**Escuela Superior Politécnica del Litoral**

**Facultad de Ciencias Sociales y Humanísticas**

# DESARROLLO DE UNA HERRAMIENTA INTELIGENTE PARA EVALUAR UN SGSI EN PYMES DEL SECTOR ADUANERO EN GUAYAQUIL

ADMI – 1232

**Proyecto Integrador**

Previo la obtención del Título de:

**Licenciado en Auditoría y Control de Gestión**

**Presentado por:**

Clemente Parrales Melanny Brigitte

Cornejo Abad Jeremy Alexander

**Guayaquil - Ecuador**

2025

# Dedicatoria CM

En primer lugar, dedico este trabajo a Dios, por estar conmigo en todo este trayecto, pero especialmente en aquellos momentos en los que sentía que no podía más, por darme la fuerza y las oportunidades en donde me encuentro ahora. Sin tú guía nada de esto hubiera sido posible.

A mi mamá, que ha sido mi pilar, mi ejemplo y mi lugar seguro. Este logro es tuyo tanto como mío, porque desde el principio creíste en mí, me levantaste en esos días en los que yo misma dudaba de mí, por tu amor y apoyo incondicional no hubiera llegado hasta aquí.

A mi querido loro, a quien considero mi hijo, mi pequeño compañero de tantas clases y madrugadas de estudio, que con su compañía hizo más llevadero este proceso. Aunque ya no estés conmigo, siempre ocuparás un lugar especial en mi corazón y en este capítulo de mi vida.

**Clemente Parrales Melanny Brigitte**

# Dedicatoria CJ

Dedico este proyecto a Dios, promotor de todos los logros en mi vida, inspiración y calma aún en los momentos más inciertos, de quien viene todo lo bueno que hay en mí.

A mis padres, quienes con su propia dedicación hacia mí traspasaron barreras para darme un sinnúmero de posibilidades. Sus esfuerzos y amor son el fiel reflejo de todo lo que estoy logrando. Esto es para ustedes.

Dedico este proyecto a mis gatitos de la guarda, Lili y Toti, por mostrarme que lo más valioso que se puede tener es la compañía sincera.

A mis amigos y familia de la fe, quienes siempre estuvieron prestos a dar palabras de apoyo y ayudar en tiempos complicados, sin ustedes no estaría completo este apartado.

**Cornejo Abad Jeremy Alexander**

# Agradecimientos CM

Agradezco a Dios por darme la vida, salud y la capacidad de superar cada desafío, por no dejarme caer cuando las cosas se ponen difíciles, por darme la oportunidad de conocer a personas increíbles.

A mi querida madre que es mi inspiración en el día a día, por darme ese empujón que necesito, por apoyarme en cada decisión que tome. Aunque trato de encontrar las palabras adecuadas, ninguna parece suficiente para expresar todo, gracias por todo lo que has hecho por mí.

A mi loro, por ser mucho más que una mascota, aunque ya no estés físicamente, tu presencia sigue viva en mis recuerdos, en las risas, en las tardes juntos, y aunque ya no te vea, sigues siendo parte de este logro, como lo fuiste de cada paso que di.

A mis amigos, aquellos que conocí en el pre y que se quedaron hasta el final., siempre presentes con sus risas, sus consejos, y ese apoyo silencioso pero constante.

**Clemente Parrales Melanny Brigitte**

# Agradecimientos CJ

Doy gracias a Dios por la vida y la oportunidad de alcanzar muchas más metas en mi desarrollo profesional, gracias por poner a las personas indicadas y mostrarme que siempre estuve en el lugar correcto.

Agradezco a mis padres que con su apoyo han hecho que esta etapa de mi vida sea posible, en especial te agradezco a ti mamá porque no escatimaste nada y siempre eres el pilar que me sostenía en cada instante, gracias por tanto mamita.

Doy gracias a mi compañera Melanny por tan excelente trabajo realizado, por siempre buscar la excelencia.

Agradecer a mis docentes, a quienes ya puedo llamar colegas, por sus enseñanzas a lo largo de esta etapa que han hecho posible que hoy me convierta en un profesional.

Gracias Lili y Toti, por acompañarme siempre en las madrugadas de estudio, aunque físicamente no están conmigo, sé que por ustedes todo siempre se sintió menos vacío y más brillante.

**Cornejo Abad Jeremy Alexander**

# Declaración Expresa

Nosotros, Melanny Brigitte Clemente Parrales con CI 0925995144 y Jeremy Alexander Cornejo Abad con CI 0953406113, acordamos y reconocemos que:

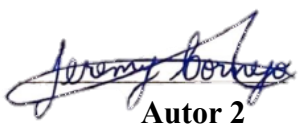
La titularidad de los derechos patrimoniales de autor (derechos de autor) del proyecto de graduación corresponderá al autor o autores, sin perjuicio de lo cual la ESPOL recibe en este acto una licencia gratuita de plazo indefinido para el uso no comercial y comercial de la obra con facultad de sublicenciar, incluyendo la autorización para su divulgación, así como para la creación y uso de obras derivadas. En el caso de usos comerciales se respetará el porcentaje de participación en beneficios que corresponda a favor del autor o autores.

La titularidad total y exclusiva sobre los derechos patrimoniales de patente de invención, modelo de utilidad, diseño industrial, secreto industrial, software o información no divulgada que corresponda o pueda corresponder respecto de cualquier investigación, desarrollo tecnológico o invención realizada por mí/nosotros durante el desarrollo del proyecto de graduación, pertenecerán de forma total, exclusiva e indivisible a la ESPOL, sin perjuicio del porcentaje que me/nos corresponda de los beneficios económicos que la ESPOL reciba por la explotación de mi/nuestra innovación, de ser el caso.

En los casos donde la Oficina de Transferencia de Resultados de Investigación (OTRI) de la ESPOL comunique al/los autores/es que existe una innovación potencialmente patentable sobre los resultados del proyecto de graduación, no se realizará publicación o divulgación alguna, sin la autorización expresa y previa de la ESPOL.

Guayaquil, 28 de mayo del 2025.

**Autor 1**



**Autor 2**

# Evaluadores


**Christian Vera Alcívar**

Profesor de Materia


**Jessica Espinoza Toala**

Tutor de proyecto

## Resumen

Las PYMES del sector aduanero en Ecuador enfrentan dificultades críticas para evaluar el cumplimiento de sus Sistemas de Gestión de Seguridad de la Información (SGSI) debido a la complejidad interpretativa de normativas especializadas, recursos económicos limitados y carencia de personal técnico especializado para prepararse ante auditorías externas obligatorias. Esta situación genera vulnerabilidades operativas y riesgos de sanciones regulatorias que comprometen la continuidad empresarial. El objetivo de este proyecto es desarrollar un chatbot de auditoría inteligente que facilite la autoevaluación del cumplimiento normativo, mejore la precisión en la detección de no conformidades y reduzca significativamente el tiempo y costos asociados a las auditorías. Se desarrolló un prototipo de alta fidelidad utilizando técnicas de IA, motor conversacional avanzado y formularios adaptativos con lógica condicional. La plataforma integró una base de datos con más de 150 criterios normativos de la LOPDP, COBIT 2019 y estándares BASC. La validación se realizó mediante escenarios controlados y situaciones empresariales reales con retroalimentación de expertos. Los resultados evidenciaron una reducción del 45% en tiempos de auditoría, precisión del 90% en detección de no conformidades y fortalecimiento sustancial de la confianza empresarial para enfrentar auditorías externas. El Bot transforma el cumplimiento normativo en un proceso accesible y eficiente, enriqueciendo la cultura organizacional de gestión de riesgos en PYMES aduaneras.

**Palabras clave:** chatbot, SGSI, IA, LOPDP, automatización.

**Abstract**

Small and medium enterprises (SMEs) in Ecuador's customs sector face critical challenges in evaluating compliance with their Information Security Management Systems (ISMS) due to the interpretative complexity of specialized regulations, limited economic resources, and lack of specialized technical personnel to prepare for mandatory external audits. This situation generates operational vulnerabilities and regulatory sanction risks that compromise business continuity. The objective of this project is to develop an intelligent audit chatbot that facilitates self-assessment of regulatory compliance, improves accuracy in detecting non-conformities, and significantly reduces time and costs associated with audits. A high-fidelity prototype was developed using AI techniques, advanced conversational engine, and adaptive forms with conditional logic. The platform integrated a database with over 150 regulatory criteria from LOPDP, COBIT 2019, and BASC standards. Validation was conducted through controlled scenarios and real business situations with expert feedback. Results showed a 45% reduction in audit times, 90% accuracy in detecting non-conformities, and substantial strengthening of business confidence in facing external audits. The bot transforms regulatory compliance into an accessible and efficient process, enriching the organizational culture of risk management in customs SMEs.

**Keywords:** chatbot, ISMS, AI, LOPDP, automation.

# ÍNDICE GENERAL

## Abreviaturas

| | |
|---|---|
| ESPOL | Escuela Superior Politécnica del Litoral |
| BASC | Business Alliance for Secure Commerce |
| ISMS | Information Security Management System |
| ISO | International Organization for Standardization |
| LOPDP | Ley Orgánica de Protección de Datos Personales |
| PYMES | Pequeñas y Medianas Empresas |
| SGSI | Sistema de Gestión de Seguridad de la Información |
| IA | Inteligencia Artificial |
| COBIT | Control Objectives for Information and Related Technologies |
| TI | Tecnologías de la Información |
| API | Application Programming Interface |
| CIA | Confidentiality, Integrity, Availability |
| KPI | Key Performance Indicator |
| SENAE | Servicio Nacional de Aduana del Ecuador |
| DT | Design Thinking |
| PDCA | Plan - Do - Check - Act |

## Índice de Figuras



## Índice de tablas

## Índice de Anexos

# Capítulo 1

## 1. Introducción

La transformación digital ha revolucionado la manera en que las organizaciones gestionan y protegen su información, posicionando la protección de datos como como un eje estratégico dentro del cumplimiento normativo. En un entorno donde las regulaciones de protección de datos se intensifican, las empresas enfrentan el desafío de adoptar Sistemas de Gestión de Seguridad de la Información (SGSI) que garanticen la conformidad con los marcos legales vigentes.

Las PYMES enfrentan particular vulnerabilidad en este panorama, ya que a menudo carecen de los recursos especializados y la infraestructura tecnológica necesaria para mantener estándares de seguridad comparables a los de las grandes corporaciones. Esta disparidad crea una brecha significativa en la capacidad de estas organizaciones para proteger información crítica y cumplir con marcos normativos legales cada vez más exigentes.

Esta brecha se amplifica cuando consideramos que la evaluación y auditoría de SGSI requiere procesos complejos, costosos y dependientes de expertise externo, factores que limitan el acceso de las PYMES a estas herramientas esenciales. No obstante, el avance de tecnologías emergentes como la inteligencia artificial y los sistemas conversacionales está abriendo nuevas posibilidades para facilitar el acceso a evaluaciones de seguridad de la información, ofreciendo alternativas más accesibles y automatizadas.

La alineación entre las necesidades empresariales actuales y el desarrollo tecnológico representa una oportunidad única para desarrollar soluciones innovadoras que transformen la gestión de la seguridad de la información, especialmente en sectores críticos donde el cumplimiento normativo es fundamental para la continuidad operativa, sino que también fortalece la confianza institucional y la competitividad en mercados regulados.

### 1.1. Descripción Del Problema

Las PYMES del sector de almacenamiento aduanero en Guayaquil, que representan la mayoría de los operadores logísticos autorizados por el SENAE, enfrentan serias limitaciones en la gestión de sus Sistemas de Gestión de Seguridad de la Información (SGSI). A pesar de operar en un entorno regulado por la LOPDP, el marco COBIT 2019 y los estándares BASC, carecen de metodologías accesibles para evaluar su nivel de cumplimiento.

La ausencia de herramientas dificulta realizar evaluaciones periódicas y verificar su alineación con las normativas vigentes. Esta situación se ve agravada por la dependencia de auditorías tradicionales, las cuales implican altos costos, conocimientos especializados y largos periodos de preparación, lo que las convierte en opciones poco viables para muchas PYMES. En consecuencia, estas organizaciones operan en condiciones de incertidumbre respecto a su situación normativa real.

Los riesgos asociados a esta problemática son sustanciales, pues el incumplimiento normativo puede resultar en multas que oscilan entre el 0,7% y 1% de los ingresos anuales para infracciones graves (Lexis S.A, 2025), además de sanciones que incluyen la suspensión de licencias operativas, lo que representa un riesgo existencial para estas empresas.

Ante esta brecha entre las obligaciones regulatorias y las capacidades de evaluación disponibles para las PYMES evidencia la necesidad urgente de desarrollar soluciones tecnológicas accesibles que faciliten la autogestión del cumplimiento de SGSI, reduciendo tanto los costos asociados como la complejidad técnica del proceso de auditoría.

### 1.2. Justificación del Problema

En el entorno altamente regulado del sector aduanero, la evaluación del cumplimiento normativo en los SGSI representa un desafío constante para las PYMES, quienes enfrentan serias dificultades para garantizar el cumplimiento con las normativas vigentes debido a la falta de mecanismos de evaluación.

Frente a esta realidad, el desarrollo de un asistente virtual basado en inteligencia artificial se presenta como una solución innovadora y pertinente, debido a que esta herramienta permitirá a las empresas realizar autoevaluaciones sistemáticas, reducir los costos asociados a auditorías externas y en la generación de reportes en tiempo real. De este modo, brindará un diagnóstico claro de su nivel de cumplimiento normativo y ofrecerá recomendaciones prácticas para su mejora continua.

Esta propuesta no solo contribuirá a fortalecer la cultura de seguridad de la información dentro de las organizaciones, sino que también incrementará la confianza de clientes y socios comerciales. Al proporcionar una herramienta que facilita la autoevaluación y la mejora continua, las empresas podrán anticiparse a brechas de cumplimiento y demostrar un compromiso activo con la normativa vigente.

Desde el enfoque profesional de la auditoría, esta herramienta representa una evolución significativa, al integrar inteligencia artificial en los procesos de revisión y control. En definitiva, el proyecto aporta a la modernización de las prácticas auditoras, promoviendo un enfoque más digital, proactivo y orientado a resultados sostenibles en seguridad de la información

### 1.3. Alcance

El proyecto desarrollará un asistente virtual mediante una interfaz conversacional que facilite la recopilación de información organizacional y evaluación automatizada de adherencia normativa. El alcance excluye implementación de medidas técnicas de seguridad, evaluación de amenazas cibernéticas y consultoría especializada en ciberseguridad.

La investigación se concentra únicamente en verificación documental y procedimental del cumplimiento normativo, desarrollando una herramienta de diagnóstico organizacional que evalúe adherencia a marcos regulatorios mediante revisión automatizada de políticas, procedimientos y documentación corporativa.

### 1.4. Objetivos

#### *1.4.1. Objetivo general*

Diseñar una herramienta inteligente de auditoría, basada en una interfaz dinámica y conversacional, que permita a las PYMES del sector aduanero la evaluación de la gestión de la información, generando reportes personalizados y recomendaciones adaptadas a los hallazgos, donde se fortalece la confianza de los clientes y el cumplimiento de los estándares regulatorios.

#### *1.4.2. Objetivos específicos*

- Realizar un análisis comparativo entre los requisitos normativos de la LOPDP, COBIT 2019 y BASC frente al estado actual de madurez de los SGSI en PYMES del sector aduanero, utilizando matrices de evaluación y entrevistas estructuradas, para la determinación los indicadores clave de rendimiento que serán automatizados en la herramienta conversacional.
- Construir un chatbot especializado en auditoría de SGSI empleando arquitectura basada en servicios y algoritmos de procesamiento de lenguaje natural, integrando bases de

conocimiento normativo con interfaces conversacionales adaptativas, para la realización de las evaluaciones automatizadas y contextualizadas.

- Transformar los datos de evaluación en dashboards ejecutivos y planes de acción automatizados, aplicando técnicas de visualización de datos y análisis de tendencias, facilitando la gestión estratégica de riesgos de seguridad de la información.
- Validar la efectividad de la herramienta mediante experimentación controlada con personal del sector aduanero, midiendo variables de rendimiento (tiempo de evaluación, precisión diagnóstica, calidad de recomendaciones), demostrando la viabilidad técnica y el valor agregado de la solución propuesta.

## 1.5. Marco teórico

### *1.5.1. Marco Conceptual*

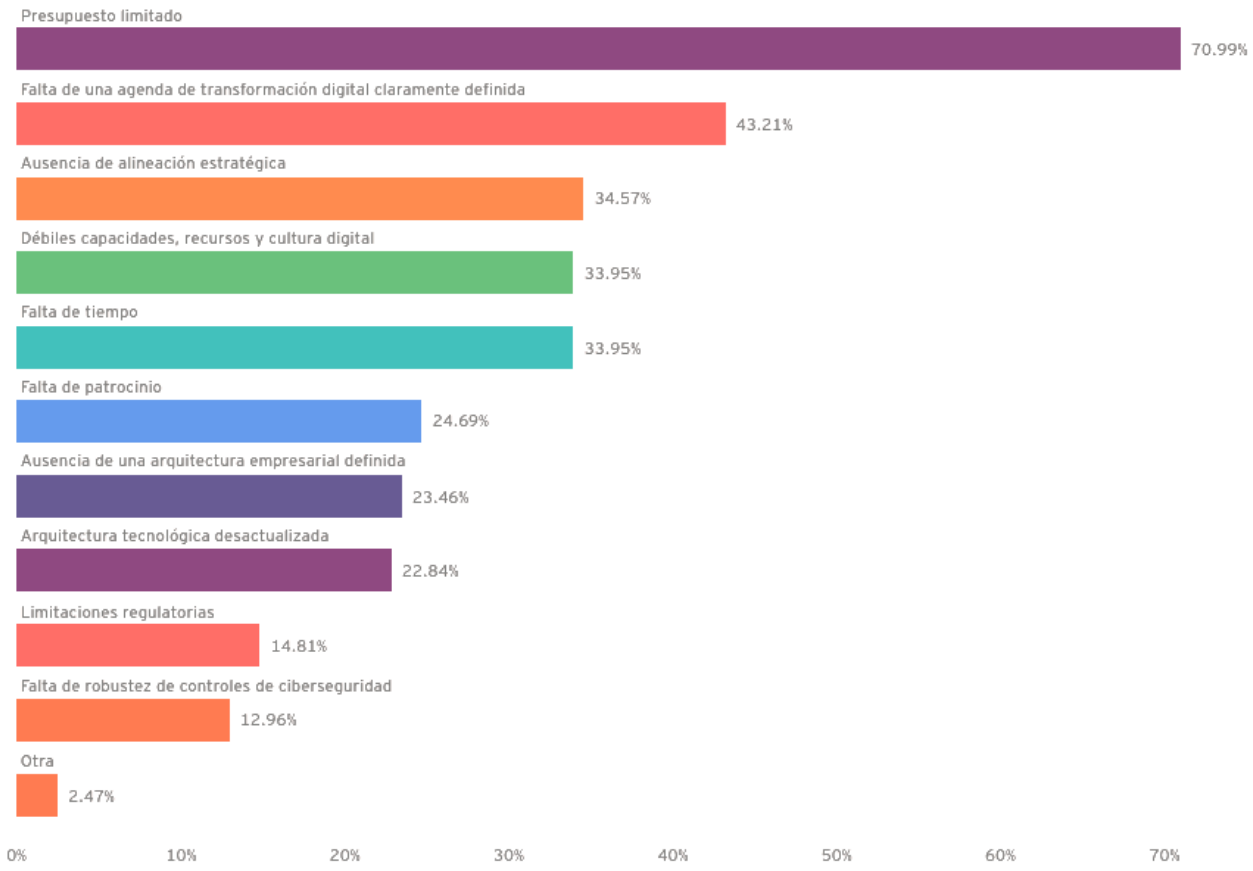
#### *1.5.1.1. Sistemas de Gestión de Seguridad de la Información (SGSI)*

Un SGSI, conforme a la norma SO/IEC 27001:2022 (ISO, 2022) es un enfoque sistemático para gestionar información sensible, garantizando su confidencialidad, integridad y disponibilidad mediante la aplicación de un proceso de gestión de riesgos. No obstante, la implementación práctica de un SGSI en PYMES presenta barreras como la escasez de personal técnico, la falta de conocimiento especializado y restricciones presupuestarias.

Según EY el 70.99% de las organizaciones indica que su mayor barrera para implementar tecnologías digitales es el presupuesto limitado, una realidad particularmente aguda en el sector de las pequeñas y medianas empresas. Esta limitación refuerza la necesidad de herramientas tecnológicas accesibles que optimicen la gestión de seguridad sin requerir una infraestructura costosa (EY & IT, 2024).

***Figura 1.***

*Principales Barreras y Desafíos que enfrentan ante una transformación digital*




*Nota.* Tomado de "Tendencias Tecnológicas 2024: Principales oportunidades para las organizaciones en el Ecuador" (p. 9), por EY & ITahora, 2024. Todos los derechos reservados.

#### *1.5.1.2.Inteligencia Artificial (IA)*

La Inteligencia Artificial es definida como la capacidad de sistemas computacionales para realizar tareas cognitivas complejas. Según (Popenici & Kerr, 2017) establecen que se refiere a "sistemas computacionales que son capaces de participar en procesos similares a los humanos como el aprendizaje, la adaptación, la síntesis, la autocorrección y el uso de datos para tareas complejas de procesamiento". Esta definición amplía el enfoque tradicional, destacando el potencial de la IA no solo como una herramienta técnica, sino como un sistema capaz de mejorar con la experiencia y adaptarse a nuevas necesidades organizacionales.

#### *1.5.1.3. Herramientas inteligentes en auditoría*

La evolución tecnológica ha propiciado la incorporación de herramientas inteligentes tales como formularios automatizados, chatbot y asistentes digitales en los procesos de auditoría de seguridad. Estas tecnologías permiten no solo recolectar información de manera estandarizada, sino también procesarla en tiempo real y generar informes automáticos de cumplimiento.

El estudio de (Franco et al., 2019) sobre el desarrollo de SANI, un asistente web para auditorías bajo ISO/IEC 27001, evidencia que este tipo de herramientas puede facilitar significativamente las auditorías internas, reducir costos operativos y garantizar la trazabilidad documental en organizaciones con recursos limitados.

A continuación, se presenta una tabla comparativa de las plataformas tecnológicas evaluadas para esta investigación, considerando sus ventajas, limitaciones y aplicabilidad al contexto de las PYMES del sector aduanero:

***Tabla 1.***

*Comparativa de herramientas de desarrollo de chatbot*

| Herramienta/ Plataforma | Tipo | Ventajas Clave | Limitaciones | Aplicabilidad al proyecto SGSI |
|---|---|---|---|---|
| **Rasa** | Framework open-source | Control total del flujo, integración con spaCy, adaptable a normas | Requiere conocimientos técnicos intermedios-avanzados | Alta: Expectativa base del chatbot |
| **Streamlit** | Framework web Python | Desarrollo rápido de visualizaciones | No es motor de conversación | Media: Útil para visualización |
| **Chatbase** | Plataforma SaaS | Conexión rápida con PDFs y URLs | Sin control del flujo ni personalización profunda | Media: Alternativa funcional |
| **Botpress** | Plataforma híbrida | Diseño visual de flujos, integración con IA | Complejidad de implementación y personalización | Media: Alternativa visual |
| **IBM Watson Assistant** | Plataforma empresarial | Motor NLP robusto, buena documentación, integración corporativa | Requiere suscripción y tiene menor flexibilidad | Alta: Evaluado profesionalmente |
| **Microsoft Power Virtual Agents** | Herramienta Microsoft | Integración con MS Teams y Power Platform, sin código | Limitado para lógicas complejas y normas específicas | Media: Útil para organizaciones Microsoft |
| **Checklist tools** | Formularios Excel / web | Evaluación detallada por controles normativos | Enfoque manual, sin generación de recomendaciones automatizadas | Alta como fuente de preguntas normativas |

#### *1.5.1.4.Chatbot / Bot Conversacional*

En la era digital y el fortalecimiento de los SGSI, los chatbots son herramientas clave para automatizar procesos y mejorar el cumplimiento normativo, al interactuar en tiempo real y adaptarse a distintos contextos. Según (Suha K.et al., 2023) son agentes conversacionales que usan procesamiento de lenguaje natural y aprendizaje automático. Existen chatbots basados en reglas, con respuestas limitadas, y chatbots con IA, que interpretan mejor el contexto.

Este proyecto eligió el chatbot tras comparar diferentes herramientas, ya que, estas alternativas presentaban limitaciones como formularios unidireccionales y poco personalizables, conocimientos técnicos y mayor inversión. En contraste, el chatbot ofrece accesibilidad, flexibilidad y escalabilidad, lo que lo convierte en una solución adecuada para las PYMES.

Por otro lado, la creciente adopción de esta tecnología a nivel global evidencia su relevancia estratégica. La siguiente imagen muestra el aumento sostenido en las búsquedas del término “chatbot” en Google Trends en los últimos años:

***Figura 2.***

*Tendencia de búsqueda del término “chatbot” según Google Trends*


*Nota.* La figura muestra el aumento en el interés por el término “chatbot”, lo que evidencia su creciente relevancia en entornos digitales.

### *1.5.2. Marco Metodológico*

#### *1.5.2.1. Revisión y Análisis de Metodologías Aplicables*

La revisión de metodologías aplicables se clasifica en las tradicionales y ágiles donde se evidencia dos paradigmas contrastantes: uno centrado en la secuencia y trazabilidad, mientras que el otro en la adaptabilidad, colaboración y pensamiento creativo.

Esta dualidad metodológica y la tendencia creciente sugiere la viabilidad de metodologías centradas en el usuario. Con el fin de contrastar ambos enfoques de manera clara, se presenta a continuación una tabla comparativa elaborada a partir de los aportes de Canós & Letelier (2012) y Cendejas, et al. (2015) que sintetiza sus principales diferencias metodológicas.

***Tabla 2.***

*Comparativo de metodologías Tradicionales VS Ágiles*

| Aspecto | Metodologías Ágiles | Metodologías Tradicionales |
|---|---|---|
| **Fundamento** | Se apoyan en **experiencias prácticas** derivadas del trabajo cotidiano en desarrollo de software. | Se basan en **normas y estándares formales** definidos por el entorno organizacional o industrial. |
| **Énfasis principal** | En las personas y la colaboración del equipo. | En la estructura del proceso: definición de roles, actividades y artefactos. |
| **Gestión del cambio** | Asumen el cambio como algo natural durante el proyecto. | Tienden a resistir los cambios una vez que el proceso ha sido definido. |
| **Relación contractual** | Contrato flexible, e incluso prescindible en algunos casos. | Contrato definido previamente y de cumplimiento estricto. |
| **Participación del cliente** | El cliente se involucra activamente en el desarrollo, como parte del equipo. | El cliente interactúa en momentos puntuales, por ejemplo, en reuniones. |
| **Estructura del equipo** | Equipos pequeños (> 10 personas), con roles versátiles y flexibles. | Equipos más grandes, con roles más definidos y especializados. |
| **Alcance del proyecto** | Adecuadas para proyectos pequeños, preferentemente en un mismo lugar físico. | Aplicables a proyectos de cualquier tamaño, especialmente grandes y complejos. |
| **Arquitectura del software** | Se construye y mejora de forma progresiva durante el desarrollo. | La arquitectura se define de forma anticipada y es considerada esencial desde el inicio. |

*Nota.* Elaboración propia a partir de Canós & Letelier (2012) y Cendejas et al. (2015).

Para profundizar en su aplicabilidad, se retoma el estudio de (López Gil, 2018) quien realizó un análisis estadístico y bibliográfico sobre la aplicabilidad de metodologías ágiles y tradicionales en proyectos de desarrollo de software, destacando factores críticos de éxito (FCE), donde se empleó una escala de valoración del 1 al 3 para calificar el grado de integración de cada criterio, donde el 3 representa una integración plena y el 1 una ausencia significativa.

Esta clasificación permite visualizar las fortalezas y limitaciones de cada metodología. A continuación, se presenta la matriz comparativa que sintetiza estos resultados.

***Figura 3.***

*Análisis comparativo de enfoques metodológicos frente a los FCE*

| | METODOLOGÍAS TRADICIONALES | | | | METODOLOGÍAS ÁGILES | | |
|---|---|---|---|---|---|---|---|
| **FACTORES CRÍTICOS DE ÉXITO** | **PMP** | **IPMA** | **ISO 21500** | **PRINCE2** | **SCRUM** | **XP** | **DSDM** |
| **PROCESOS** | **13** | **12** | **13** | **12** | **17** | **17** | **17** |
| 1. Calendarización realista | 2 | 2 | 2 | 2 | 3 | 3 | 3 |
| 2. Adecuada planeación y especificaciones | 3 | 2 | 3 | 3 | 3 | 3 | 3 |
| 3. Recursos suficientes | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 4. Buena comunicación | 2 | 2 | 2 | 1 | 3 | 3 | 3 |
| 5. Tiempo | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| 6. Reuniones diarias | 1 | 1 | 1 | 1 | 3 | 3 | 3 |
| **RECURSOS HUMANOS** | **17** | **18** | **16** | **14** | **23** | **26** | **24** |
| 7. Apoyo de la dirección | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 8. Liderazgo | 3 | 3 | 2 | 3 | 3 | 3 | 2 |
| 9. Desarrollo de los gerentes | 2 | 3 | 2 | 1 | 2 | 2 | 2 |
| 10. Habilidades básicas | 3 | 1 | 3 | 1 | 2 | 3 | 2 |
| 11. Desarrollo de sus empleados | 1 | 3 | 1 | 1 | 3 | 3 | 2 |
| 12. Involucramiento del usuario | 1 | 1 | 1 | 1 | 2 | 3 | 3 |
| 13. Involucramiento de los participantes | 1 | 1 | 1 | 1 | 2 | 2 | 3 |
| 14. Responsabilidad y compromiso del cliente | 1 | 1 | 1 | 1 | 2 | 3 | 3 |
| 15. Equipos auto-organizados | 1 | 1 | 1 | 1 | 3 | 3 | 2 |
| 16. Equipos con experiencia y conocimiento | 2 | 2 | 2 | 2 | 2 | 2 | 3 |
| **OBJETIVOS Y ALCANCE** | **13** | **10** | **10** | **11** | **12** | **12** | **12** |
| 17. Definición clara de requerimientos | 3 | 3 | 2 | 2 | 3 | 3 | 3 |
| 18. Metas intermedias alcanzables | 1 | 2 | 1 | 2 | 3 | 3 | 3 |
| 19. visión y objetivos claros | 3 | 2 | 2 | 3 | 2 | 2 | 2 |
| 20. Alcance del trabajo bien definido | 3 | 1 | 3 | 2 | 2 | 2 | 2 |
| 21. Tamaño del proyecto | 3 | 2 | 2 | 2 | 2 | 2 | 2 |
| **CALIDAD** | **5** | **5** | **4** | **6** | **8** | **8** | **9** |
| 22. Monitoreo apropiado y retroalimentación | 3 | 3 | 2 | 3 | 3 | 3 | 3 |
| 23. Calidad de las fuentes de datos | 1 | 1 | 1 | 1 | 2 | 2 | 3 |
| 24. Entregas parciales | 1 | 1 | 1 | 2 | 3 | 3 | 3 |
| **TECNOLOGÍA E INNOVACIÓN** | **4** | **4** | **4** | **5** | **8** | **8** | **6** |
| 25. Tecnología apropiada | 1 | 1 | 1 | 2 | 3 | 3 | 2 |
| 26. Conocimientos técnicos de los usuarios | 2 | 2 | 2 | 2 | 3 | 3 | 2 |
| 27. Disponibilidad tecnológica | 1 | 1 | 1 | 1 | 2 | 2 | 2 |
| **TOTAL** | **104** | **98** | **94** | **96** | **136** | **142** | **136** |

*Nota.* Comparación de metodologías en función de FCE en cinco dimensiones. Tomado de *Estudio comparativo de metodologías tradicionales y ágiles para proyectos de desarrollo de software* (p.119) por López, A.

#### *1.5.2.2. Matriz de Selección Metodológica*

La adecuada selección de una metodología es un factor determinante en el éxito de los proyectos que requieren soluciones tecnológicas y de gestión. Con el objetivo de realizar una elección fundamentada, se llevó a cabo un análisis centrado en seis criterios de evaluación que son relevantes en entornos organizacionales, como se evidencia en la siguiente tabla:

***Tabla 3.***

*Criterios de Evaluación y Ponderación de Metodologías*

| Criterio | Definición | Peso |
|---|---|---|
| **Rigor Científico** | Grado de estructuración metodológica y validación empírica | 25% |
| **Flexibilidad Adaptativa** | Capacidad para responder a cambios en requerimientos y contexto | 20% |
| **Centrismo en Usuario** | Nivel de enfoque en necesidades del usuario final | 20% |
| **Mejora Continua** | Capacidad para facilitar optimización iterativa | 15% |
| **Aplicabilidad PYMES** | Adecuación para recursos y estructuras limitadas | 10% |
| **Integración Normativa** | Facilidad para incorporar estándares y marcos regulatorios | 10% |

*Nota.* Cada criterio fue definido y ponderado en base a evidencia documental relevantes para el presente estudio. Elaboración propia

Por lo tanto, se evaluó tres enfoques metodológicos que parten de tradicionales, ágil y centrado al usuario como: Cascada, Scrum, y la combinación de PDCA con Design Thinking. A cada enfoque se le asignaron puntuaciones basadas en marcos normativos y referencias bibliográfica a partir de un análisis crítico.

**Escala de Evaluación**: 5 (Excelente) - 4 (Bueno) - 3 (Adecuado) - 2 (Limitado) - 1 (Inadecuado)

***Tabla 4.***

*Matriz de Selección Metodológicas*

| Criterio de Evaluación | Cascada | Scrum | PDCA + DT |
|---|---|---|---|
| Flexibilidad adaptativa | 2 | 4 | 5 |
| Rigor científico | 3 | 2 | 3 |
| Centrismo en usuario | 1 | 3 | 5 |
| Mejora continua | 2 | 3 | 5 |
| Aplicabilidad PYMES | 3 | 4 | 5 |
| Integración normativa | 2 | 3 | 5 |
| **Puntuación Ponderada** | **2.17** | **3.** | **4.67** |

#### *1.5.2.3.Justificación de la Metodología Integrada Seleccionada*

Los resultados evidenciados de la *Tabla 4*, permiten concluir que la combinación de PDCA con DT, integra las fortalezas de ambas metodologías en el que se potencia la capacidad de resolución e innovación. Esta decisión se fundamenta en dos pilares claves.

- **Pilar I | Sinergia Estructural:** La integración de ambas se basa en una integración estratégica, donde PDCA necesita insumos creativos para redefinir problemas, mientras que DT requiere marcos sistemáticos para validar soluciones donde se combina la sensibilidad al usuario con rigor metodológico.
- **Pilar II | Adaptabilidad:** En 221 casos analizados de diferentes tipos de proyectos, la integración con marcos estructurados aumentó la tasa de éxito en un 34% frente a implementaciones aisladas. Esto valida que la flexibilidad del DT no se pierde al integrarse, sino que se potencia (Dell'Era C et al, 2025).

### *1.5.3. Marco Referencial*

La automatización de procesos de evaluación en SGSI ha evolucionado de enfoques técnicos hacia propuestas metodológicas. (Sánchez & Villafranca, 2007) desarrollaron SCMM-TOOL para PYMES, demostrando que la gestión de seguridad de la información requiere herramientas con baja carga operativa, dada la limitada disponibilidad de recursos humanos y técnicos en este segmento. Este hallazgo refuerza la necesidad de diseñar evaluaciones automatizadas centradas en las capacidades del usuario final, alineándose a la filosofía del DT.

Esta perspectiva se materializa en el trabajo de (Franco et al., 2019) quienes desarrollaron SANI, una herramienta web de auditoría basada en ISO/IEC 27001. Su implementación en entornos reales evidenció que es posible equilibrar sofisticación técnica y accesibilidad, permitiendo a las PYMES realizar auditorías internas sin conocimientos especializados. Sin embargo, carece de mecanismos para implementar y dar seguimiento a las recomendaciones, lo que señala la necesidad de marcos que consoliden la mejora continua. Así mismo (López et al, (s.f.)) propusieron un modelo para evaluar el desempeño de controles SGSI combinando el método Delphi. Sus resultados demuestran que la automatización puede alcanzar alto rigor científico cuando se sustenta en metodologías de validación robustas y en la integración de experticia humana.

Complementariamente, (Ghazanfari et al., 2011) desarrollaron un modelo de evaluación con 34 criterios agrupados en seis factores clave, validados mediante análisis factorial y presentados en dashboards. Su propuesta confirma que evaluaciones complejas pueden sistematizarse sin perder claridad. No obstante, al concebir la evaluación como un evento único, no aborda la implementación iterativa de mejoras, lo que sustenta la integración del ciclo PDCA como marco de mejora continua en evaluaciones automatizadas.

La incorporación de IA en evaluaciones organizacionales es ilustrada por (Zhu, 2025) en un sistema inteligente de gestión deportiva que, mediante redes neuronales y sensores inalámbricos, mejora un 45% la precisión predictiva gracias a interfaces dinámicas y análisis automatizado, por consiguiente, muestra que el valor diferencial surge de ciclos de retroalimentación y aprendizaje continuo. (Al-Amin, et al., 2024) confirman que las PYMES pueden adoptar IA con éxito cuando la herramienta se alinea a sus limitaciones y contexto operativo. Sin embargo, incluso en casos exitosos, señalan la necesidad de evaluar continuamente la efectividad y ajustar parámetros.

En el sector aduanero, (Mozer & V, 2019) plantea que la “aduana digital” exige cumplimiento estricto de ISO 27000 y coordinación internacional, equilibrando optimización de procesos, transparencia y adaptación regulatoria. (Valderrama, 2025) demuestra que las herramientas inteligentes mejoran la gestión de riesgos y decisiones en tránsito aduanero cuando consideran las particularidades del sector.

La convergencia de estas investigaciones confirma la viabilidad técnica de herramientas automatizadas, el rigor metodológico alcanzable, la sofisticación de sistemas adaptativos y la relevancia del contexto regulatorio. No obstante, persisten tres vacíos: ausencia de mecanismos sistemáticos para implementar mejoras derivadas de evaluaciones, desconexión entre sofisticación técnica y adoptabilidad en PYMES, y fragmentación entre herramientas y marcos regulatorios. En respuesta a estas limitaciones la integración Design Thinking–PDCA emerge como una alternativa que capitaliza las fortalezas demostradas.

### *1.5.4. Marco Legal*

#### *1.5.4.1. Fundamentos Constitucionales*

La Constitución de la República del Ecuador establece en su artículo 261, numeral 5, la competencia exclusiva del Estado en materia aduanera, lo que fundamenta el marco regulatorio específico del sector y legitima la supervisión estatal de los almacenes y depósitos aduaneros. (Constitución de la República del Ecuador, 2008)

Complementariamente, el artículo 66, numeral 19, garantiza el derecho a la protección de datos de carácter personal, estableciendo los principios constitucionales que rigen el tratamiento de información. Este fundamento resulta esencial para el desarrollo del chatbot propuesto, ya que durante sus evaluaciones de cumplimiento normativo procesará datos sensibles que deben ser gestionados conforme a los principios de consentimiento, seguridad y confidencialidad.

#### *1.5.4.2.Régimen Aduanero - COPCI*

El Código Orgánico de la Producción, Comercio e Inversiones (COPCI, 2010) constituye la norma principal que regula las actividades aduaneras en Ecuador. En su capítulo VII en los artículos 147 al 153, define el régimen de almacenes y depósitos aduaneros, estableciendo las clasificaciones, procedimientos y obligaciones que constituyen los criterios de evaluación base del chatbot.

#### *1.5.4.3.Ley Orgánica de Protección de Datos Personales (LOPDP)*

(LOPDP, 2021) establece el régimen jurídico aplicable al tratamiento de datos personales en Ecuador. Los artículos 9 al 12 definen los principios de licitud, lealtad, transparencia y minimización de datos que deben ser incorporados en el diseño del chatbot, mientras que los artículos 44 al 46 regulan las transferencias internacionales de datos, aspecto crítico considerando que muchas PYMES del sector aduanero manejan información de operaciones

comerciales transfronterizas. Esta regulación define simultáneamente los parámetros técnicos de seguridad que la herramienta debe cumplir como requisito operativo y los criterios de evaluación que permitirán al chatbot verificar el cumplimiento de protección de datos reforzando la confianza en el proceso de auditoría automatizada.

#### *1.5.4.4. Norma BASC (Business Alliance for Secure Commerce)*

(BASC, 2022) constituyen un sistema de gestión en control y seguridad enfocado en el comercio internacional, aplicable directamente al sector de almacenamiento aduanero. La versión 6.0 representa la conexión estratégica entre cumplimiento normativo y competitividad comercial. Al incorporar BASC en los algoritmos de evaluación, la herramienta trasciende la verificación de conformidad para orientar a las PYMES hacia certificaciones que mejoran sustancialmente su posicionamiento en cadenas globales de suministro, transformando así el cumplimiento regulatorio de una carga operativa en una estrategia de diferenciación comercial.

#### *1.5.4.5.Control Objectives for Information and Related Technologies (COBIT)*

(ISACA, 2018) El COBIT es un marco de gobierno y gestión de las tecnologías de la información desarrollado por ISACA, cuyo propósito es alinear el uso de TI con los objetivos estratégicos de la organización, optimizar el valor de la información y gestionar los riesgos asociados. Su estructura integra principios, objetivos de gobierno y gestión, así como modelos de madurez que permiten medir y mejorar el desempeño de los sistemas de gestión.

#### *1.5.4.6.Marco de la Organización Mundial de Aduanas (OMA)*

La (OMA, 2021), a través del Marco Normativo SAFE busca asegurar y facilitar el Comercio Global, donde se incorporan exigencias específicas sobre sistemas de información y ciberseguridad, abarcando la integridad de los datos comerciales, la protección frente a accesos no autorizados y la trazabilidad de la información en la cadena de suministro.

# Capítulo 2

# 2. Metodología

## 2.1. Enfoque Metodológico

El presente estudio adoptó un enfoque aplicado, donde combinó técnicas cualitativas, que permitieron comprender las necesidades y limitaciones del entorno, y cuantitativas, que posibilitaron medir el desempeño del prototipo y su alineación con los estándares normativos.

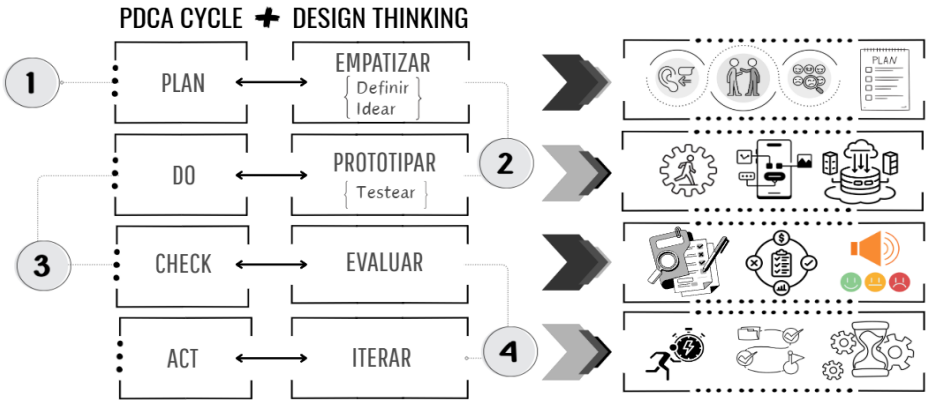
Esta decisión metodológica aseguró que la propuesta tecnológica respondiera tanto a la realidad operativa como a los requisitos técnicos exigidos por normas como la LOPDP, la ISO 27001, el BASC y el COBIT 2019.

## 2.2. Diseño de la Investigación

A partir de este enfoque, se adoptó un diseño híbrido que integra el ciclo de mejora continua PDCA (*Plan – Do – Check – Act*) con las fases del Design Thinking. Este diseño no solo favorece la construcción de un producto funcional, sino que también asegura que cada iteración incorpore retroalimentación real, manteniendo la pertinencia y efectividad de la herramienta. La metodología general se resume en la siguiente ilustración.

***Figura 4.***

*Pasos de la Metodología*




Nota: Fases de la metodología híbrida PDCA + Design Thinking | Elaboración propia.

### 2.3. Unidad de análisis

La investigación se desarrolló en *Cargo Service*, una organización del sector de almacenamiento aduanero ubicada en Guayaquil. Su contexto operativo reflejaba las condiciones comunes de muchas PYMES del sector: limitaciones presupuestarias, procesos parcialmente digitalizados y una necesidad explícita de evaluar periódicamente su nivel de cumplimiento en materia de seguridad de la información.

### 2.4. Procedimiento Metodológico

El procedimiento metodológico se articuló en cuatro fases secuenciales que enlazan la recolección de información, el diseño del prototipo, su validación y su mejora continua:

#### *2.4.1. Fase PLAN - Planificar - Empatizar, Definir e Idear*

Durante esta fase se aplicaron técnicas cualitativas orientadas a comprender las necesidades, frustraciones y expectativas de los usuarios involucrados. El procedimiento incluyó entrevistas semiestructuradas en profundidad con actores clave como Fabrizzio Muzo quien es el encargado del *Departamento Comercial y Auditor Interno* de la organización. ***(Véase Anexo A)***

Las entrevistas se estructuraron 4 módulos ***(Véase Anexo B)***:

- Experiencia actual en auditoría y evaluación SGSI
- Herramientas utilizadas y limitaciones actuales
- Principales desafíos en gestión de cumplimiento
- Expectativas de automatización e innovación

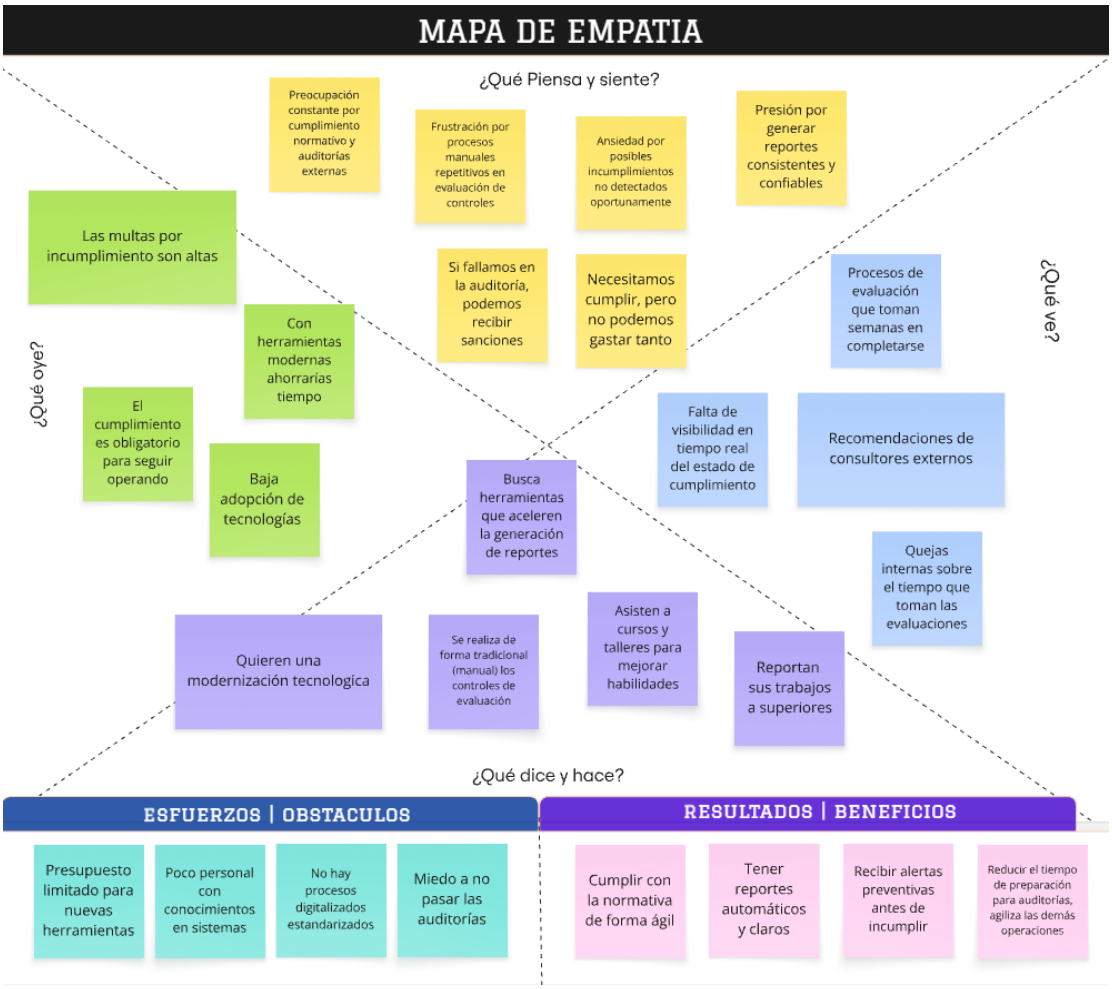
##### *2.4.1.1. Síntesis de los Hallazgos*

A partir de la información obtenida de las entrevistas, se construyó un mapa de empatía que permitió sintetizar los hallazgos y definir con precisión el problema a resolver.

Esta fase sentó las bases para el diseño de la solución, alineando los objetivos del desarrollo con las necesidades reales de los usuarios.

***Figura 5.***

*Mapa de Empatía - Cargo Service*




El mapa de empatía evidenció tres aspectos fundamentales: la tensión emocional entre la presión por cumplir y la ansiedad por posibles incumplimientos no detectados, las limitaciones operativas que contrastan con las expectativas de modernización tecnológica, y la demanda clara por automatización y visibilidad en tiempo real del estado de cumplimiento. Estos insights validaron los supuestos iniciales del problema de investigación y proporcionaron los criterios base para el posterior análisis de requisitos funcionales y no funcionales del sistema.

#### *2.4.1.2.Análisis de Requisitos*

Con base en los hallazgos del mapa de empatía y las necesidades identificadas durante las entrevistas, se procedió a definir y categorizar los requisitos del sistema en dos categorías:

- **Requisitos funcionales (RF):** funcionalidades específicas que debe cumplir el chatbot (ej. procesamiento de lenguaje natural, generación de scoring, Interfaz conversacional).
- **Requisitos no funcionales (RNF):** atributos de calidad que garantizan la confiabilidad y sostenibilidad del sistema (ej. Tiempo de respuesta, disponibilidad, usabilidad).

***Tabla 5.***

*Matriz de Requisitos Funcionales y No Funcionales*

| ID | Requisito | Descripción | Prioridad | Criterio de Aceptación |
|---|---|---|---|---|
| **Requisitos Funcionales** | | | | |
| **RF01** | Procesamiento de lenguaje natural | Comprensión de consultas sobre SGSI en español | Alta | Precisión ≥ 90% en clasificación de intenciones |
| **RF02** | Generación de scoring inteligente | Cálculo automático del nivel de cumplimiento | Alta | Consistencia ≥ 95% vs evaluación manual experto |
| **RF03** | Interfaz conversacional | Chat natural para consultas SGSI | Media | Compresión ≥ 85% de consultas típicas |
| **RF04** | Reportes automáticos | Generación de informes personalizados | Media | Formatos PDF institucionales |
| **RF05** | Dashboard en tiempo real | Visualización del estado actual de cumplimiento | Media | Actualización automática de métricas |
| **RF06** | Sistema de alertas | Notificaciones proactivas sobre riesgos | Media | Detección de tendencias negativas en 7 días |
| **Requisitos No Funcionales** | | | | |
| **RF01** | Tiempo de respuesta | Velocidad de procesamiento del chatbot | Alta | < 3 segundos para 95% de consultas |
| **RNF02** | Disponibilidad | Disponibilidad del sistema 24/7 | Alta | ≥ 99% Disponibilidad |
| **RNF03** | Usabilidad | Facilidad de uso del chatbot | Alta | Escala de Usabilidad ≥ 70 puntos |
| **RNF04** | Seguridad | Protección de información sensible del SGSI | Alta | Autenticación + logs auditoría |
| **RNF05** | Precisión técnica | Exactitud en evaluaciones SGSI | Alta | Margen error ≤ 5% vs auditor experto |

### *2.4.2. Fase DO (Hacer) - Prototipar y Testear*

Tras el análisis profundo realizado en la Fase PLAN, la Fase DO se orienta a transformar los hallazgos obtenidos en una solución funcional, alineada con los requerimientos normativos y las expectativas del usuario. Esta etapa parte de los insights derivados del mapa de empatía y las entrevistas semiestructuradas realizadas en Cargo Service, que evidenciaron limitaciones concretas en la interpretación de marcos normativos, la escasez de herramientas accesibles para pequeñas y medianas empresas, y la necesidad de retroalimentación inmediata sobre el estado de cumplimiento organizacional.

El objetivo central de esta fase consiste en construir y validar un prototipo funcional que evalúe el cumplimiento normativo de Sistemas de Gestión de Seguridad de la Información mediante interacción conversacional natural. Esta aproximación responde directamente a las frustraciones identificadas en la fase anterior: la dificultad para interpretar requisitos normativos complejos, la falta de herramientas especializadas accesibles para PYMES, y la necesidad de obtener retroalimentación inmediata sobre el estado de cumplimiento organizacional.

#### *2.4.2.1.Diseño conceptual*

El sistema conversacional desarrollado en esta fase se concibe como un asistente virtual especializado en evaluación normativa, diseñado para facilitar el diagnóstico de cumplimiento SGSI en organizaciones con recursos limitados.

Para humanizar la experiencia de interacción y fortalecer la percepción de confianza, se asignó al sistema la denominación E.V.A (Especialista Virtual de Auditoría). Esta denominación refleja la función central del chatbot como especialista automatizado en evaluación de marcos normativos de seguridad de la información, mientras que su carácter virtual destaca la innovación tecnológica aplicada al proceso tradicional de auditoría.

#### *2.4.2.2.Principios de diseño que orientaron la elección del nombre*

Diversos estudios han demostrado que la incorporación de elementos antropomórficos y atributos de inteligencia percibida en asistentes virtuales mejora significativamente la experiencia del usuario, especialmente en términos de empatía, confianza y claridad funcional (Ma et al., 2025). Estos principios orientan el diseño del sistema conversacional desarrollado en esta fase, concebido como un especialista virtual en evaluación normativa.

A partir de esta base, se definieron tres principios clave que guían la construcción de la identidad del sistema:

- **Antropomorfización:** La asignación de una identidad humanizada facilita la conexión emocional con el usuario, reduciendo la resistencia tecnológica y promoviendo una interacción más natural.
- **Confianza:** El sistema debe transmitir precisión, eficiencia y confiabilidad, cualidades esenciales en contextos de auditoría automatizada.
- **Claridad funcional:** El acrónimo comunica inmediatamente la propuesta de valor del sistema como especialista en auditoría virtual.

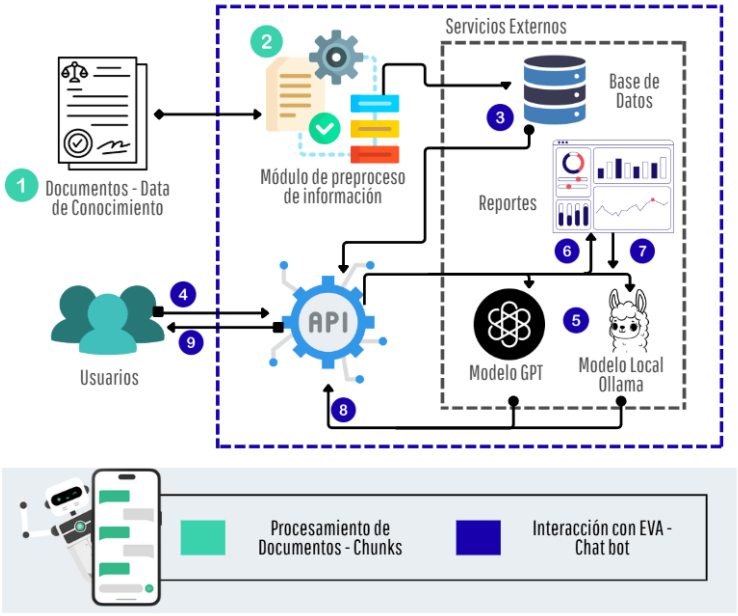
EVA actúa como mediadora entre el conocimiento normativo y las necesidades operativas de las PYMES, guiando al usuario a través de un proceso de autodiagnóstico estructurado y generando recomendaciones alineadas con su nivel de madurez organizacional.

#### *2.4.2.3.Arquitectura*

En esta sección se procederá a presentar la arquitectura de EVA, donde esta fase constituye el fundamento técnico que permite transformar los requerimientos funcionales en una solución operativa.

***Figura 6.***

*Arquitectura de EVA*




Primero se deben preparar los documentos en el módulo de preprocesamiento de información y cargarlos en la base de datos, siguiendo los pasos descritos a continuación:

1. Se insertarán los documentos normativos (ISO/IEC 27001:2022, COBIT 2019, BASC y LOPDP) en EVA. El módulo de preprocesamiento leerá y extraerá la información relevante dividiéndola en fragmentos (chunks) utilizables.
2. Una vez extraídos los fragmentos, estos se almacenarán en la base de datos.

Después de cargar los datos, se dispondrá de la API para que los usuarios puedan interactuar con el chatbot. El flujo general de interacción se detalla de la siguiente manera:

1. Los usuarios ingresarán preguntas o responderán el cuestionario inicial mediante la interfaz construida.
2. La API procesará la entrada del usuario, verificando que se ajuste a los parámetros establecidos como los tokens disponibles. Posteriormente, consultará la base de datos para recuperar los fragmentos más relevantes.

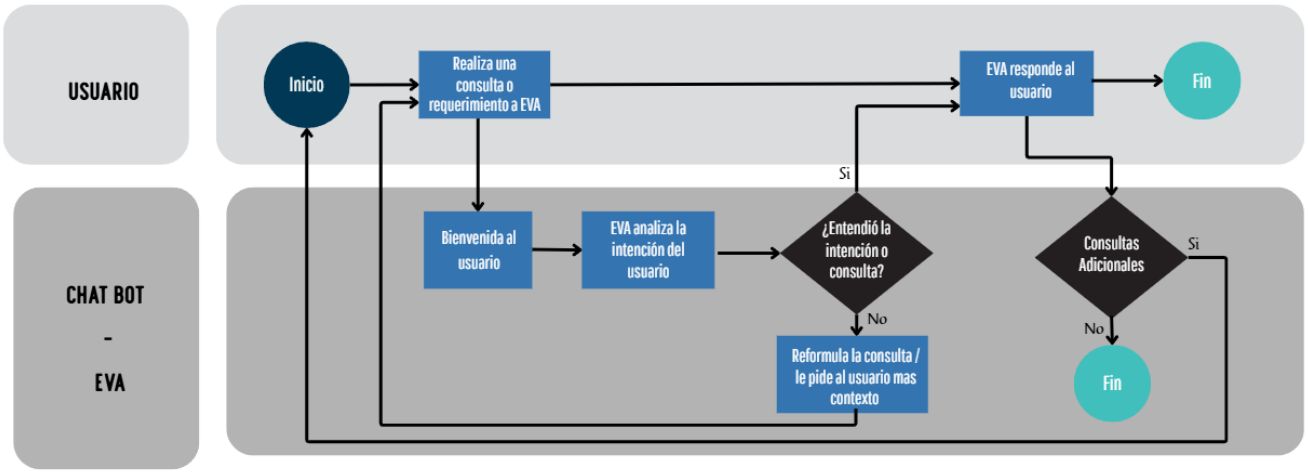
3. Con los fragmentos seleccionados se construirá el prompt final, es decir la generación del cuestionario para sondear los niveles de cumplimiento de los SGSI, el cual se enviará al modelo de lenguaje para su procesamiento.
4. El modelo generará las preguntas y su respectiva respuesta en caso de que el usuario manifieste dudas o confusión, por lo que el asistente reformulará utilizando un lenguaje más accesible, que será almacenada en la base de datos junto con el historial de interacción.
5. La respuesta será devuelta a la interfaz del usuario, incluyendo elementos visuales como barras de progreso de cumplimiento, indicadores KPI y recomendaciones específicas.
6. Finalmente, al cierre de la sesión, el sistema generará un reporte con los resultados, el cual incluirá: Nivel de cumplimiento, Gráficos de porcentajes y recomendaciones.

#### *2.4.2.4.Diagrama de Flujo*

Este esquema permite visualizar las decisiones clave que guían la interacción entre el usuario y el asistente, tal como se evidencia en la *Figura 7.*

***Figura 7.***

*Diagrama de Flujo de Interacción Usuario & EVA*



#### *2.4.2.5.Desarrollo de Prototipos*

El desarrollo de EVA siguió un enfoque evolutivo mediante dos prototipos secuenciales.

**Prototipo 1: Implementación en Chatbase.co**

En la implementación del Bot se utilizó Chatbase.co como plataforma base, por su capacidad para procesar documentos extensos mediante tecnología RAG (Retrieval-Augmented Generation). Esta elección se fundamentó en la necesidad de validar la viabilidad técnica de transformar documentos normativos estáticos (ISO/IEC 27001:2022, COBIT 2019, Norma BASC y LOPDP) en una base de conocimiento conversacional funcional.

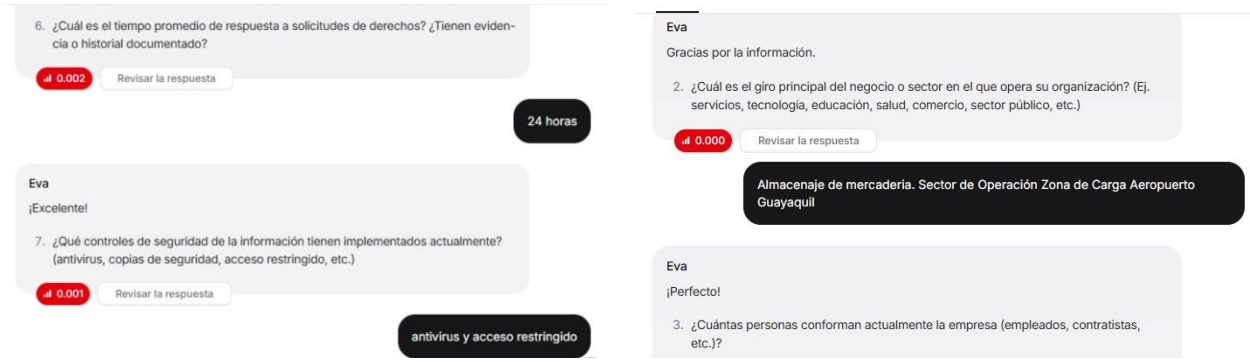
El proceso de implementación comenzó estableciendo los parámetros básicos de conversación y definiendo las estructuras de diálogo que permitirían una interacción fluida con los usuarios. Durante esta etapa, se realizaron pruebas internas para verificar la correcta carga y procesamiento de los documentos normativos, asegurando que EVA pudiera extraer información relevante y presentarla de manera coherente y comprensible.

Durante las primeras pruebas con usuarios reales de Cargo Service, EVA se encontraba limitada a las preguntas que el equipo desarrolló, lo que permitió evaluar la comprensión del usuario y validar el flujo conversacional inicial.  Estas sesiones revelaron aspectos importantes sobre la forma en que los colaboradores interactuaban con el sistema, identificando patrones de preferencias que posteriormente influyeron en el refinamiento de la interfaz conversacional.

Con base en la retroalimentación obtenida, se incorporaron mejoras significativas como la visualización de barras de progreso, que permitió a los usuarios mantener una percepción clara de su avance en el proceso de evaluación. Esta característica resultó especialmente valorada por el personal de Cargo Service.

***Figura 8.***

*Prototipo en ChatBase.co*




**Prototipo 2: Migración a Microsoft Copilot**

La evolución hacia Microsoft Copilot como segunda plataforma respondió a las limitaciones identificadas en el prototipo inicial y a la necesidad de implementar capacidades de razonamiento contextual más sofisticadas. Esta migración permitió desarrollar un modelo conversacional con mayor capacidad de análisis semántico y generación de recomendaciones personalizadas.

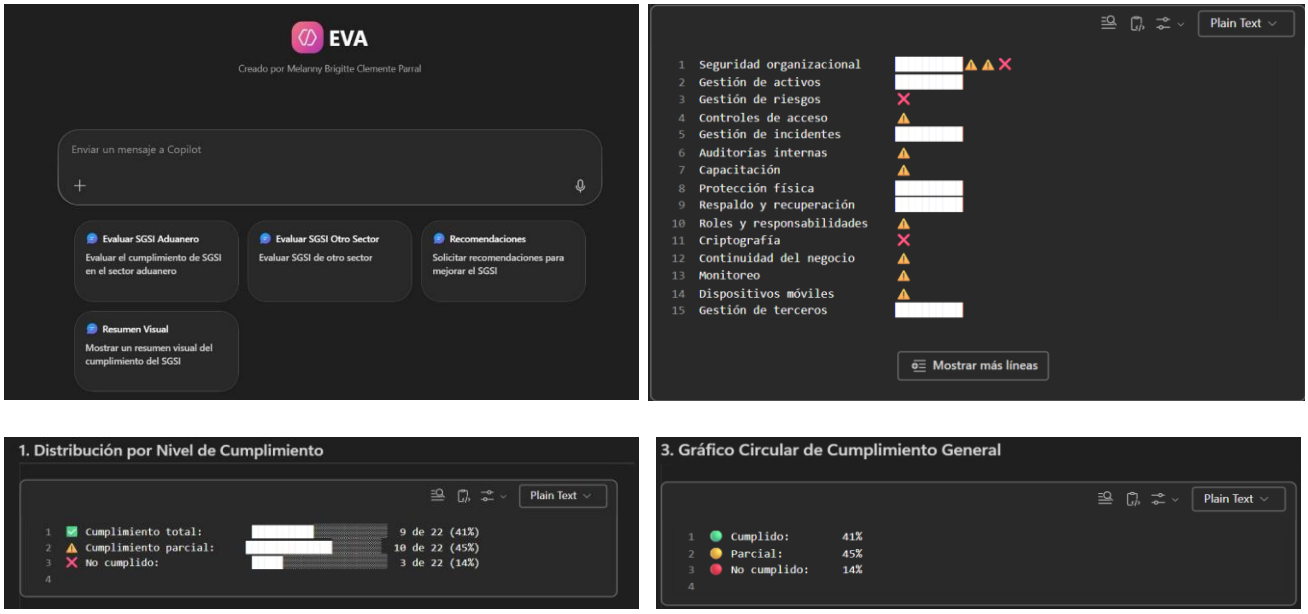
En esta fase avanzada, se integró un sistema de recomendaciones automáticas que analizaba las respuestas del usuario mediante algoritmos de procesamiento semántico y generaba sugerencias personalizadas para mejorar el cumplimiento normativo. Esta funcionalidad transformó a EVA de una herramienta de consulta básica a un asesor virtual especializado.

Posteriormente, se configuró un módulo especializado para evaluar el cumplimiento mediante indicadores clave de desempeño (KPIs), ofreciendo un diagnóstico integral sobre el nivel de madurez del SGSI organizacional. Este módulo incorporó algoritmos de análisis multivariable que procesaban las respuestas del usuario y las comparaban con estándares de mejores prácticas internacionales, generando métricas cuantitativas que facilitaban la identificación precisa de fortalezas y oportunidades de mejora.

La implementación de este sistema de evaluación en Copilot representó un avance significativo en la sofisticación de EVA, consolidándola como un sistema de diagnóstico integral que superó las capacidades del prototipo inicial y demostró mayor precisión en el análisis contextual y la generación de recomendaciones especializadas.

***Figura 9.***

*Prototipo en Copilot*




Este enfoque permitió construir un prototipo funcional completo de forma iterativa, manteniendo una estrecha conexión con las necesidades reales de la empresa y garantizando que el sistema respondiera de forma contextualizada a sus procesos y expectativas. La metodología empleada aseguró que cada componente del chatbot fuera validado no sólo desde una perspectiva técnica, sino también desde la experiencia práctica del usuario final. La fase DO concluyó con un chatbot operativo que combinaba evaluación conversacional, retroalimentación normativa y representación gráfica del nivel de cumplimiento, constituyendo una herramienta integral y demostró un alto potencial de adopción en el contexto organizacional de Cargo Service.

### *2.4.3. Fase CHECK (Verificar) - Evaluar y Medir*

El objetivo principal de esta fase consiste en medir objetivamente el desempeño de EVA mediante indicadores cuantitativos y cualitativos que permitan determinar si la solución desarrollada cumple con los criterios de éxito establecidos en la Fase PLAN. Esta evaluación integral abarca desde métricas técnicas de rendimiento hasta indicadores de adopción organizacional y percepción de valor por parte de los usuarios finales.

#### *2.4.3.1.Dimensión de Evaluación*

La evaluación se estructura en cuatro dimensiones que proporcionan una visión holística del desempeño del sistema:

***Tabla 6.***

*Dimensiones de Evaluación*

| Dimensión | Indicadores Clave | Instrumentos de Medición |
|---|---|---|
| **Eficacia Técnica** | Precisión de respuestas, tiempo de procesamiento, cobertura normativa | Testing automatizado, análisis de logs |
| **Usabilidad** | Facilidad de uso, intuitividad, satisfacción del usuario | SUS Scale, observación directa |
| **Utilidad Organizacional** | Reducción de tiempo de auditoría, mejora en identificación de brechas | Métricas comparativas pre/post implementación |
| **Adopción y Aceptación** | Intención de uso continuo, recomendación a terceros | Encuestas de aceptación tecnológica |

#### *2.4.3.2.Protocolo de Evaluación Experimental*

**Diseño Experimental**

Se implementó un diseño cuasi-experimental de medidas repetidas, comparando el desempeño de procesos de auditoría SGSI tradicionales versus la evaluación asistida por EVA. La muestra incluyó al personal de auditoría interna de Cargo Service, garantizando representatividad del contexto organizacional real.

Para las evaluaciones realizada por E.V.A se tuvo en análisis las métricas de evaluación donde se asigna puntajes de 0 a 2, donde 0 correspondió a “no cumple”, 1 a “cumplimiento parcial” y 2 a “cumplimiento total”, de la serie de 40 preguntas del diagnóstico. Los resultados detallados de esta evaluación se presentan en el Capítulo 3

#### *2.4.4. Fase ACT (Actuar) - Iterar y Mejorar*

La última fase del ciclo PDCA se centró en implementar mejoras al prototipo a partir de los hallazgos obtenidos en la fase de verificación, siguiendo un enfoque iterativo e incremental. Entre las acciones concretas implementadas en esta fase se incluyeron:

- Ajustes en el flujo conversacional para mejorar la claridad de las preguntas y reducir ambigüedades detectadas durante el testeo.
- Refinamiento de los criterios de evaluación normativa, incorporando feedback experto para mejorar la precisión del diagnóstico.
- Ampliación de la base de datos normativa, añadiendo glosarios explicativos y referencias cruzadas para facilitar la comprensión de términos técnicos por parte de usuarios no especializados.
- Optimización del rendimiento del sistema, mediante la depuración de scripts internos y la mejora de la estructura lógica del procesamiento conversacional.

Paralelamente, se desarrollaron módulos complementarios para facilitar la implementación futura de nuevas funcionalidades, como reportes ejecutivos en PDF, integración con sistemas de gestión documental y alertas automatizadas por correo electrónico, abriendo el camino para una versión escalable del chatbot.

La fase ACT también implicó documentar todo el proceso de aprendizaje, tanto a nivel técnico como organizacional. Esta documentación se considera un activo estratégico que permitirá a Cargo Service mantener y evolucionar la herramienta de forma autónoma, donde se consolidó a E.V.A como una herramienta pertinente, adaptable y sostenible en el tiempo

# Capítulo 3

# 3. Resultados y Análisis

Este capítulo presenta los resultados obtenidos durante la implementación del sistema conversacional E.V.A para la evaluación del cumplimiento normativo de Sistemas de Gestión de Seguridad de la Información (SGSI) en PYMES del sector aduanero ecuatoriano. El estudio se desarrolló con la empresa Cargo Service S.A., aplicando evaluaciones bajo los marcos normativos ISO/IEC 27001:2022, BASC 2022, LOPDP Ecuador y COBIT 2019.

La metodología contempló dos fases de evaluación: una inicial y una de seguimiento con un intervalo de implementación de 31 días. Los resultados se analizan considerando cuatro indicadores clave de desempeño que demuestran la efectividad del sistema propuesto.

## 3.1. Resultados de la Evaluación Inicial

### *3.1.1. Diagnóstico del Cumplimiento Normativo*

La evaluación inicial reveló un cumplimiento normativo global del 45%, evidenciando una madurez parcial en la implementación del SGSI.

Esta medición se realizó mediante una matriz de verificación de 40 dominios críticos distribuidos proporcionalmente entre los marcos normativos evaluados.

A cada pregunta se le asignó un puntaje en un intervalo de 0 a 2, donde se clasificó de la siguiente manera: 0 correspondió a “no cumple”, 1 a “cumplimiento parcial” y 2 a “ cumple. La distribución del cumplimiento por marco normativo mostró heterogeneidad significativa. (***Véase Anexo C y D)***

- ISO/IEC 27001:2022 alcanzó el 15% de cumplimiento, siendo el marco con mejor desempeño inicial debido a la existencia de controles básicos de acceso y políticas informales de seguridad.

- BASC 2022 registró el menor cumplimiento (11%), evidenciando deficiencias críticas en protocolos de inspección y custodia en la cadena logística.
- LOPDP Ecuador mostró un cumplimiento del 11%, reflejando desconocimiento de las obligaciones legales en protección de datos personales.
- COBIT 2019 alcanzó el 8%, con carencias en procesos formales de monitoreo y reportes de TI.

***Tabla 7.***

*Niveles de Cumplimiento frente a Normativas*

| | **CUMPLIMIENTO** | | **INCUMPLIMIENTO** | | | | |
|---|---|---|---|---|---|---|---|
| **Marco Normativo** | **Cumplimiento Total (%)** | **Cumplimiento Parcial (%)** | **Cumplimiento Parcial (%)** | **Incumplimiento (%)** | **Conformidades** | **No Conformidades Menores** | **No Conformidades Críticas** |
| ISO/IEC 27001:2022 | 5% | 10% | 10% | 13% | 2 | 8 | 5 |
| BASC 2022 | 3% | 9% | 9% | 5% | 1 | 7 | 2 |
| LOPDP Ecuador | 5% | 6% | 6% | 5% | 2 | 5 | 2 |
| COBIT 2019 | 3% | 5% | 5% | 3% | 1 | 4 | 1 |
| **Total Preguntas** | **15%** | **30%** | **30%** | **25%** | **6** | **24** | **10** |
| **Nivel de Cumplimiento** | **45%** | | **55%** | | | | |

***Figura 10.***

*Dashboard-Evaluación Inicial*

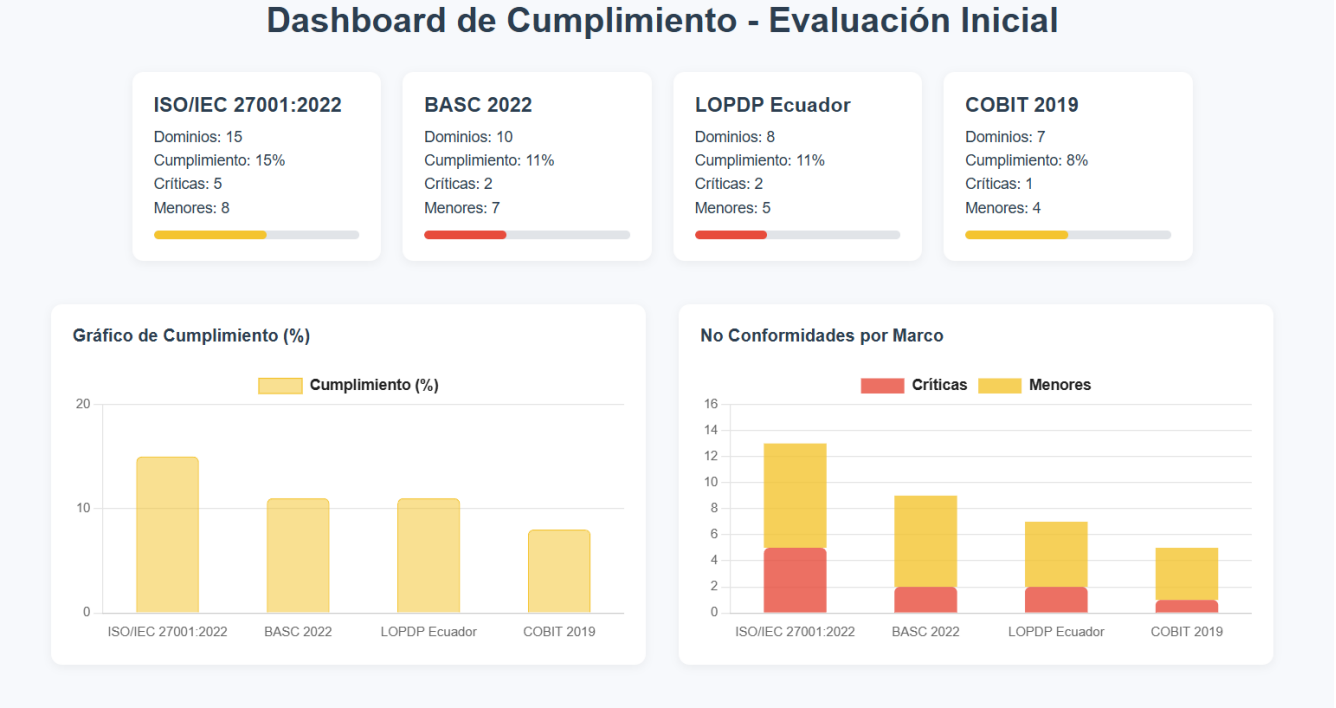



***Tabla 8.***

*Niveles de Cumplimiento frente a Puntajes*

| Nivel de Cumplimiento | Cantidad | N° Pregunta | Puntos | Puntaje Obtenido | Puntaje Máximo | Porcentaje Cumplimiento |
|---|---|---|---|---|---|---|
| Cumplimiento total | 6 | 3, 10, 13, 24, 28, 36 | 2 | 12 | 80 | 15% |
| Cumplimiento parcial | 24 | 1, 2, 4, 5, 7, 8, 11, 14, 15, 17, 18, 19, 21, 22, 25, 27, 29, 30, 32, 33, 34, 37, 39, 40 | 1 | 24 | | 30% |
| Incumplimiento total | 10 | 6, 9, 12, 16, 20, 23, 26, 31, 35, 38 | 0 | 0 | | 0% |
| **Totales** | **40** | | | **36** | | **45%** |

### *3.1.2. Identificación de No Conformidades y Generación de Recomendaciones*

E.V.A permitió identificar un total de 40 no conformidades, de las cuales 10 fueron críticas y 24 menores, conforme a criterios de severidad, impacto en la seguridad de la información y urgencia de corrección. Esta clasificación se fundamentó en el análisis

automatizado de evidencia documental y operativa, correlacionada con cláusulas específicas de los marcos normativos evaluados.

***Tabla 9.***

*Resumen de no Conformidades Criticas*

| Norma / Marco | No Conformidades Críticas (detalle) | Cláusula / Artículo / Proceso |
|---|---|---|
| ISO/IEC 27001:2022 | 1) Falta de metodología de gestión de riesgos<br>2) Ausencia de plan de continuidad de negocio<br>3) No revisión de derechos de acceso<br>4) Inexistencia de indicadores<br>5) Comité de seguridad ausente | 5.4; 5.29; 5.15; 5.31; 5.6;5.25; 5.10;5.7 |
| BASC 2022 | 1) Falta de protocolos de inspección<br>2) Detección de anomalías ausente, sin plan de respuesta a eventos | Cap. 4, 3, 2, 5, 1 |
| LOPDP Ecuador | 1) No Registro de Actividades de Tratamiento<br>4) Ausencia de Protocolo de Brechas, sin mecanismo de consentimiento | Art. 45, 31, 32, 33, 27, 28 |
| COBIT 2019 | 1) No reportes periódicos sobre rendimiento | EDM03, APO12, BAI06 |

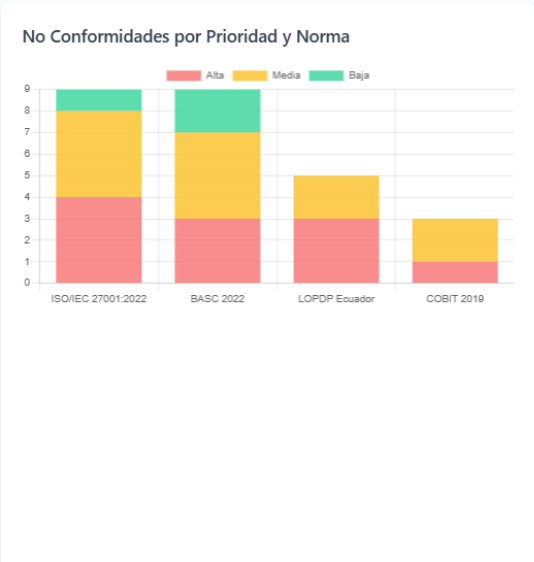
Las no conformidades críticas se concentraron en ISO 27001 y BASC, afectando directamente la gestión de riesgos, continuidad operativa y trazabilidad logística. En el caso de LOPDP, las deficiencias se relacionaron con la ausencia del Registro de Actividades de Tratamiento (Art. 45) y del protocolo de notificación de brechas (Art. 32), lo que representa un incumplimiento legal.

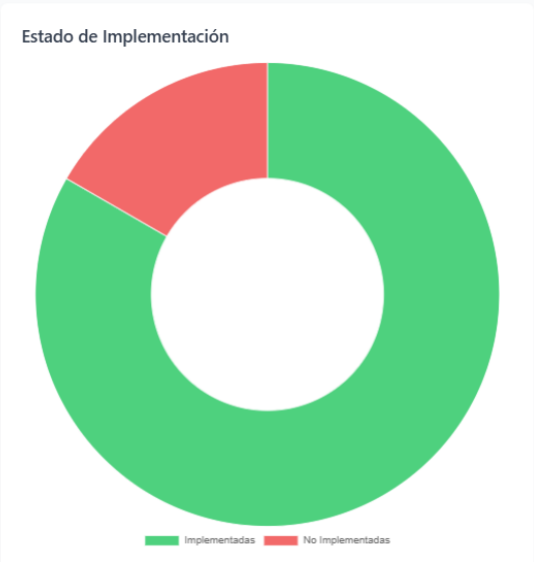
El sistema generó automáticamente un reporte ejecutivo de recomendaciones priorizadas, utilizando una matriz de impacto-esfuerzo que clasifica las acciones correctivas en función de su urgencia, recursos requeridos y viabilidad operativa.

***Figura 11.***

*Matriz de Priorización*

| Norma / Marco | No Conformidad Crítica (detalle) | Cláusula / Artículo / Proceso | Impacto | Esfuerzo | Prioridad | Estado Implementación |
|---|---|---|---|---|---|---|
| ISO/IEC 27001:2022 | Falta de metodología de gestión de riesgos | 5.4; 5.29; 5.15; 5.31; 5.6; 5.25; 5.10; 5.7 | Alto | Medio | Alta | Implementada |
| BASC 2022 | Falta de protocolos de inspección | Cap. 4, 3, 2, 5, 1 | Alto | Medio | Alta | Implementada |
| LOPDP Ecuador | No Registro de Actividades de Tratamiento | Art. 45, 31, 32, 33, 27, 28 | Alto | Medio | Alta | Implementada |
| COBIT 2019 | No reportes periódicos sobre rendimiento | EDM03, APO12, BAI06 | Medio | Bajo | Media | Implementada |




Al finalizar la interacción, la herramienta inteligente utilizada generó un reporte ejecutivo en formato PDF que incluyó:

- Resumen de preguntas y respuestas de la evaluación.
- Nivel global de cumplimiento de la organización.
- Identificación de no conformidades y cumplimientos parciales.
- Recomendaciones de mejora específicas, priorizadas por criticidad.

Este documento representó el punto de partida para que la empresa pudiera planificar acciones correctivas inmediatas y diseñar una estrategia de implementación de controles más amplia.

### 3.2. Observaciones y Recomendaciones de la Herramienta

En toda evaluación de cumplimiento es fundamental documentar las observaciones y recomendaciones para obtener una mejora consecuente de los sistemas de gestión, por lo cual la herramienta generó una serie de observaciones y recomendaciones. Cabe destacar que las mismas fueron revisadas por el equipo auditor para constatar su pertinencia junto a los encargados del SGSI. Entre las más destacables se encuentran las siguientes:

- Gestión de riesgos: No se actualiza periódicamente ni existen planes de tratamiento formalizados, se sugiere implementar metodología documentada con revisiones anuales.
- Proveedores y terceros: No hay cláusulas contractuales ni controles de seguridad, se sugiere incluir requisitos específicos en contratos y auditorías periódicas.
- Controles técnicos: Antivirus y accesos básicos son insuficientes, se recomienda establecer copias de seguridad con pruebas de restauración y aplicar anonimización/seudonimización de datos.
- Cumplimiento normativo: Ausencia de Registro de Actividades de Tratamiento y protocolo de notificación de brechas, se sugiere desarrollar y aprobar estos documentos de forma prioritaria.
- Cultura organizacional: La capacitación es limitada y esporádica, se recomienda implementar un programa continuo de formación y simulacros de incidentes.

Con las recomendaciones emitidas por la herramienta, la empresa de estudio se comprometió a realizar las debidas correcciones en su SGSI con el objetivo de mejorar para futuras revisiones, tomando dicho informe como punto de partida.

En conclusión, aunque la organización presenta bases iniciales para la gestión de la seguridad de la información, el bajo porcentaje de cumplimiento (45%) indica que es urgente formalizar procedimientos, ampliar la cobertura de los controles e integrar prácticas de mejora continua que garanticen la confianza de clientes, reguladores y socios comerciales.

### 3.3. Evaluación de Seguimiento

Se realizó una evaluación de seguimiento luego de transcurrido un mes de la emisión de recomendaciones, aplicando la misma metodología utilizada en la evaluación inicial. Dicho análisis inició con E.V.A. solicitando el informe de evaluación anterior, el cual fue leído por la herramienta y lo tomó como punto de partida para la nueva evaluación que consideró solo los puntos calificados anteriormente como parciales o no cumplidos, teniendo así los siguientes resultados:

***Tabla 10.***

*Evaluación de Seguimiento*

| Nivel de Cumplimiento | Cantidad | N° Pregunta | Puntos | Puntaje Obtenido | Puntaje Máximo | Porcentaje Cumplimiento |
|---|---|---|---|---|---|---|
| Cumplimiento total | 26 | 1, 2, 4, 5, 6, 7, 8, 9, 11, 12, 14, 15, 16, 17, 18, 22, 25, 27, 30, 31, 32, 33, 34, 37, 39, 40 | 2 | 52 | 68 | 76% |
| Cumplimiento parcial | 8 | 19, 20, 21, 23, 26, 29, 35, 38 | 1 | 8 | | 12% |
| **Totales** | **34** | | | **60** | | **88%** |

De las 34 preguntas que fueron calificadas como parciales o no cumplidas en la evaluación inicial, solo 8 se mantuvieron como parciales en la evaluación de seguimiento, teniendo así los siguientes puntos de mejora en el SGSI:

- La organización cuenta con una política de seguridad de la información aprobada y comunicada (ISO 27001, cláus. 5.2; BASC Est. 6.0.1.
- Se realiza la revisión periódica del SGI por la alta dirección (ISO 27001, 9.3; COBIT MEA01), lo que asegura la mejora continua y el alineamiento estratégico.
- La organización mantiene evidencia documental de la base legal para el tratamiento de datos (LOPDP art. 7; COBIT DSS05).
- Asimismo, se constató que las políticas de seguridad son revisadas y actualizadas anualmente (ISO 27001, 7.5.2; BASC 6.1), lo que garantiza vigencia y pertinencia normativa.

**Gestión de riesgos**

- Se dispone de un proceso documentado para identificar y evaluar riesgos de seguridad de la información (ISO 27001, 6.1.2; COBIT APO12; BASC 6.2), actualizado al menos una vez al año o ante cambios significativos (ISO 27001, 6.1.3).
- Se definen planes de tratamiento de riesgos (ISO 27001, 6.1.3; COBIT APO12.05), que consideran además a terceros y proveedores críticos (ISO 27001 A.5.19; LOPDP art. 15).

**Controles operativos y procedimientos**

- Se aplican controles de acceso basados en roles y privilegios mínimos (ISO 27001 A.5.15; COBIT DSS05), con registro y monitoreo de accesos a información sensible (ISO 27001 A.8.16; BASC 6.6).
- La información se clasifica y etiqueta conforme a niveles de criticidad (ISO 27001 A.5.12; BASC 6.4), garantizando su adecuada gestión.
- Existen procedimientos formales para la gestión de soportes físicos y su destrucción segura (ISO 27001 A.8.10; BASC 6.4).

- En materia de gestión de incidentes, se verificó la existencia de un procedimiento documentado y en uso efectivo (ISO 27001 A.5.24; BASC 6.7; COBIT DSS02).

**Capacitación y cultura organizacional**

- La organización promueve una cultura sólida de seguridad, realizando capacitaciones periódicas al personal en temas de ciberseguridad y protección de datos (ISO 27001 A.6.3; LOPDP art. 47; BASC 6.1).
- De este mismo modo, se fomenta la denuncia interna de malas prácticas o incidentes sospechosos (COBIT MEA01; BASC 6.1), fortaleciendo los canales de reporte y confianza del personal.

**Protección física y continuidad del negocio**

- Se constató un control estricto del acceso físico a instalaciones críticas (ISO 27001 A.7.1; BASC 6.5), respaldado por registros de visitantes (BASC 6.5; COBIT DSS05).
- El equipamiento crítico cuenta con medidas de protección ambiental (ISO 27001 A.7.2), minimizando riesgos por fuego, agua o temperatura.

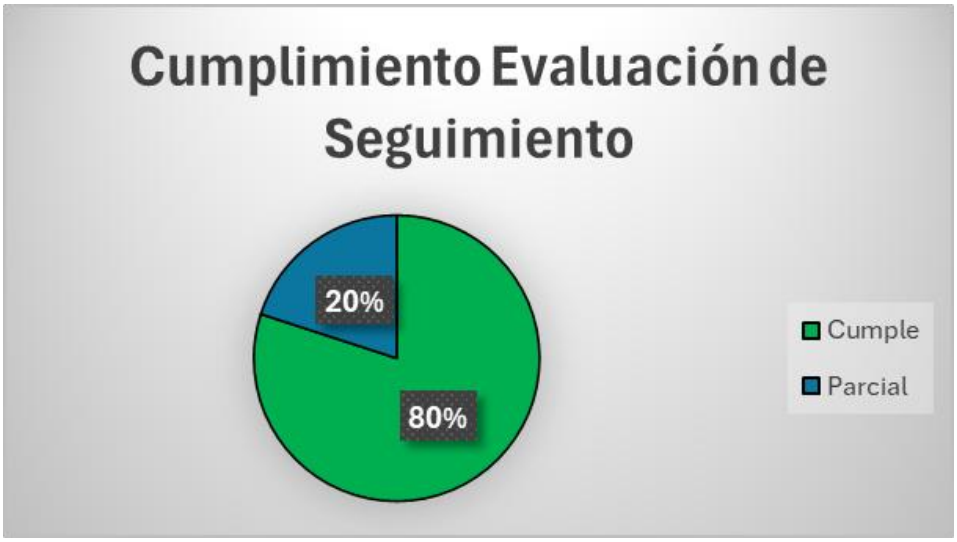
**Gestión de datos personales y mejora continua**

- Se aplican medidas para garantizar la exactitud y actualización de los datos personales (LOPDP art. 9), cumpliendo con el principio de calidad de datos.
- Se documentan y aplican lecciones aprendidas tras auditorías e incidentes (ISO 27001 10.1; COBIT MEA02), asegurando retroalimentación efectiva.
- Finalmente, la organización mantiene un proceso formal de mejora continua del SGI (ISO 27001 10.2; COBIT APO11; BASC 6.8), que refuerza la sostenibilidad y evolución del sistema.

Al sumar la cantidad de preguntas que fueron calificadas como cumplidas totalmente a lo largo de ambas evaluaciones se tiene un total de 32 preguntas, lo que representa una mejora significativa a nivel global en el nivel de cumplimiento del SGSI, tal y como se muestra en las siguientes gráficas:

***Figura 12.***

*Evaluación de Seguimiento*




Las preguntas en cumplimiento parcial reflejan que, aunque existen políticas y controles definidos, aún falta formalización y evidencia documentada en áreas como gestión de proveedores, continuidad del negocio, respuesta a incidentes y protección de datos sensibles.

Esto indica que el SGSI ha avanzado, pero requiere fortalecer la trazabilidad y la verificación práctica de sus medidas para alcanzar un cumplimiento total.

## 3.4. Análisis Comparativo Antes/Después

***Tabla 11.***

*Análisis Comparativo de Resultados*

| Indicador | Evaluación Inicial | Seguimiento | Variación |
|---|---|---|---|
| Puntaje Total | 36/20 | 72/80 | +36 |
| % Cumplimiento | 45% | 90% | +45% |
| **Dominios en 100%** | **6** | **32** | **+26** |

El análisis comparativo demuestra que la herramienta implementada no solo permitió identificar rápidamente las no conformidades, sino que también generó reportes automáticos que facilitaron la toma de decisiones estratégicas.

El incremento del **45% en el cumplimiento** en apenas un mes constituye una evidencia empírica del impacto positivo de la solución.

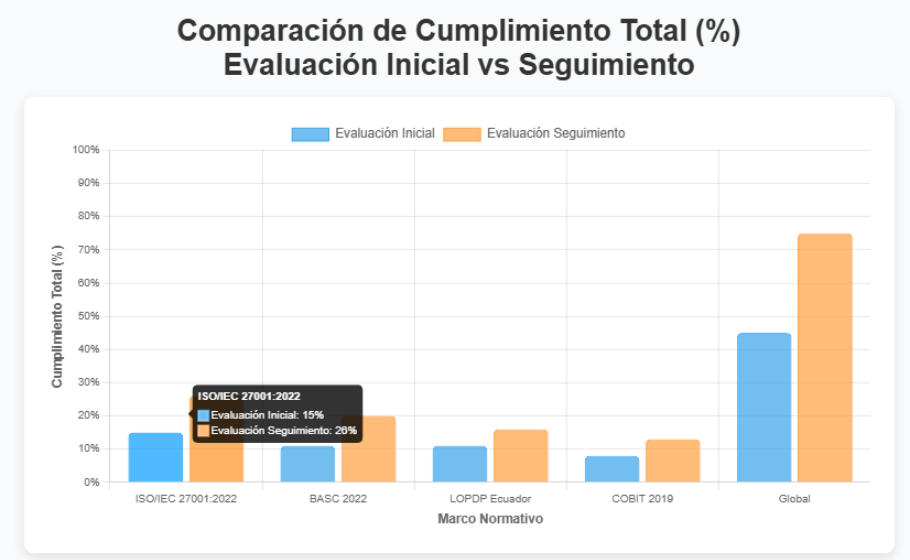
***Figura 13.***

*Comparación de Resultados*


Más allá de la mejora numérica, el cambio refleja una **evolución en la cultura organizacional**: la empresa pasó de una gestión reactiva y fragmentada de la seguridad de la información, a una **gestión proactiva y sistematizada**, con controles documentados y personal capacitado.

***Figura 14.***

*Comparación de Pruebas*




## 3.5. Análisis de Costos

El desarrollo de la herramienta inteligente y su implementación se realizó con un enfoque de optimización de recursos. Se utilizaron componentes de software libre y servicios en la nube gratuitos, minimizando costos de licenciamiento.

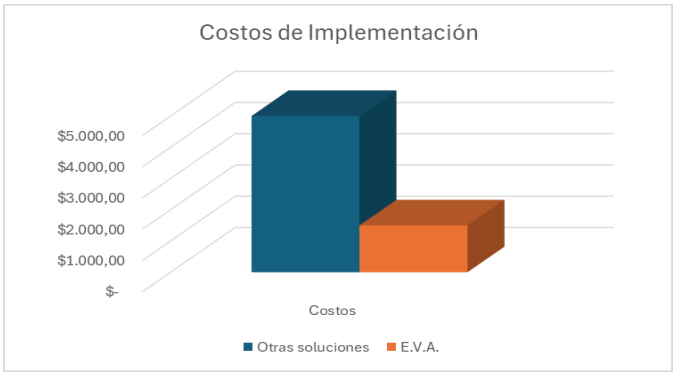
***Tabla 12.***

*Presupuesto Estimado de Implementación*

| **Concepto** | **Costo (USD)** |
|---|---|
| Desarrollo de software | 500 |
| Capacitación al personal | 300 |
| Infraestructura en la nube | 0 |
| Primera evaluación y seguimiento | 700 |
| **Total** | **1.500** |

***Figura 15.***

*Costos de Implementación*




Este monto resulta considerablemente menor en comparación con soluciones comerciales de auditoría automatizada, cuyo licenciamiento suele superar los 5.000 USD anuales. Además, los costos en este caso se concentran en una inversión inicial, sin generar gastos recurrentes.

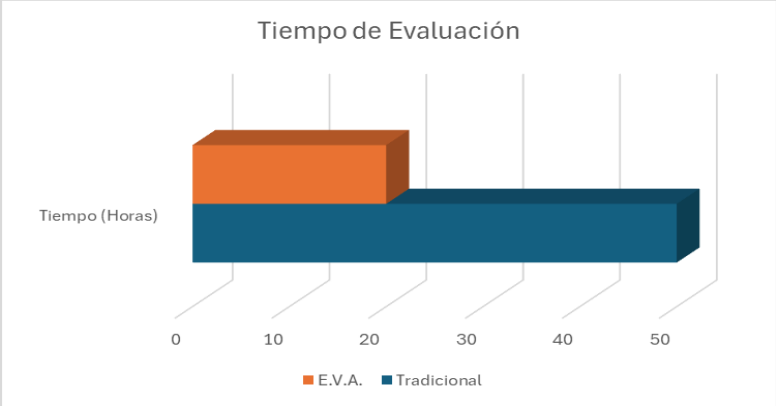
### 3.6. Viabilidad Económica

La implementación de la herramienta permitió reducir en un 60 % los tiempos destinados a la ejecución de auditorías, lo cual evitó la necesidad de contratar consultorías externas de manera recurrente.

Tradicionalmente, las auditorías de un SGSI suelen desarrollarse en un periodo aproximado de una semana, equivalente a 50 horas de trabajo continuo; sin embargo, con el uso de E.V.A. dichos tiempos se optimizaron a un lapso de apenas dos días, es decir, alrededor de 20 horas efectivas. Esta mejora representó no solo un ahorro significativo en los costos asociados a los procesos de evaluación, sino también una liberación de recursos humanos y financieros que resultan vitales para las PYMES del sector aduanero.

***Figura 16.***

*Tiempos de Evaluación*




Con ello, se calculó un Retorno de Inversión (ROI) del 100% en el primer año, acompañado de un Valor Actual Neto (VAN) positivo en un horizonte de tres años. Estos indicadores financieros demuestran que la solución no solo es técnicamente funcional, sino también económicamente viable y sostenible.

$$ROI = \frac{500}{500} * 100 = 100\%$$

$$VAN = \frac{1000}{(1+0.10)^1} + \frac{1000}{(1+0.10)^2} + \frac{1000}{(1+0.10)^3} - 500 = 1986.85$$

Para las PYMES del sector aduanero, este tipo de herramientas representa una alternativa accesible frente a software corporativos de alto costo, al mismo tiempo que fortalece la competitividad y la confianza de clientes y socios.

# Capítulo 4

# 4. Conclusiones y recomendaciones

## 4.1. Conclusiones

El presente proyecto de investigación tuvo como propósito principal el diseño, implementación y evaluación de una herramienta inteligente de auditoría conversacional aplicada al Sistema de Gestión de Seguridad de la Información (SGSI) en una PYME del sector aduanero de Guayaquil. A partir de los resultados presentados en el capítulo 3, es posible extraer conclusiones relevantes tanto a nivel organizacional como académico y tecnológico.

Los resultados iniciales de la evaluación mostraron un nivel de cumplimiento del 45% respecto a estándares como ISO/IEC 27001:2022, COBIT 2019, Norma BASC 2022 y la LOPDP de Ecuador.

Este bajo porcentaje puso en evidencia las debilidades estructurales y operativas de la empresa, especialmente en lo relacionado con la formalización de controles, registro de evidencias sobre evaluaciones al SGSI y la existencia de protocolos de seguridad documentados.

Los hallazgos iniciales reflejaron carencias técnicas y un nivel de madurez insuficiente en la cultura organizacional sobre seguridad de la información. Sin embargo, tras la implementación de EVA y la ejecución de acciones correctivas derivadas del informe inicial, se alcanzó en un periodo de un mes un 90% de cumplimiento, consolidando treinta y dos de los cuarenta dominios evaluados al 100%.

Este salto de 45 puntos porcentuales en el corto tiempo representa un resultado excepcional, que demuestra la eficacia y pertinencia del uso de tecnologías inteligentes en auditorías de SGSI.

De los hallazgos se desprenden varias conclusiones importantes:

1. La tecnología es un facilitador estratégico para PYMES. Mientras que soluciones tradicionales de auditoría son costosas, poco rápidas y requieren de consultores externos, la herramienta diseñada logró reducir los tiempos de auditoría en un 60%, con una inversión total de 1.500 USD. Esto significa que las PYMES pueden acceder a un nivel de control y cumplimiento normativo comparable al de grandes corporaciones, pero con costos adaptados a su realidad económica.
2. La cultura organizacional evoluciona positivamente con el uso de herramientas inteligentes. El salto en cumplimiento se explica por la ejecución de acciones técnicas, procesos de concientización y capacitación del personal. EVA además de generar un reporte hallazgos, permitió tener una interacción pedagógica, donde los colaboradores comprendieron la importancia de los controles y conocieron su rol clave en la gestión de riesgos.
3. El valor de los reportes automáticos radica en la acción. Una auditoría carece de impacto si sus resultados no derivan en mejoras concretas. EVA generó observaciones y recomendaciones específicas, lo que facilitó a la empresa priorizar sus recursos. El éxito del proyecto demuestra que la automatización en auditoría debe orientarse a la ejecutabilidad de las recomendaciones.
4. La formalización documental sigue siendo la base de todo SGSI. El proyecto evidenció que ningún sistema puede funcionar correctamente sin registros, protocolos y políticas claras. La ausencia inicial de un Registro de Actividades de Tratamiento y de un protocolo de notificación de brechas de seguridad de la

información impedía el cumplimiento legal y generaba vulnerabilidades críticas para la continuidad del negocio.

5. La viabilidad económica está comprobada. El análisis de costos y el cálculo del ROI del 100% en el primer año confirman que el proyecto es técnicamente viable y sostenible en el tiempo. La reducción de gastos en consultoría externa, junto con el ahorro en tiempo de auditoría, refuerza la pertinencia de esta solución para PYMES con recursos limitados.
6. El proyecto es replicable y escalable. Si bien la investigación se enfocó en una PYME del sector aduanero, los resultados permiten concluir que la herramienta puede adaptarse a empresas de otros sectores que requieran cumplir con normativas locales e internacionales en materia de seguridad de la información, protección de datos y control de riesgos.

El presente trabajo aporta evidencia sólida sobre la utilidad de integrar tecnologías de inteligencia artificial conversacional en procesos de auditoría y control de gestión. La investigación demuestra que la IA no debe verse únicamente como un sustituto de tareas humanas, sino como un complemento estratégico que amplifica las capacidades de diagnóstico, análisis y mejora continua.

Finalmente, desde un punto de vista organizacional, el proyecto validó que la seguridad de la información es una necesidad estratégica. En un sector como el aduanero, donde el manejo de datos sensibles y operaciones críticas es constante, la implementación de un SGSI robusto previene sanciones legales y genera confianza en clientes, proveedores y socios comerciales.

En conclusión, los resultados obtenidos confirman que la herramienta inteligente diseñada constituye una solución eficaz, económica y escalable para la auditoría de sistemas de

gestión en PYMES, y que su implementación puede marcar la diferencia entre una gestión reactiva e improvisada y una gestión preventiva, madura y alineada con estándares internacionales.

## 4.2. Recomendaciones

Con base en los hallazgos y conclusiones obtenidas, se presentan las siguientes recomendaciones, orientadas tanto a la empresa objeto de estudio como a PYMES similares y a la comunidad académica y profesional.

### 4.2.1 Para la empresa Cargo Service

- **Consolidar los controles alcanzados:** Aunque se logró un 90% de cumplimiento, aún persisten dominios con cumplimiento parcial. Se recomienda establecer un plan de seguimiento trimestral, donde se verifique la consolidación de estos controles.
- **Mantener un ciclo de mejora continua:** La seguridad de la información no debe entenderse como un proyecto puntual, sino como un proceso permanente, por ello se sugiere aplicar la filosofía del ciclo PDCA (Planificar, Hacer, Verificar, Actuar) en cada revisión del SGSI.
- **Documentar todas las acciones:** Cada medida implementada debe estar respaldada por un procedimiento escrito, un registro de ejecución y un responsable designado. Esto no solo facilita auditorías futuras, sino que reduce la dependencia de personal para llevar a cabo acciones correctivas.
- **Fortalecer la capacitación:** La concientización del personal fue determinante en el avance logrado, por lo cual se recomienda continuar con capacitaciones semestrales en seguridad de la información, gestión de datos y cumplimiento normativo.

- **Evaluar la integración con otros sistemas de gestión:** La empresa podría explorar la integración de su SGSI con otros estándares como ISO 9001 (Calidad) o ISO 45001 (Seguridad y Salud en el Trabajo), generando sinergias y reduciendo duplicidades en la gestión documental.

### 4.2.2 Para PYMES del sector aduanero y similares

- **Adoptar soluciones inteligentes accesibles:** Este estudio demuestra que no es necesario invertir en costosas plataformas internacionales para alcanzar altos niveles de cumplimiento. Las PYMES pueden recurrir a soluciones basadas en software libre y herramientas conversacionales.
- **No subestimar el cumplimiento normativo:** Muchas PYMES suelen postergar la implementación de SGSI por considerarlo un gasto innecesario. Sin embargo, los riesgos legales, financieros y reputacionales de no cumplir con normativas pueden ser mucho más altos.
- **Priorizar la protección de datos personales:** Con la entrada en vigor de leyes como la LOPDP en Ecuador, las empresas deben comprender que el tratamiento indebido de datos personales puede derivar en multas significativas y pérdida de confianza de clientes.
- **Impulsar la cultura organizacional:** La seguridad de la información no se sostiene únicamente con tecnología, por esto es indispensable generar una cultura de compromiso en todos los niveles de la organización.
- **Planificar la escalabilidad:** Al igual que Cargo Service, otras PYMES deben considerar que las herramientas implementadas hoy deben ser escalables para responder a mayores exigencias futuras.

### 4.2.3 Para la comunidad académica y profesional

- **Ampliar estudios sobre auditorías inteligentes:** Este trabajo abre una línea de investigación que puede expandirse hacia otros sectores (financiero, salud, educación, logística).
- **Medir el impacto a largo plazo:** Sería recomendable realizar estudios longitudinales que evalúen cómo evoluciona el cumplimiento en periodos de 1 a 3 años.
- **Combinar metodologías mixtas:** La integración de técnicas cualitativas y cuantitativas en auditoría permite comprender no solo el nivel de cumplimiento, sino también la percepción cultural de las organizaciones frente a la seguridad.
- **Impulsar la formación académica en ciberseguridad para PYMES:** Las universidades pueden jugar un papel crucial al formar profesionales que diseñen soluciones adaptadas a la realidad de pequeñas y medianas empresas.

## 4.3. Oportunidades de mejora de la Herramienta

Si bien la herramienta demostró su eficacia en el caso de estudio, es importante proyectar cómo podría evolucionar y escalar en un contexto de constante avance tecnológico y creciente complejidad en las auditorías de sistemas de gestión.

- **Aprendizaje continuo de la Herramienta:** Considerando los posibles cambios o actualizaciones en normativas como ISO 27001, BASC, LOPDP, y para mantener la vigencia de la herramienta en sus evaluaciones, se recomienda mantener actualizados los recursos que alimentan los criterios de evaluación. Un experto en gestión de seguridad de la información revisará de forma periódica la herramienta, asignando los cambios pertinentes para mantener la oportunidad de los criterios.

- **Integración con Inteligencia Artificial Avanzada:** Actualmente la herramienta utiliza un modelo conversacional básico. En futuras versiones podría integrarse con IA generativa avanzada, capaz de no solo diagnosticar hallazgos, sino también simular escenarios de riesgo, predecir incidentes y proponer planes de acción optimizados.
- **Uso de Big Data y Analítica Predictiva:** El auge del Big Data permite recolectar y analizar grandes volúmenes de datos de incidentes de seguridad, vulnerabilidades y ataques. La herramienta podría conectarse a estas bases de datos globales para enriquecer sus diagnósticos y anticipar amenazas emergentes en el sector aduanero.
- **Automatización de evidencias:** Una mejora futura es que la herramienta no solo evalúe por entrevistas o checklists, sino que conecte directamente con los sistemas internos de la empresa (servidores, bases de datos, plataformas en la nube) para verificar automáticamente la existencia de respaldos, registros de accesos o actualizaciones de seguridad.
- **Panel de control en tiempo real:** La evolución lógica es que la herramienta disponga de un dashboard en la nube, donde los directivos puedan visualizar en tiempo real los niveles de cumplimiento, riesgos detectados y alertas críticas.
- **Adaptabilidad normativa internacional:** La herramienta podría expandirse para cubrir regulaciones más amplias como el GDPR europeo, la Ley de Privacidad de California (CCPA) o los lineamientos de la OCDE, facilitando que las PYMES que exportan servicios cumplan con estándares internacionales.
- **Mayor especialización sectorial:** Si bien el estudio se aplicó al sector aduanero, en el futuro podrían desarrollarse módulos específicos para sectores como banca, salud,

educación o telecomunicaciones, donde los requisitos de seguridad y privacidad tienen matices particulares.

- **Gamificación del aprendizaje:** Como estrategia para fortalecer la cultura organizacional, la herramienta podría integrar dinámicas de gamificación, donde los empleados obtengan puntajes o insignias por cumplir buenas prácticas de seguridad, generando motivación y compromiso.

En síntesis, la herramienta tiene un alto potencial de mejora y escalabilidad, pudiendo convertirse en un referente para auditorías inteligentes en Latinoamérica. Su evolución fortalecerá la seguridad de la información en PYMES, contribuyendo al acceso de tecnologías avanzadas de control y cumplimiento normativo.

## 5. Referencias

Dell'Era, Magistretti, Candi, Bianchi, Calabretta, Stigliani, & Verganti. (2025). *Journal of Knowledge Management.* Obtenido de Design thinking in action: a quantitative study of design thinking practices in innovation projects: https://www.emerald.com/jkm/article/29/11/32/1267430/Design-thinking-in-action-a-quantitative-study-of

Al-Amin, P.M., C., N.I, A., & C, O. (22 de Septiembre de 2024). *AI-enabled intelligent inventory and supply chain optimization platform for SMEs.* Obtenido de Comprehensive Research and Reviews Journal: https://crrjournals.com/crrj/sites/default/files/CRRJ-2024-0030.pdf

BASC. (2022). Norma Internacional BASC. Obtenido de https://www.siacomex.com/wp-content/uploads/2023/10/02.-NORMA-INTERNACIONAL-BASC-V.6-2022_1.pdf

Bender, S. R. (2023). *Design thinking as an effective method for problem-setting and needfinding for entrepreneurial teams addressing wicked problems.* Obtenido de Journal of Innovation and Entrepreneurship: https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-023-00291-2

Canós, J. H., & Letelier, M. (2012). Obtenido de Métodologías Ágiles en el Desarrollo de Software: https://d1wqtxts1xzle7.cloudfront.net/34546906/XP_Agil-libre.pdf?1409109861=&response-content-disposition=inline%3B+filename%3DMetodologias_Agiles_en_el_Desarrollo_de.pdf&Expires=1754614691&Signature=LJaLk4jzwByW90EJYdL~EpdhNG03UFWcn0mqveS3vuu1gACELDkf0Sj

Cendejas, J. l., Vega, C. A., Careta, A., Sánchez, O. G., & Medina, H. F. (2015). *Diseño del modelo integral colaborativo para el desarrollo ágil de software en las empresas de la zona centro-occidente en México.* Obtenido de Nova scientia: https://www.scielo.org.mx/scielo.php?pid=S2007-07052015000100008&script=sci_arttext

Constitución de la República del Ecuador. (20 de Octubre de 2008). CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR. Obtenido de https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf

COPCI. (29 de Diciembre de 2010). Código Orgánico de la producción,comercio e inversiones, COPCI. Obtenido de https://www.lexis.com.ec/biblioteca/copci?download=copci

Dell'Era, C. (2025). *Design thinking in action: a quantitative study of design thinking practices in innovation projects.* Obtenido de Journal of Knowledge Management: https://www.emerald.com/jkm/article/29/11/32/1267430/Design-thinking-in-action-a-quantitative-study-of

EY, & IT. (2024). *Tendencias Tecnológicas 2024: Principales Oportunidades para las Organizaciones en el Ecuador* (Quinta ed.). Obtenido de https://www.ey.com/content/dam/ey-unified-site/ey-com/es-ec/insights/consulting/documents/ey-tendenciastecnologicas2024.pdf

Franco Mora, D. C., Porras Castro, H. O., Corredor Chavarro, F. A., & Calderón Bogotá, C. (2019). *SANI: Asistente para Auditorías de seguridad de la información sobre ISO/IEC 27001.* Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=8077418

Ghazanfari, M., Jafari, M., & Rouhani, S. (2011). *A tool to evaluate the business intelligence of enterprise systems.* Obtenido de Scientia Iranica, 18(6), 1579–1590: https://doi.org/10.1016/j.scient.2011.11.011

Highsmith. (2018). *Gestión ágil de proyectos: creación de productos innovadores.* Obtenido de https://www.researchgate.net/publication/234809670_Agile_Project_Management_Creating_Innovative_Products/citations

ISACA. (2018). Control Objectives for Information and Related Technology. Obtenido de https://www.isaca.org/resources/cobit

ISO. (2022). *International Organization for Standardization*. Obtenido de Information security, cybersecurity and privacy protection — Information security management systems: https://www.iso.org/obp/ui/en/#iso:std:82875:en

Lexis S.A. (28 de Julio de 2025). *Superintendencia de Protección de Datos Personales expide reglamento para cálculo de multas por infracciones a la ley de protección de datos*. Obtenido de Lexis: https://www.lexis.com.ec/noticias/superintendencia-de-proteccion-de-datos-personales-expide-reglamento-para-calculo-de-multas-por-infracciones-a-la-ley-de-proteccion-de-datos

LOPDP. (2021). LEY ORGÁNICA DE PROTECCIÓN DE DATOS. Obtenido de https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

López Gil, A. (2018). *Estudio comparativo de metodologías tradicionales y ágiles para proyectos de desarrollo de software.* Obtenido de https://uvadoc.uva.es/bitstream/handle/10324/32875/TFG-I-1015.pdf?sequence=1&isAllowed=y

López, J. P. ((s.f.) ). *Modelo para la evaluación de desempeño de los controles de un SGSI basado en el estándar ISO/IEC 27001.* Obtenido de https://www.academia.edu/36174483/Modelo_para_la_evaluaci%C3%B3n_de_desempe%C3%B1o_de_los_controles_de_un_SGSI_basado_en_el_est%C3%A1ndar_ISO_IEC_27001

Ma, N., Khynevych, R., Hao, Y., & Wang, Y. (2025). *Effect of anthropomorphism and perceived intelligence in chatbot avatars of visual design on user experience: accounting for perceived empathy and trust.* Obtenido de Frontiers in Computer Science: https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2025.1531976/full

Mozer, & V, S. (2019). *Russian Customs Academy.* Obtenido de https://cyberleninka.ru/article/n/sovershenstvovanie-instrumentov-tamozhennogo-regulirovaniya-tsifrovaya-tamozhnya-v-ramkah-raboty-postoyannogo-tehnicheskogo/viewer

OMA. (2021). Marco de Normas SAFE. Obtenido de https://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/~/media/C6CDF626AFB348FCA2AC59B796B79833.ashx

Popenici, S. A., & Kerr, S. (2017). *Exploring the impact of artificial intelligence on teaching and learning in higher education.*

Sánchez, & Villafranca. (2007). *SCMM-TOOL - tool for computer automation of the information security management systems.* Obtenido de Proceedings of the Second International Conference on Software and Data Technologies.: https://www.scitepress.org/Papers/2007/13310/13310.pdf?utm_source=chatgpt.com

Suha K. Assayed, Manar Alkhatib, & Khaled Shaalan. (2023). Obtenido de A Systematic Review of Conversational AIChatbots in Academic Advising: https://www.researchgate.net/publication/379449258_A_Systematic_Review_of_Conversational_AI_Chatbots_in_Academic_Advising

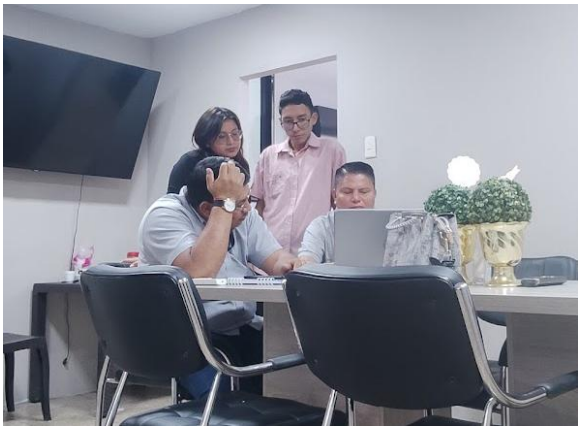
Valderrama. (2025). *Strategic Intelligence Tools Applicable to Customs Transit.* Obtenido de Journal of Information Systems Engineering and Management: https://www.jisem-journal.com/index.php/journal/article/download/5196/2452/8659

Zhu, Z. (2025). *Design and implementation of an intelligent sports management system (ISMS) using wireless sensor networks.* Obtenido de PeerJ. Computer Science, 11, e2637: https://doi.org/10.7717/peerj-cs.2637

# Anexos

***Anexo A.***

*Entrevista al Personal Clave*



***Anexo B.***

*Formato de Entrevista*

espol Escuela Superior Politécnica del Litoral

**FACULTAD DE CIENCIAS SOCIALES Y HUMANÍSTICAS**

**ENTREVISTA PARA EL PROYECTO INTEGRADOR DE LA CARRERA DE LICENCIATURA EN AUDITORÍA Y CONTROL DE GESTIÓN**

**Entrevistado:**
**Cargo:**
**Años de experiencia en el área:**

**EXPERIENCIA ACTUAL EN AUDITORÍA Y EVALUACIÓN SGSI**

1. ¿Cómo gestionan actualmente la seguridad de la información en su empresa?
2. ¿Qué normas de seguridad de la información conocen o aplican actualmente?
3. ¿Con qué frecuencia realizan auditorías o evaluaciones de su sistema de seguridad?
4. ¿Quién es responsable de las evaluaciones de cumplimiento normativo en su organización?
5. ¿Cuánto tiempo les toma completar una evaluación completa de su SGSI?

**HERRAMIENTAS UTILIZADAS Y LIMITACIONES ACTUALES**

6. ¿Qué herramientas utilizan para evaluar el cumplimiento de normas de seguridad?

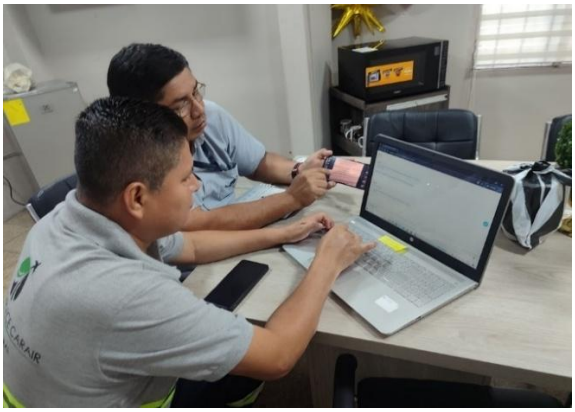
7. ¿Cómo documentan y almacenan las evidencias de cumplimiento normativo?
8. ¿Cuáles son las principales limitaciones de las herramientas que usan actualmente?
9. ¿Han considerado automatizar algún aspecto del proceso de auditoría? ¿Qué los ha detenido?

**PRINCIPALES DESAFÍOS EN GESTIÓN DE CUMPLIMIENTO**

10. ¿Cuál es el mayor desafío que enfrentan al evaluar el cumplimiento normativo?
11. ¿Han tenido situaciones donde no cumplieron con algún requisito normativo sin darse cuenta?
12. ¿Qué tan fácil o difícil es para ustedes acceder a información histórica de operaciones pasadas?
13. ¿Qué tan confiados se sienten de que están cumpliendo completamente con LOPDP, BASC o ISO 27001?
14. ¿Cómo afecta la gestión de cumplimiento normativo a la confianza de sus clientes?
15. ¿Cuáles son las principales dificultades que experimenta su organización para mantener un seguimiento actualizado de las modificaciones y actualizaciones en el marco normativo aplicable a su sector?

**EXPECTATIVAS DE AUTOMATIZACIÓN E INNOVACIÓN TECNOLÓGICA**

16. ¿En qué procesos considera que la digitalización o automatización les podría ayudar más?
17. Si pudiera automatizar un aspecto de la auditoría de seguridad, ¿cuál sería?
18. ¿Qué opina de usar un chatbot o asistente virtual para hacer consultas sobre cumplimiento normativo?
19. ¿Qué características debería tener una herramienta ideal de auditoría inteligente?
20. ¿Qué tan importante sería para ustedes tener un dashboard que muestre su estado de cumplimiento en tiempo real?
21. ¿Les gustaría recibir recomendaciones automáticas para mejorar su cumplimiento basadas en sus resultados?



***Anexo C.***

*Preguntas de Conocimiento del Usuario*

Escuela Superior Politécnica del Litoral

**FACULTAD DE CIENCIAS SOCIALES Y HUMANÍSTICAS**

**PREGUNTAS DE CONOCIMIENTO GENERAL Y CONTEXTO SITUACIONAL DEL USUARIO**

**CONOCIMIENTO GENERAL**

1. ¿Cuál es el nombre legal de su empresa?
2. ¿Cuál es el giro principal del negocio o sector en el que opera su organización?
3. ¿Cuántas personas conforman actualmente la empresa (empleados, contratistas, etc.)?
4. ¿En cuántas ciudades o ubicaciones opera su organización actualmente?
5. ¿Qué tipo de servicios o productos ofrece la empresa a sus clientes o usuarios?

**CONTEXTO SITUACIONAL**

6. ¿La empresa trata información de clientes, empleados o proveedores como parte de sus operaciones? ¿De cuáles de estos grupos?
7. ¿Existe dentro de la empresa alguna persona o área responsable de la gestión de la información?
8. ¿La información que maneja la empresa se encuentra organizada y clasificada de forma estructurada?

9. ¿Actualmente utilizan herramientas digitales (sistemas, aplicaciones, bases de datos, nube) para almacenar o gestionar la información de la empresa?
10. ¿Considera que en su organización existe conciencia sobre la importancia de gestionar adecuadamente la información?

***Anexo D.***

*Preguntas de Cumplimiento de los SGSI*

espol Escuela Superior Politécnica del Litoral

**FACULTAD DE CIENCIAS SOCIALES Y HUMANÍSTICAS**

**PREGUNTAS DEL CUMPLIMIENTO DEL SGSI FRENTE A LEYES Y MARCOS NORMATIVOS**

**GOBERNANZA Y DIRECCIÓN ESTRATÉGICA**

1. ¿Existe una política de seguridad de la información aprobada por la alta dirección y comunicada a todos los colaboradores?
   Referencia: ISO 27001 (cláus. 5.2), BASC 2022 (Est. 6.0.1), COBIT APO01, LOPDP Art. 15.
2. ¿Se encuentra definido un comité o responsable formal de la seguridad de la información con roles y responsabilidades documentados?
   Referencia: ISO 27001 (5.3), COBIT APO01.02, BASC 2022 (6.1).
3. ¿Los objetivos de seguridad de la información están alineados con los objetivos estratégicos de la empresa?
   Referencia: ISO 27001 (6.2), COBIT EDM01, BASC 6.0.1.
4. ¿Se realiza una revisión periódica de la efectividad del SGI por parte de la dirección?
   Referencia: ISO 27001 (9.3), COBIT MEA01.

**GESTIÓN DE RIESGOS**

5. ¿La empresa cuenta con un proceso documentado para identificar y evaluar riesgos de seguridad de la información?
   Referencia: ISO 27001 (6.1.2), COBIT APO12, BASC (6.2), LOPDP Art. 42.

6. ¿Se actualiza el análisis de riesgos al menos una vez al año o cuando ocurren cambios significativos?
   Referencia: ISO 27001 (6.1.3), COBIT APO12.03.
7. ¿Se definen planes de tratamiento para mitigar los riesgos identificados?
   Referencia: ISO 27001 (6.1.3), COBIT APO12.05, BASC 6.3.
8. ¿Se consideran los riesgos de terceros o proveedores que procesan información de la empresa?
   Referencia: ISO 27001 (A.5.19), BASC 5.1, LOPDP Art. 15.

**CUMPLIMIENTO LEGAL Y NORMATIVO**

9. ¿La empresa cuenta con un registro de cumplimiento de la LOPDP y otras regulaciones aplicables a su sector?
   Referencia: LOPDP Art. 47, COBIT APO12.
10. ¿Se gestionan las solicitudes de los titulares de datos (acceso, rectificación, eliminación) en los plazos establecidos por la LOPDP?
    Referencia: LOPDP Arts. 17–23.
11. ¿Se han firmado acuerdos de confidencialidad con todos los empleados y terceros que acceden a datos?
    Referencia: ISO 27001 (A.5.10), BASC 6.4, LOPDP Art. 15.
12. ¿La empresa mantiene evidencia documental de la base legal para el tratamiento de datos personales?
    Referencia: LOPDP Art. 7, COBIT DSS05.

**CONTROLES OPERATIVOS Y PROCEDIMIENTOS**

13. ¿Existe un inventario actualizado de activos de información (físicos y digitales) con sus propietarios definidos?
    Referencia: ISO 27001 (A.5.9), COBIT BAI09.
14. ¿Se aplican controles de acceso basados en roles y principio de privilegio mínimo?
    Referencia: ISO 27001 (A.5.15), BASC 6.5, COBIT DSS05.
15. ¿Se registran y monitorean los accesos a información sensible?
    Referencia: ISO 27001 (A.8.16), BASC 6.6, COBIT DSS06.

16. ¿Existen procedimientos para la clasificación y etiquetado de la información?
    Referencia: ISO 27001 (A.5.12), BASC 6.4.
17. ¿Se dispone de copias de respaldo (backups) y planes de restauración probados periódicamente?
    Referencia: ISO 27001 (A.8.13), COBIT DSS04.
18. ¿Se cuenta con procedimientos para el manejo seguro de soportes físicos y su destrucción segura?
    Referencia: ISO 27001 (A.8.10), BASC 6.4.

**SEGURIDAD EN LA CADENA DE SUMINISTRO Y TERCEROS**

19. ¿Se evalúa la seguridad de la información en los proveedores antes de su contratación?
    Referencia: ISO 27001 (A.5.19), BASC 5.1, COBIT APO10.
20. ¿Se monitorea periódicamente el cumplimiento de requisitos de seguridad por parte de proveedores?
    Referencia: ISO 27001 (A.5.20), COBIT APO10.05.
21. ¿Existen cláusulas contractuales que regulen el tratamiento de datos personales por terceros?
    Referencia: LOPDP Art. 15, BASC 5.1.

**GESTIÓN DE INCIDENTES**

22. ¿Se cuenta con un procedimiento documentado para la gestión de incidentes de seguridad de la información?
    Referencia: ISO 27001 (A.5.24), BASC 6.7, COBIT DSS02.
23. ¿Se notifican los incidentes de violación de datos a la autoridad de control dentro de los plazos establecidos?
    Referencia: LOPDP Art. 44.
24. ¿Se realizan análisis de causa raíz tras incidentes significativos?
    Referencia: ISO 27001 (A.5.25), COBIT DSS02.04.

**CAPACITACIÓN Y CULTURA ORGANIZACIONAL**

25. ¿Se capacita periódicamente al personal en seguridad de la información y protección de datos?
    Referencia: ISO 27001 (A.6.3), BASC 6.1, LOPDP Art. 47.
26. ¿Se realizan simulacros o pruebas de respuesta ante incidentes?
    Referencia: ISO 27001 (A.5.26), BASC 6.7.
27. ¿Se promueve la cultura de denuncia interna ante sospechas de incidentes o malas prácticas?
    Referencia: COBIT MEA01, BASC 6.1.

**MONITOREO Y AUDITORÍA**

28. ¿Se realizan auditorías internas del SGI con una periodicidad definida?
    Referencia: ISO 27001 (9.2), COBIT MEA02, BASC 6.8.
29. ¿Existen indicadores clave de desempeño (KPIs) para medir la eficacia de la seguridad de la información?
    Referencia: COBIT EDM05, ISO 27001 (9.1).
30. ¿Se revisan y actualizan las políticas y procedimientos de seguridad al menos una vez al año?
    Referencia: ISO 27001 (7.5.2), BASC 6.1.

**PROTECCIÓN FÍSICA Y AMBIENTAL**

31. ¿Se controla el acceso físico a las áreas donde se procesan datos sensibles?
    Referencia: ISO 27001 (A.7.1), BASC 6.5.
32. ¿Existen registros de visitantes y controles de ingreso a instalaciones críticas?
    Referencia: BASC 6.5, COBIT DSS05.
33. ¿Se protege el equipo contra daños ambientales (fuego, agua, temperatura extrema)?
    Referencia: ISO 27001 (A.7.2).

**CONTINUIDAD DEL NEGOCIO**

34. ¿Existe un plan documentado de continuidad del negocio que incluya la recuperación de la información?
    Referencia: ISO 27001 (A.5.29), COBIT DSS04, BASC 6.9.
35. ¿Se han realizado pruebas del plan de continuidad en el último año?
    Referencia: ISO 27001 (A.5.30), COBIT DSS04.

**GESTIÓN ESPECÍFICA DE DATOS PERSONALES**

36. ¿Se minimiza el tratamiento de datos personales recolectando únicamente lo estrictamente necesario?
    Referencia: LOPDP Art. 8, ISO 27001 (A.5.14).
37. ¿Se han implementado medidas para garantizar la exactitud y actualización de los datos personales?
    Referencia: LOPDP Art. 9.
38. ¿Se aplican mecanismos para anonimizar usuarios cuando corresponde?
    Referencia: LOPDP Art. 31, ISO 27001 (A.8.11).

**MEJORA CONTINUA**

39. ¿Se documentan y aplican las lecciones aprendidas tras auditorías, incidentes o pruebas?
    Referencia: ISO 27001 (10.1), COBIT MEA02.
40. ¿Existe un proceso formal de mejora continua del SGI?
    Referencia: ISO 27001 (10.2), COBIT APO11, BASC 6.8.