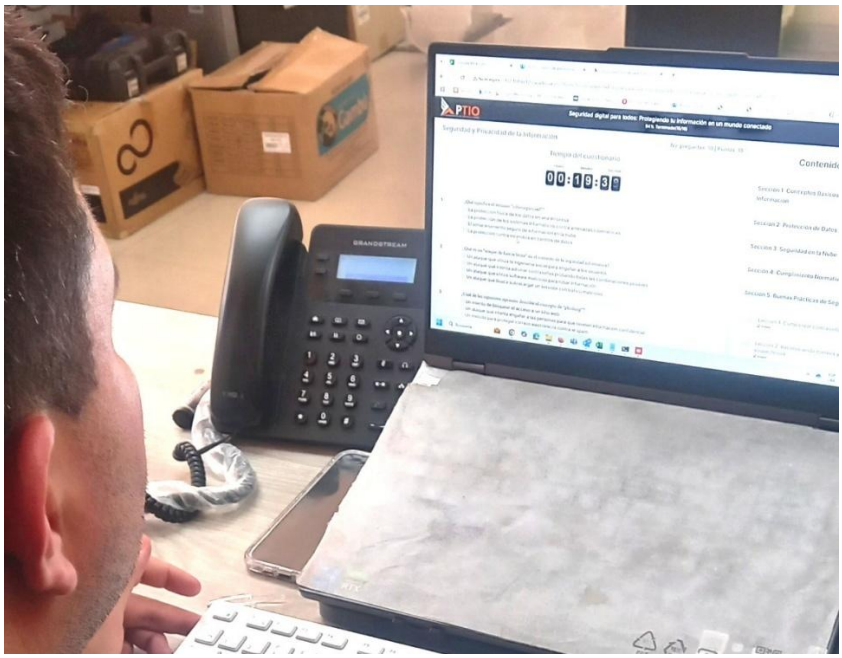
**Figura 32**
*Pantalla de la capacitación*




***Nota.*** Pantalla de inicio de curso, se observa el temario y las lecciones activas mientras no se completen las siguientes se mantienen bloqueadas.

- Evaluación final: Prueba para medir la mejora en los conocimientos adquiridos después del uso de la herramienta web.

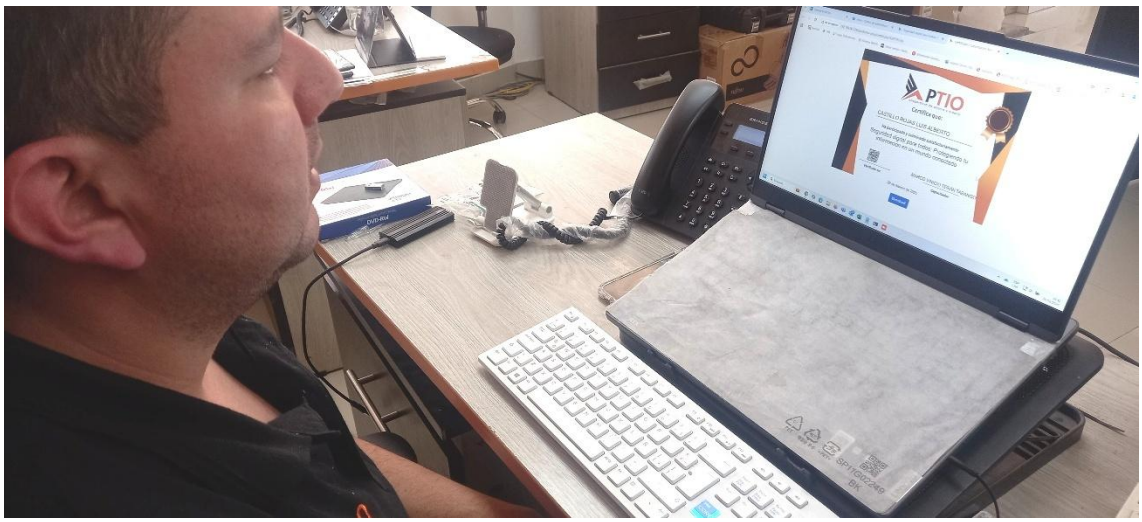
**Figura 33**
*Inicio evaluación*



***Nota.*** Funcionario de la Cooperativa Pilahuin Tio LTDA., al finalizar la capacitación recibe una evaluación para evaluar el conocimiento obtenido.

- Entrega de certificado de aprobación: Se propuso una nota mínima adquirida en la evaluación final para acceder al certificado de aprobación del curso.

**Figura 34**
*Generación de certificado de aprobación*




***Nota.*** Funcionario de la Cooperativa Pilahuin Tio LTDA., revisando el certificado de aprobación de la capacitación.

**Tabla 27**
*Detalles de la aplicación de la herramienta web*

| | |
|---|---|
| **Fecha:** | 17 de febrero de 2025 al 19 de febrero de 2025 |
| **Participantes:** | Funcionarios de la Cooperativa Pilahuin Tío LTDA., conformada por un total de 143 personas, quienes provienen de diversas áreas, tanto administrativas como operativas. |
| **Temario de la capacitación:** | • Sección 1: Conceptos Básicos de Seguridad de la Información<br>  ○ Lección 1: ¿Qué es la seguridad de la información y por qué es importante?<br>  ○ Lección 2: Tipos de ciberataques: phishing, fuerza bruta y malware<br>  ○ Lección 3: Herramientas básicas de protección (antivirus, cortafuegos)<br>• Sección 2: Protección de Datos Personales |

- Lección 1: Principios de la Ley de Protección de Datos en Ecuador
    - Lección 2: Datos personales vs. datos sensibles
    - Lección 3: Consejos para proteger tu información en línea
- Sección 3: Seguridad en la Nube
    - Lección 1: ¿Cómo funciona la seguridad en la nube?
    - Lección 2: Autenticación multifactor y cifrado de datos
    - Lección 3: Privacidad y acceso seguro en la nube
- Sección 4: Cumplimiento Normativo y Legislación
    - Lección 1: ¿Qué es el cumplimiento normativo en ciberseguridad?
    - Lección 2: Registro de actividades de tratamiento de datos
    - Lección 3: Principales normas y regulaciones en seguridad informática
- Sección 5: Buenas Prácticas de Seguridad
    - Lección 1: Cómo crear contraseñas seguras
    - Lección 2: Reconociendo correos y enlaces sospechosos
    - Lección 3: Seguridad en redes Wi-Fi y dispositivos personales
- Cuestionario Previo Obtención de Certificado
    - Seguridad y Privacidad de la Información

**Fotos evidencia:**

**Figura 35**

*Funcionaria haciendo uso de la herramienta web.*

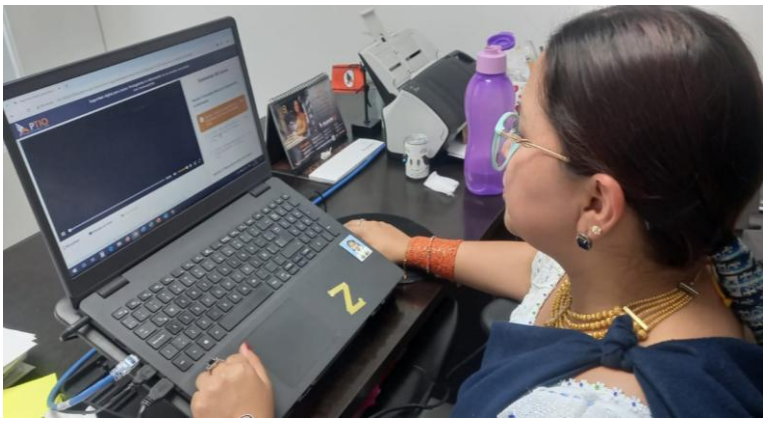


**Figura 36**

*Pantalla lista de cursos, pantalla alumno.*

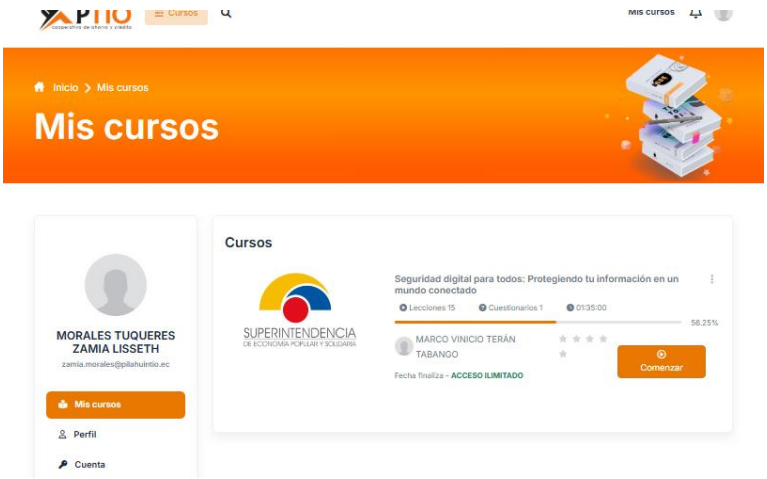



**Figura 37**

*Pantalla progreso de curso, pantalla alumno.*

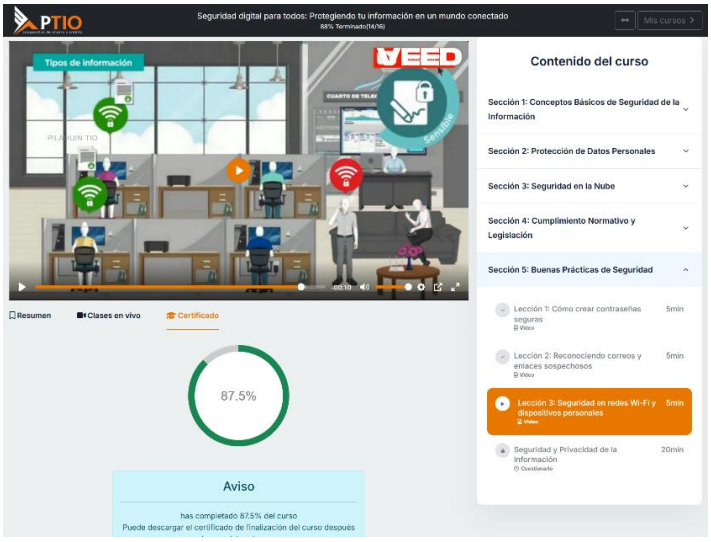
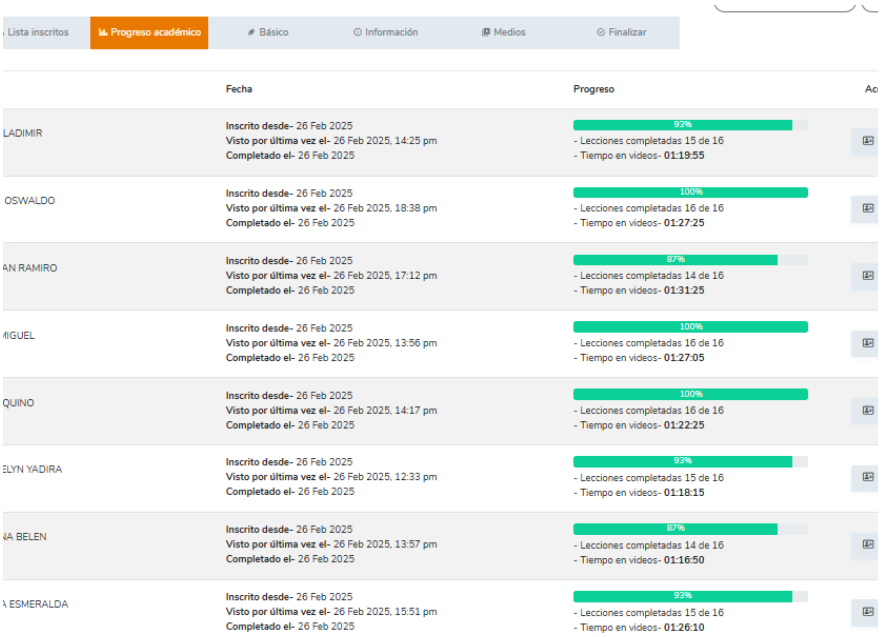


**Figura 38**

*Certificado de aprobar capacitación.*


**Figura 39**

*Pantalla progreso del curso, pantalla Instructor.*




***Nota.*** Elaborado por el autor. Detalles de herramienta web de capacitación a funcionarios de Cooperativa Pilahuin Tio LTDA.

Los resultados obtenidos a través de la plataforma permitieron analizar la evolución del conocimiento del personal, focalizando oportunidades de mejora y fortalecimiento en materia de Seguridad de la Información. En la siguiente sección, se presentan los datos obtenidos y su interpretación.

### 4.3 Evaluación de conocimientos

Una vez que los funcionarios de la Cooperativa Pilahuin Tío completaron el uso de la herramienta web de capacitación en Seguridad de la Información, Protección de Datos y Normativa, se llevó a cabo una evaluación para medir los conocimientos adquiridos en los diferentes módulos. Esta evaluación permitió verificar el impacto de la capacitación y determinar si se logró el objetivo de fortalecer la comprensión de la normativa vigente.

Además, se analizó la efectividad del proceso mediante la revisión de los resultados obtenidos y la cantidad de certificados emitidos a través de la plataforma. Para la obtención de dichos certificados, los participantes debieron demostrar competencias en cinco dominios clave:

- Conceptos Básicos de Seguridad de la Información
- Protección de Datos Personales
- Seguridad en la Nube
- Cumplimiento Normativo y Legislación
- Buenas Prácticas de Seguridad

La sección siguiente muestra los resultados específicos de esta evaluación.

### 4.4 Análisis de Resultados

Luego de la implementación de la herramienta web diseñada para la capacitación en Seguridad de la Información y Protección de Datos Personales en la Cooperativa Pilahuin Tío LTDA., se llevó a cabo un análisis detallado de los resultados obtenidos a partir de la evaluación final. Este proceso permitió identificar el grado de impacto de la formación en el nivel de conocimiento del personal, así como evaluar la efectividad del programa en la transmisión de conceptos clave relacionados con la seguridad de la información.

Los resultados se compararon con la evaluación diagnóstica inicial para determinar la mejora en la comprensión de los conceptos abordados. Como parte del análisis, se consideraron indicadores clave como el porcentaje de respuestas correctas en cada dominio temático, la tasa de participación en la evaluación final y la cantidad de certificados emitidos a los empleados que completaron satisfactoriamente los módulos de capacitación.

En la Tabla 28, se presentan los resultados detallados de la evaluación, reflejando el progreso alcanzado por los participantes en los cinco temas principales:

- Conceptos Básicos de Seguridad de la Información
- Protección de Datos Personales
- Seguridad en la Nube
- Cumplimiento Normativo y Legislación
- Buenas Prácticas de Seguridad

Estos resultados proporcionan una visión clara sobre la efectividad de la herramienta web y permiten identificar áreas de oportunidad para futuras mejoras en la capacitación del personal.

***Tabla 28***

Resultados obtenidos

| Dominio | Pregunta | Diagnóstico | | Evaluación | | Impacto | |
|---|---|---|---|---|---|---|---|
| | | Nro. | % | Nro. | % | (Mejora) | |
| Conceptos Básicos de Seguridad de la Información | 1 | 72 | 50,35% | 130 | 90,91% | 41% | 35,14% |
| | 2 | 95 | 66,43% | 139 | 97,20% | 31% | |
| | 3 | 92 | 64,34% | 134 | 93,71% | 29% | |
| | 4 | 83 | 58,04% | 140 | 97,90% | 40% | |
| Protección de Datos Personales | 5 | 87 | 60,84% | 135 | 94,41% | 34% | 33,92% |
| | 6 | 83 | 58,04% | 132 | 92,31% | 34% | |
| Seguridad en la Nube | 7 | 85 | 59,44% | 134 | 93,71% | 34% | 36,71% |
| | 8 | 77 | 53,85% | 133 | 93,01% | 39% | |
| Cumplimiento Normativo y Legislación | 9 | 83 | 58,04% | 137 | 95,80% | 38% | 38,11% |
| | 10 | 83 | 58,04% | 138 | 96,50% | 38% | |
| Buenas Prácticas de Seguridad | 11 | 92 | 64,34% | 138 | 96,50% | 32% | 34,97% |
| | 12 | 86 | 60,14% | 138 | 96,50% | 36% | |
| | 13 | 84 | 58,74% | 137 | 95,80% | 37% | |
| | 14 | 84 | 58,74% | 135 | 94,41% | 36% | |
| | 15 | 89 | 62,24% | 136 | 95,10% | 33% | |

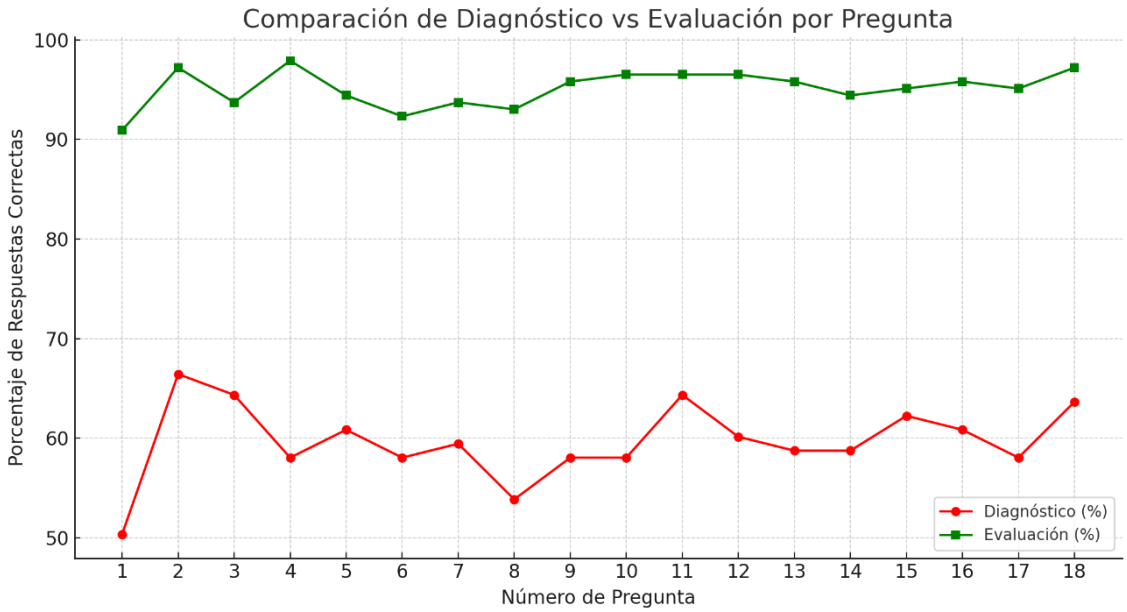
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 16 | 87 | 60,84% | 137 | 95,80% | 35% | |
| | 17 | 83 | 58,04% | 136 | 95,10% | 37% | |
| | 18 | 91 | 63,64% | 139 | 97,20% | 34% | |
| **Total (Promedio)** | | | | | | **35,77%** | |

***Nota.*** Elaborado por el autor. Detalles de los resultados obtenidos Diagnóstico versus Evaluación.

Los resultados alcanzados tras la ejecución de la evaluación demuestran una mejora significativa en los conocimientos de Seguridad de la Información del personal de la Cooperativa Pilahuin Tío LTDA. Antes de la capacitación, los niveles de acierto en el diagnóstico inicial variaban entre el **50,35% y el 66,43%**, mientras que en la evaluación final estos valores se incrementaron hasta un rango de **90,91% a 97,90%**. En promedio, se registró una mejora del **35,77%** en el nivel de conocimientos de los participantes.

**Figura 40**

*Comparación de diagnóstico versus evaluación por pregunta*

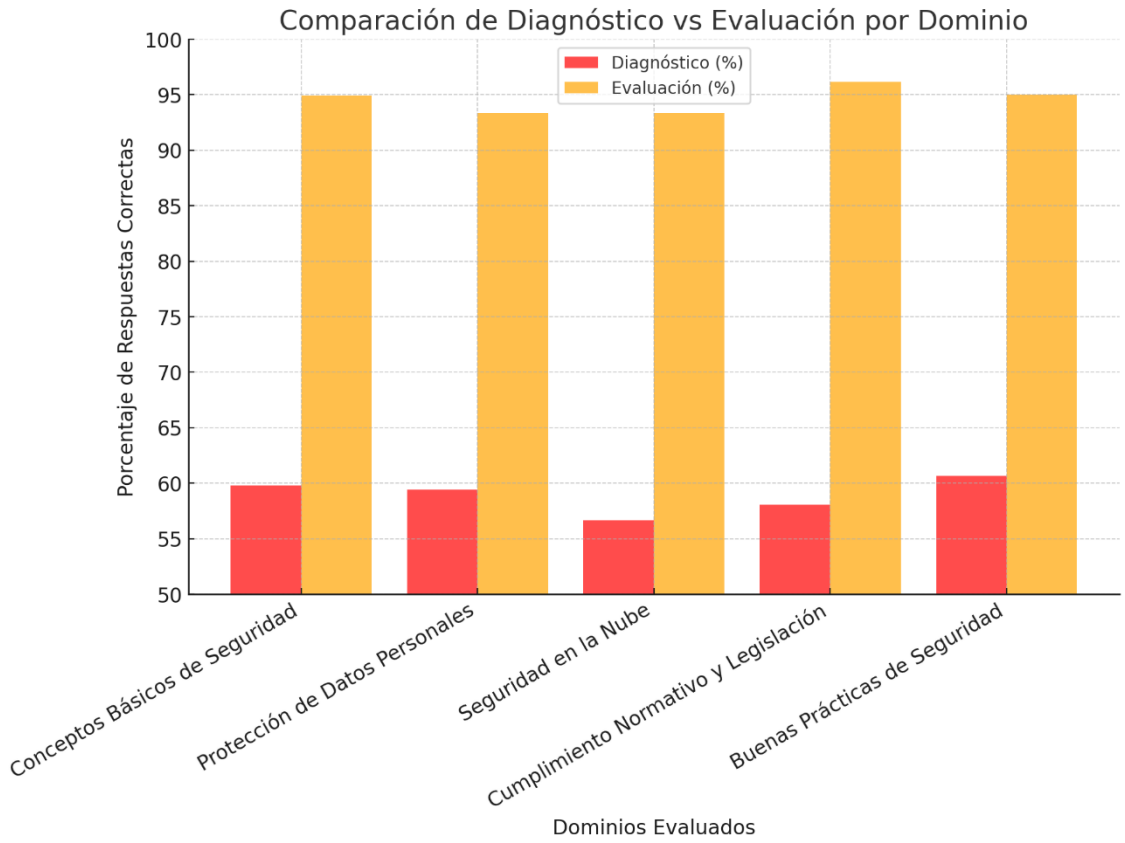



Entre los dominios evaluados, el mayor impacto se observó en **Cumplimiento Normativo y Legislación**, con una mejora del **38,11%**, seguido de **Seguridad en la Nube** con **36,71%** y **Protección de Datos Personales** con **33,92%**. Esto indica que los participantes lograron una mejor comprensión de los aspectos regulatorios y normativos, así como de las medidas necesarias para proteger la información en entornos digitales.

Por otro lado, aunque la mejora en **Conceptos Básicos de Seguridad de la Información** y **Buenas Prácticas de Seguridad** fue ligeramente menor (**35,14% y 34,97%**, respectivamente), los resultados finales muestran que la mayoría de los participantes adquirieron conocimientos sólidos, con niveles de aprobación superiores al **90% en la evaluación final** en todas las áreas.

**Figura 41**

*Comparación de diagnóstico versus evaluación por dominio*




En conclusión, la capacitación permitió aumentar significativamente los conocimientos del personal, con una mejora promedio del **35,77%** en todos los dominios evaluados. Este resultado confirma la efectividad de la herramienta web y la estrategia de capacitación implementada. No obstante, para asegurar la retención del conocimiento y fomentar una cultura de seguridad sostenible, se recomienda la realización de sesiones de refuerzo y evaluaciones periódicas.

## CONCLUSIONES

Las amenazas vinculadas a la seguridad de la información en la Cooperativa Pilahuin Tío LTDA., estaban directamente relacionados con el desconocimiento de los empleados sobre los principios fundamentales de seguridad, privacidad y normativas vigentes. Antes de la capacitación, los niveles de conocimiento sobre seguridad informática presentaban deficiencias que podrían haber comprometido la protección de la información institucional.

Los resultados obtenidos reflejan una mejora significativa en el nivel de conocimientos del personal, con un incremento promedio del **35,77%** en las evaluaciones realizadas después de la capacitación. Se destacan mejoras en **Cumplimiento Normativo y Legislación** (**38,11%**), **Seguridad en la Nube** (**36,71%**) y **Protección de Datos Personales** (**33,92%**), lo que indica una mayor comprensión de las regulaciones y las medidas de protección necesarias en entornos digitales.

El éxito del programa de capacitación se refleja en que más del **90% de los participantes** lograron responder correctamente en la evaluación final. Esto sugiere que el personal está ahora mejor preparado para enfrentar amenazas de seguridad informática en sus actividades diarias.

Se recomienda la implementación continua de programas de formación y desarrollo, con el propósito de consolidar y fortalecer la cultura de seguridad de la información dentro de la organización, asegurando la aplicación sostenida de las mejores prácticas a lo largo del tiempo.

## RECOMENDACIONES

Basándose en los resultados alcanzados al poner en marcha la herramienta web para valorar los conocimientos en seguridad y privacidad de la información, se aconseja seguir extendiendo estas iniciativas a escala nacional, incluyendo a otras entidades financieras segmento 1 pertenecientes al Sector Popular y Solidario. Es esencial que la valoración del personal sea constante y flexible conforme aparezcan nuevas amenazas o modificaciones en la regulación de seguridad del organismo regulador del sector financiero popular y solidario del Ecuador.

Además, se propone que los hallazgos de las evaluaciones no solo se empleen para evaluar el saber, sino también como un instrumento para detectar áreas de mejora en las instituciones, facilitando la implementación de programas de formación especializados. La retroalimentación y la adaptación de los contenidos al perfil individual de cada usuario serán fundamentales para conservar la participación y la eficacia del programa.

Finalmente, se sugiere incorporar la aplicación con sistemas de vigilancia y seguimiento de la seguridad de la información, con el fin de que las instituciones aseguren la aplicación efectiva de las políticas de protección de datos y que los trabajadores se mantengan al día ante los retos emergentes que presenta el ambiente digital.

# REFERENCIAS


Ministerio de Telecomunicaciones y Sociedad de la Información. (08 de 2022). *Asobanca.* Obtenido de https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf

Aguilera, M., & Blanco, M. (1987). *Investigación cualitativa.* Madrid: Ministerio de Educación y Ciencia.

Asamblea Nacional del Ecuador. (11 de 2012). *LEY DE COMERCIO ELECTRONICO, FIRMAS Y*. Obtenido de telecomunicaciones.gob.ec: https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf

Asamblea Nacional del Ecuador, A. (2018). *Registro Oficial Órgano de la Republica del Ecuador.* Obtenido de Ley Orgánica de Protección de Datos Personales. Registro Oficial Suplemento 553: https://www.registroficial.gob.ec/index.php/registro-oficial-electronico/registro-oficial-suplemento-553

Bandiera, R. (2019). *Diseño e Desarrollo Web con CodeIgniter 3.* Castelfranco, Italia: ISBN 978-0-244-4551-3- Libro Electrónico.

Castillo, J. E. (20 de 10 de 2020). *Usuario final, el eslabón más débil de la seguridad informática*. Obtenido de strategamagazine.com: https://strategamagazine.com/usuario-final-el-eslabon-mas-debil-de-la-seguridad-informatica/

Cidhpda, E. (04 de 2023). *Qué es la Ley de Protección de Datos Personales en Ecuador*. Obtenido de cidhpdaecuador.org: https://www.cidhpdaecuador.org/ley-de-proteccion-de-datos

Corporación Nacional de Finanzas Populares y Solidarias, C. (26 de 05 de 2021). *finanzaspopulares.gob.ec.* Obtenido de finanzaspopulares.gob.ec: https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Gutiérrez, N. (17 de 02 de 2022). *preyproject*. Obtenido de https://preyproject.com/es/blog/30-estadisticas-seguridad-informatica

Hernández, R., Fernández, C., & & Baptista, M. (2014). *Metodología de la investigación.* México D.F: McGraw-Hill.

ISO, I. O. (2013). *Information technology — Security techniques — Information security management systems — Requirements.* Switzerland: ISO/IEC 2013. Obtenido de Security techniques – Information security management systems – Requirements.

Juan J. Lugo Marín, H. E. (2020). Evaluación de gestión de seguridad de la información. *Qualitas*, 16.

Navarrete, J. (14 de 09 de 2020). *BDO Ecuador*. Obtenido de https://www.bdo.ec/es-ec/noticias/2020/ecuador-en-riesgo-ciberataques?gclid=EAIaIQobChMI--vn7sr8_gIVUQlMCh1O7guOEAAYAiAAEgJGbfD_BwE

NQA. (2023). Obtenido de https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Ñaupas Paitán, H., Mejía Mejía, E., Novoa Ramírez, E., & Villagómez Paucar, A. (2014). *Metodología de la investigación Cuantitativa - Cualitativa y Redacción de la Tesis.* Bogotá: Ediciones de la U.

Ortiz, e. L. (31 de 07 de 2024). *revistagestion.ec*. Obtenido de https://revistagestion.ec/analisis-economia-y-finanzas/otavalo-busca-consolidarse-como-polo-economico-ademas-de-turistico-y/

Pilahuin Tio, L. (2020). *Pilahuin Tio LTDA*. Obtenido de Pilahuin Tio LTDA: https://www.pilahuintio.ec/historia-ptio/

Sampier, H. (2014). *Metodología de la Investigación.* México D.F: Sexta.

Santa Gadea, K. D., Gadea, W. F., & Vera - Quiñonez, S. (2018). *Rompiendo Barreras en la Investigación.* Machala: Editorial UTMACH.

Schwaber, K., & Sutherland, J. (2017). *The Scrum Guide*. Obtenido de https://www.scrumguides.org/scrum-guide.html

SEPS. (15 de 11 de 2021). Obtenido de https://www.seps.gob.ec/wp-content/uploads/Norma-ISO-27001.pdf

SEPS, S. d. (2022). *RESOLUCIÓN NO. SEPS-IGS-IGT-IGJ-INGINT-INTIC-INSESF-INR-DNSI-2022-002.* Quito.

SEPS, S. D. (18 de 05 de 2023). *SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA.* Obtenido de https://servicios.seps.gob.ec/gosf-internet/paginas/consultarOrganizaciones.jsf

Solidaria, S. d. (3 de 05 de 2022). *Superintendencia de Economía Popular y Solidaria*. Obtenido de Superintendencia de Economía Popular y Solidaria: https://www.seps.gob.ec/wp-content/uploads/SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002.pdf

Superintendencia de Economía Popular y Solidaria. (s.f.). *Superintendencia de Economía Popular y Solidaria*. Obtenido de Superintendencia de Economía Popular y Solidaria: https://www.seps.gob.ec/institucion/segmentacion-de-esfps/

Tamayo y Tamayo, M. (2003). *EL PROCESO DE LA INVESTIGACIÓN CIENTÍFICA.* MEXICO: EDITORIAL LIMUSA. S.A.

Tamayo y Tamayo, M. (2008). *EL PROCESO DE LA INVESTIGACIÓN CIENTÍFICA.* MEXICO: EDITORIAL LIMUSA.

Urtiaga, G. ((n.d)). *Administrar MySQL y MariaDB.* (n.p): AprendeIT.

Vega Briceño, E. (2021). *SEGURIDAD DE LA INFORMACIÓN.* Alicante: ÁREA DE INNOVACIÓN Y DESARROLLO, S.L.

# ANEXOS

## ANEXO A

## ENCUESTA DIAGNOSTICO DIGITAL

### Seguridad y Privacidad de la Información

Este cuestionario busca conocer qué tanto sabes sobre cómo proteger la información personal y mantener la seguridad en línea, y qué prácticas sigues para cuidar tus datos. El objetivo es identificar áreas en las que puedas mejorar y aprender más sobre cómo mantener tu información segura.

* Indica que la pregunta es obligatoria

1.- ¿Qué significa el término "ciberseguridad"? *

- El almacenamiento seguro de información en la nube.
- La protección física de los datos en una empresa.
- Desconozco el tema.
- La protección contra incendios en centros de datos
- La protección de los sistemas informáticos contra amenazas cibernéticas.

2.- ¿Qué es un "ataque de fuerza bruta" en el contexto de la seguridad informática? *

- Un ataque que busca sobrecargar un servidor con tráfico malicioso.
- Desconozco el tema.
- Un ataque que intenta adivinar contraseñas probando todas las combinaciones posibles.
- Un ataque que utiliza la ingeniería social para engañar a los usuarios.
- Un ataque que utiliza software malicioso para robar información.

3.- ¿Cuál de las siguientes opciones describe el concepto de "phishing"? *

- Desconozco el tema.
- Una práctica para enviar mensajes publicitarios no deseados.
- Un ataque que intenta engañar a las personas para que revelen información confidencial.
- Un intento de bloquear el acceso a un sitio web.
- Un método para proteger correos electrónicos contra el spam.

4.- ¿Qué es un "antivirus" y cuál es su función principal? *

- Una plataforma para almacenar datos en la nube.
- Un programa para crear contraseñas seguras.
- Desconozco el tema.
- Un sistema de autenticación de dos factores.
- Una herramienta para proteger contra virus y malware.

5.- ¿Qué es la "Ley Orgánica de Protección de Datos Personales" en Ecuador y cuál es su propósito? *

- Un conjunto de pautas para proteger la propiedad intelectual en línea.
- Una regulación que protege los datos personales y garantiza los derechos de privacidad de las personas.
- Desconozco el tema.
- Un protocolo para el manejo seguro de información financiera en instituciones bancarias.
- Una legislación que regula el uso de dispositivos electrónicos personales.

6.- ¿Qué se considera un dato confidencial en el contexto de la protección de datos personales? *

- Información sobre productos o servicios de una empresa.
- Información que puede identificar directa o indirectamente a una persona.
- Desconozco el tema.
- Documentos impresos almacenados en una oficina.
- Datos que están disponibles públicamente en internet.

7.- ¿Qué es la "autenticación multifactor" y por qué es importante en la seguridad de la información en la nube? *

- Una técnica para cifrar datos almacenados en la nube.
- Un estándar de seguridad para proteger servidores de bases de datos.
- Un método para proteger las contraseñas de las cuentas de usuario.
- Desconozco el tema.
- Un proceso que requiere múltiples formas de verificación de identidad para acceder a una cuenta.

8.- ¿Cuál de las siguientes afirmaciones describe el concepto de "privacidad de la información" en la nube? *

- La capacidad de acceder a los datos desde cualquier ubicación sin restricciones.
- El control total de los datos por parte del proveedor de servicios en la nube.
- La práctica de compartir datos personales en redes sociales sin restricciones.
- La protección de los datos contra el acceso no autorizado y su uso indebido.
- Desconozco el tema.

9.- ¿Qué es un registro de actividades de tratamiento de datos personales? *

- Una política para el uso adecuado de contraseñas en una organización.
- Desconozco el tema.
- Un protocolo para la destrucción segura de datos obsoletos.
- Un documento donde se registra y documenta el procesamiento de datos personales, incluyendo detalles como quién accede a los datos, cuándo y con qué propósito.
- Una herramienta para cifrar datos sensibles almacenados en servidores.

10.- ¿Qué significa el término "cumplimiento normativo" en el contexto de la seguridad de la información? *

- La implementación de medidas de seguridad para proteger la información confidencial.
- Desconozco el tema.
- La protección de los datos contra el acceso no autorizado y su uso indebido.
- La capacidad de una empresa para recuperarse de un incidente de seguridad.
- El cumplimiento de las leyes y regulaciones relacionadas con la protección de datos.

11.- ¿Cuál de las siguientes acciones ayuda a proteger la privacidad de los datos personales? *

- Compartir datos personales en redes sociales.
- Utilizar conexiones seguras (HTTPS) al enviar información confidencial.
- Almacenar contraseñas en un archivo de texto sin cifrar.
- Desconozco el tema.
- Compartir información personal con desconocidos.

12.- ¿Qué es una "cookie" en el contexto de la seguridad de la información en línea? *

- ◯ Desconozco el tema.
- ◯ Un tipo de virus informático.
- ◯ Una técnica para cifrar mensajes de correo electrónico.
- ◯ Un archivo que almacena información sobre la actividad del usuario en un sitio web.
- ◯ Un software para proteger la privacidad en línea.

13.- ¿Qué es un "ataque de ingeniería social"? *

- ◯ Desconozco el tema.
- ◯ Un ataque que intenta engañar a las personas para que revelen información confidencial.
- ◯ Un ataque que utiliza la fuerza bruta para acceder a contraseñas.
- ◯ Un ataque que utiliza malware para robar datos.
- ◯ Un ataque que utiliza redes sociales para difundir spam.

14.- ¿Qué es la seguridad de la red? *

- ◯ Un programa de ejercicios físicos en el lugar de trabajo.
- ◯ Un método para protegerse contra incendios en el lugar de trabajo.
- ◯ Un protocolo para enviar correos electrónicos cifrados.
- ◯ Un conjunto de medidas para proteger los datos y los sistemas informáticos contra amenazas cibernéticas.
- ◯ Desconozco el tema.

15.- ¿Por qué es importante mantener el software actualizado en un dispositivo? *

- ◯ Desconozco el tema.
- ◯ Para aumentar la velocidad de conexión a internet.
- ◯ Para mejorar el rendimiento del dispositivo.
- ◯ Para reducir el espacio de almacenamiento.
- ◯ Para corregir vulnerabilidades de seguridad.

16.- ¿Cuál es una medida para proteger una contraseña? *

- ◯ Desconozco el tema.
- ◯ Compartirla con amigos y familiares.
- ◯ Mantenerla en un archivo de texto en el escritorio.
- ◯ Utilizar la misma contraseña para múltiples cuentas.
- ◯ Crear una contraseña única y compleja.

17.- ¿Por qué es importante no hacer clic en enlaces sospechosos en correos electrónicos? *

- ◯ Porque pueden proporcionar acceso a descuentos exclusivos.
- ◯ Para aumentar el tráfico en el sitio web.
- ◯ Para mejorar la seguridad de la cuenta de correo electrónico.
- ◯ Porque pueden contener virus o malware.
- ◯ Desconozco el tema.

18.- ¿Cuál de las siguientes acciones pone en riesgo la privacidad de los datos personales? *

- ◯ Utilizar conexiones seguras (HTTPS) al enviar información confidencial.
- ◯ Proteger el acceso a cuentas con autenticación multifactor.
- ◯ Usar una VPN para conexiones en redes públicas.
- ◯ Compartir datos personales en redes sociales.
- ◯ Desconozco el tema..

## ANEXO B

## MATRICES DE VALIDACIÓN

**UNIVERSIDAD TÉCNICA DEL NORTE**
Resolución No. 001-073 CEAACES-2013-13
INSTITUTO DE POSGRADO

IBARRA - ECUADOR
Facultad de Posgrado

**FORMACIÓN EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Esta encuesta tiene como objetivo analizar y evaluar el nivel de conocimiento en seguridad y privacidad de la información, de los funcionarios de las instituciones financieras segmento 4 y 5 de la Provincia de Imbabura.

**Lea detenidamente las preguntas y escoja la opción que usted considere conveniente.**

**Consentimiento informado**

1. Acepta participar en la investigación descrita de forma libre y voluntaria. Su participación puede ser suspendida en cualquier momento, sin que esto traiga ningún tipo de consecuencias negativas para usted o a la institución. Este estudio no presenta riesgos identificables para su integridad física o psicológica.
   Los datos solicitados para la aplicación de este cuestionario son anónimos y serán manejados bajo absoluta confidencialidad. Estos datos estarán guardados en archivo electrónico, codificados con clave de acceso y custodiados por el Investigador Responsable.

   Ante cualquier duda, puede comunicarse con el responsable de esta investigación, Ingeniero Marco Teran Tabango, mediante correo electrónico mvterant@utn.edu.ec.

   ○ Si
   ○ No

**Datos informativos**

2. Género
   ○ Masculino
   ○ Femenino
   ○ Otro

3. Edad
   - ○ 18-21 años
   - ○ 22-25 años
   - ○ 26-29 años
   - ○ 30 años o más

4. Nivel de Educación
   - ○ Educación Primaria
   - ○ Educación Secundaria (Bachillerato)
   - ○ Educación Superior
   - ○ Estudios de Posgrado

**Disponibilidad Tecnológica en el Trabajo**

5. ¿Posee dispositivos tecnológicos en su puesto de trabajo con conexión a internet?

| | Si | No |
|---|---|---|
| Computador de escritorio | ○ | ○ |
| Laptop | ○ | ○ |
| Tablet | ○ | ○ |
| Smartphone | ○ | ○ |
| Smart TV | ○ | ○ |

6. ¿Cuál es el dispositivo tecnológico que más usa para acceder a internet?
   - ○ Computador de escritorio
   - ○ Laptop
   - ○ Tablet
   - ○ Smartphone
   - ○ Smart TV

## Seguridad y Privacidad de la Información

*La seguridad de la información es un componente esencial en el mundo digital actual. Mediante la implementación de prácticas y tecnologías adecuadas, las organizaciones pueden proteger sus datos contra amenazas cibernéticas y garantizar la confidencialidad, integridad y disponibilidad de la información. La adopción de políticas de seguridad, el uso de cifrado, la autenticación de usuarios y la concienciación sobre las mejores prácticas son algunas de las medidas clave para mitigar riesgos y salvaguardar los activos de información de una organización en un entorno cada vez más interconectado y vulnerable a ataques informáticos (Smith, 2020).*

## Tema 1: Conceptos Básicos de Seguridad de la Información

7. ¿Qué significa el término "ciberseguridad"?
   - ○ A) La protección física de los datos en una empresa
   - ○ B) La protección de los sistemas informáticos contra amenazas cibernéticas
   - ○ C) El almacenamiento seguro de información en la nube
   - ○ D) La protección contra incendios en centros de datos

8. ¿Qué es un "ataque de fuerza bruta" en el contexto de la seguridad informática?
   - ○ A) Un ataque que utiliza la ingeniería social para engañar a los usuarios
   - ○ B) Un ataque que intenta adivinar contraseñas probando todas las combinaciones posibles
   - ○ C) Un ataque que utiliza software malicioso para robar información
   - ○ D) Un ataque que busca sobrecargar un servidor con tráfico malicioso

9. ¿Cuál de las siguientes opciones describe mejor el concepto de "phishing"?
   - ○ A) Un intento de bloquear el acceso a un sitio web
   - ○ B) Un ataque que intenta engañar a las personas para que revelen información confidencial
   - ○ C) Un método para proteger correos electrónicos contra el spam
   - ○ D) Una práctica para enviar mensajes publicitarios no deseados

10. ¿Qué es un "software antivirus" y cuál es su función principal?
    - A) Un programa para crear contraseñas seguras
    - B) Una herramienta para proteger contra virus y malware
    - C) Un sistema de autenticación de dos factores
    - D) Una plataforma para almacenar datos en la nube

**Tema 2: Protección de Datos Personales**

11. ¿Qué es la "Ley Orgánica de Protección de Datos Personales" en Ecuador y cuál es su propósito?
    - A) Una legislación que regula el uso de dispositivos electrónicos personales
    - B) Una regulación que protege los datos personales y garantiza los derechos de privacidad de los individuos
    - C) Un conjunto de pautas para proteger la propiedad intelectual en línea
    - D) Un protocolo para el manejo seguro de información financiera en instituciones bancarias

12. ¿Qué se considera un dato confidencial en el contexto de la protección de datos personales?
    - A) Información que puede identificar directa o indirectamente a una persona.
    - B) Datos que están disponibles públicamente en internet.
    - C) Documentos impresos almacenados en una oficina
    - D) Información sobre productos o servicios de una empresa.

**Tema 3: Seguridad en la Nube**

13. ¿Qué es la "autenticación multifactor" y por qué es importante en la seguridad de la información en la nube?
    - A) Un método para proteger las contraseñas de las cuentas de usuario
    - B) Un proceso que requiere múltiples formas de verificación de identidad para acceder a una cuenta
    - C) Una técnica para cifrar datos almacenados en la nube
    - D) Un estándar de seguridad para proteger servidores de bases de datos

14. ¿Cuál de las siguientes afirmaciones describe mejor el concepto de "privacidad de la información" en la nube?
    - ○ A) El control total de los datos por parte del proveedor de servicios en la nube
    - ○ B) La protección de los datos contra el acceso no autorizado y su uso indebido
    - ○ C) La capacidad de acceder a los datos desde cualquier ubicación sin restricciones
    - ○ D) La práctica de compartir datos personales en redes sociales sin restricciones

**Tema 4: Cumplimiento Normativo y Legislación**

15. ¿Qué es un registro de actividades de tratamiento de datos personales?
    - ○ A) Un documento donde se registra y documenta el procesamiento de datos personales, incluyendo detalles como quién accede a los datos, cuándo y con qué propósito.
    - ○ B) Una herramienta para cifrar datos sensibles almacenados en servidores.
    - ○ C) Un protocolo para la destrucción segura de datos obsoletos
    - ○ D) Una política para el uso adecuado de contraseñas en una organización.

16. ¿Qué significa el término "cumplimiento normativo" en el contexto de la seguridad de la información?
    - ○ A) El cumplimiento de las leyes y regulaciones relacionadas con la protección de datos
    - ○ B) La implementación de medidas de seguridad para proteger la información confidencial
    - ○ C) La capacidad de una empresa para recuperarse de un incidente de seguridad
    - ○ D) La protección de los datos contra el acceso no autorizado y su uso indebido

**Tema 5: Buenas Prácticas de Seguridad**

17. ¿Cuál de las siguientes acciones es una buena práctica para proteger la privacidad de los datos personales?
    - ○ A) Compartir datos personales en redes sociales
    - ○ B) Almacenar contraseñas en un archivo de texto sin cifrar
    - ○ C) Utilizar conexiones seguras (HTTPS) al enviar información confidencial
    - ○ D) Compartir información personal con desconocidos

18. ¿Qué es una "cookie" en el contexto de la seguridad de la información en línea?
    - ○ A) Un tipo de virus informático
    - ○ B) Un archivo que almacena información sobre la actividad del usuario en un sitio web
    - ○ C) Una técnica para cifrar mensajes de correo electrónico
    - ○ D) Un software para proteger la privacidad en línea

19. ¿Qué es un "ataque de ingeniería social"?
    - ○ A) Un ataque que utiliza la fuerza bruta para acceder a contraseñas
    - ○ B) Un ataque que intenta engañar a las personas para que revelen información confidencial
    - ○ C) Un ataque que utiliza malware para robar datos
    - ○ D) Un ataque que utiliza redes sociales para difundir spam

20. ¿Qué es la "seguridad de la red" y por qué es importante?
    - ○ A) Un programa de ejercicios físicos en el lugar de trabajo
    - ○ B) Un conjunto de medidas para proteger los datos y los sistemas informáticos contra amenazas cibernéticas
    - ○ C) Un método para protegerse contra incendios en el lugar de trabajo
    - ○ D) Un protocolo para enviar correos electrónicos cifrados

21. ¿Por qué es importante mantener el software actualizado en un dispositivo?
    - ○ A) Para reducir el espacio de almacenamiento
    - ○ B) Para mejorar el rendimiento del dispositivo
    - ○ C) Para corregir vulnerabilidades de seguridad
    - ○ D) Para aumentar la velocidad de conexión a internet
22. ¿Cuál es una medida efectiva para proteger una contraseña?
    - ○ A) Compartirla con amigos y familiares
    - ○ B) Utilizar la misma contraseña para múltiples cuentas
    - ○ C) Mantenerla en un archivo de texto en el escritorio
    - ○ D) Crear una contraseña única y compleja
23. ¿Por qué es importante no hacer clic en enlaces sospechosos en correos electrónicos?
    - ○ A) Porque pueden contener virus o malware
    - ○ B) Para aumentar el tráfico en el sitio web
    - ○ C) Porque pueden proporcionar acceso a descuentos exclusivos
    - ○ D) Para mejorar la seguridad de la cuenta de correo electrónico

**Tabla con las respuestas para el cuestionario:**

| Pregunta | Respuesta Correcta |
|---|---|
| 7 | B |
| 8 | B |
| 9 | B |
| 10 | B |
| 11 | B |
| 12 | A |
| 13 | B |
| 14 | B |
| 15 | A |
| 16 | A |
| 17 | C |
| 18 | B |
| 19 | B |
| 20 | B |
| 21 | C |
| 22 | D |
| 23 | A |

| | |
|---|---|
| **Proyecto:** | HERRAMIENTA WEB PARA EVALUACIÓN DE LA EFICACIA CON RESPECTO A LA FORMACIÓN EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA TODO EL PERSONAL, EN LAS INSTITUCIONES DEL SECTOR POPULAR Y SOLIDARIO DENTRO DEL SEGMENTO CUATRO Y CINCO, DE LA PROVINCIA DE IMBABURA. |
| **Autor:** | Marco Vinicio Terán Tabango |
| **Objetivo:** | Desarrollar una aplicación web para evaluar los conocimientos de los funcionarios de las instituciones financieras acerca de la seguridad y privacidad de la información basado la normativa de la superintendencia de economía popular y solidaria. |

| | |
|---|---|
| **Fecha de envío para la evaluación del experto:** | 15 de Abril de 2024 |
| **Fecha de revisión del experto:** | 01 de Mayo de 2024 |

## VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN (CUESTIONARIO - ENCUESTA)

**Instrucciones:** En la siguiente matriz marque con una X el criterio de evaluación según corresponda en cada ítem. De ser necesario realice la observación en el apartado correspondiente.

| **INSTRUMENTO DE EVALUACIÓN CUALITATIVO** | | | |
|---|---|---|---|
| **ITEMS** | **CRITERIOS DE EVALUACIÓN** | | |
| | **MUCHO** | **POCO** | **NADA** |
| Instrucción breve, clara y completa. | X | | |
| Formulación clara de cada pregunta. | X | | |
| Comprensión de cada pregunta. | X | | |
| Coherencia de las preguntas en relación con el objetivo. | X | | |
| Relevancia del contenido | X | | |
| Orden y secuencia de las preguntas | X | | |
| Número de preguntas óptimo | X | | |

Observaciones:

Las preguntas son claras y responden al objetivo del instrumento de investigación. Se debe considerar algunos comentarios en ciertas preguntas que a continuación se explica.

A continuación, marque con una X en el criterio de evaluación según el análisis de cada pregunta que conforma el cuestionario, las cuales se encuentran representadas en el siguiente instrumento de evaluación como ítem. De ser necesario realice la observación en el casillero correspondiente.

| **INSTRUMENTO DE EVALUACIÓN CUANTITATIVO** | | | | |
|---|---|---|---|---|
| **CRITERIOS DE EVALUACIÓN** | | | | **OBSERVACIONES** |
| **Ítem** | **Dejar** | **Modificar** | **Eliminar** | |
| 1 | X | | | |
| 2 | X | | | |
| 3 | X | | | |
| 4 | X | | | |
| 5 | X | | | |
| 6 | X | | | |
| 7 | X | | | |
| 8 | X | | | |
| 9 | | X | | Quitar la palabra “mejor” porque no se está comprobando que es mejor en base a qué criterio. |
| 10 | | X | | Se recomienda separar la pregunta. Está preguntando dos cosas diferentes en la misma pregunta eso confunde al encuestado. O puede mejorar la pregunta uniendo los dos criterios. |
| 11 | | X | | Se recomienda separar la pregunta. Está preguntando dos cosas diferentes en la misma pregunta eso confunde al encuestado. O puede mejorar la pregunta uniendo los dos criterios. |
| 12 | X | | | |
| 13 | | X | | Se recomienda separar la pregunta. Está preguntando dos cosas diferentes en la misma pregunta eso confunde al encuestado. O puede mejorar la pregunta uniendo los dos criterios. |
| 14 | | X | | Quitar la palabra “mejor” porque no se está comprobando que es mejor en base a qué criterio. |
| 15 | X | | | |
| 16 | X | | | |
| 17 | X | | | |
| 18 | X | | | |
| 19 | X | | | |
| 20 | | X | | Se recomienda separar la pregunta. Está preguntando dos cosas diferentes en la misma pregunta eso confunde al |

| | | | | |
|---|---|---|---|---|
| | | | | encuestado. O puede mejorar la pregunta uniendo los dos criterios. |
| 21 | X | | | |
| 22 | | X | | Quitar la palabra “efectiva” porque no se está comprobando que es efectivo en base a qué criterio. |
| 23 | X | | | |

1002334835 CATHY PAMELA GUEVARA VEGA
Firmado digitalmente por 1002334835 CATHY PAMELA GUEVARA VEGA
Fecha: 2024.05.01 07:57:55 -05'00'

.....

Firma del Evaluador
C.C.: 1002334835

| | |
|---|---|
| Apellidos y nombres completos | Guevara Vega Cathy Pamela |
| Título académico | Doctor en Ingeniería Informática |
| Institución de Educación Superior | Universidad de Sevilla |
| Correo electrónico | cguevara@utn.edu.ec |
| Teléfono | 0988313052 |