TEMA:

Sistema de Gestión de Seguridad de la Información Orientado a Empresas De Servicios Auxiliares de Entidades Financieras

AUTOR:

Angel Eduardo Orellana Román

PROYECTO PRESENTADO PARA OPTAR AL TÍTULO EN:

Tecnólogo en Desarrollo de Software

TUTOR ACADÉMICO:

Ing. Marco Aurelio Guamán

CUENCA – ECUADOR, 2025

CARRERA DE DESARROLLO DE SOFTWARE

CERTIFICACIÓN DEL TUTOR

Aprobación del Trabajo de Titulación

Doy fe que el trabajo desarrollado por el estudiante: ANGEL EDUARDO ORELLANA ROMÁN, con el título "SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ORIENTADO A EMPRESAS DE SERVICIOS AUXILIARES DE ENTIDADES FINANCIERAS" cumple con los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del jurado examinador que se designe

Atentamente,

MARCO GUAMÁN BUESTAN

CI: 0301707030

DECLARACIÓN DE AUTORÍA DEL TRABAJO

Yo, Orellana Román Angel Eduardo, estudiante del Instituto Tecnológico Superior Particular Sudamericano de la ciudad de Cuenca - Ecuador, que cursó la Tecnología en Desarrollo de Software, declaro en forma libre y voluntaria que la presente investigación que versa sobre "Sistema de Gestión de Seguridad de la Información Orientado a Empresas De Servicios Auxiliares de Entidades Financieras" así como las expresiones vertidas en la misma, son autoría de la compareciente, quien ha realizado en base a recopilación bibliográfica, consultas de internet y consultas de campo.

En consecuencia, asumo la responsabilidad de la originalidad de la misma y el cuidado al remitirme a las fuentes bibliográficas respectivas para fundamentar el contenido expuesto.

Atentamente,

Orellana Román Angel Eduardo

CI:0704785872

DERECHOS DE AUTOR

DEDICATORIAS

Con profunda gratitud, se entrega este trabajo a aquellos que han sido un apoyo incondicional en cada aspecto personal:

Quiero dedicar este proyecto a las personas que en todo momento me han apoyado. A mis padres quienes no han perdido la fe en que yo pueda conseguir este título profesional, este logro también es de ustedes.

A mi familia, mi esposa y mis hijos que son la inspiración más grande que tengo para seguir buscando un mejor futuro y siempre a aspirar a más, como persona y profesional.

Y a Dios, quien ha llenado mi camino de personas maravillosas con quienes siempre he podido contar y que ahora son parte del exitoso termino de esta etapa de mi vida.

AGRADECIMIENTOS

Gracias Padre Celestial por permitirme estar hoy en estas instancias. Sin tu bendición nada sería posible.

Gracias familia por su apoyo, su paciencia y cariño, por esperar de mí siempre un poco más en todo aspecto y ser una inspiración.

Gracias al Instituto Tecnológico Superior Particular Sudamericano, y a sus docentes, quien nos brinda la oportunidad de aspirar a un mejor futuro a través de su gestión educativa superior y particularmente por comprender la situación de quienes debemos dividir el tiempo entre el trabajo, la familia y los estudios.

ÍNDICE

INDICE DE TABLAS

INDICE DE ILUSTRACIONES

RESUMEN

Actualmente, el creciente uso de tecnologías digitales genera una gran cantidad de información, incrementando su importancia y siendo vital en la toma de decisiones y el desarrollo organizacional. Sin embargo, este crecimiento también expone a las organizaciones a mayores riesgos de seguridad al aumentar la cantidad de medios de comunicación que proteger lo que refuerza la necesidad de implementar sistemas que protejan esta información (Himeur et al., 2022, como se citó en Nikiforova, 2022).

Al ser BESTTECH SAS, una empresa dedicada al desarrollo de software y que se desempeña como proveedor de servicios auxiliares para entidades financieras, adquiere una gran responsabilidad para mantener segura la información que sus clientes le comparten para el desarrollo de sus actividades. Sin embargo, no dispone de un SGSI, que garantice la confidencialidad, integridad y disponibilidad de los activos de información generando riesgos internos y para sus clientes.

El propósito es diseñar e implementar un SGSI basado en el estándar ISO/EC 27001:2022, y generar los controles, políticas, procedimientos y manuales que permitan mitigar el riesgo operativo interno brindando la seguridad exigida por sus clientes y las entidades de control del ámbito financiero cooperativo. Esta implementación se realizó adoptando el estándar internacional ISO/ICE 27003. La investigación exigió definir el SoA, que se realizó a partir del resultado del análisis de GAP al inicio del proyecto pudiendo determinar los activos de información, procesos y actividades involucradas que también permitió la identificación de vulnerabilidades, cálculo del riesgo, definir la criticidad que representa el riesgo y los controles necesarios para su mitigación. Se evidencio que es imperativa la implementación del SGSI por la carencia de controles, incluso en procesos básicos, donde no se consideraban medidas de seguridad generando niveles críticos de inseguridad de los activos de la información.

Palabras clave: Sistema, gestión, seguridad, información, financiero.

ABSTRACT

Currently, the growing use of digital technologies generates a large amount of information, increasing its importance and making it vital in decision-making and organizational development. However, this growth also exposes organizations to greater security risks by increasing the number of communication channels that need to be protected, reinforcing the need to implement systems that protect this information (Himeur et al., 2022, as cited in Nikiforova, 2022).

As BESTTECH SAS is a company dedicated to software development and acts as an auxiliary service provider for financial institutions, it has a great responsibility to keep the information that its clients share with it for the development of their activities secure. However, it does not have an Information Security Management System (ISMS) in place to guarantee the confidentiality, integrity, and availability of information assets, creating internal risks and risks for its clients.

The purpose is to design and implement an ISMS based on the ISO/EC 27001:2022 standard and to generate the controls, policies, procedures, and manuals that will mitigate internal operational risk, providing the security required by its clients and the regulatory entities in the cooperative financial sector. This implementation was carried out by adopting the international standard ISO/ICE 27003. The research required defining the SoA, which was done based on the results of the GAP analysis at the beginning of the project, making it possible to determine the information assets, processes, and activities involved, which also allowed for the identification of vulnerabilities, risk calculation, definition of the criticality represented by the risk, and the controls necessary for its mitigation. It became clear that the implementation of the ISMS was imperative due to the lack of controls, even in basic processes, where security measures were not considered, generating critical levels of insecurity for information assets.

Key words: System, management, security, information, financial.

INTRODUCCIÓN

Actualmente, las organizaciones consideran un pilar fundamental a los activos de información que mantienen, debido al poder de decisión que permite su análisis. Si nos enfocamos a las entidades financieras estos activos son más valiosos.

Este sector está es constantemente amenazado por ciber criminales y cada participante de este ámbito puede volverse un objetivo. Por ende, es vital que las empresas que funcionan como proveedores de servicios auxiliares tomen las medidas necesarias para mitigar el riesgo siendo la más representativa y adecuada, la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).

BESTTECH SAS, empresa dedicada al desarrollo de software financiero (Core Financiero), como proveedor de un servicio auxiliar y consiente de la real importancia de un SGSI, ha decidido aprobar su implementación brindando la apertura y apoyo necesarios para culminar cada actividad de este con éxito permitiendo el desarrollo expedito del proyecto de tesis presentado.

La propuesta presentada nace del riesgo inherente de seguridad de la información que actualmente se mantiene en la empresa por la falta de controles, políticas y buenas prácticas que pueden repercutir en efectos no deseados como la fuga de información, vulnerabilidades en el código fuente entre otras consecuencias que afectarían de forma directa a los clientes, como cooperativas, cajas, etc., disminuyendo la confianza de los usuarios hacia el sector financiero cooperativo.

Este proyecto expondrá el lector las fases de implementación de un SGSI en una empresa de desarrollo de software financiero y podrá conocer las particulares necesidades y exigencias en seguridad de la información que implica trabajar en este giro de negocio.

Como objetivos y producto final esperado se detectarán las vulnerabilidades en los procesos internos, pudiendo establecer los controles, políticas, procedimientos y manuales necesarios para robustecer la seguridad y proteger los activos de información que están bajo la responsabilidad de la empresa, generando confianza, fortaleciendo la relación con los clientes y fomentando la cultura de seguridad de la información vital para este sector.

Objetivos de la investigación

Implementar un Sistema de Gestión Seguridad de la información (SGSI) aplicando el estándar internacional ISO/IEC/27001 en una empresa de Cuenca especializada en el desarrollo de software para entidades financieras (Core Financiero) a partir de los resultados del análisis GAP.

Realizar un análisis de riesgos para identificar vulnerabilidades en los procesos de desarrollo de software y gestión de datos de clientes.

Satisfacer los requisitos de seguridad de los clientes y otras partes interesadas.

Cumplir con los objetivos de seguridad de información de la organización.

Diseñar y documentar políticas y procedimientos de seguridad de la información

Cumplir con las regulaciones, leyes y obligaciones sectoriales.

Proponer un plan de auditoría interna para la evaluación de los controles implementados en el SGSI.

Preguntas de investigación

¿Cuáles son los riesgos de seguridad de la información más relevantes en una empresa de desarrollo de software financiero que justifican la implementación de un SGSI?

¿Qué controles del Anexo A de la ISO/IEC 27001:2022 son prioritarios para proteger la confidencialidad, integridad y disponibilidad de la información en el ciclo de desarrollo de software financiero?

¿Cómo impacta la implementación de un SGSI en los procesos operativos y de desarrollo de software en una empresa de software financiero?

¿Qué factores críticos deben considerarse para la implementación exitosa y efectiva de un SGSI en una empresa dedicada al desarrollo de software financiero?

¿Cuáles son los beneficios tangibles e intangibles que obtiene una empresa de desarrollo de software financiero tras implementar un SGSI?

Justificación

En la era digital, la seguridad de la información se ha convertido en un pilar crítico para las organizaciones, especialmente en el sector financiero, donde los datos sensibles y las transacciones requieren altos estándares de protección. El aumento exponencial de ciberataques, como ransomware, phishing y brechas de datos, ha expuesto vulnerabilidades en los sistemas informáticos, generando pérdidas millonarias y daños reputacionales. "*Según el Verizon Data Breach Investigations Report (2023), el sector financiero concentra el 23% de los ciberataques a nivel global, siendo el más vulnerable después del sector tecnológico"*, lo que demuestra la urgencia de implementar soluciones robustas.

Además, el cumplimiento de regulaciones como la Ley Orgánica de Protección de Datos Personales (LOPD) en Ecuador o estándares internacionales como ISO 27001 exige que las empresas adopten medidas proactivas para garantizar la confidencialidad, integridad y disponibilidad de la información. Un SGSI no solo mitiga riesgos, sino que también fortalece la competitividad de las organizaciones al demostrar su compromiso con la protección de datos.

Este proyecto tiene como objetivo diseñar e implementar un SGSI adaptado a las necesidades de una empresa desarrolladora de software que presta servicios a entidades financieras. Su finalidad es proteger los activos informáticos (datos, aplicaciones e infraestructura) mediante controles técnicos y administrativos. Garantizar el cumplimiento normativo con los requerimientos legales y contractuales exigidos por los clientes del sector financiero. Generar confianza en los clientes al asegurar que sus datos están gestionados bajo estándares internacionales.

Este proyecto beneficia directamente a la empresa de desarrollo de software donde laboro, que contará con un marco estructurado para gestionar riesgos, evitar sanciones por incumplimiento y diferenciarse en el mercado como un proveedor seguro. También el personal interno, que adquirirá conocimientos en ciberseguridad y mejores prácticas.

A las entidades financieras clientes, quienes verán reforzada la seguridad de sus sistemas al estar respaldados por un proveedor con un SGSI implementado, y a los usuarios finales, cuyos datos personales y transacciones estarán mejor protegidos, previniendo robos de identidad o fraudes.

Concluyendo, la implementación de este SGSI no solo responde a una necesidad técnica, sino que también aporta valor estratégico al alinear la operación de la empresa con los desafíos actuales de la ciberseguridad. Este proyecto contribuirá a la

sostenibilidad del negocio, la fidelización de clientes y la protección de un ecosistema digital cada vez más amenazado.

CAPÍTULO I: PROBLEMÁTICA

Las empresas dedicadas al desarrollo de software y que directamente colaboran con las operaciones de las entidades financieras deben manipular altos volúmenes de información siendo también muy variada, entre ellas datos personales de clientes, información crediticia, capacidad de pago, ingresos mensuales, entre otra información que por su magnitud debe ser tratada con los estándares adecuados de seguridad.

En este contexto para BESTTECH SAS, empresa proveedora de servicios auxiliares, es imperativo la implementación un SGSI que permita a la empresa de desarrollo, establecer políticas, controles, procedimientos y metodologías para salvaguardar este tipo de información, acogiendo las buenas prácticas y extendiendo la cultura de seguridad de la información en todos sus procesos internos.

Actualmente, en la empresa antes mencionada los controles para manipular la información, como la recibida desde los clientes o interna como el código fuente, es muy escasa en ciertas actividades volviendo vulnerable cada proceso y poniendo en riesgo su integridad, confidencialidad y disponibilidad.

Entre otros aspectos, se carece de un inventario de activos de información ocasionando un manejo inadecuado de los datos al desconocer su criticidad para los interesados.

El presente proyecto busca fortalecer la seguridad de la información, evaluando su estado inicial en este aspecto y minimizando los riesgos asociados a ser víctimas de

un ciberataque, fugas de información e incumplimiento normativo lo que generaría un aumento en la confianza de los clientes y usuarios del sector cooperativo.

Bajo este contexto es inevitable las preguntas como:

¿Cómo identifico las vulnerabilidades o brechas de seguridad de la información que existen en la empresa?

¿Cómo determino el riesgo que generan estas vulnerabilidades en la seguridad de la información?

¿Cuáles son los activos de información que debe proteger el SGSI?

¿Cómo identifico los controles de la norma ISO/EC27001:2022 puedo aplicar en la implementación del SGSI para mitigar el riesgo?

¿Qué aspectos técnicos u organizacionales pueden ser un desafío para la implementación exitosa del SGSI?

CAPÍTULO II: MARCO REFERENCIAL

2.1 Marco Teórico

En la actualidad el crecimiento tecnológico es vertiginoso, y cada aspecto de la vida de las personas se interconecta con mayor facilidad. Bajo esta premisa, la cantidad de información que circula en la red es inconmensurable, sin embargo, eso no significa que transita de forma segura.

Pero hay ámbitos en donde la seguridad de la información es prioridad y uno de ellos es el sector financiero, que por obvios motivos está bajo constante amenaza y las instituciones se han dedicado a fortalecer medidas de seguridad para proteger sus activos de información.

Uno de los pilares utilizados para resguardar la información es la implementación de la ISO/EC 27001, que es el estándar internacional más aceptado para garantizar la seguridad de los activos de información.

Las entidades financieras cuentan con proveedores de servicios auxiliares para solventar necesidades de automatización de procesos y son estas las encargadas de manejar sus bancos de información críticos, lo que vuelve imperativo que estas empresas dedicadas a dar soporte en el sector financiero implementen sistemas de seguridad que garanticen la integridad, confidencialidad y disponibilidad de los datos.

Para ello lo más recomendado es la implementación de un SGSI bajo el estándar propuesto por la ISO/ECm27001. Esta metodología propone actuar acorde al marco de trabajo Planificar, Hacer, Verificar y Actuar (PDVA) lo que permitirá una actitud proactiva frente a los riesgos de seguridad (Ladino et al, 2011).

Este sistema de seguridad se basa en los riesgos, por ende, dentro de su implementación se realiza un análisis para identificar y tratar los riesgos vinculados con la información. Adicional, la gestión del riesgo debe estar alineada con los objetivos estratégicos de la organización, de manera especial debido a su giro de negocio de desarrollo de software constantemente amenazado (Tipton y Nozaki, 2012).

Uno de los factores para una implementación exitosa es el apoyo y compromiso de la alta dirección quien está encargada de facilitar recursos económicos, la colaboración del personal que labora dentro de la empresa, liderando con compromiso el desarrollo del proyecto maximizando su efectividad para afrontar las amenazas se seguridad (Von Solms y Van Niekerk, 2013).

La seguridad de la información no solo depende del área de tecnología sino también del personal que maneja los datos y que constantemente debe ser capacitado

para asimilar la importancia de mantener segura la información a su cargo (Whitman y Mattord, 2010).

El objetivo de implementar un SGSI es garantizar los principios de integridad, confidencialidad y disponibilidad de la información, pilares esenciales que si no son considerados pueden ocasionar verdaderos desastres económicos que disminuiría la confianza del cliente directamente ((Rodríguez, Fernández y Fernández, 2023) y entre muchas de las medidas que contempla esta metodología están los controles de acceso basados en roles para evitar ingresos no autorizados (Marreros, Acosta y Mendoza, 2024).

Sin embargo, un sistema de seguridad exitoso debe crearse a medida de la empresa y sus objetivos de seguridad, basado en su entorno donde se deben considerar las amenazas a las que está expuesto y las vulnerabilidades (Stallings,2017).

Una vez implementado el SGSI se debe realizar una auditoría interna para verificar que las medidas de seguridad implementadas se están aplicando por el personal maximizando su efectividad. El SGSI ingresa en un ciclo de mejora continua donde periódicamente será evaluado y que los controles están vigentes para afrontar las nuevas exigencias de seguridad (Humphrey,1989).

Por último, se debe considerar la legislación nacional que a través de la Ley Protección de Datos Personales dispuesta desde el 2021 en Ecuador, advierte tomar el enfoque de privacidad desde el diseño, que intenta mitigar el riesgo de seguridad de las primeras etapas de implementación de un sistema (Cavoukian, 2009).

2.1 Marco Contextual

La seguridad de la información ha cobrado creciente importancia en el contexto ecuatoriano, especialmente en empresas dedicadas al desarrollo de software, las cuales

manejan datos sensibles de clientes y usuarios. En la ciudad de Cuenca, varias organizaciones del sector tecnológico han adoptado prácticas de desarrollo ágil y arquitecturas basadas en la nube, lo cual incrementa su exposición a riesgos cibernéticos.

La ausencia de políticas robustas de seguridad en muchas de estas empresas representa una vulnerabilidad crítica, especialmente ante amenazas como el robo de propiedad intelectual, la fuga de datos personales o ataques dirigidos. En este contexto, la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001:2022 se presenta como una estrategia clave para fortalecer los niveles de protección en los procesos internos y garantizar la confianza de los clientes y socios comerciales.

BESTTECH SAS opera en el sector del desarrollo de software a medida, brindando soluciones informáticas a clientes locales y nacionales. Sin embargo, como muchas pequeñas y medianas empresas de este rubro, carece de un enfoque organizacional y técnico para gestionar los riesgos asociados a la información. Este escenario plantea la necesidad urgente de adoptar un SGSI para proteger los activos de información, asegurar la continuidad del negocio y cumplir con requisitos normativos cada vez más exigentes, como últimamente lo es la Ley Orgánica de Protección de Datos Personales del Ecuador.

2.3 Marco Conceptual

Para comprender el alcance y objetivos de la presente investigación, es necesario definir los conceptos clave utilizados en su desarrollo y que hacen referencia a la gestión de seguridad de la información y su aplicación en entornos de desarrollo de software:

Alcance

Aspectos y áreas de la organización que abarca el SGSI (ISO/EC27000, 2024).

Amenaza

Origen de un evento no deseado, puede perjudicar a la organización o parte de ella (ISO/EC27000, 2024).

Análisis de riesgos

Actividad realizada para entender la afectación que podría causar la materialización del riesgo proporcionando una magnitud o nivel de riesgo (ISO/EC27000, 2024).

Confidencialidad

Termino que hace alusión a que la información no puede ser expuesta a quien no este autorizado (ISO/EC27000, 2024).

Control

Son las medidas enfocadas a disminuir el riesgo estableciendo las políticas, los procedimientos, las prácticas y las estructuras organizativas para modificar el riesgo de seguridad a niveles aceptable para la organización (ISO/EC27000).

Control correctivo

Medida implementada para reforzar o corregir un control que no cumplió con mitigar el riesgo de forma efectiva y que permitió la materialización del riesgo (ISO/EC27000, 2024).

Control preventivo

Medida establecida para evitar que una amenaza llegue a materializarse gestionando el riesgo (ISO/EC27000, 2024).

Declaración de aplicabilidad

Apartado donde se registra los controles del Anexo A de la ISO/EC 27001 que pueden aplicados en la organización a partir de la evaluación de riesgos. Es necesario registrar la justificación de la inclusión o exclusión de los controles (ISO/EC 27001, 2022).

Disponibilidad

Describe la propiedad de la información para estar disponible para su utilización cuando sea requerida (ISO/EC27000, 2024).

Evento de seguridad de la información

Ocurrencia identificada de un sistema, servicio o estado de la red que indica una posible violación de información seguridad política o fallo de control, o una situación previamente desconocida que puede ser relevante para la seguridad (ISO/EC27000).

Gestión de riesgos

Conjunto de actividades orientadas a mitigar y controlar el riesgo de una organización (ISO/EC27000, 2024).

Identificación de riesgos

Actividades realizadas para encontrar los riesgos y describirlos (ISO/EC27000, 2024).

Impacto

Se describe como la magnitud de la afectación de forma negativa debido a un incidente de seguridad. El impacto puede ser medido de forma monetaria, reputacional, legal, etc. (ISO/EC27000, 2024).

Incidente de seguridad de la información

Evento o serie de eventos que pueden comprometer la integridad de la información pudiendo afectar las operaciones de la organización de manera parcial o total.

Integridad

Propiedad de salvaguardar la exactitud y el estado completo de los activos (ISO/EC27000).

Organización

Normalmente una entidad o persona con actividades definidas para conseguir sus objetivos estratégicos. Esta entidad puede estar bajo supervisión de un organismo de control (ISO/EC27000, 2024).

Plan de tratamiento de riesgos

Plan de actividades establecidas para remediar una situación de riesgo que no se puede aceptar mediante el uso de controles o medidas de seguridad (ISO/EC27000).

Política

Intenciones y dirección de una organización, tal como lo expresa formalmente su alta dirección (ISO/EC27000).

Proceso

Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas (ISO/EC27000).

Propietario del riesgo

Persona o entidad con responsabilidad y autoridad para gestionar un riesgo (ISO/EC27000).

Riesgo

Posibilidad de que una amenaza pueda materializarse a través de la explotación de vulnerabilidades de un sistema o proceso. Este suceso puede provocar daños en la organización. Su cálculo es posible con el producto del impacto por la probabilidad (ISO/EC27000, 2024).

Riesgo residual

Es el riesgo que el control implementado no puede eliminar y que persiste tras tratar el riesgo (ISO/EC27000, 2024).

Seguridad de la información

Conjunto de medidas y prácticas orientadas a proteger la confidencialidad, integridad y disponibilidad de la información ante amenazas internas o externas (ISO/IEC 27000).

Sistema de Gestión de la Seguridad de la Información (SGSI)

Conjunto de elementos interrelacionados que puede contemplar la estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua (ISO/EC27000).

Tratamiento de riesgos

Proceso de modificar el riesgo, mediante la implementación de controles (ISO/EC27000, 2024).

Vulnerabilidad

Punto débil en la seguridad de un activo o control que puede ser explotada por una o más amenazas (ISO/EC27000, 2024).

ISO/IEC 27001

Es un estándar internacional que define los requerimientos para SGSI. Su primera publicación fue en 2005; segunda edición en 2013, la tercera y actual edición se la realiza en 2022 incluyendo como alcance ciberseguridad y protección de la privacidad. Es la norma en base a la cual se certifican los SGSI a nivel mundial.

Gestión de riesgos

Proceso sistemático para identificar, analizar y tratar los riesgos que podrían afectar los activos de información, guiado por la norma ISO/IEC 27005.

Controles de seguridad

Medidas administrativas, técnicas o físicas implementadas para reducir los riesgos a niveles aceptables. Se clasifican comúnmente en preventivos, detectivos y correctivos (ISO/IEC 27002).

Desarrollo seguro de software

Práctica que consiste en incorporar principios y controles de seguridad desde las primeras fases del ciclo de vida del software, a través de metodologías como DevSecOps.

Privacidad y protección de datos personales

Principios y mecanismos legales y técnicos que aseguran el tratamiento legítimo, proporcional y seguro de la información personal, conforme al RGPD y la ISO/IEC 27701.

PDCA

Plan-Do-Check-Act. Este modelo se basa en un ciclo iterativo de las actividades planificar, realizar, verificar y actuar. Donde en cada nueva iteración se puede obtener una mejor versión de la implementación anterior.

CAPÍTULO III: METODOLOGÍA DE INVESTIGACIÓN

Este proyecto se desarrollará realizando un análisis documental y normativo con la recolección de datos empíricos recopilados a través de técnicas aplicadas en la organización. Se analizará el estado actual de la empresa para establecer un estado inicial de la aplicación de la seguridad de la información para luego proponer un plan de tratamiento de riesgos basado en la ISO/EC 27001 que este alineado a los objetivos de la empresa.

3.1 Enfoque de investigación

Este trabajo se desarrolló con un enfoque cuantitativo, a través del cual se podrán obtener datos medibles, generando la estadística necesaria que permitirá conocer el nivel de conocimiento y aplicación por parte del personal involucrado acerca de la norma ISO/IEC 27001:2022 en la empresa desarrolladora de software. Este enfoque permite conocer el estado actual de la empresa en cuanto al manejo de la seguridad de la información por parte del personal interno y de los usuarios finales que utilizaran el core financiero.

Según Hernandez, Fernandez y Baptista (2014), una característica del enfoque cuantitativo es la recolección de datos para validar una hipótesis, sin embargo, en este caso ese enfoque será utilizado para obtener información diagnóstica acerca del conocimiento del personal involucrado con respecto a la seguridad de la información.

En esta investigación se utilizarán encuestas para la obtención de los datos, dirigidas a colaboradores de distintas áreas de la empresa y de usuarios finales. Este enfoque nos proporcionará una visión general y confiable acerca de la concienciación de la norma ISO/IEC de las partes interesadas. Adicionalmente, podrá facilitar la toma de decisiones durante la implementación de medidas correctivas que introducirá el SGSI.

3.2 Tipo de investigación

El presente trabajo corresponde a una investigación descriptiva aplicada, y su finalidad es realizar la implementación práctica de un SGSI en una empresa dedicada al desarrollo de software especializado para entidades financieras, basado en la norma ISO/IEC 27001:2022. Mencionando a Tamayo y Tamayo (2004), el objetivo de la investigación aplicada es utilizar teorías ya existentes, adaptarlas según sea el caso de estudio o el problema concreto para resolver. La problemática que impulsa este caso robustecer las medidas de seguridad para proteger la información mediante el uso de un modelo internacional normado y validado.

3.3 Corte de la investigación

Para esta investigación se utiliza un diseño transversal (o diseño de corte), que permite recopilar datos en un punto específico del tiempo sin realizar seguimiento longitudinal. Una característica de este enfoque es su rapidez**,** economía y muy adecuado para evaluar estados actuales de variables como cumplimiento de normas, percepción de riesgos o adopción de buenas prácticas. Si bien no permite establecer relaciones causales, permite identificar con eficacia asociaciones para futuras investigaciones (Wang & Cheng, 2020).

Las características de este diseño se acoplan a la metodología adoptada para el estudio, donde se plantea obtener una primera visión organizacional del estado actual de la empresa para resguardar adecuadamente la información a su cargo. Este primer contacto nos dará la pauta para el desarrollo del proyecto y en sus fases finales será el punto de comparación y validación de resultados.

Dado que el proyecto se enfoca en la implementación y verificación del SGSI en un entorno práctico, no amerita un estudio longitudinal de variables que dependen del tiempo.

El análisis o diseño transversal es suficiente para adquirir los resultados y alcanzar las metas establecidas. Sin embargo, la empresa entrara en un proceso de maduración que poco a poco se puede extender de acuerdo lo necesite en el futuro.

3.4 Instrumentos y técnicas para el levantamiento de la información

Para el diseño, desarrollo e implementación del SGSI, se emplearon las siguientes técnicas e instrumentos:

Técnicas

Revisión bibliográfica y documental. Análisis de artículos de implementación de SGSI, manuales técnicos de la ISO/EC 27000, 27001, Requisitos SGSI, 27002 Guía de Implementación de Controles, 27003 Guía de Implementación SGSI, 27005 Gestión de Riesgo SGSI, 27701 Protección de datos personales, normativa de la SEPS acerca de la Seguridad de la Información para Entidades del Sector Financiero Popular y Solidario (Superintendencia de la Economía Popular y Solidaria).

Encuestas. Como técnica principal para recopilar información se utilizará la encuesta que estará compuesta por preguntas (22) cerradas permitiendo obtener información específica y comparable de forma rápida. Así se podrá medir el nivel de comprensión, percepción y aplicación acerca de la seguridad de la información.

Se utilizará Google Forms para proporcionar la encuesta lo que también facilita la tabulación y análisis de datos. Los grupos de interés a los cuales va dirigida la encuesta son:

- Desarrolladores de Software

- QA / Testing
- DevOps
- Gestión / Dirección de área
- Usuarios administrativos / áreas funcionales (RRHH, Finanzas, Comercial, etc.)

3.5 Población y muestra

El presente desarrollo investigativo se realizó con la participación de los dueños de los procesos de cada área y quienes participan en el desarrollo de las actividades.

Población

Los siguientes grupos principales conforman la población, vinculados con el uso de activos de información:

Desarrolladores de Software. Que elaboran directamente las funcionalidades del software financiero manejando IDEs de desarrollo, bases de datos internas y externas, repositorios en la nube y respaldos de código fuente y datos.

QA / Testing. Que se encarga del testeo y verificación de funcionalidades del producto final de software antes de ser utilizado por el cliente o usuario final.

DevOps. Es quien administra la infraestructura (física o en la nube) para asegurar que los entornos de desarrollo, pruebas y producción estén correctamente configurados y disponibles. También se encarga de controlar las versiones del software y coordinar despliegues progresivos o reversión ante errores.

Gestión / Dirección de área. Es quien planifica, coordina, supervisa y evalúa el trabajo dentro del departamento de desarrollo de software y que sus actividades siempre estén alineadas con los objetivos estratégicos de la empresa.

Usuarios administrativos / áreas funcionales (RRHH, Finanzas, Comercial, etc.). Colaboradores o usuarios finales quienes operan en el Core Financiero en distintas áreas de las entidades financieras.

Muestra

Internamente dado que la empresa es relativamente pequeña y existe un solo encargado para cada área, menos desarrolladores los cuales con tres, prácticamente la muestra fue el universo completo en cada área. Sin embargo, para los usuarios finales, la muestra tuvo variaciones de entre el 10 y 20 por ciento de cada área encuestada.

3.6 Metodología de trabajo

Por la naturaleza del proyecto de investigación se utilizó la Guía de Implementación estructurada en la ISO/EC 27003, que nos proporciona orientación practica y útil para una empresa que está en proceso de implementación de un SGSI conforme a los requisitos de la norma ISO/EC 27001. Esta guía nos permite identificar las fases y actividades en un proceso ordenado y eficiente.

Entre otras actividades nos ayudará en:

Contribuye a obtener el compromiso y apoyo de la alta dirección para implementar el SGSI.

Definir el alcance de la implementación.

Facilita la toma de decisiones para establecer los recursos necesarios para el éxito de la implementación.

Definir roles de cada colaborador en los procesos internos de la empresa.

Permite establecer plazos más acertados para el cumplimiento de actividades de implementación del SGSI.

CAPÍTULO IV: ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

Este capítulo presenta el análisis detallado de los resultados obtenidos a partir de la encuesta aplicada en diferentes áreas clave dentro de la empresa de desarrollo, donde se incluyen al equipo de desarrollo, QA/Testing, DevOps, Gestión/Dirección de área y usuarios finales de una empresa cliente. El objetivo de esta recolección de datos fue identificar el nivel de conocimiento, percepción y prácticas actuales referentes a la seguridad de la información, así como detectar debilidades (vulnerabilidades), amenazas y oportunidades que afectan al entorno organizacional.

Estos resultados se interpretan en función de los objetivos específicos del estudio, donde se evalúa el estado inicial de la organización en relación con los controles establecidos en la implementación de la norma ISO/IEC 27001:2022 considerando los pocos controles de seguridad, la alta dependencia tecnológica y la exposición a riesgos informáticos reales.

Este análisis proporciona una base objetiva para sustentar las decisiones técnicas y estratégicas adoptadas en el diseño del SGSI, facilitando la priorización de acciones correctivas y preventivas según los hallazgos más relevantes identificados en cada grupo de interés. La interpretación de los datos busca, además, evidenciar la evolución de la organización en su camino hacia el fortalecimiento de su postura de seguridad de la información.

A través de este análisis podemos sustentar la toma de decisiones técnicas y organizativas propuestas por el SGSI, nos ayuda a determinar las acciones correctivas y preventivas con una prioridad acorde a la situación real de la empresa y generar una proyección de madurez organizacional respecto a la seguridad de la información.

El análisis de las encuestas se realizó utilizando una hoja de cálculo de Excel importando la información desde Google Forms.

Preguntas de la encuesta:

Sección 1: Datos generales

1. Área a la que pertenece:

[ ] Desarrollo de Software
[ ] QA / Testing
[ ] DevOps
[ ] Gestión / Dirección de área
[ ] Usuarios administrativos / áreas funcionales (RRHH, Finanzas, Comercial, etc.)

2. Tiempo de trabajo en la empresa:

[ ] Menos de 1 año
[ ] 1 a 3 años
[ ] Más de 3 años

3. ¿Ha recibido formación en seguridad de la información en el último año?

[ ] Sí
[ ] No

Sección 2: Conocimiento y prácticas personales

4. ¿Con qué frecuencia cambia sus contraseñas de acceso a sistemas o plataformas?

[ ] Cada 3 meses o menos
[ ] Cada 6 meses
[ ] Una vez al año
[ ] Nunca

5. ¿Utiliza autenticación multi factor (MFA) en las plataformas críticas de trabajo?

[ ] Siempre
[ ] A veces
[ ] Nunca
[ ] No sabe si está habilitado

6. ¿Evita compartir credenciales con otros colaboradores?

[ ] Siempre
[ ] A veces
[ ] Nunca

7. ¿Conoce y aplica políticas internas sobre uso adecuado del correo electrónico y dispositivos?

[ ] Sí, totalmente
[ ] Conozco algunas
[ ] No conozco ninguna

8. ¿Cuán preparado(a) se siente para identificar correos o enlaces sospechosos (phishing)?

[ ] Muy preparado(a)
[ ] Algo preparado(a)
[ ] Poco preparado(a)
[ ] Nada preparado(a)

Sección 3: Percepción y cultura de seguridad

9. La empresa promueve una cultura de seguridad de la información en su entorno laboral.

[ ] Totalmente de acuerdo
[ ] De acuerdo
[ ] En desacuerdo
[ ] Totalmente en desacuerdo

10. ¿Considera que la seguridad de la información es una responsabilidad compartida por todo el personal?

[ ] Totalmente de acuerdo
[ ] De acuerdo
[ ] En desacuerdo
[ ] Totalmente en desacuerdo

11. En caso de detectar una vulnerabilidad o incidente, ¿sabe cómo y a quién reportarlo?

[ ] Sí
[ ] No
[ ] No estoy seguro(a)

12. ¿Cree que un SGSI es fundamental para incrementar la seguridad de la información y los procesos de la empresa?

[ ] Sí, definitivamente
[ ] Tal vez
[ ] No
[ ] No conozco qué es un SGSI

Sección 4: Opinión general

13. ¿Qué nivel de riesgo considera que enfrenta la empresa frente a amenazas de ciberseguridad?

[ ] Muy alto
[ ] Alto
[ ] Moderado
[ ] Bajo
[ ] Muy bajo

14. ¿Cree necesario recibir más formación en temas de seguridad de la información?

[ ] Sí
[ ] No
[ ] No lo sé

15. ¿Existe un control para el ingreso al edificio de la institución y sus agencias?

[ ] Sí
[ ] No

16. ¿Se controla la asistencia utilizando un registro biométrico?

[ ] Sí
[ ] No

17. ¿Ingresa a su equipo de trabajo (PC) usando una contraseña segura?

[ ] Sí
[ ] No

18. ¿Ingresa a su correo electrónico utilizando una contraseña segura?

[ ] Sí
[ ] No

19. ¿Su equipo bloquea la pantalla por inactividad?

[ ] Sí
[ ] No

20. ¿Conoce de un método seguro de desecho de documentos físicos?

[ ] Sí
[ ] No

21. ¿Existen medidas de seguridad adecuadas para acceder al cuarto de servidores?

[ ] Sí
[ ] No

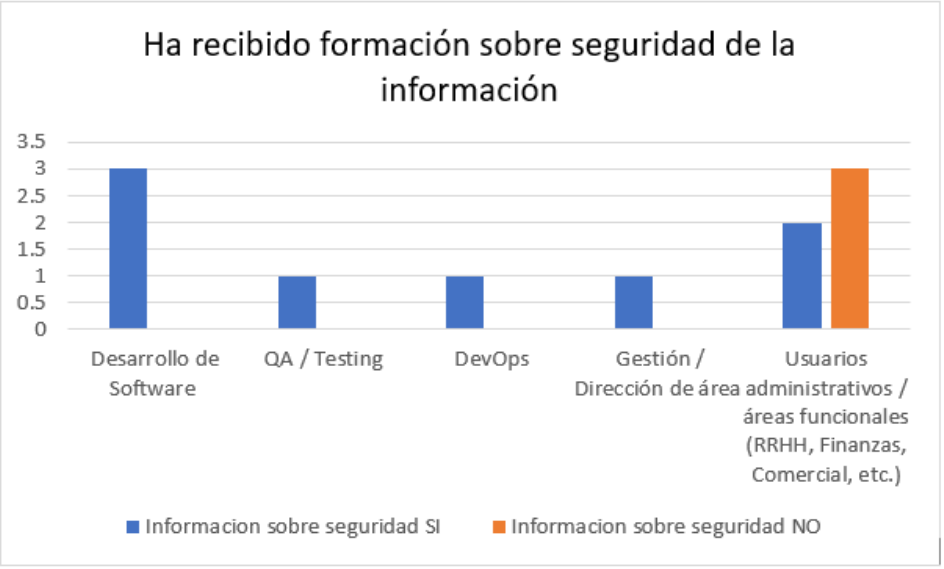
22. ¿Desea dejar un comentario adicional sobre la seguridad de la información en la empresa?

4.1 Resultados de Estudios Previos Relevantes

La tabulación de los datos nos brinda los siguientes resultados:

Figura 1

Gráfica porcentual de las respuestas a la pregunta 3.

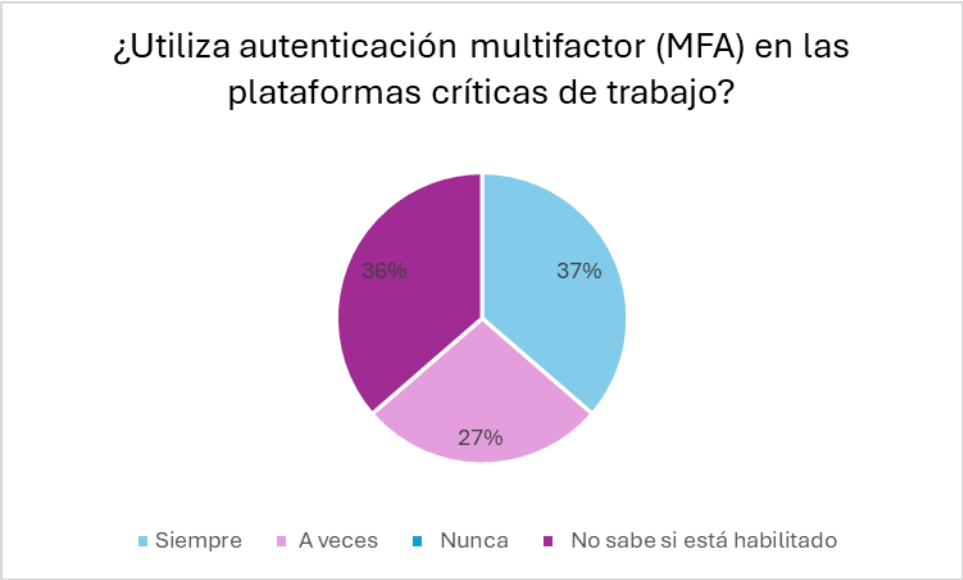


Nota: Creación propia

El 100% de la muestra indica que los encuestados de los departamentos de desarrollo de software, QA/ Testing, DevOps y Gestión/ Dirección de área recibieron formación sobre información de seguridad durante el último año mientras que en el departamento de Usuarios el 40% recibió información y el 60% no recibió formación.

Figura 2

Gráfica porcentual de las respuestas a la pregunta 5.

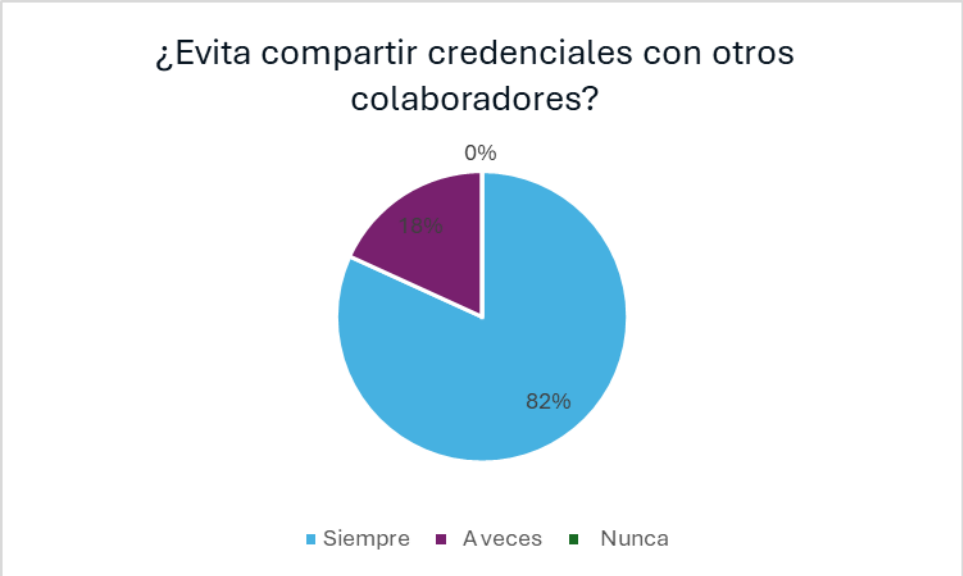


Nota: Creación propia

El 37% de la muestra utiliza autenticación multi factor (MFA), el 36% no sabe si está habilitado y un 27% lo utiliza a veces 0% de la muestra considera nunca utilizarlos.

Figura 3

Gráfica porcentual de las respuestas a la pregunta 6.



Nota: Creación propia.

El 82% de los encuestados siempre evita compartir credenciales con otros colaboradores y el 18% a veces.

Figura 4

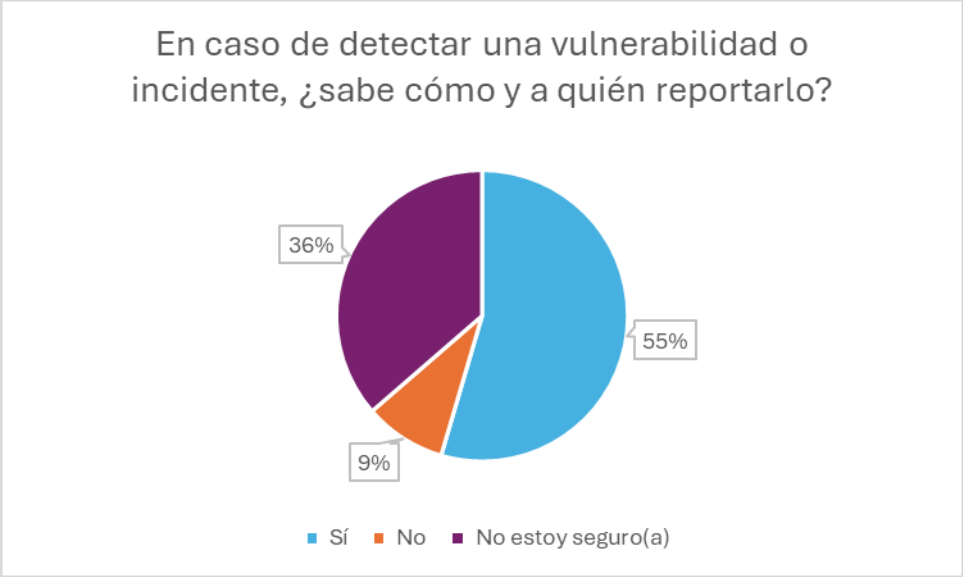
Gráfica porcentual de las respuestas a la pregunta 10.

Nota: Creación propia.

El 100% de los encuestados respondieron que están totalmente de acuerdo lo que nos indica que los colaboradores comprenden la importancia de proteger la información.

Figura 5

Gráfica porcentual de las respuestas a la pregunta 11.

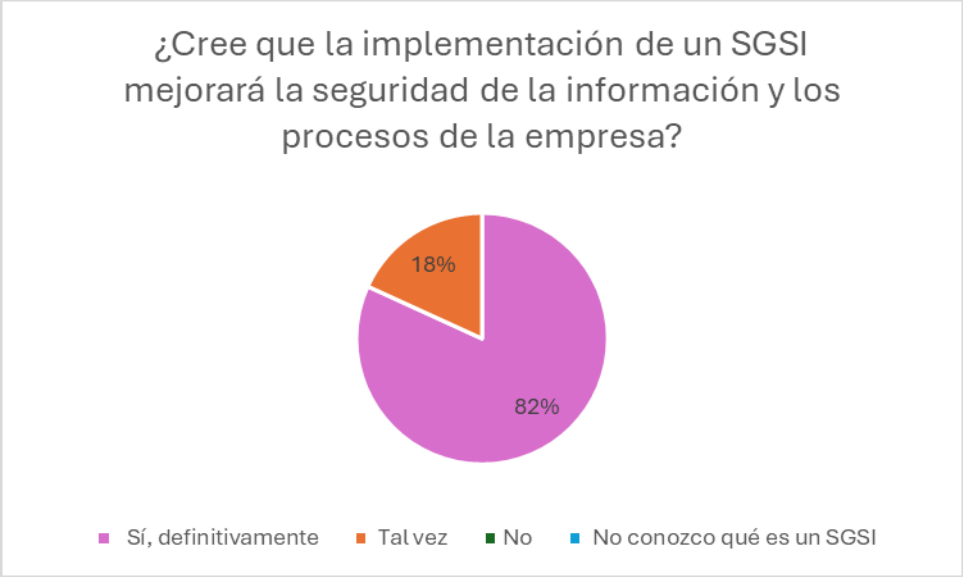


Nota: Creación propia.

El 55% de la muestra tiene conocimiento sobre cómo y a quien reportar en caso de presentarse una vulnerabilidad de la información, el 36% representa una debilidad en este proceso puesto que respondieron que no están seguros de cómo y a quien deben reportarlo y el 9% restante desconocen a quien deben reportarlo.

Figura 6

Gráfica porcentual de las respuestas a la pregunta 12.

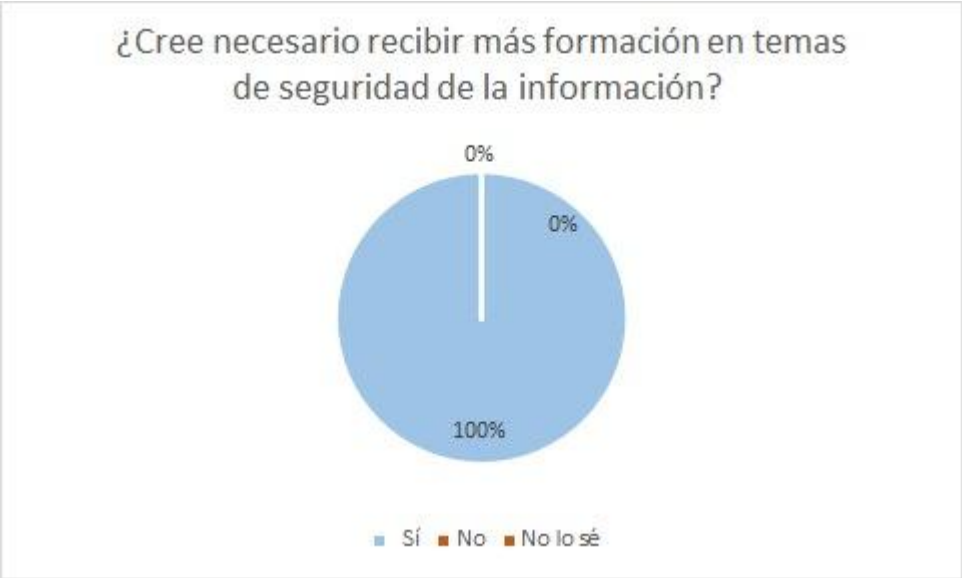


Nota: Creación propia.

El 82% de los encuestados responden que sí, definitivamente lo que representa una alta aceptación del SGSI por lo que se puede optimizar procesos internos, el 18% responde que tal vez lo que sugiere que no están seguros de los resultados de aplicar un SGSI.

Figura 7

Gráfica porcentual de las respuestas a la pregunta 14.



Nota: Creación propia.

El 100% del tamaño de la muestra responde de forma afirmativa lo que nos indica que el personal reconoce la falta de información relacionada con la implementación de SGSI basada en la norma ISO27001.

CAPÍTULO V: PROPUESTA DE INVESTIGACIÓN

En este capítulo se detalla la metodología de implementación del SGSI, mismo que se guía en la propuesta de la ISO/EC27003. Aquí se describen fases de diseño de SGSI, las etapas de implementación y su desarrollo a detalle ajustado una empresa de desarrollo de software que es proveedor de servicios auxiliares.

5.1 Fases del diseño de un SGSI

Tabla 1

Fases de diseño del SGSI

Fase	Entregables
1. Conseguir el apoyo de la dirección para comenzar un proyecto SGSI	Consentimiento de la Dirección para comenzar el proyecto SGSI
2. Definición del alcance, sus límites y política del SGSI	Alcance y límites del SGSI
	Política del SGSI
3. Análisis de requerimientos de seguridad de la información	Requerimientos de seguridad de la información
	Activos de información
	Resultados de la evaluación de seguridad
	Notificación escrita de aprobación por la dirección para implementar el SGSI
4. Evaluar los riesgos y planear su tratamiento	Plan de tratamiento de riesgos
	SoA, incluidos los objetivos de control y los controles seleccionados
5. Diseñar el SGSI	Plan de implementación del proyecto final de SGSI

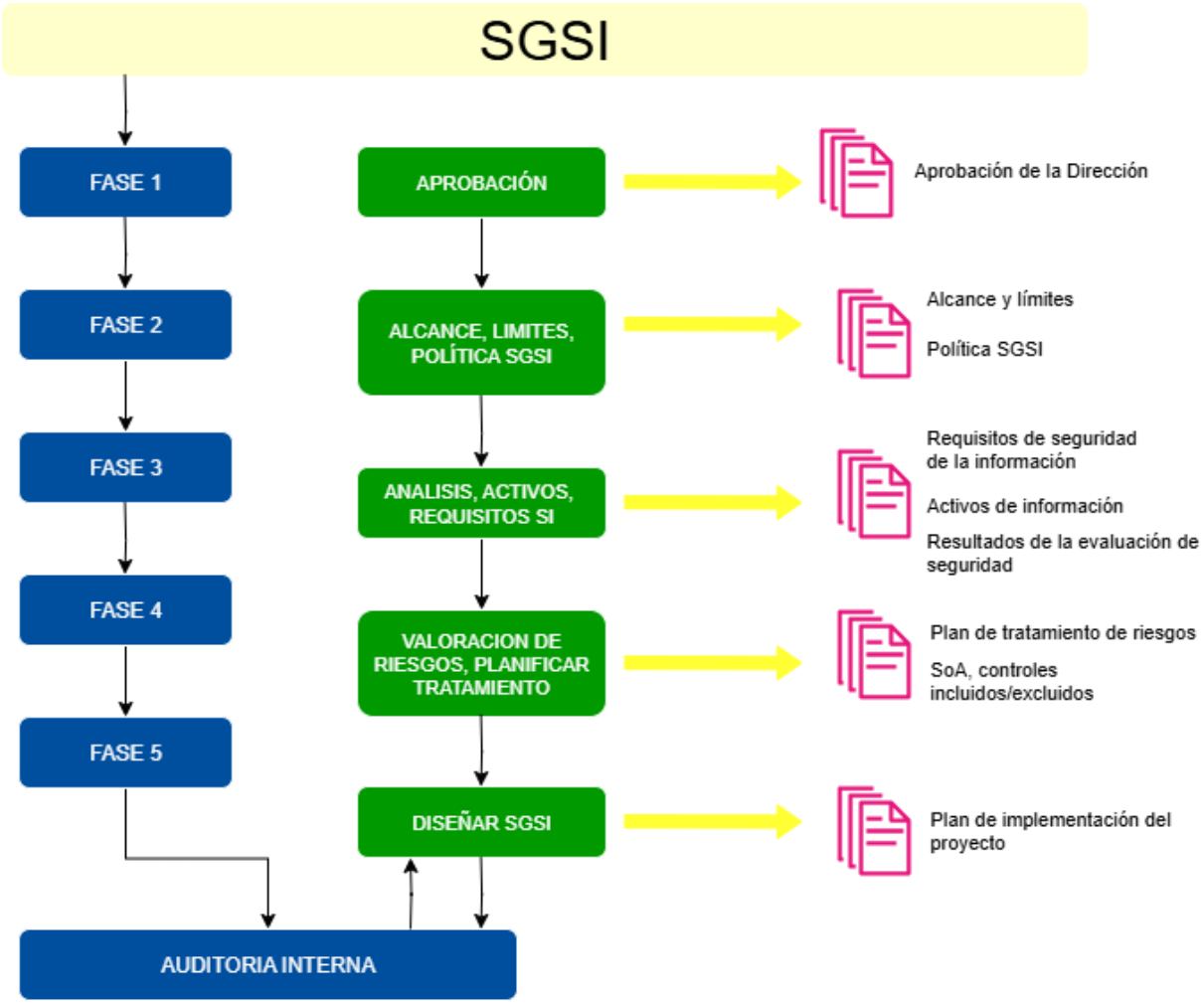
Nota: Creación propia.

En esta tabla se describen las actividades y los entregables que se deben generar para la implementación exitosa del SGSI.

5.2 Diagrama de flujo de las Fases del SGSI

Figura 8

Diagrama de flujo de las fases para desarrollar el SGSI



Nota: Creación propia

5.3 Desarrollo de la implementación

A continuación, se explica a detalle la implementación del SGSI siguiendo la secuencia cronológica de las actividades registradas en el Diagrama Gantt. El Diagrama Gantt se elaboró basado en el análisis de las fases de diseño del SGSI.

5.3.1 Aprobación de la dirección para implementar el SGSI

Para cumplir con éxito esta actividad la alta gerencia debe estar convencida de la necesidad de un SGSI, lo cual permitirá realizar las actividades contando con el apoyo y recursos necesarios para una implementación exitosa. Para formalizar esta aprobación es necesario una constancia firmada que apoye el proyecto en todos sus frentes. El formato de este documento está en el Anexo 1, entregables, Aprobación para el Inicio de la Implementación del SGSI.

5.3.2 Definición del alcance del SGSI

El alcance del SGSI de la empresa BESTTECH SAS comprende la gestión de la seguridad de la información en las actividades de desarrollo, pruebas, implantación (migración) y soporte de software especializado para entidades financieras, incluyendo:

El diseño, desarrollo y mantenimiento de software financiero para entidades del sector financiero.

Las actividades de implantación y soporte remoto en los sistemas de información de las entidades financieras clientes.

La gestión de código fuente a través de repositorios de control de versiones (Git).

El manejo, transferencia y resguardo de información sensible y confidencial proporcionada por los clientes para pruebas, implantación y soporte, incluyendo datos financieros y personales.

El servidor de pruebas y almacenamiento de código fuente ubicado en las instalaciones de la empresa.

Los equipos de trabajo utilizados por los desarrolladores y personal técnico en el cumplimiento de sus funciones. Las comunicaciones y conexiones remotas realizadas con los clientes para brindar soporte y servicios de implantación.

Este proyecto de desarrolló con la finalidad de tener un sistema de seguridad robusto para hacer frente a las amenazas actuales, considerando las necesidades de las partes interesadas relevantes, los requisitos legales y regulatorios aplicables, así como los compromisos contractuales con las entidades financieras clientes.

5.3.3 Política General de Seguridad de la Información

El SGSI que se implemente en la organización debe estar acorde con los objetivos de la empresa, para lo cual es necesario que antes de su implementación esté vigente una política organizacional que oriente las actividades posteriores. Bajo esta necesidad se ha implementado la Política General de Seguridad de la Información que establece la línea base para la protección de la información y de sus principios.
En este documento se encuentra en la lista de entregables.

5.3.4 Requisitos de Seguridad de la Información

Para el cumplimiento de este apartado es la ISO/EC 27001 la que nos brinda los requisitos a cubrir para que la seguridad de la información sea integral, sin embargo, estos requisitos pueden ser establecidos a partir de las necesidades de la propia organización. Para definir los requisitos es necesario realizar un análisis de los activos de información, como y cuando son utilizados en cada proceso interno o externo e identificar las vulnerabilidades y amenazas.

5.3.5 Análisis de contexto y FODA

Este análisis tiene como objetivo identificar y estudiar los factores internos y externos que afectan a BESTTECH SAS para obtener los resultados esperados tras la implementación del SGSI. Se expondrá el contexto en el cual BESTTECH SAS mantiene sus operaciones y establecer una base sólida para la planificación y mejora continua del SGSI. A continuación:

Factores Externos

- Alta demanda de seguridad por parte de instituciones financieras.
- Regulaciones locales sobre protección de datos (Ley Orgánica de Protección de Datos Personales en Ecuador).
- Avances tecnológicos constantes en ciberseguridad.
- Riesgo creciente de ataques cibernéticos dirigidos a software financiero.
- Expectativas de cumplimiento normativo por parte de socios y clientes.
- Cambios económicos o políticos que puedan impactar el entorno tecnológico o legal.

Factores Internos

- Cultura organizacional orientada al desarrollo de software seguro.
- Recursos humanos especializados pero limitados en número.
- Procesos críticos: desarrollo de software, soporte técnico, gestión de la seguridad de la información.
- Necesidad de gestionar accesos remotos seguros para el equipo de desarrollo.
- Acceso de terceros a datos y sistemas.
- Alianzas estratégicas con otras empresas para la explotación del software financiero.

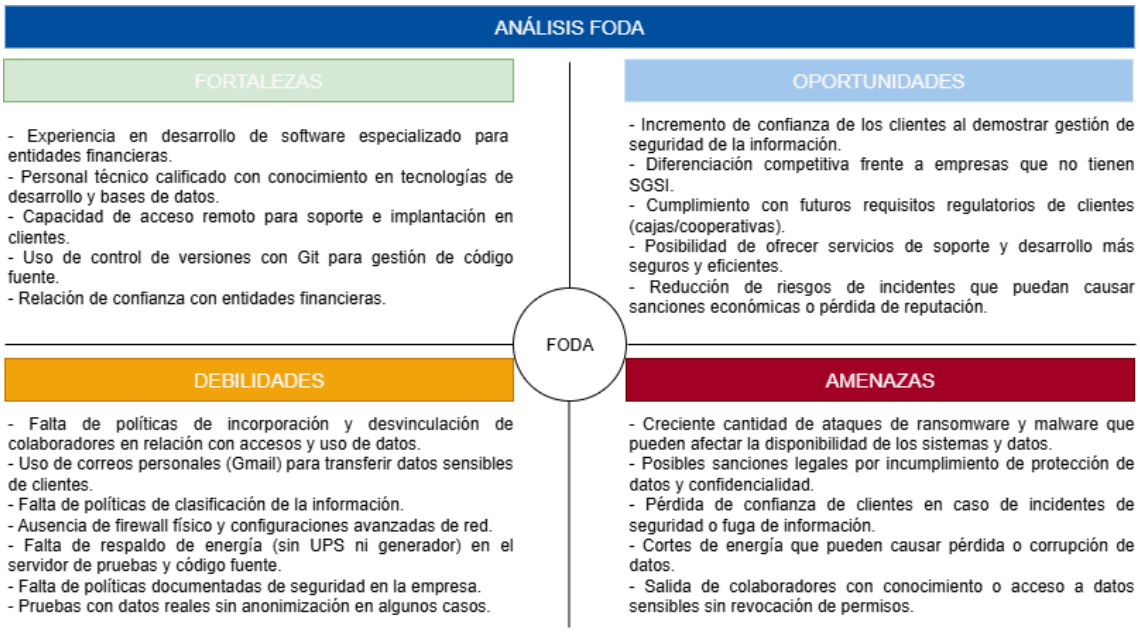
- Necesidad de garantizar la continuidad del negocio y la protección de la infraestructura tecnológica.

5.3.6 FODA

Este análisis muy utilizado nos permite realizar una autoevaluación rápida que ayuda a la organización a tener una proyección a futuro considerando aspectos a favor y muchas otras oportunidades de mejora. También permite considerar aquellos aspectos que afectarían a la empresa de forma negativa para cumplir sus objetivos.

Figura 9

Análisis FODA



Nota: Creación propia.

La imagen nos indica el resultado del análisis FODA.

5.3.7 Análisis GAP

Se realizará un análisis GAP para conocer el estado actual de la empresa referente a seguridad de la información. Este análisis permitirá conocer las oportunidades de mejora que debe acatar la empresa para mejorar la seguridad de la

información en todos sus procesos. Así también, se podrá identificar que controles del Anexo A norma ISO/EC 27002 pueden ser aplicados para cumplir con los requisitos de la ISO/EC 27001. Se establecerán las posibles brechas de seguridad y la acción requerida para disminuir el riesgo.

A través de este análisis también podremos determinar la prioridad de cada brecha de seguridad encontrada y disponer los recursos acordes a su impacto en la organización y sus objetivos.

Las columnas que serán registradas en esté análisis son los siguientes:

Número. Número que indica de ítem registrado de forma secuencial.

Requisito ISO/IEC 27001:2022 / Control Anexo A. Requisito de la norma ISO/EC 27001 que debe solventado para la correcta implementación de esta.

Estado Actual. Registro detallado de la situación actual observada al momento del análisis GAP. Por ejemplo, Accesos no gestionados formalmente, no hay revocación al desvincular personal.

Brecha identificada. Se registra el detalle de la vulnerabilidad de seguridad encontrada a partir de la columna Estado Actual. Por ejemplo, riesgo de acceso indebido.

Acción requerida. Se detalla la acción necesaria para eliminar la brecha de seguridad o disminuir su impacto.

Prioridad. Se registra la prioridad que considere acorde a la afectación de la brecha de seguridad y la atención requerida. Para el desarrollo de esta implementación utilizaremos baja, media y alta.

La Tabla 2 contiene los resultados del análisis GAP presente en el Anexo 1.

5.3.8 Activos de información

Identificación. Como próximo paso se deben identificar los activos de información que son utilizados en casa proceso interno de la empresa. Estos serán identificados a través de la comunicación establecida con cada colaborador la descripción de sus actividades.

Clasificación. Una vez identificados los activos de información, estos serán clasificados como internos o externos (datos del cliente).

La Tabla 3 contiene la clasificación de los activos de información en el Anexo 1.

5.3.9 Definición de procesos utilizando SIPOC

Es necesario definir los procesos de manera clara y simple lo que nos permite identificar sin complicaciones a los actores clave, entradas y salidas en cada actividad lo cual es primordial para mejorar la seguridad de un proceso. Para este propósito, en este proyecto es necesario implementar una tabla la cual contendrá las siguientes columnas:

Entidad. Registramos el nombre de la entidad responsable del proceso.

Proceso. Registramos el nombre del proceso que estamos analizando. Por ejemplo, Desarrollo de Software, Migración.

Subproceso. Registramos el nombre del proceso que estamos analizando (Si corresponde). Por ejemplo, Generación de respaldos que pertenecería al proceso de Migración.

Proveedor (S). Registramos el nombre del proveedor que entrega los insumos necesarios para realizar el proceso, pudiendo ser un cliente interno, externo, departamento, cargo entre otros dependiendo del proceso.

Entrada (I). Se registra la o las entradas necesarias para ejecutar el proceso. Por ejemplo, requisitos funcionales y no funcionales.

Proceso (P). Secuencia de actividades que transforma los insumos en productos o servicios. Por ejemplo, Codificación y pruebas.

Salida (O). Se registra los resultados o productos generados por el proceso. Por ejemplo, software funcional.

Clientes (C). Se registra al cliente o destinatario de los productos o servicios generados. Por ejemplo, usuario final.

La Tabla 8 contiene los resultados del método SIPOC en el Anexo 1.

5.3.10 Mapa de procesos

Adicional a la tabla anteriormente descrita es necesario realizar un mapa de procesos para identificar su flujo, activos de información que intervienen y los posibles riesgos inherentes en su desarrollo.

Se debe implementar una tabla para llevar a cabo este registro en donde se tienen las siguientes columnas:

Numero (Nro.). Número de registro secuencial que identifica cada proceso.

Proceso. Se registra el nombre del proceso que se está analizando.

Activos involucrados. Se registran los activos de información que son utilizados en el proceso.

Riesgos principales. Se registra el o los riesgos identificados en los procesos o actividades que contiene.

La Tabla 9 contiene el resultado de mapear los procesos, presente en el Anexo 1.

5.3.11 Riesgos de Seguridad de la Información

Para una implementación exitosa del SGSI es necesario precisar de una metodología que permita una gestión adecuada del riesgo cuyas características aporten a:

a) Establecer criterios sobre riesgos de seguridad de la información incluyendo:

1. Los criterios para la aceptación del riesgo.

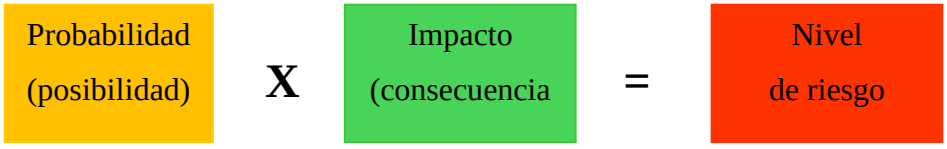
2. Brindar el criterio para realizar la valoración del riesgo referente al resguardo de la información.

b) Garantice que las evaluaciones posteriores del riesgo de seguridad de la información generan resultados válidos y comparables.

c) Identificación de los riesgos que pueden comprometer la información.

Nivel de riesgo: Dimensión de un riesgo expresada numéricamente a través del producto de la probabilidad por el impacto. Los riesgos de seguridad de la información son los asociados a la pérdida de sus características básicas.

Para calcular el nivel de riesgo se utiliza la siguiente formula:



5.3.12 Matriz de riesgos

Una vez definidos los procesos, subprocesos, actividades y activos de información que intervienen es necesario determinar el nivel de riesgo mediante el cálculo antes indicado. Para esto se levantará una tabla en donde con ayuda del dueño del proceso se colocará un valor entre uno (1) y tres (3) para dar un asignar un nivel de riesgo.

La tabla indicada contará con las siguientes columnas:

Activo de información. Se registra el activo de información el cual considerado en los procesos y al cual se le calcula el riesgo.

Amenaza. Se registra la amenaza identificada el riesgo principal descrito en el mapa de procesos.

Vulnerabilidad. Se registra la vulnerabilidad o brecha identificada en el análisis GAP según corresponda.

Probabilidad. Se ingresa un valor numérico entre 1 y 3 analizando con el dueño del proceso la probabilidad de que se materialice una amenaza.

Impacto. Se ingresa un valor numérico entre 1 y 3 analizando con el dueño del proceso la gravedad del impacto en la empresa en caso de la materialización de una amenaza.

Riesgo. Registrar el valor numérico producto de la probabilidad por el impacto.

Nivel de riesgo. Una vez calculado el riesgo en esta columna se debe registrar el nivel de riesgo según corresponda para lo cual dispone de estos niveles: bajo, medio, alto y crítico.

Acción de tratamiento. Se registra la acción necesaria y dable que a través del análisis de factibilidad puede implementarse para mitigar el riesgo calculado y disminuir el nivel de riesgo.

Responsable. Se registra el nombre del área o cargo del responsable de implementar la acción de tratamiento.

La Tabla 4 contiene los resultados la Matriz de Riesgos en el Anexo 1.

5.3.13 Declaración de Aplicabilidad (SoA)

En este documento se identifican los controles de seguridad del Anexo 1 de la ISO/EC 27001 que pueden ser aplicados para tratar los riesgos de seguridad de acuerdo con el entorno actual de la organización. Es necesario justificar su inclusión o exclusión si fuera el caso.

Esta tabla esta compuestas por las siguientes columnas:

Controles del Anexo A. Lista de los 93 controles del Anexo A de la ISO/EC 27001 aplicables según las necesidades identificadas después del análisis de riesgo. Deben incluirse todos los controles.

Descripción del control. En esta columna se registra la descripción de cada control que ayuda a definir su inclusión o exclusión.

Aplicable. Se registra SI o NO para indicar si es aplicable o no.

Justificación aplicabilidad/exclusión. Se registra el motivo por el cual el control se incluye o se excluye.

Estado de implementación. Se registra el estado actual del control en caso de que se lo incluyera para tratar el riesgo. Los estados que se pueden registrar son: Implementado, En implementación, No Aplica.

Observación. Se ingresa una observación adicional si fuese necesario.

La tabla 6 con los controles identificados como aplicables, se presenta en el Anexo 1.

5.3.14 Plan de tratamiento de Riesgos

Este es un documento fundamental en la implementación del SGSI al aplicar el estándar de la ISO/EC 27001. Su objetivo es definir y gestionar las acciones necesarias reducir o eliminar los riesgos identificados durante el análisis de riesgos.

A continuación, describimos las columnas que forman parte de este documento:

Identificador del riesgo. Este dato hace referencia al código o número de riesgo identificado.

Riesgo identificado. Se ingresa la descripción del riesgo identificado.

Nivel de riesgo. Se registra el riesgo inicial antes de la implementación de su tratamiento.

Acción de tratamiento. Se ingresa la o las acciones necesarias para dar tratamiento al riesgo identificado.

Responsable. Persona o área encargada de realizar la acción de tratamiento.

Fecha de inicio. Se registra la fecha en la cual va a iniciar la implementación del tratamiento del riesgo.

Fecha fin. Se registra la fecha en la cual va a finalizar la implementación del tratamiento del riesgo.

Estado. Se registra el estado del tratamiento. Esta columna puede tomar estos estados: En proceso, No iniciado, Finalizado.

Nivel de riesgo residual. Nivel de riesgo después de aplicar el tratamiento.

La tabla 5 contiene el Plan de Tratamiento de Riesgos, se presenta en el Anexo 1.

5.3.15 Implementación de controles

En esta etapa se implementan los controles técnicos, organizativos, físicos y legales definidos en el SoA para reducir los riesgos identificados. Se definen los roles y se asignan responsabilidades a cada encargado para implementar y mantener cada control las cuales deben estar debidamente documentadas. Aquí también se debe incluir la documentación que servirá de evidencia para la auditorias posteriores. Se establecen los controles técnicos para cada área de la empresa según el riesgo que se desea reducir. Se redactarán las políticas, procedimientos, instructivos y registros necesarios para operar los controles. Así también, analizará la adquisición de software y hardware necesario para implementar los controles de seguridad con cada jefe de área y la gerencia. A partir del Plan de Capacitación, se llevará a cabo la socialización de los controles definidos en las diferentes políticas, procedimientos y demás instructivos en las diferentes áreas de trabajo de la empresa. Esto se llevaría desarrollará con cada colaborador individualmente para solventar cualquier duda acerca de las medidas de seguridad. Se aprovecharía esta oportunidad para obtener una retroalimentación asegurando que la medida expuesta este acorde a la necesidad de cada actividad y

proceso. En caso de ser necesario se llevaría a cabo la firma de documentos, como el Acuerdo de Confidencialidad por parte del personal que maneja información confidencial de la empresa y de sus clientes. Cada capacitación debe tener su acta firmada por el o los participantes para el debido registro y control.

Este proceso debe llevarse de tal forma que se integre de la manera más natural con los procesos de la organización sin causar obstáculos en su operatividad.

Al completar esta etapa la organización se encuentra preparada para avanzar al seguimiento, medición y eficacia de los controles implementados.

5.3.16 Capacitación del personal

Esta etapa es vital para el éxito del SGSI y su eficacia dado que es aquí donde se asegura que los colaboradores comprendan la magnitud de no resguardar la información y conozcan el origen de cada política y procedimiento y su relevancia para la organización. Para realizar las capacitaciones se considerarán el resultado de las evaluaciones y análisis anteriores. También se tomarán en cuenta los resultados de la encuesta realizada en el análisis anterior. Cada capacitación sea individual o en grupo constara del registro de asistentes y su debida acta.

Considerando el tamaño de la empresa estas actividades cubren los aspectos necesarios para fomentar una cultura de seguridad dentro de la organización.

5.3.17 Auditoría interna del SGSI

Una vez implementados los controles y que cada rol y responsabilidad han sido establecidos es necesario realizar una auditoría interna del SGSI con la finalidad de comprobar su aplicación y eficacia. Determinar que se protege adecuadamente la confidencialidad, integridad y disponibilidad de la información, identificar incumplimientos o proponer acciones necesarias para corregir algún aspecto de

procedimientos. De los resultados de la auditoria puede desarrollarse un plan de acciones correctivas para solventar necesidades no consideradas o recomendaciones.

Es necesario tomar en cuenta que el SGSI es dinámico y esta propenso a cambios según las necesidades de la organización y del entorno en el que desarrolla sus actividades por lo que se debe llevar un proceso de mejora continua y maduración. Por ahora uno de los objetivos de la empresa es mejorar en el aspecto seguridad de la información, pero esta etapa es crucial para a futuro poder obtener una certificación.

5.3.18 Revisión por la Dirección

Cada documento debe ser debidamente revisado por la Dirección ya que se carece un comité de seguridad, por ende, la Administración será el encargado de verificar de que cada política, procedimiento, manual o instructivo este alineado con los objetivos de la empresa y que correspondan perfectamente con la reducción de los riesgos identificados. Esta actividad deberá realizarse en conjunto con el Encargado de Seguridad quien será primordial apoyo para temas técnicos. Así también, es la Dirección quien establece la factibilidad de adquisición de software o hardware necesario para la implementación del SGSI y tiene la última palabra en esta decisión.

CRONOGRAMA DE ACTIVIDADES

Para establecer un orden en el desarrollo de las etapas de implementación se ha elaborado un diagrama de Gantt donde se definen las actividades, el tiempo en el que se van a realizar, así como su progreso.

	Gantt Implementación Sistema de Gestión de Seguridad de la Información						
Nro.	**Actividad**	**Mes 1 (marzo)**	**Mes 2 (abril)**	**Mes 3 (mayo)**	**Mes 4 (junio)**	**Mes 5 (julio)**	**Mes 6 (agosto)**
1	Compromiso de la Dirección y definición de alcance						
2	Identificación de partes interesadas y requisitos						
3	Análisis de contexto y FODA						
4	Análisis GAP						
5	Identificación de activos de información						
6	Análisis de riesgos (matriz de riesgos)						
7	Declaración de aplicabilidad (SoA) inicial						
8	Plan de tratamiento de riesgos						
9	Redacción de políticas y procedimientos de SGSI						
10	Implementación de controles (tecnológicos y operativos)						
11	Capacitación al personal						
12	Auditoría interna del SGSI						
13	Revisión por la dirección						

CONCLUSIONES

La implementación de este proyecto tiene algunas conclusiones, acerca del ámbito técnico, organizacional, y personal. Implementar un SGSI es un proyecto laborioso sin importar el tamaño de la organización en donde se vaya a implantar tiene una gran magnitud ya que se involucran muchas áreas de una empresa. Desde la Alta Dirección hasta los niveles operativos el compromiso debe ser completo pues es un cambio no solo técnico y organizacional sino también cultural. Cabe destacar que son necesarias nociones básicas en Seguridad de la Información para implementar un proyecto de este tipo.

Cumplimiento del Objetivo General

Con la implementación del SGSI en cada una de sus etapas se pudo apreciar el cambio que trae consigo la concienciación de los riegos en la seguridad de la información. A nivel técnico son cada vez más los controles necesarios debido a la digitalización que trae consigo mucha integración, pero también se deben extender las medidas adecuadas para conservar la integridad, confidencialidad y disponibilidad de los datos.

Conclusión en Relación con los Objetivos Específicos

Se puede concluir que es básico en el ámbito financiero un SGSI, debido a las amenazas constantes al sector y que el costo que conlleva esta implementación es una inversión a corto y mediano plazo, pues se está generando una garantía para los clientes cada vez más conscientes en la seguridad de la información.

Para finalizar, se alcanzaron los objetivos propuestos dentro tiempo planificado, se logró obtener resultados comparativos después de la implementación en ciertas áreas

de la empresa, la misma que quedo encaminada en el proceso de mejora continua del SGSI teniendo ya una herramienta para la evaluación. Con esto se logrará tener una ventaja estratégica frente a sus competidores que era unos de los principales objetivos de la organización.

RECOMENDACIONES

A nivel institucional

Dado a la realidad actual de las tecnologías y de su avance vertiginoso es necesario profundizar en la seguridad de la información. Es un segmento de estudio que cada vez abarca más áreas de la vida cotidiana de las personas y es importante generar una cultura acerca de la seguridad de la información. Ecuador ya tiene una Ley de Protección de Datos Personales lo que puede abrir muchas oportunidades, sin embargo, para saberlas aprovechar es necesario ahondar en el estudio de la rama de la seguridad de la información.

A nivel técnico

En el aspecto técnico, el SGSI ingresa en el ciclo de mejora continua, por lo tanto, es necesaria una revisión periódica de los controles implementación para evaluar su efectividad. Así también, las políticas y procedimientos deben ser actualizados para que estén acorde a las necesidades de la organización, de sus objetivos estratégicos y del entorno donde desarrolla sus actividades comerciales.

A nivel teórico

El desarrollo e implementación de este proyecto está basado en la familia de la ISO 27000, principalmente en la ISO/EC 27001, sin embargo, se recomienda considerar estándares como COBIT o NIST SP 800-53, para extender el ámbito de controles utilizables y robustecer la seguridad ya implementada.

REFERENCIAS

Cavoukian, A. (2009). *Privacy by Design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

Humphrey, W. S. (1989). Managing the software process. Addison-Wesley.

ISO/IEC. (2024). *ISO/IEC 27000:2024 Information security, cybersecurity and privacy protection — Information security management systems — Fundamentals and vocabulary*. International Organization for Standardization.

ISO/IEC. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization.

ISO/IEC. (2022). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls*. International Organization for Standardization.

ISO/IEC. (2019). *ISO/IEC 27005:2018 Information security risk management*. International Organization for Standardization.

ISO/IEC. (2019). *ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*. International Organization for Standardization.

Ladino, N. H., Cabra, F. A., & Rojas, D. A. (2011). Sistema de gestión de seguridad de la información (SGSI) para pequeñas empresas. *Revista Ingenierías Universidad de Medellín*, 10(18), 139–156. https://revistas.udem.edu.co/index.php/ingenierias/article/view/627

Marreros, M., Acosta, K., & Mendoza, J. (2024). Controles de acceso en plataformas SaaS: análisis y propuesta de implementación. Revista de Seguridad Informática Aplicada, 12(1), 33–48.

McGraw, G. (2006). *Software security: Building security in*. Addison-Wesley.

Nikiforova, O. (2022). *Data security as a top priority in the digital world: Challenges and best practices*. arXiv preprint arXiv:2206.06814. https://arxiv.org/abs/2206.06814

Moncada, J., & Israel, G. (2018). Factores organizacionales que influyen en la implementación de un SGSI. *Revista Colombiana de Computación*, 19(2), 115–128.

Rodríguez, C., Fernández, A., & Fernández, J. (2023). Seguridad de la información en el comercio electrónico: retos y soluciones. *Revista Iberoamericana de Tecnologías de la Información*, 16(3), 45–62.

Stallings, W. (2017). *Effective Cybersecurity: A Guide to Using Best Practices and Standards*. Addison-Wesley.

Tipton, H. F., & Nozaki, M. (2012). *Information security management handbook* (6th ed.). Auerbach Publications.

Von Solms, B., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wang, X., & Cheng, Z. (2020). *Cross-sectional studies: strengths, weaknesses, and recommendations*. *Chest*, *158*(1), S65–S71. https://doi.org/10.1016/j.chest.2020.03.012

Whitman, M. E., & Mattord, H. J. (2010). *Principles of Information Security* (3rd ed.). Cengage Learning.

Anexo 1

Tabla 2

Resultados del análisis GAP

Tabla de análisis GAP					
Nro.	**Requisito ISO/IEC 27001:2022 / Control Anexo A**	**Estado actual**	**Brecha identificada**	**Acción requerida**	**Prioridad**
1	Política de seguridad de la información	No existe política formal documentada	No se cuenta con política aprobada por dirección	Redactar e implementar política de SGSI	Alta
2	Control de accesos	Accesos no gestionados formalmente, no hay revocación al desvincular personal	Riesgo de accesos indebidos	Establecer procedimiento de control de accesos y bajas	Alta
3	Clasificación de la información	No existe política ni procedimiento de clasificación	No se identifica el nivel de criticidad de los datos	Crear política y procedimiento de clasificación	Alta
4	Copias de seguridad	Se realizan copias informales, sin procedimientos definidos	Riesgo de pérdida de datos	Documentar e implementar política de respaldos	Alta
5	Seguridad física	Servidor sin gabinete seguro ni control de acceso físico	Riesgo de robo o daño físico	Adquirir gabinete seguro y establecer control físico	Alta
6	Protección contra malware	Sin antivirus en servidor, antivirus básico en equipos	Riesgo de infecciones	Implementar antivirus corporativo y políticas de uso	Alta
7	Firewall y seguridad de red	No se cuenta con firewall físico ni configuración avanzada	Riesgo de accesos externos no autorizados	Configurar firewall local y evaluar firewall perimetral	Alta
8	Gestión de incidentes de seguridad	No existe procedimiento para notificar y gestionar incidentes	Respuesta reactiva ante incidentes	Definir procedimiento de gestión de incidentes	Media
9	Concientización y capacitación	No existe capacitación formal en seguridad	Riesgo de errores humanos	Establecer plan de capacitaciones periódicas	Media
10	Control de documentos	Documentación no controlada ni versionada	Dificultad de control y actualización	Implementar control de versiones de documentos	Media
11	Auditoría interna	No se realizan auditorías internas	No hay retroalimentación sobre el SGSI	Planificar auditorías internas	Baja
12	Revisión por la dirección	No se ha realizado revisión por la dirección	Falta de supervisión de alta gerencia	Planificar revisión de dirección	Baja
13	SoA	No existe SoA	No se tiene un registro de controles aplicables	Elaborar SoA tras análisis de riesgos	Alta

Nota: Creación propia.

Tabla 3

Identificación de activos de la información.

Activos de información	
Activo	**Clasificación**
Datos de clientes en pruebas	Externo
Repositorios de código (Git)	Interno
Equipos personales de desarrollo	Interno - externo
Conexiones remotas a servidores de clientes	Interno - externo
Información confidencial en correos	Interno - externo
Servidor de código fuente y pruebas	Interno
Datos de clientes en producción	Externo

Nota: Creación propia.

Tabla 4

Análisis de riesgo utilizando una matriz de riesgos

Matriz de Riesgos								
Activo de información	**Amenaza**	**Vulnerabilidad**	**Probabilidad (1-3)**	**Impacto (1-3)**	**Riesgo (PxI)**	**Nivel de riesgo**	**Acción de tratamiento**	**Responsable**
Datos de clientes en pruebas	Acceso no autorizado	Uso de datos reales sin anonimización	2	3	6	Alto	Implementar anonimización de datos y acceso controlado	Responsable SGSI
Repositorios de código (Git)	Fuga de código fuente	Accesos sin MFA ni roles definidos	2	3	6	Alto	Configurar MFA y control de accesos en Git	Responsable de TI
Equipos personales de desarrollo	Malware / Ransomware	Sin antivirus corporativo ni cifrado	2	2	4	Medio	Instalar antivirus y cifrado de disco, restringir software	Responsable de TI
Conexiones remotas a servidores de clientes	Intercepción de datos	Conexiones sin VPN	1	3	3	Bajo	Usar VPN y cifrado de extremo a extremo	Responsable de TI
Información confidencial en correos	Fuga de información	Falta de política de uso de correo	2	2	4	Medio	Crear política de uso seguro de correo y capacitación	Responsable SGSI
Servidor de código fuente y pruebas	Pérdida de datos por corte de energía	Falta de respaldo de energía (sin UPS ni generador)	2	3	6	Alto	Adquirir UPS y plan de contingencia ante cortes eléctricos	Responsable de TI
Servidor de código fuente y pruebas	Infección por malware	Sin antivirus	2	2	4	Medio	Instalar antivirus compatible y monitoreo de integridad	Responsable de TI
Datos de clientes	Fuga de datos en transferencia	Uso de correo personal sin cifrado ni control	3	3	9	Crítico	Usar cuentas corporativas con cifrado y protocolos seguros	Responsable SGSI
Datos de clientes	Fuga de información	Falta de clasificación de la información recibida	2	3	6	Alto	Implementar clasificación de información recibida	Responsable SGSI
Código fuente y datos en manos de colaboradores	Acceso no autorizado tras salida de colaborador	Falta de política de salida y revocación de accesos	2	3	6	Alto	Establecer política de salida y revocación de accesos	Responsable SGSI
Código fuente y datos en manos de colaboradores	Uso indebido de información y código	Falta de política de uso de información y código	2	3	6	Alto	Crear política de uso de información y código fuente	Responsable SGSI

Nota: Creación propia

Tabla 5

Plan de acción de riesgos

Plan de Tratamiento de Riesgos de SGSI								
ID riesgo	**Riesgo identificado**	**Nivel de riesgo**	**Acción de tratamiento**	**Responsable**	**Fecha Inicio**	**Fecha Fin**	**Estado**	**Nivel de riesgo residual**
R-01	Acceso no autorizado a datos de clientes en pruebas	Alto	Implementar anonimización de datos y control de acceso por roles	Responsable SGSI	4/8/2025	20/8/2025	No iniciado	Bajo
R-02	Fuga de código fuente en repositorios Git	Alto	Configurar MFA en Git, control de accesos y revisión de permisos periódicamente	Responsable de TI	6/8/2025	30/8/2025	No iniciado	Alto
R-03	Malware/Ransomware en equipos de desarrollo	Medio	Instalar antivirus corporativo, actualizar sistemas y restringir instalaciones de software	Responsable de TI	15/8/2025	15/9/2025	No iniciado	Medio
R-04	Intercepción de datos en conexiones remotas	Bajo	Configurar uso obligatorio de VPN y cifrado de extremo a extremo en accesos remotos	Responsable de TI	1/9/2025	30/9/2025	No iniciado	Medio
R-05	Fuga de información por uso de correos personales	Medio	Crear cuentas de correo corporativo con cifrado y política de uso seguro	Responsable SGSI	15/9/2025	15/10/2025	No iniciado	Bajo
R-06	Pérdida de datos por corte de energía en servidor	Alto	Adquirir e instalar UPS para el servidor y plan de contingencia de respaldos automáticos	Responsable de TI	1/10/2025	15/11/2025	No iniciado	Bajo
R-07	Daño físico o robo del servidor de pruebas	Alto	Ubicar el servidor en gabinete seguro y con acceso restringido	Responsable de TI	1/11/2025	30/12/2025	No iniciado	Medio
R-08	Infección de servidor por malware	Medio	Instalar antivirus compatible en Linux y monitoreo de integridad	Responsable de TI	1/9/2025	30/9/2025	No iniciado	Medio
R-09	Acceso no autorizado a servidor por falta de firewall	Alto	Configurar firewall local robusto y evaluar firewall perimetral	Responsable de TI	1/11/2025	30/11/2025	No iniciado	Medio
R-10	Fuga de información por falta de clasificación	Alto	Implementar política de clasificación de la información	Responsable SGSI	15/7/2025	30/7/2025	En proceso	Bajo
R-11	Acceso no autorizado tras salida de colaboradores	Alto	Crear política de desvinculación y revocación inmediata de accesos	Responsable SGSI	1/7/2025	15/7/2025	En proceso	Bajo

R-11	Uso indebido de información y código por colaboradores	Alto	Establecer política de uso de información y cláusulas de confidencialidad	Responsable SGSI	1/7/2025	15/7/2025	En proceso	Medio

Nota: Creación propia

Tabla 6

Declaración de aplicabilidad, controles incluidos del Anexo A de la ISO/EC27001.

Declaración de aplicabilidad (SoA)					
Nro.	**Controles Anexo A**	**Aplicable**	**Justificación aplicabilidad/ exclusión**	**Estado de Implementación**	**Observación**
1	**5. Controles organizacionales**				
2	5.1. Políticas de Seguridad de la Información	SI	Información documentada requerida.	En Proceso	
3	5.2. Roles y responsabilidades de seguridad de la información	SI	Poder determinar responsabilidades.	En Proceso	
4	5.3. Separación de funciones	SI	Poder ejercer control y supervisión.	En Proceso	
5	5.4. Responsabilidades de Gestión	SI		En Proceso	
6	5.5. Contacto con las autoridades	SI	Principalmente para conocer actualizaciones de la ficha tecnica elaborada por la SEPS.	En Proceso	
7	5.6. Contacto con grupos de interés especial	NO	No aplica actualmente	No Aplica	
8	5.7. Inteligencia de Amenazas	NO	No existe personal necesario para lograr este control	No Aplica	
9	5.8. Seguridad de la información en la gestión de proyectos	SI	Las políticas de control se aplicaran en todos los procesos de la empresa	No Iniciado	
10	5.9. Inventario de información y otros activos asociados	SI	Necesario para conocer los requerimientos de seguridad de la empresa	No Iniciado	

11	5.10. Uso aceptable de la información y otros activos asociados	SI	Es necesario controlar buen uso de los activos de informacion	No Iniciado
12	5.11. Devolución de activos	SI	Es necesario para mantener los activos de información solo bajo tenencia de personal activo en la empresa	No Iniciado
13	5.12. Clasificación de la información	Si	Se hará un inventario de activos de la información.	
14	5.13. Etiquetado de información	NO	No se aplica actualmente.	No aplica
15	5.14. Transferencia de información	No	No se transfiere información actualmente	No aplica
16	5.15. Control de acceso	SI	Necesario para controlar el acceso a los activos de información internos y externos	No Iniciado
17	5.16. Gestión de identidad	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
18	5.17. Información de autenticación	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
19	5.18. Derechos de acceso	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
20	5.19. Seguridad de la información en las relaciones con los proveedores	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
21	5.20. Abordar la seguridad de la información en los acuerdos con los proveedores	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
22	5.21. Gestión de la seguridad de la información en la cadena de suministro de las TIC	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
23	5.22. Seguimiento, revisión y gestión de cambios de servicios de proveedores	NO	NO se ajusta a la realidad actual de la empresa	No aplica

24	5.23. Seguridad de la información para el uso de servicios en la nube	NO	NO se ajusta a la realidad actual de la empresa. No mantiene información en la nube	No Aplica
25	5.24. Planificación y preparación de la gestión de incidentes de seguridad de la información	SI	Necesario para hacer frente un acceso no autorizado	No Iniciado
26	5.25. Evaluación y decisión sobre eventos de seguridad de la información	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
27	5.26. Respuesta a incidentes de seguridad de la información	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
28	5.27. Aprender de los incidentes de seguridad de la información	NO	NO se ajusta a la realidad actual de la empresa. No se mantiene una base de conocimiento.	No Aplica
29	5.28. Recolección de evidencia	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
30	5.29. Seguridad de la información durante la interrupción	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
31	5.30. Preparación de las TIC para la continuidad del negocio	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
32	5.31. Requisitos legales, estatutarios, reglamentarios y contractuales	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
33	5.32. Derechos de propiedad intelectual	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
34	5.33. Protección de registros	SI	Necesario para mantener la confidencialidad de los datos	No Iniciado
35	5.34. Privacidad y protección de la información identificable de la persona (PII)	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
36	5.35. Revisión independiente de la seguridad de la información.	NO	NO se ajusta a la realidad actual de la empresa	No Aplica

37	5.36. Cumplimiento de políticas, normas y estándares de seguridad de la información	SI	Se contempla su realización en el ciclo de mejora continua	No Iniciado
38	5.37. Procedimientos operativos documentados	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
39	**6. Controles de personas**			
40	6.1. Chequeo	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
41	6.2. Términos y condiciones de empleo	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
42	6.3. Concientización, educación y capacitación en seguridad de la información	SI	Necesario para concientizar al personal acerca de la importancia de mantener seguros los datos.	No Iniciado
43	6.4. Proceso Disciplinario	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
44	6.5. Responsabilidades después de la terminación o cambio de empleo	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
45	6.6. Acuerdos de confidencialidad o no divulgación	SI	Necesario para mantener la confidencialidad de los datos.	No Iniciado
46	6.7. Trabajo remoto	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
47	6.8. Informes de eventos de seguridad de la información	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
48	**7. Controles Físicos**			

49	7.1. Perímetro de seguridad física	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
50	7.2. Entrada física	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
51	7.3. Asegurar oficinas, salas e instalaciones	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
52	7.4. Monitoreo de seguridad física	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
53	7.5. Protección contra amenazas físicas y ambientales.	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
54	7.6. Trabajar en áreas seguras	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
55	7.7. Escritorio despejado y pantalla despejada	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
56	7.8. Emplazamiento y protección de equipos	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
57	7.9. Seguridad de los activos fuera de las instalaciones	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
58	7.10. Medios de almacenamiento	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
59	7.11. Utilidades de apoyo	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
60	7.12. Seguridad del cableado	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
61	7.13. Mantenimiento de equipos	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
62	7.14. Eliminación segura o reutilización de equipos	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
63	**8. Controles Tecnológicos**			

64	8.1. Dispositivos de punto final de usuario	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
65	8.2. Derechos de acceso privilegiado	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
66	8.3. Restricción de acceso a la información	SI	Comtemplado en los procedimientos de acceso seguro-	No Iniciado
67	8.4. Acceso al código fuente	SI	Comtemplado en los procedimientos de acceso seguro-	No Iniciado
68	8.5. Autenticación segura	SI	Comtemplado en los procedimientos de acceso seguro-	No Iniciado
69	8.6. Gestión de capacidad	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
70	8.7. Protección contra malware	SI	Mantener los equipos seguros de los desarrolladores.	No Iniciado
71	8.8. Gestión de vulnerabilidades técnicas	SI	Contemplado en el análisis GAP	En Proceso
72	8.9. Gestión de la configuración	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
73	8.10. Eliminación de información	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
74	8.11. Enmascaramiento de datos	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
75	8.12. Prevención de fuga de datos	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
76	8.13. Copia de seguridad de la información	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
77	8.14. Redundancia de las instalaciones de procesamiento de información	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
78	8.15. Inicio sesión	NO	NO se ajusta a la realidad actual de la empresa	No Aplica

79	8.16. Actividades de seguimiento	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
80	8.17. Sincronización de reloj	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
81	8.18. Uso de programas de utilidad privilegiados	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
82	8.19. Instalación de software en sistemas operativos	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
83	8.20. Seguridad de la red	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
84	8.21. Seguridad de los servicios de red.	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
85	8.22. Segregación de redes	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
86	8.23. Filtrado web	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
87	8.24. Uso de criptografía	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
88	8.25. Ciclo de vida de desarrollo seguro	NO	NO se ajusta a la realidad actual de la empresa	No Aplica
89	8.26. Requisitos de seguridad de la aplicación	NO	No se aplica en la empresa por el momento.	No Aplica
90	8.27. Principios de arquitectura e ingeniería de sistemas seguros	NO	No se aplica en la empresa por el momento.	No Aplica
91	8.28. Codificación segura	SI	Necesario para la creación de código seguro.	No Iniciado
92	8.29. Pruebas de seguridad en desarrollo y aceptación	NO	No se aplica en la empresa por el momento.	No Aplica
93	8.30. Desarrollo subcontratado	NO	No se aplica en la empresa.	No Aplica
94	8.31. Separación de los entornos de desarrollo, prueba y producción	SI	Necesaria para realizar el testeo.	No Iniciado
95	8.32. Gestión del cambio	NO	No se aplica en la empresa.	No Aplica

96	8.33. Información de la prueba	NO	No se aplica en la empresa.	No Aplica
97	8.34. Protección de los sistemas de información durante las pruebas de auditoría	NO	No se aplica en la empresa.	No Aplica

Tabla 7

Lista de documentos entregables resultado de la investigación

Documentación a generar basada en las vulnerabilidades			
Documento	**Tipo**	**Descripción**	**Código**
Política de Seguridad de la Información	Política	Establece los principios, objetivos y compromisos de seguridad en la empresa.	SGSI-POL-COM-001
Procedimiento de Control de Accesos y su registro	Procedimiento	Define cómo otorgar, modificar y revocar accesos a sistemas, repositorios, servidores.	SGSI-PROC-CA-001
Política de Clasificación de la Información	Política	Clasificación y etiquetado de información según criticidad y confidencialidad.	SGSI-POL-CI-001
Procedimiento de Copias de Seguridad y Restauración	Procedimiento	Define frecuencia, responsables, medios y verificación de respaldos.	SGSI-PROC-CSR-001
Procedimiento de Gestión de Incidentes de Seguridad	Procedimiento	Define pasos para notificar, registrar, analizar y tratar incidentes de seguridad.	SGSI-PROC-GIS-001
Política de Uso Aceptable de Recursos Tecnológicos	Política	Regula el uso de computadoras, correos, internet, dispositivos USB, etc.	SGSI-POL-UR-001
Procedimiento de Gestión de Activos	Procedimiento	Define el inventario y control de activos de información, hardware y software.	SGSI-PROC-GAC-001
Procedimiento de Actualización y Parcheo de Sistemas	Procedimiento	Describe cómo mantener actualizados sistemas operativos y aplicaciones.	SGSI-PROC-ASIS-001
Política de Protección contra Malware	Política	Establece medidas de uso de antivirus y restricciones de instalación de software.	SGSI-POL-PAM-001
Procedimiento de Conexiones Remotas Seguras	Procedimiento	Describe cómo realizar conexiones seguras usando VPN y cifrado.	SGSI-PROC-CREM-001
Formato de Registro de Incidentes de Seguridad	Registro	Documento de evidencia para registrar cada incidente de seguridad.	SGSI-REG-IS-001

Formato de Entrega y Devolución de Activos	Registro	Documento firmado en la entrega o devolución de equipos de trabajo.	SGSI-REG-DEVAC-001
Plan de Concienciación y Capacitación en Seguridad de la Información	Plan	Define capacitaciones periódicas en seguridad de la información.	SGSI-PLAN-CAP-001
Declaración de Aplicabilidad (SoA)	Documento SGSI	Registra los controles aplicados, justificando su selección o exclusión.	
Matriz de Riesgos	Documento SGSI	Calculamos el nivel de riesgo	
Mapa de Procesos	Documento SGSI	Mapea cada proceso localizando los activos de información que manejan	
Plan de tratamiento de Riesgos	Documento SGSI	Plan de acción para mitigar el riesgo calculado determinando responsables y tiempos	
Gantt de Actividades	Documento SGSI	Cronogramar de actividades para la implementación del SGSI	
Análisis GAP	Documento SGSI	Análisis inicial de la situación actual de la empresa respecto a la seguridad de la información	

Nota: Creación propia.

Tabla 8

Matriz método SIPOC

Definición de procesos y subprocesos							
Entidad	**Proceso**	**Subproceso**	**S**	**I**	**P**	**O**	**C**
BESTTECH SAS	Desarrollo de software		Cliente interno o externo, Analistas de requisitos, Líder técnico	Requisitos funcionales y no funcionales, estándares de desarrollo, herramientas de programación, control de versiones.	1.- Análisis de requerimientos 2.- Diseño técnico 3.- Codificación Pruebas (QA) 4.- Control de versiones 5.- Despliegue	Software funcional, documentación técnica, versiones liberadas, repositorio actualizado	Usuario final, equipo de soporte, cliente externo/interno

BESTTECH SAS	Reclutamiento de personal		Jefe de desarrollo	Perfil del puesto, requerimientos técnicos, solicitudes de contratación, currículums.	1.- Publicación de vacante 2.- Revisión de hojas de vida 3.- Entrevistas técnicas y de RRHH 4.- Evaluación 5.- Selección 6.- Firma de contrato y acuerdos de confidencialidad	Desarrollador contratado, expediente laboral, cuenta de usuario (provisional o permanente), accesos configurados	Área de desarrollo, Líder de proyecto
BESTTECH SAS	Migración		Cliente (equipo técnico y funcional), equipo de soporte TI interno, equipo de desarrollo, proveedor del core financiero	Copias de la base de datos del cliente (en producción), estructura de datos actual, manuales técnicos del cliente, scripts de extracción, herramientas de migración, políticas de seguridad.	1.- Recepción y validación de la data 2.- Generación de respaldo y eliminación 3.- Limpieza/normalización 4.- Transformación y carga a ambiente nuevo 5.- Validación 6.- Liberación a producción	Datos migrados al core financiero, respaldo de seguridad, logs del proceso, informe técnico de migración	Cliente final, equipo de soporte post-producción, auditores, responsables del SGSI
BESTTECH SAS	Migración	Generación de respaldo y eliminación	Equipo de migración, equipo de TI, cliente (equipo técnico), responsables del SGSI	Respaldos de bases de datos del cliente, políticas de retención y eliminación de información, procedimientos de respaldo y restauración, medios de almacenamiento (discos, nubes, cintas), herramientas de cifrado	1.- Recepción de respaldos 2.- Verificación de integridad 3.- Almacenamiento seguro (cifrado y control de acceso) 4.- Uso temporal para validaciones 5.- Eliminación segura tras validación final o almacenamiento según política de retención	Datos almacenados de forma segura o certificados de eliminación segura (bitácora de eliminación), informe de respaldo y restauración, registros de auditoría del proceso.	Cliente final, equipo de soporte post-producción, auditores internos/externos, responsables de SGSI
BESTTECH SAS	Migración	Transformación de datos	Equipo de desarrollo y migración, equipo técnico del cliente, analistas de datos, responsable del core financiero	Estructura de la base de datos original del cliente, diccionario de datos del core financiero, reglas de homologación, scripts de transformación, matrices de equivalencia, políticas de calidad de datos.	1.- Análisis de estructura actual 2.- Definición de correspondencias de campos 3.- Aplicación de transformaciones (tipos de datos, formatos, codificaciones) 4.- Validación de integridad y consistencia 5.- Revisión con cliente 6.- Aprobación técnica	Archivos transformados o scripts ejecutables, estructura de datos compatible con el core, informe de calidad de datos, registro de incidencias de transformación	Equipo de implementación del core, cliente final, soporte técnico, auditores internos, responsables del SGSI

CLIENTE	Gestión de usuarios y accesos	Departamento de TI, RRHH, Responsable del área	Solicitud de alta o modificación de usuario, políticas de acceso, perfiles de puesto.	1.- Revisión de solicitud 2.- Aprobación 3.-Creación de cuenta 4.-Asignación de permisos 5.-Registro y notificación	Usuario creado o modificado, credenciales entregadas, logs de acceso	Empleados, auditores internos, responsables de seguridad

Nota: Creación propia.

Tabla 9

Mapa de procesos identificados

Mapa de Procesos			
Nro.	**Proceso**	**Activos involucrados**	**Riesgos principales**
1	Desarrollo de software	Código fuente, repositorios Git, estaciones de trabajo	Fuga de código, acceso no autorizado, malware, pérdida de datos.
2	Pruebas con datos de clientes	Datos de clientes (financieros y personales), servidor pruebas	Uso de datos reales sin anonimización, fuga de datos, pérdida de datos.
3	Implantación y soporte remoto	Conexiones remotas, datos de clientes, laptops de soporte	Intercepción de datos, acceso no autorizado, fuga de información.
4	Gestión de versiones	Repositorios Git, código fuente	Fuga de código, acceso no autorizado, falta de control de cambios.
5	Recepción de datos de clientes	Correos electrónicos, datos de clientes	Fuga de información, falta de clasificación de datos.
6	Resguardo y almacenamiento de información	Servidor de pruebas, código fuente, respaldos	Pérdida de datos por cortes de energía, daño físico, acceso no autorizado.
7	Vinculación y desvinculación de personal	Código fuente, repositorios Git, estaciones de trabajo, Servidor de pruebas, código fuente, respaldos, datos de clientes, conexiones remotas.	Uso de datos reales sin anonimización, fuga de datos, pérdida de datos, fuga de código.

Nota: Creación propia.