EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

TECNOLÓGICO NACIONAL DE MÉXICO

Tecnológico Nacional de México

Instituto Tecnológico Superior de Guasave

Tesis

Propuesta de un Sistema de Gestión de Seguridad de la Información aplicado al proceso de facturación de una agencia aduanal bajo el estándar ISO/IEC 27001:2022

Presentada por

Sandra Guadalupe Nieblas Castro

Como requisito para la obtención de grado de

Ingeniera en Gestión Empresarial

Directora de tesis

MAP. Elizabeth Salinas Rosales

Codirectora de tesis

Mtra. Arikani Soberanes Félix

Guasave, Sinaloa, México. Febrero de 2026

Instituto Tecnológico Superior de Guasave

AGRADECIMIENTOS

Quiero expresar mi más sincero agradecimiento a mi asesora de tesis, la MAP. Elizabeth Salinas Rosales, por su valiosa orientación y acompañamiento en el desarrollo de este trabajo, su experiencia y compromiso fueron fundamentales para la investigación, agradezco profundamente su paciencia y apoyo constante, sin su guía la culminación de este proyecto no habría sido posible.

De igual manera le agradezco a todos mis docentes, quienes a lo largo de mi formación compartieron sus conocimientos, experiencias y orientación.

Finalmente agradezco a la institución por brindarme una formación académica y las herramientas necesarias para mi desarrollo profesional.

DEDICATORIA

A mi familia,

Quienes son un pilar fundamental en mi vida y el motor que me impulsa día a día a seguir adelante, gracias por su amor incondicional, su apoyo y ser esa luz en el camino que me brinda fortaleza en los momentos más difíciles. A cada integrante de mi familia, gracias por su comprensión y palabras de aliento durante este proceso, este logro es el reflejo de todo el apoyo que me han brindado.

A mí misma,

Por la fortaleza y el crecimiento como persona que tuve que desarrollar a lo largo de este recorrido, por no rendirme a pesar de las dificultades y por mantenerme firme aun cuando el cansancio se hacía presente, este camino fue de muchos retos que a pesar de ellos nunca pensé en rendirme, aunque se viera cada vez más complicado.

Me dedico este logro por la disciplina, constancia y valentía que mostré en este proceso, hoy reconozco el gran esfuerzo y empeño que le puse a esta meta y me siento profundamente orgullosa de mi por concluirla.

RESUMEN

La seguridad de la información toma un papel en las organizaciones cada vez más importante, específicamente para aquellas que manejan gran cantidad de información sensible como datos fiscales, financieros y de operaciones aduanales, ya que actualmente, la ciberdelincuencia es cada vez más común, por ello la importancia de proteger la confidencialidad, integridad y disponibilidad de la información a través de una propuesta de un Sistema de Gestión de Seguridad de la Información (SGSI) con base en el Anexo A de la norma ISO/IEC 27001:2022 enfocado en el área de facturación, con el objeto de salvaguardar los activos de información de la empresa.

La metodología utilizada para el trabajo fue con un enfoque descriptivo, no experimental y transversal, utilizados con herramientas de recolección de información como entrevistas, observación de los procesos, un check list basado en el Anexo A de la norma ISO/IEC 27001:2022, un análisis FODA, una matriz de riesgos y diagramas de flujo, instrumentos que fueron de gran utilidad para el análisis de datos y toma de decisiones del SGSI.

Finalmente, a través de cada uno de estos instrumentos se obtuvo un producto integral en el que se tomaron en cuenta puntos críticos para la formación del sistema, en el que se especificaron las políticas a seguir en diferentes aspectos de sus procesos operativos, enriqueciendo y aportando a la organización en el fortalecimiento de procesos internos, su imagen en el mercado y sobre todo generando mayor confianza con sus clientes con un enfoque de seguridad de la información.

Palabras claves: Seguridad de la información, SGSI, ISO/IEC 27001:2022, triada de la información, gestión de riesgos.

ABSTRACT

Information security is taking an increasingly important role in organizations, especially for those that handle large amounts of sensitive information such as tax, financial, and customs operations data, since cybercrime is becoming more common. Therefore, it is crucial to protect the confidentiality, integrity, and availability of information through the proposal of an Information Security Management System (ISMS) based on Annex A of the ISO/IEC 27001:2022 standard, focused on the billing area, with the aim of safeguarding the company's information assets.

The methodology used for the work was with a descriptive, non-experimental, and cross-sectional approach, utilizing information-gathering tools such as interviews, process observation, a checklist based on Annex A of the ISO/IEC 27001:2022 standard, a SWOT analysis, a risk matrix, and flowcharts, instruments that were very useful for data analysis and decision-making of the ISMS.

Finally, through each of these instruments, a comprehensive product was obtained in which critical points for the formation of the system were taken into account. It specified the policies to be followed in different aspects of its operational processes, enriching and contributing to the organization by strengthening internal processes, its market image, and, above all, generating greater trust with its clients with an information security approach.

Keywords: Information security, ISMS, ISO/IEC 27001:2022, information triad, risk management.

ÍNDICE.

ÍNDICE DE TABLAS.

ÍNDICE DE FIGURAS.

INTRODUCCIÓN.

La seguridad de la información se ha convertido en un factor fundamental en las organizaciones debido al aumento del uso de tecnologías emergentes y el manejo de datos sensibles. Proteger la información ante cualquier amenaza como accesos no autorizados, ciberataques, perdidas de datos, alteraciones, divulgaciones, entre otros riesgos, es una tarea que todas las organizaciones deberían atender. Como señalan Martinez y Mosquera (2020) uno de los activos más importantes de la era actual es la información, siendo este uno de los puntos más críticos de las empresas por el grado de sensibilidad que puedan representar. El implementar medidas de prevención como un SGSI prepara a las organizaciones ante riesgos que pudieran ser fatales para las compañías, según reportes del periódico universal, en México se registraron 59 millones de ciberataques al día en el primer trimestre del 2025 siendo el phishing la amenaza con mayor presencia (Galaván, 2025).

El Sistema de Gestión de Seguridad de la Información funciona como instrumento a las empresas para identificar y gestionar los riesgos asociados con la seguridad de la información, mediante la aplicación de controles de buenas prácticas de seguridad de la información, siendo una herramienta clave para la formación de nuevas relaciones comerciales y generar confianza en los clientes al sustentar sus operaciones en una norma internacional tan importante como la norma ISO/IEC 27001:2022

El presente proyecto fue elaborado en las instalaciones de una agencia aduanal en la que se maneja una gran cantidad de información sensible de alta criticidad dentro del área de facturación. El trabajo se centra en el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) con base en los controles del Anexo A de la norma ISO/IEC 27001:2022, identificando la situación actual de la entidad en cuanto al nivel de cumplimientos de dichos controles y proponer medidas correctivas de seguridad y gestión de riesgos.

El documento se encuentra estructurado primero por las generalidades del proyecto como planteamiento del problema, justificación y objetivos, siguiendo con el marco

teórico con conceptos que sientan las bases de la investigación, en el siguiente apartado se aborda la metodología empleada para el análisis del proyecto y los instrumentos empleados en la recolección de información, posteriormente se exponen los resultados obtenidos para la elaboración del Sistema de Gestión de Seguridad de la Información y finalmente se presentan las conclusiones y recomendaciones.

1. Planteamiento del problema.

En las agencias aduanales mexicanas, el proceso de facturación electrónica mediante CFDI y la gestión de pedimentos implica el manejo constante de información fiscal, financiera y aduanal altamente sensible. La creciente digitalización de estos procesos ha incrementado la exposición de los datos a posibles brechas de seguridad cuando no se cuenta con un Sistema de Gestión de Seguridad de la Información (SGSI) formalmente implementado.

Esta situación no solo representa un riesgo para la operación interna de las agencias, sino que también puede afectar la seguridad en la cadena logística, el comercio exterior y el cumplimiento normativo (Hernández, 2025). Este contexto se vuelve aún más crítico si se considera que en México se registraron más de 324 mil millones de intentos de ciberataques durante 2024, afectando aproximadamente al 27 % de las empresas, entre ellas organizaciones del sector logístico y aduanal, lo que evidencia la vulnerabilidad actual de estos procesos frente a amenazas cibernéticas cada vez más sofisticadas (ESET, 2025; Padua, 2025). En este contexto, surge la necesidad de evaluar el nivel de cumplimiento de los controles de seguridad de la información y proponer un SGSI basado en la norma ISO/IEC 27001:2022 aplicado específicamente al proceso de facturación de una agencia aduanal.

2. Justificación.

La implementación de un SGSI basado en la norma ISO/IEC 27001:2022 en el proceso de facturación de una agencia aduanal se justifica ante el acelerado proceso de digitalización del comercio exterior mexicano y la necesidad de proteger información fiscal y aduanal. La norma ISO/IEC 27001 no solo establece controles técnicos y organizacionales, sino que promueve un enfoque sistemático basado en la gestión de riesgos, contribuyendo a la reducción de incidentes de seguridad y al fortalecimiento de la confianza de los clientes (International Organization for Standardization (ISO, 2022).

Desde una perspectiva práctica, el desarrollo de esta propuesta permitirá evaluar el nivel actual de cumplimiento de la empresa respecto a los controles del Anexo A, identificar los principales riesgos del proceso de facturación y diseñar medidas preventivas y correctivas acordes con sus capacidades operativas y tecnológicas. Esto contribuirá a mejorar la eficiencia operativa, la protección de datos sensibles y el cumplimiento de las disposiciones legales en materia fiscal y de protección de datos.

En el ámbito académico, la investigación aporta un referente aplicado sobre la implementación de sistemas de gestión basados en normas ISO en el sector de servicios logísticos y aduanales en México, un campo con limitada evidencia empírica documentada, lo que fortalece la vinculación entre la teoría y la práctica profesional.

3. Hipótesis.

La implementación parcial de un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en ISO/IEC 27001:2022 en el área de facturación de una empresa aduanal permitirá mejorar el nivel de cumplimiento de los controles de seguridad de la información y reducir los riesgos asociados a la pérdida, alteración o acceso no autorizado a datos sensibles.

4. Objetivos.

4.1 General.

Diseñar una propuesta de Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022 para su aplicación en el proceso de facturación en una empresa aduanera, con el fin de fortalecer la confidencialidad, integridad y disponibilidad de la información crítica.

4.2 Específicos.

1. Diagnosticar el nivel de cumplimiento actual de la empresa con respecto a los controles del Anexo A de la norma ISO/IEC 27001:2022.

2. Identificar los principales riesgos de seguridad de la información en el proceso de facturación.
3. Diseñar propuesta de medidas preventivas y correctivas que reduzcan la exposición a amenazas, basado en la norma ISO/IEC 27001:2022.

5. MARCO TEÓRICO.

5.1 Fundamentos de la Seguridad de la Información.

En un mundo cada vez más digitalizado, la información se ha convertido en uno de los activos más valiosos para cualquier organización. Para una agencia aduanal, esta afirmación es aún más crítica: datos fiscales, detalles de operaciones de comercio exterior, información de clientes y documentos gubernamentales conforman la esencia de su operación diaria. Perder el control sobre esta información no es solo un inconveniente técnico; puede significar multas, pérdida de confianza comercial, e incluso la interrupción de la cadena de suministro internacional. Esta sección explora los conceptos básicos que sirven como cimientos para cualquier sistema de protección, desde la clásica triada CID (confidencialidad, integridad y disponibilidad), hasta las amenazas y vulnerabilidades que enfrentan los procesos digitales actuales.

5.1.1 Concepto y evolución de la seguridad de la información.

La seguridad de la información puede definirse como la práctica de proteger la información de accesos no autorizados, uso, divulgación, interrupción, modificación o destrucción, con el fin de preservar su confidencialidad, integridad y disponibilidad (ISO/IEC 27000, 2018). Sin embargo, este concepto no ha sido estático, su evolución ha estado ligada al desarrollo tecnológico, mientras que en el pasado se centraba en la custodia física de documentos en archivos, hoy debe abordar desafíos complejos como el ciber espionaje y las filtraciones masivas de datos en la nube (Whitman y Mattord, 2021).

Para una organización moderna, la seguridad de la información ya no es un lujo o un tema exclusivo del departamento de Tecnologías de Información (TI); es una función estratégica que impacta directamente en la operatividad, el cumplimiento legal y la reputación corporativa. Implementar medidas robustas de seguridad es, en esencia, una inversión en la continuidad y credibilidad del negocio, especialmente en sectores

regulados como el aduanal, donde un incidente puede detener operaciones y desgastar la confianza de los clientes en minutos.

5.1.2 La Triada CID: Confidencialidad, Integridad y Disponibilidad.

El corazón de la seguridad de la información late en tres principios interdependientes, conocidos como la Triada CID (o CIA Triad, por sus siglas en inglés): Confidencialidad, Integridad y Disponibilidad, como se muestra en la figura 1. Esta tríada no es solo una lista de buenos deseos; es un marco de evaluación que guía el diseño e implementación de cualquier control de seguridad (Centro Criptológico Nacional, 2023).

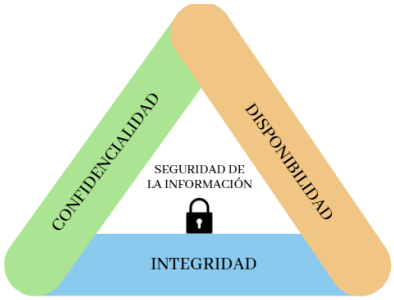
Confidencialidad: Se refiere a que la información solo sea accesible para aquellas personas o sistemas autorizados. Ejemplo en la agencia aduanal: Los pedimentos de un cliente importador no deben ser visibles para sus competidores. Un control típico es el cifrado de archivos sensibles y la gestión estricta de permisos en los sistemas.

Integridad: Garantiza que la información sea exacta, completa y no haya sido alterada de manera no autorizada. Ejemplo en la facturación: El XML de un CFDI, una vez timbrado por el SAT, no debe poder modificarse en su monto, folio o datos del receptor. Aquí, las firmas digitales y los controles de versión son mecanismos clave.

Disponibilidad: Asegura que la información y los sistemas necesarios para acceder a ella estén operativos cuando se requieran. Ejemplo crítico: El sistema de facturación electrónica debe estar funcionando durante las horas de cierre de operaciones, pues una caída implicaría no poder emitir comprobantes y detener embarques. Las copias de seguridad y los planes de recuperación ante desastres sostienen este principio. En conjunto, la triada CID proporciona una lente simple pero poderosa para evaluar cualquier riesgo.

Figura 1.

Principios de la seguridad Triada CID



Nota. Elaboración propia

5.1.3 Amenazas vulnerabilidades y riesgos en los sistemas de seguridad.

Para proteger la información, primero debemos entender a qué nos enfrentamos. En seguridad, se distinguen tres conceptos clave que suelen confundirse: amenaza, vulnerabilidad y riesgo. Una amenaza es cualquier evento o agente que pueda causar daño (ejemplo: un hacker, un programa maligno, un empleado descontento). Una vulnerabilidad es una debilidad o fallo en un sistema, procedimiento o control que esa amenaza podría explotar (ejemplo: un software sin parches, una contraseña débil, una política de acceso laxa). El riesgo es la probabilidad de que una amenaza materializada explote una vulnerabilidad y el impacto negativo resultante (Stoneburner et al., 2002).

Las amenazas a la seguridad de la información son diversas y evolucionan constantemente. Para el proceso de facturación, algunas de las más relevantes incluyen:

Malware: Software malicioso que puede robar datos o cifrarlos para pedir un rescate.

Phishing: Tácticas que buscan engañar a los empleados para que revelen credenciales o información sensible. Un correo falso que parezca del SAT dirigido al personal de facturación es una amenaza muy creíble.

Accesos no autorizados: Ya sea por credenciales robadas, configuraciones erróneas o el uso de cuentas compartidas. Esto viola directamente la confidencialidad.

Errores humanos o negligencia: La eliminación accidental de archivos, el envío de información a destinatarios equivocados o la mala configuración de un sistema son causas frecuentes de incidentes.

Ataques de denegación de servicio: Buscan saturar los sistemas para hacerlos inaccesibles, afectando la disponibilidad de los portales de facturación o del propio SAT.

Ataque de amenaza persistente (APT): Consta de un avanzado ciberataque durante cierto tiempo amplio en el que el atacante no descubierto adquiere acceso a la red e información de la entidad en cuestión.

Red de robots (botnet): También conocido como “robot network”, es un conjunto de dispositivos conectados que conforman una red la cual se encuentra afectada y controlada remotamente por el atacante.

Ataque de descarga oculta: Código infectado que se descarga en los dispositivos de manera automática al visitar sitos webs que regularmente no son confiables, logrando que los dispositivos sean vulnerables y ponga en riesgo la seguridad.

Ataque de denegación de servicio distribuido (DDos): Estos ataques utilizan robots (botnets) que saturan los sitios web para realizar un bloqueo de servicios a los usuarios.

Ransomware: Consta de un ataque de extorsión de la mano del malware que cifra y retiene la información de una organización hasta que este pague por el rescate de esta.

5.1.4 Vulnerabilidad informática.

Si las amenazas son los "delincuentes", las vulnerabilidades son las "puertas y ventanas sin cerrar" de la organización. Estas debilidades pueden ser de naturaleza muy diversa, y es crucial identificarlas para priorizar su corrección. Como señala (Muñoz, 2018) las vulnerabilidades informáticas son aquellas probabilidades de que acontezca un suceso o se presente un error en el software o hardware que ponga en riesgo la información y sea débil ante un hacker o atacante. Dichas vulnerabilidades puedes corresponder a posibles fallos o errores en las configuraciones que se clasifican en diferentes categorías:

Vulnerabilidad física: Las que suceden por debilidades del entorno físico que pudieran afectar los dispositivos, servidores o redes dando paso a los atacantes. Algunos ejemplos son los accesos no autorizados a equipos, falta de controles de acceso y dispositivos extraviados o robados.

Vulnerabilidad natural: Eventos naturales que puedan poner en riesgo la integridad de la información que provienen por fenómenos del entorno o desastres naturales, mismos que no dependen del fallo humano o tecnológico, como lo son los incendios, inundaciones, terremotos, entre otros.

Vulnerabilidad humana: Los que por errores, descuidos, actos malintencionados, negligencia, malas prácticas, manipulación, uso inapropiado o falta de capacitación afectan los sistemas, estos son de los errores más comunes, ya que aún con tecnología de calidad el error humano sigue siendo una actividad manual y a conciencia.

Vulnerabilidades de Hardware: Debilidades técnicas o físicas en los componentes de un sistema informático, causados por fallos de fabricación, mala calidad, deterioro o falta de mantenimiento.

Vulnerabilidades de dispositivos móviles: Suceden cuando por fallos, descuidos o malas configuraciones alguien no autorizado pueda acceder a la información de los dispositivos móviles, a través de memorias USB, conexiones de WI-FI sin protección, instalaciones de aplicaciones no confiables o robos.

Vulnerabilidades de software: Errores de programación o con fallos de programación en los sistemas operativos o programas que pueden deberse a sistemas sin actualizar, permisos mal establecidos o programación insegura.

Vulnerabilidad económica: Se manifiesta principalmente cuando la organización no cuenta con los recursos económicos necesarios para mantener y actualizar su sistema de seguridad

5.1.5 Buenas prácticas y Cultura de Seguridad.

Implementar controles tecnológicos avanzados es inútil si no se sostienen sobre bases de buenas prácticas y una cultura organizacional de seguridad. La tecnología es una

herramienta, pero las personas son tanto el eslabón más fuerte como el más débil en la cadena de seguridad. Por ello, las buenas prácticas comienzan con la concienciación y capacitación continua del personal, desde la alta dirección hasta el auxiliar operativo (Correa Sánchez, 2020).

Todos deben entender su rol en la protección de la información, reconocer amenazas, entre estos se encuentran los accesos no autorizados, mala gestión de contraseñas, uso indebido, negligencia por parte de los colaboradores, falta de conocimiento en el tema de seguridad por parte de los trabajadores, medidas de seguridad débiles, falta de controles, sistemas desactualizados, entre otros, por ello la importancia de tener buenas prácticas internas (Artunduaga, et al. 2023).

Capacitar al personal es uno de los principales pasos a los que se debe acudir para fomentar una cultura de seguridad de la información, brindarles el conocimiento y herramientas necesarias para que adquieran habilidades de resolución de problemas en dado caso de que se presente alguno que ponga en riesgo la integridad, confidencialidad y disponibilidad de la información (Sánchez, 2020).

Integrar mecanismos de defensa que puedan detectar fallas en redes de comunicación que puedan ser amenazas, monitoreo de los dispositivos utilizados y las redes que utiliza, visualización de patrones de tráfico en las redes de comunicación, implementación de WAN (Wide Area Network) para los enlaces y conexiones, contar con controles de seguridad para evitar accesos no autorizados y monitoreo a los sistemas de información con envío de alertas en caso de un incidente (ASF, 2024).

Exigir a los usuarios una firma en contrato de confidencialidad, contar con protocolos de verificación de identidad a los usuarios para evitar accesos no autorizados, evitar el uso de agentes externos o correos sin cifrado, hacer responsable a los usuarios de proteger la información de autentificación, evitar tener registros en papel o dispositivos portátiles, contar con contraseñas seguras que no sean basadas en información personal del usuario, que no contenga patrones o caracteres consecutivos, lo

suficientemente extensa para ser segura y fácil de recordar y cambiarlas periódicamente (NMK-I-27002-NYCE-2015)

Adquirir tecnologías de seguridad avanzadas que se utilicen para la encriptación de datos, autentificación biométrica y crear conciencia y compromiso en los trabajadores para superas los retos de implementación y adopción (Coello, 2024).

Utilizar la herramienta de encriptación de datos, para proteger la información a través de la decodificación y cifrado para evitar filtraciones y accesos no autorizados, de tal forma que se mantengan íntegros los datos tanto para el emisor como el receptor, por otro lado, una buena práctica en las empresas es una política de contraseñas fuertes, incluir pasos de autentificación, contar con contraseñas complejas y cambiarlas periódicamente (360, 2024).

Comprender estos fundamentos sobre la triada CID, la naturaleza de las amenazas y vulnerabilidades, y la importancia de las buenas prácticas es esencial, pero insuficiente para lograr una protección sostenible y sistemática. Para ello, las organizaciones necesitan un marco de trabajo estructurado que ordene estos esfuerzos: un Sistema de Gestión. En el siguiente apartado, exploraremos cómo los sistemas de gestión, y en particular el ciclo de mejora continua PDCA (Plan-Do-Check-Act) por sus siglas en inglés, proporcionan la metodología para integrar la seguridad de la información en el corazón de las operaciones de una agencia aduanal.

5.2 Sistemas de Gestión en las Organizaciones.

5.2.1 Concepto y Propósito de los Sistemas de Gestión en las Organizaciones.

Un sistema de gestión puede entenderse como el conjunto de elementos interrelacionados que una organización establece para dirigir y controlar sus actividades con el fin de alcanzar objetivos específicos (ISO, 2015). Estos elementos incluyen políticas, procesos, recursos y documentación que trabajan de manera sinérgica. En el ámbito de los servicios, como los ofrecidos por una agencia aduanal, un sistema de gestión proporciona la oportunidad para garantizar que los procesos

críticos como la facturación electrónica se ejecuten de manera consistente, confiable y alineada con los requisitos legales y las expectativas del cliente.

5.2.2 El Enfoque de Procesos: La Organización como una Red de Actividades.

Este enfoque conceptualiza la organización no como un conjunto de departamentos o aislados, sino como una red dinámica e interconectada de procesos (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI, 2019). Un proceso es un conjunto de actividades mutuamente relacionadas que transforman entradas en salidas, agregando valor en cada etapa (ISO, 2015). En el contexto de una agencia aduanal, el proceso de facturación es un ejemplo claro: toma como entrada los datos de la operación y los transforma en un comprobante fiscal digital (CFDI) que cumple con las normativas fiscales.

Aplicar el enfoque de procesos al área de facturación de una agencia aduanal implica desglosar la actividad global de facturar en subprocesos secuenciales e interdependientes:

1) Recepción de datos del cliente/operación

2) Validación y cruce de información

3) Captura en el sistema

4) Timbrado del CFDI

5) Envío y notificación al cliente

6) Archivo y respaldo.

Cada uno de estos eslabones maneja información sensible y presenta vulnerabilidades específicas. Un sistema de gestión se inserta en este flujo, identificando en cada punto qué activos de información están en juego y qué controles se necesitan para protegerlos.

5.2.3 Ciclo de mejora continua (PDCA: Plan–Do–Check–Act)

El ciclo PHVA (Planificar-Hacer-Verificar-Actuar) como se muestra en la figura 2, también conocido como PDCA por sus siglas en inglés ó ciclo de Deming, constituye el principio operativo fundamental que impulsa la mejora continua en un sistema de gestión, esta metodología enfocada en la calidad a través de 4 etapas que trabajan en conjunto para detectar la raíz de los problemas y soluciones de los procesos, (Arias, 2019).

Planear (plan): Durante esta fase se estudia la causa raíz de la problemática seleccionada, se define el alcance que el proceso tendrá, definiendo objetivos claros y cuantificables y los recursos que se necesitarán para su ejecución, es la parte donde se realiza un diagnóstico de la situación actual que permita el análisis.

Hacer (do): Implementar el plan realizado en la etapa anterior, durante esta fase se pueden realizar cambios que aporten mejoras antes de ejecutarlo, se debe organizar al equipo de trabajo, asignación de actividades y responsabilidades, funciona como una primera prueba de lo planeado.

Verificar (check): Evaluar y recopilar los resultados que el plan seguido ha tenido, se puede utilizar herramientas de apoyo como gráficos, indicadores, matrices, check list, cuadros y diagramas, funcionada para detectar posibles errores o fallas que se puedan tener.

Actuar (act): Finalmente durante esta etapa se busca ejecutar todas aquellas correcciones que se han identificado para buscar la mejora continua del proyecto o proceso, se aplican medidas correctivas y a partir de aquellas que se aplican se reinicia el ciclo nuevamente.

Figura 2.

Ciclo de Deming (PHVA)

Nota. En base a *González, et al., (2020)*

Su aplicación en una empresa aduanal para el proceso de facturación sería algo tangible: en la fase de planificación, se identificaría el riesgo de acceso no autorizado al sistema de emisión de CFDI; en la ejecución, se implementaría un sistema de autenticación; durante la verificación, se auditarían los registros de acceso para detectar anomalías; y finalmente, en la actuación, se ajustarían las alertas en base a los hallazgos, reiniciando el ciclo. Esta metodología cíclica asegura que el SGSI no sea un proyecto con fin, sino un proceso vivo de adaptación y perfeccionamiento.

5.2.4 Importancia de los sistemas de gestión en las organizaciones.

La implementación de sistemas de gestión formalizados trasciende el cumplimiento normativo para convertirse en una ventaja competitiva sostenible. En sectores

complejos y regulados, como el logístico y aduanal, contar con un marco de gestión reconocido internacionalmente genera un activo intangible clave: confianza. Esta confianza se traduce en reputación frente a clientes y socios comerciales, quienes perciben una operación más confiable y segura. Internamente, estos sistemas institucionalizan una cultura organizacional de mejora continua, disciplina operativa y toma de decisiones basada en evidencia. Estructuran el conocimiento, reducen la variabilidad de los procesos y optimizan el uso de recursos, lo que conduce directamente a una mayor eficiencia y una reducción de costos por errores o incumplimientos

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

5.3.1 Definición y objetivos de un SGSI.

Un Sistema de Gestión de Seguridad de la Información (SGSI) es una estructura que integra políticas, procedimientos, controles y responsabilidades orientadas a proteger los activos informativos de una organización. De acuerdo con la ISO/IEC 27001:2023, un SGSI se basa en la gestión de riesgos y busca asegurar que los controles aplicados sean acordes a las amenazas existentes (UNE, 2023). Implementarlo implica tanto el compromiso directivo como la participación del personal, dado que el sistema es tan fuerte como el eslabón humano que lo sostiene.

Así mismo se considera un conjunto de procesos relacionados entre sí fundado en un enfoque hacia los riesgos de una organización, cuyo propósito es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información (ISO/IEC, 2016).

5.3.2 Estructura de un SGSI.

La norma ISO/IEC 27001:2022 hace referencia a que un SGSI tiene como objetivo proteger la información y los sistemas de Tecnología de Información (TI) respecto a la triada de la información y se conforma por distintos bloques, de los cuales no todos son de carácter obligatorio (Erik Gremeyer, 2022), como se muestra en la figura 3.

1. **Contexto de la organización:** Definir el alcance que tendrá el SGSI, tener claro los límites que este tendrá y los activos involucrados. Se realiza un diagnóstico del entorno de la empresa para conocer la situación actual en que se encuentra, comprender cual es el contexto correcto es la clave para empezar con el proyecto, ya que es la base y el sustento para la toma de decisiones.

2. **Liderazgo y compromiso:** La norma exige a la alta dirección tener el liderazgo suficiente para transmitir el compromiso que esta tiene a los colaboradores, lograr y comunicar que ellos también tengan el compromiso exigido, también se encarga de liderar que las políticas y controles se cumplan, así como la asignación de roles y responsabilidades, además de incorporar una nueva cultura organizacional enfocada en la protección de datos.

3. **Objetivos del SI:** Definir los objetivos que servirán como base para el diseño del SGSI y las medidas necesarias, se determina como se van a lograr los objetivos, los recursos requeridos, y una calendarización de estos con responsabilidades.

4. **Política de SI:** La alta dirección es responsable de establecer una política general de seguridad de la información que sea lo suficientemente clara para justificar el desarrollo del SGSI y que se encuentre alineada a los objetivos plateados de un inicio, así como de divulgar dicha política a todo el personal de manera clara y concisa.

5. **Roles, responsabilidades y competencias:** Asignar y documentar los roles y responsabilidades a cada una de las partes involucradas en el proyecto para que cada colaborador conozca sus funciones, además de garantizar que los trabajadores tengan y desarrollen las competencias necesarias para el rol que este desempeña.

6. **Gestión de riesgos:** Se identifican evalúan y analizan los riesgos que puedan ser una amenaza para la seguridad de la información, se plantean las

vulnerabilidades que los activos puedan tener y el planteamiento de acciones correctivas que funcionen como tratamientos para cada uno de estos riesgos, así como la definición de criterios de aceptación y tipo de tratamiento.

7. **Evaluación del desempeño y KPI:** Su objetivo es medir el nivel de eficiencia del SGSI, utiliza indicadores para evaluar que tanto se cumplen los objetivos planteados, evalúa el rendimiento que este ha tenido y funcionan para identificar áreas de oportunidad.

8. **Documentación:** La norma exige que cada uno de los procesos del SGSI, así como sus políticas se encuentren correctamente documentadas, para su correcta implementación y control, además de que se encuentren disponibles cuando se requieran, así mismo, el tener todo documentado permite tener una trazabilidad del proyecto.

9. **Comunicación:** Es necesario que exista armonía en la comunicación entre las diferentes áreas involucradas para transmitir de forma correcta y asertiva evitando mal entendidos o errores, se debe describir cómo será tanto la comunicación interna como externa a través del desarrollo de un plan de comunicación.

10. **Conciencia:** La alta dirección debe asegurar la comprensión de las pautas de seguridad del SGSI, el propósito, los riesgos involucrados, los efectos que este tiene y el trabajo que conlleva sostenerlo, este objetivo se puede lograr con campañas de concientización a los trabajadores y hacer una retroalimentación con sus necesidades y aportaciones.

11. **Relaciones con proveedores:** Se deben establecer políticas específicas para los servicios externos que ocupa la compañía para asegurar que estos cumplan con los estándares de seguridad de la información que requiere, con la finalidad de proteger y salvaguardar los datos, se deben estableces criterios para el control de estos en acuerdos o contratos.

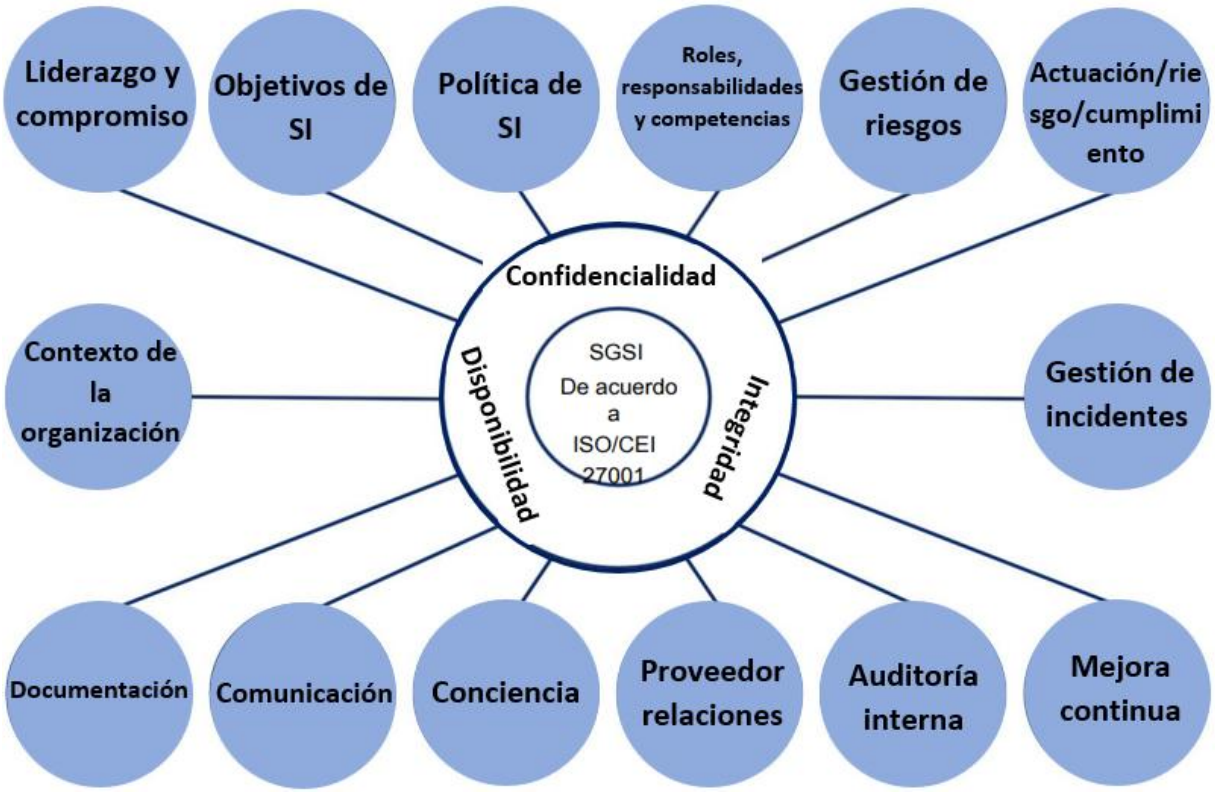
12. **Auditoría interna:** Tiene como objetivo monitorear y dar un seguimiento a las medidas del SGSI y asegurar que esté cumpliendo con sus objetivos y requisitos planteados en la norma, así como verificar si está siendo efectivo.

13. **Gestión de incidentes:** Se busca la correcta gestión de incidentes, llevar un control y monitoreo, tener un procedimiento de gestión, garantizar que estos sean tratados y con seguimiento, se busca que la empresa se encuentre preparada ante un percance y reducir su impacto.

14. **Mejora continua:** Se debe garantizar que el SGSI se actualice y mejore de acuerdo con los lineamientos planteados en la norma, se busca corregir errores y lograr una evolución positiva, se pueden utilizar metodologías de apoyo como el ciclo PHVA (Planificar, Hacer, Verificar y Actuar) este es un recurso de gran utilidad para fortalecer los procesos y hacer que el SGSI no se estanque o quede obsoleto.

Figura 3.

Componentes de un SGSI según ISO/IEC 27001:2022



Nota. Tomado de (Erik Gremeyer, 2022)

5.3.3 Beneficios y retos de implementar un SGSI

Contar con un SGSI tiene grandes ventajas para las organizaciones, entre las que se destacan la confianza interna y externa que pueden transmitir con esta herramienta, las personas reconocen que la institución cuenta con medidas de seguridad, permite mejores negociaciones con nuevos clientes y fomenta una publicidad orgánica por medio de recomendaciones (Group, 2022).

Reduce los riesgos de perder información, permite que las empresas tengan una herramienta como base en caso de incidentes, ayuda a que los riesgos sean gestionados y documentados, mejora la eficiencia de las empresas al tener un plan de acción que los resguarda y protege, mejora la toma de decisiones basadas en datos históricos, establece metodologías de mejora continua, permite tener un control de la organización (Guacanés Castro, 2022).

5.3.4 Herramientas útiles para elaborar un SGSI.

El método más utilizado y sugerido por la norma para el diseño de un SGSI, es el ciclo PDCA que permite evaluar los resultados de este, facilita el proceso de implementación con bases y procesos sólidos que funcionan entre sí para trabajar por una mejora continua, este ciclo consiste en 4 principales pasos (Plan, Do, Check, Act) que en conjunto reducen fallas y mejora la eficiencia operativa y resolución de conflictos (Guacanés Castro, 2022).

5.4 Norma ISO/IEC 27001.

5.4.1 Orígenes, finalidad y ámbito de aplicación de la norma ISO/IEC 27001.

La norma ISO/IEC 27001, publicada y mantenida por ISO y la Comisión Electrotécnica Internacional (IEC), ofrece un marco internacional para gestionar de manera sistemática la seguridad de la información. Su objetivo es ayudar a las organizaciones a identificar riesgos, aplicar controles adecuados y establecer procesos de mejora

continua (UNE, 2023). Para sectores que manejan información sensible, la adopción de esta norma representa una base sólida para fortalecer su madurez en ciberseguridad.

El artículo científico De la Cruz et al. (2023) refuerza esta idea al destacar que ISO 27001 se ha consolidado como el estándar más utilizado a nivel mundial para garantizar la protección de los datos en entornos digitales, particularmente en ámbitos con alto volumen de transacciones, como el comercio electrónico. En la tabla 1 se muestra la familia que conforma la ISO 27000.

Tabla 1.

Familia ISO 27000.

Familia ISO 27000	
Norma	**Descripción de la norma**
iso/iec 27000	Sistema de gestión de seguridad de la información. Visión general y vocabulario.
iso/iec 27001	Sistema de gestión de seguridad de la información. Requerimientos.
iso/iec 27002	Código de práctica para controles de seguridad de la información.
iso/iec 27003	Guía para la implementación del sistema de gestión de seguridad de la información.
iso/iec 27004	Gestión de seguridad de la información. Monitoreo, medición, análisis y evaluación.
iso/iec 27005	Gestión del riesgo de seguridad de la información.
iso/iec 27006	Requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.
iso/iec 27007	Guía para la auditoría de sistemas de gestión de seguridad de la información.
iso/iec tr 27008	Guía para auditores sobre los controles de seguridad de la información.
iso/iec 27009	Requerimientos para la aplicación de la iso/iec 27001 en sectores específicos.
iso/iec 27010	Gestión de seguridad de la información para comunicaciones intersectoriales e interorganizacionales.
iso/iec 27011	Guía de gestión de seguridad de la información para organizaciones de telecomunicaciones basado en la iso/iec 27002.
iso/iec 27013	Guía para la implementación integrada de la iso/iec 27001 y la iso/iec 20000-1.
iso/iec 27014	Gobierno de seguridad de la información.
iso/iec tr 27015	Guía de gestión de seguridad de la información para servicios financieros.
iso/iec tr 27016	Gestión de seguridad de la información. Economía de las organizaciones.
iso/iec 27017	Código de prácticas para controles de seguridad de la información basado en la iso/iec 27002 para servicios cloud.
iso/iec 27018	Código de prácticas para la protección de la información de identificación personal (pii) en nubes públicas que actúan como procesadores pii.
iso/iec 27019	Controles de seguridad de la información para la industria de servicios energéticos.
iso/iec 27021	Requerimientos de competencia para profesionales de sistemas de gestión de seguridad de la información.
iso/iec 27799	Informática de salud-Gestión de seguridad de la información en salud utilizando iso/iec 27002.

Nota. En base a (Cely, 2021)

5.4.2 Controles principales de seguridad del Anexo A.

El anexo A de la norma ISO/IEC 27001 proporciona los controles necesarios para mitigar riesgos que afectan la seguridad de la información. En el proceso de facturación, su aplicación es importante debido al manejo de información sensible y al impacto en el cumplimiento normativo y la continuidad operativa. Este apartado presenta los controles principales seleccionados dentro del alcance del SGSI orientados a reforzar la confidencialidad, integridad y disponibilidad de la información.

A.5.1 Políticas de seguridad de la información: Definición de controles, aprobación y mantenimiento de políticas orientadas a la seguridad de la información para el marco del SGSI

A.5.7 Seguridad en relación con proveedores: Definición de los criterios a seguir en la organización del manejo de proveedores incluyendo evaluación, acuerdos de confidencialidad, cláusulas, responsabilidades y medios de seguimiento y supervisión.

A.7.5 Seguridad física: Enfocado en la prevención de accesos no autorizados que pongan en riesgo la seguridad de la información, este control se basa en la protección de los espacios, sistemas, dispositivos y servidores.

A.8.12 Protección de datos: Cuyo propósito es proteger la triada de la información (confidencialidad, integridad y disponibilidad), implementa controles que protegen los elementos que involucran información sensible, (ej. Cifrados, base de datos, respaldos y mecanismos de recuperación de datos).

A.9.4 Gestión de accesos: Delimita y establece controles de accesos bajo el principio de mínimo privilegio, asegurando la restricción de datos solo a personal autorizado de acuerdo con sus responsabilidades, establece políticas del uso de credenciales, contraseñas y usuarios.

A.16.1 Gestión de incidentes: Establece controles y procedimientos documentados sobre la respuesta a incidentes o eventos que pongan en riesgo la seguridad de la información, funciona como plan de contingencia ante estos fenómenos.

5.4.3 Etapas de implementación para la certificación.

La implementación de un SGSI requiere seguir una metodología estructurada que permita asegurar su correcta adopción y sostenibilidad en el tiempo. En este apartado se describen las principales etapas consideradas, las cuales permiten pasar de la planificación inicial a la verificación del cumplimiento, garantizando un enfoque ordenado, participativo y alineado con los objetivos de la organización.

Formar el equipo: Definir quienes estarán a cargo de la realización del proyecto del SGSI y las partes involucradas en su gestión, como tecnologías de información (TI), recursos humanos, alta dirección, el responsable principal, calidad y demás áreas involucradas.

Análisis de brechas: En esta etapa se evalúa el estado actual de la organización, se define el alcance, se identifican los controles que se implementan en los procesos, se establecen políticas y se realizan una evaluación de riesgos.

Implementación del SGSI: Para esta etapa se documentan todos los procesos de políticas y controles, se crean los lineamientos, la implementación de herramientas e instrumentos y capacitar al personal sobre el funcionamiento y políticas del SGSI que deben seguir para formar una cultura organizacional orientada a la seguridad de la información.

Auditoría interna: Esta etapa funciona como una verificación de cumplimiento del SGSI previo a la auditoría externa para obtener la certificación, se realiza un la de auditoria para la detección de no conformidades y detectar posibles fallas del sistema de gestión, se realiza un informe a la lata dirección para reportar el desempeño del sistema y aplicación de medidas correctivas.

Auditoría externa: Para la etapa final se contacta a un organismo externo certificado para realizar una auditoría externa, donde se evalúa el nivel de cumplimiento para conceder la certificación.

5.5 Gestión de Riesgos de Seguridad de la Información.

La gestión de riesgos constituye uno de los pilares del SGSI. Según la norma ISO/IEC 27005:2018, gestionar riesgos implica identificar, analizar, evaluar y tratar los riesgos que afectan a los activos informativos con el fin de minimizar su probabilidad e impacto (ISO/IEC, 2018). Este enfoque permite a las organizaciones priorizar acciones y asignar recursos de forma más eficiente.

5.5.1 Concepto de riesgos de seguridad de la información.

Se define como riesgo a toda aquella amenaza que ataque una vulnerabilidad de un activo de información poniendo en peligro la protección de los datos provocando consecuencias negativas. Dentro del SGSI un riesgo se compone de tres elementos.

Activo de información: todo aquel elemento que representa valor para la entidad (ejemplo: Datos, sistemas o procesos).

Amenaza: Suceso, evento o incidente con el potencial de generar daños negativos a los activos de la empresa, estos pueden ser de carácter interno o externo, ya sea de carácter humano, técnico, ambiental u organizacional.

Vulnerabilidad: Debilidad de los activos que es aprovechada por una amenaza para causar daño (ejemplo: Software, hardware, procesos, políticas o sistemas) (Peña, 2016).

5.5.2 Tratamiento de riesgos en el marco del SGSI.

El tratamiento de riesgos es uno de los enfoques más importantes en el SGSI, puesto que, permiten tener un esquema de posibles tratamientos con las acciones necesarias para enfrentar una incidencia, con el propósito de salvaguardar la confidencialidad, disponibilidad e integridad de la información y mantener los riesgos en niveles óptimos. Este proceso contempla 4 distintos tipos de controles según la naturaleza o grado de la amenaza como se muestra en la figura 4.

Recudir: Consiste en implementar controles de seguridad con el fin de mitigar el riesgo lo más que se pueda, dado que en ocasiones eliminarlo puede ser más costoso que el riesgo es sí.

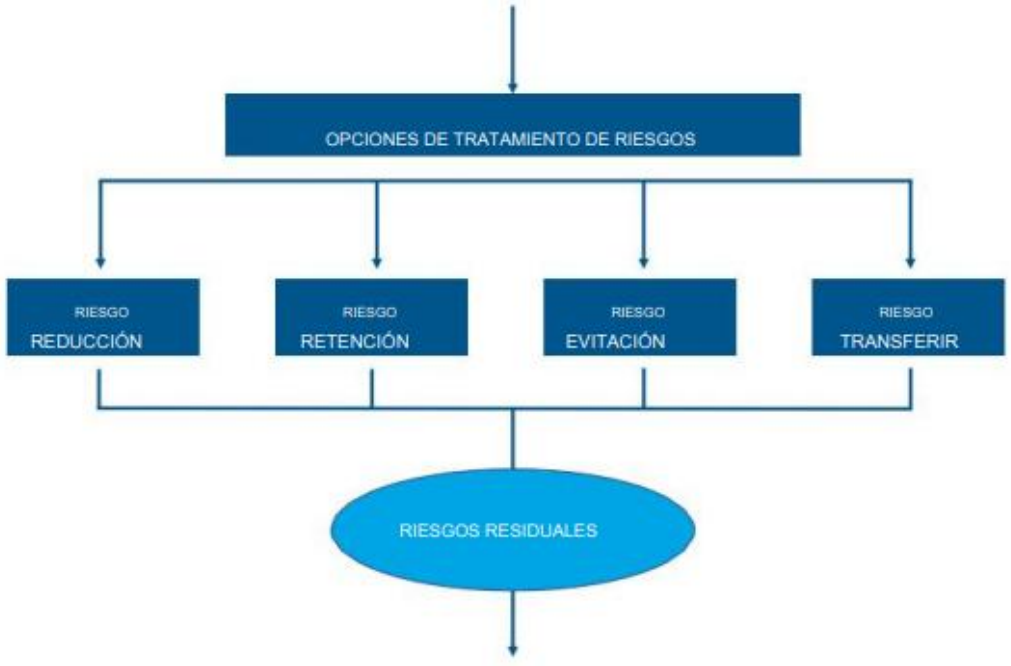
Retención: También conocido como aceptación del riesgo, enfocado en no aplicar controles extras, dado que el nivel de riesgos es mínimo y no representa un peligro latente, el tratamiento no consiste en ignorar el riesgo, simplemente estar monitoreándolo para que no represente mayor amenaza a futuro.

Evitar: Este tratamiento consiste en eliminar la actividad o factor que genere el riesgo, ya que representa un gran impacto que dífilamente podría mitigar evidentemente con controles.

Transferir: Consta en trasladar el riesgo en manos de terceros expertos en el tema, comúnmente utilizado es riesgos asociados a tecnología y servidores (Jimenez, 2022).

Figura 4.

Opciones de tratamiento de riesgos



Nota. En base (Erik Gremeyer, 2022)

5.5.3 Metodologías de gestión de riesgos.

La gestión de riesgos conforma el objetivo principal de la aplicación de un SGSI, es por ello la importancia de seguir una metodología correcta para tener una buena gestión de comprensión del riesgo presentado y el plan a seguir para tratarlo, como la metodología de 10 pasos propuesta por Penna y Pérez (2021) que explica de manera integral un procedimiento para la gestión de riesgos.

- Reconocer la exposición
- Identificar el riesgo
- Relevar controles existentes
- Medir los riesgos
- Docuementar los riesgos
- Evaluar el margen de maniobra
- Definir estrategias de riesgos
- Documentar las soluciones propuestas
- Accionar contra el riesgo
- Planificar la continuidad

5.6 Proceso de facturación en las organizaciones.

5.6.1 Concepto y finalidad del proceso de facturación.

El proceso de facturación reúne información fiscal y administrativa que debe tratarse con altos niveles de precisión y seguridad. En México, la facturación electrónica está regulada por el Servicio de Administración Tributaria (SAT), el cual establece los lineamientos para la emisión de Comprobantes Fiscales Digitales por Internet (CFDI) y sus requisitos de validación (SAT, 2023). Cualquier alteración, pérdida o acceso no autorizado a estos datos puede afectar no solo la operación, sino también el cumplimiento normativo y la relación con clientes y proveedores.

5.6.2 Clasificación de los tipos de CFDI.

En el entorno administrativo los comprobantes fiscales representan una herramienta valiosa para el respaldo de las operaciones económicas empresariales, como expone (SAT, Guía de llenado de los comprobantes fiscales digitales por Internet, s.f.) en su guía de llenado de comprobantes fiscales, los comprobantes CFDI se clasifican en 6 tipos, entre ellos los de ingreso, egreso, traslado, recepción de pagos, nómina y retenciones e información de pagos.

- **Comprobante de ingreso:** Son aquellos que confirman la legalidad de los ingresos de una persona moral o física por honorarios, prestación de servicios, arrendamientos, etc.

- **Comprobante de egreso:** Estos comprobantes se usan para el registro de devoluciones, descuentos o bonificaciones para que sean deducibles y permiten hacer correcciones a las cantidades del comprobante.

- **Comprobante de traslado:** Se utiliza para el traslado de mercancías legalmente, es un respaldo de que cumple con la normatividad fiscal y legal, se puede realizar por el traslado de propietario que es cuando el mismo lo realiza o por transportista que es cuando el propietario contrata los servicios de alguien más.

- **Comprobante de recepción de pagos:** Se usa cuando una operación es pagada parcialmente o cuando no reciben el pago de contraprestación y hace más fácil la conciliación de otras facturas contra pagos.

- **Comprobante de nómina:** Comprobante que complementa el recibo de nómina, emitido por pagos de sueldos, salarios y otros conceptos relacionados que se entregan a los trabajadores.

- **Comprobante de retenciones e información de pagos:** Se realiza cuando hay retención de impuestos, en el que se incluyen pagos en el extranjero

5.6.3 Riesgos de seguridad de la información en el proceso de facturación.

El proceso de facturación representa un punto crítico en las organizaciones, ya que es un área muy vulnerable más en cuanto a riesgos de seguridad de la información se refiere por el grado de sensibilidad de los datos que se maneja, dentro de los riesgos que pueden presentarse se originan tanto de factores externos como internos.

Riesgos por factores internos

- Accesos no autorizados a información sensible
- Perdida de datos por falta de respaldos
- Error humano
- Dependencia de plataformas digitales
- Manipulación o alteración de datos
- Uso indebido de accesos y credenciales
- Desactualizaciones de software
- Incumplimiento de políticas internas
- Falta de capacitación

Riesgos por factores externos

- Ataques cibernéticos
- Infecciones de virus y malware
- Phishing
- Suplantación de correos institucionales
- Fallas en servicios de proveedores
- Fallas en las redes de comunicación
- Fenómenos naturales

Identificar la fuente principal del riesgo, ya sea interno o externo, permite establecer medias de control en el SGSI, según la naturaleza y tipo de riesgo.

5.6.4 Información sensible utilizada en la facturación electrónica.

La facturación electrónica representa uno de ellos puntos más críticos en una agencia aduanal, dado al grado de sensibilidad de la información que se maneja en el proceso

de elaboración de una factura, información que legalmente debe estar presente para el cumplimiento normativo de las obligaciones fiscales.

Hablando específicamente de la emisión de los comprobantes fiscales (CFDI) el (SAT, 2017) plantea requisitos que de manera directa o indirecta se catalogan como información sensible entre ellos datos fiscales del emisor como Registro Federal de Contribuyente (RFC), razón social, domicilio fiscal y régimen fiscal, mismo caso para los datos fiscales del receptor además del uso del CFDI, por otro lado se aborda información financiera como impuestos, retenciones, firmas y métodos de pago, en el enfoque de agencias aduanales se visualizan datos de la operación como fechas, número de referencias, pedimentos y condiciones comerciales, así como aquella información que válida el comprobante como el folio (UUID), sellos digitales, certificados digitales y su acompañamiento XML.

5.7 Seguridad de la Información en una Agencia Aduanal.

5.7.1 Concepto y funcionalidad de agencia aduanal.

La ley aduanera en el artículo 167-D señala que “La agencia aduanal es la persona moral autorizada por el Servicio de Administración Tributaria para promover por cuenta ajena el despacho aduanero de mercancías, en los diferentes regímenes aduaneros previstos en esta Ley” (UNIÓN, 2020). Una agencia aduanal funciona como un intermediario en las exportaciones e importaciones de mercancía ante el despacho aduanero, facilitando las operaciones encargándose de múltiples tareas como:

- **Gestión de trámites:** Tramitan todos los documentos requeridos, incluyendo la elaboración de los pedimentos oficiales.

- **Operación de despacho aduanero:** Se ocupan de gestionar todo lo relacionado con la entrada y salida de mercancías del país, aplicando los diferentes regímenes aduaneros disponibles.

- **Orientación especializada:** Asesora a las empresas sobre los requisitos y protocolos que deber cumplirse para el despacho aduanero, así como las disposiciones legales

- **Calculo y pago de impuestos:** Realizan el cálculo y pago de los aranceles e impuestos correspondientes a cada operación.

- **Revisión de normas:** Comprueban que las mercancías cumplan con las regulaciones y restricciones no arancelarias aplicables.

- **Coordinación logística:** Gestionan la comunicación con transportistas, almacenes y demás participantes para que el proceso aduanal sea más rápido y eficiente.

Las agencias aduanales administran documentos críticos como pedimentos, comprobantes fiscales, datos de importadores y exportadores, así como información logística sensible. Debido a ello, requieren controles robustos para garantizar que estos datos no sean alterados o divulgados indebidamente. La Cámara Nacional de Agentes Aduanales (2023) señala que la seguridad en los procesos aduanales es indispensable para asegurar la continuidad operativa y el cumplimiento regulatorio.

De la Cruz et al., (2023) también resalta la vulnerabilidad de las transacciones electrónicas y la necesidad de adoptar estándares como ISO 27001 para proteger la información en entornos de alto riesgo como el comercio exterior.

5.7.2 Estándares mínimos de seguridad para el agente aduanal.

Las agencias aduanales manejan una gran cantidad de información sensible en sus operaciones de comercio exterior como datos fiscales, legales y personales, por lo que

la Secretaria de Económia (2016) estable los requisistos obligatorios que los agentes aduanales deben seguir para operar legalmente según lo establecido por la norma méxicana NMX-R-026-SCFI-2016.

- Sistemas de seguridad que aseguren la confidencialidad de la info9rmación
- Planes de contingencia
- Lugares alternos de resguardo de la información
- Licencias de software actualizadas
- Servicios de apoyo de sistemas de información
- Documentación de políticas
- Personal capacitado
- Sistemas de evaluación y seguimiento
- Acuerdos de confidencialidad de la información de los clientes
- Control de documentos interno y externos
- Plan de auditoría interna

5.7.3 Riesgos informáticos y amenazas específicas en operaciones aduanales.

Actualmente la seguridad en la gestión aduanera en México enfrenta desafíos prioritarios ante la seguridad para mantener la transparencia requerida en el comercio internacional, existe una lucha constante contra el contrabando, tráfico de drogas, robos entre otras actividades ilícitas como el robo de información y extorción. Entre los riesgos más comunes para las agencias se encuentran:

- Phishing
- Malware
- Robo de información
- Errores humanos
- Falta de controles de seguridad
- Falta de capacitación del personal
- Divulgación no autorizada de información

- Ataques cibernéticos a la infraestructura tecnológica
- Robo o perdida de dispositivos móviles

5.7.4 Importancia de la seguridad de la información en el comercio exterior.

Con base en lo propuesto por ((UAA), 2024) uno de los retos más importantes en las empresas es salvaguardar la información de sus clientes y asegurar su integridad, generar confianza en los clientes permite tener relaciones comerciales sólidas. La seguridad digital en el entorno del comercio internacional hace referencia al conjunto de medidas, métodos y herramientas que buscan proteger la formación de los sistemas electrónicos que se involucran en las operaciones aduaneras, entre estos se encuentran datos personales, la integridad de las operaciones, y otras medidas de ciber protección.

6. MATERIALES Y MÉTODOS.

Este apartado describe los materiales y métodos utilizados para el desarrollo de la investigación, los cuales fueron seleccionados con el objetivo de realizar un diagnóstico estructurado y confiable sobre el estado de la seguridad de la información en el proceso de facturación. La metodología adoptada se basa en un enfoque descriptivo y sistemático orientado a la identificación de riesgos, brechas y controles existentes, combinando técnicas cualitativas y cuantitativas. Este enfoque es coherente con las buenas prácticas internacionales en gestión de la seguridad de la información, donde el análisis de procesos, activos y riesgos es la base para el diseño de sistemas de gestión eficaces (National Institute of Standards and Technology, 2012).

6.1 Población y muestra.

Para diagnosticar la seguridad de la información y diseñar un SGSI viable, era necesario definir dónde y con quién se realizaría el estudio. La empresa aduanal con presencia en México y Estados Unidos cuenta con nueve sucursales. Sin embargo,

para los fines de esta investigación, se seleccionó como caso de estudio y muestra la sede de Nogales, Sonora.

Esta decisión se tomó por criterios de viabilidad y profundidad. Concentrar los esfuerzos en una sola sucursal permite un análisis más detallado y un control sobre la recolección de información, algo importante para una primera implementación parcial del SGSI. La unidad Nogales funcionó como una muestra representativa de los procesos de facturación de la empresa, donde se pudo observar, en tiempo real y con nivel de detalle, el flujo completo de la información crítica.

La población de estudio quedó conformada por todas las personas de esta sucursal cuyo trabajo implica interactuar con el proceso de facturación. Esto incluyó un espectro de roles:

- Auxiliares y personal operativo, responsables de la captura y manejo inicial de los datos.
- Coordinadores y supervisores, que validan, autorizan y gestionan los procesos.
- Personal administrativo vinculado, que maneja el archivo y la custodia documental.

Dado que el equipo del área es reducido y cada puesto tiene una función específica para el análisis, se optó por trabajar con una muestra censal. Esto significa que se incluyó en la investigación al 100% de los colaboradores disponibles, garantizando una visión integral y evitando sesgos en la comprensión de las actividades y los flujos de información sensibles.

6.2 Variables del estudio.

Para la elaboración de este proyecto se identificaron las variables que permitieron tener un planteamiento sólido para su ejecución, entre ellas se encuentra una independiente y las variables dependientes para cumplir con los objetivos del proyecto:

- **Variable independiente:**
  Cumplimiento de controles de seguridad de la información
  (Basados en el Anexo A de ISO/IEC 27001:2022)

- **Variables dependientes:**

  Nivel de riesgo asociado al proceso de facturación

  Prácticas actuales de protección de la información

  Brechas de seguridad detectadas

  Implementación o ausencia de controles tecnológicos, físicos y administrativos

Estas variables permitieron relacionar el grado de cumplimiento con el nivel de exposición a riesgos dentro del proceso.

6.3 Diseño del estudio.

El diseño utilizado fue descriptivo, no experimental y de corte transversal.

- Descriptivo, porque se analizó el estado actual del proceso de facturación en materia de seguridad de la información.
- No experimental, ya que no se manipularon variables, sino que se observó la situación tal como ocurre en la práctica.
- Transversal, porque los datos fueron recolectados en un único periodo.

Este diseño fue adecuado para evaluar el cumplimiento de controles, identificar riesgos y documentar las prácticas existentes.

6.4 Materiales e instrumentos de recogida de información.

El trabajo se lleva a cabo con la recolección de datos que combinó la aplicación de varias estrategias. El objetivo es triangular la información, contrastando lo que las personas realizan, con lo que los documentos muestran y la observación directa. Se utilizan los siguientes instrumentos.

6.4.1 Entrevistas Semiestructuradas.

Con el objetivo de comprender el flujo de trabajo desde adentro, diseñamos y aplicamos entrevistas semiestructuradas al personal clave del área de facturación y tecnologías de la información. 7.1.2

- El conocimiento tácito sobre el manejo de datos sensibles.

- La percepción de riesgos y las prácticas informales de seguridad.
- La claridad sobre roles, responsabilidades y la existencia de capacitación.
- Los procedimientos reales y los puntos de fricción en el proceso.

Este instrumento fue fundamental para mapear la brecha entre la teoría y la práctica diaria, capturando el componente humano, que suele ser el eslabón más vulnerable.

6.4.2 Check list basado en Anexo A de ISO/IEC 27001:2022

Para evaluar de manera sistemática y objetiva el estado de la seguridad, se elabora un check list sobre algunos controles del Anexo A de la norma ISO/IEC 27001:2022. Este instrumento cuantitativo nos permitió traducir un marco normativo en una serie de ítems verificables, asignándoles una puntuación clara (0=No cumple, 1=Cumple parcialmente, 2=Cumple). Su aplicación dio una línea de base numérica del nivel de cumplimiento, identificando de manera directa las áreas fuertes y las brechas críticas.

6.4.3 Observación directa y revisión documental.

Para validar y complementar la información recabada en las entrevistas y el check list, se emplea dos técnicas de verificación:

- Observación directa no participante: se registra in situ las actividades, tiempos, sistemas utilizados y el flujo físico de documentos. Esto permite identificar vulnerabilidades prácticas, por ejemplo, errores con contraseñas y pantallas desatendidas con información sensible.
- Revisión de documentos institucionales: análisis de procedimientos internos escritos, registros operativos, evidencias de sistemas y organigramas de roles. La revisión fue importante para distinguir entre lo que estaba documentado y lo que estaba implementado.

6.4.4 Herramientas de sistematización y análisis.

La información obtenida a través de los instrumentos anteriores fue organizada y analizada utilizando un conjunto de herramientas que facilitaron su síntesis:

- Microsoft Excel fue la plataforma central para consolidar los datos del check list, crear la matriz de riesgos y realizar análisis básicos.
- Diagramas de Flujo ayudaron a visualizar y refinar el mapa del proceso de facturación, identificando puntos críticos de control.
- Matrices FODA y de Riesgos, construidas específicamente para este proyecto, fueron los marcos analíticos que nos permitieron integrar los hallazgos cualitativos y cuantitativos para generar el diagnóstico integral y priorizar las acciones de la propuesta de SGSI.

6.5 Procedimiento seguido.

Para lograr el objetivo general del diagnóstico en acciones concretas, el estudio se organizó en un procedimiento secuencial de tres fases naturales. La primera de ellas tuvo como propósito fundamental conocer a profundidad el proceso de facturación antes de cualquier evaluación. Esta fase inicial sentó las bases de todo el diagnóstico, y se desarrolló a través de los siguientes tres pasos estratégicos:

6.5.1 Identificación del proceso de estudio.

El punto de partida fue una reunión de alineación con los responsables del área de facturación y de Tecnologías de Información (TI). En este espacio colaborativo, se delimitó el alcance del proceso a analizar, se identificaron los sistemas informáticos involucrados (como Plataformas de Recursos Empresariales (ERP) y las plataformas del SAT) y se definieron formalmente los roles y responsabilidades de cada participante. Este paso fue crucial para garantizar que la investigación partiera de una comprensión compartida y acotada de la realidad operativa.

6.5.2 Recolección de información preliminar.

Esta etapa consistió en recopilar y analizar documentos operativos vigentes, flujos de trabajo escritos y cualquier registro que pudiera ilustrar el funcionamiento teórico y administrativo del área. Este análisis documental permitió construir una línea base

contra la cual contrastar posteriormente la práctica observada y las declaraciones del personal.

6.5.3 Aplicación de entrevistas.

Para complementar y dar vida a la documentación, se diseñó y aplicó un ciclo de entrevistas semiestructuradas a los responsables directos de la facturación. Estas conversaciones, más allá de verificar datos, buscaron capturar el conocimiento experiencial, las rutinas no escritas, los desafíos cotidianos y la percepción que el equipo tenía sobre los controles de seguridad existentes. Las respuestas fueron transcritas y consolidadas en una tabla, lo que permitió identificar patrones, contradicciones y oportunidades de mejora desde la voz misma de los actores clave.

6.5.4 Aplicación del check list ISO/IEC 27001.

Se efectuó una exhaustiva investigación de los controles del Anexo A de la norma ISO/IEC 27001:2022, primero se revisaron y evaluaron los controles de la norma y se seleccionaron aquellos que son aplicables al área de facturación de acuerdo con el alcance y propósito del SGSI, consecutivamente, se analizó cada control seleccionado con base a la situación actual de la empresa en el contexto de cada uno verificado con evidencia documental, observación directa y declaraciones del personal.

Con la información recolectada se bosquejó una tabla en la que se asignó una calificación a cada uno conforme a su nivel de cumplimiento. Una vez diseñado se validó con el personal del área para una respuesta más clara y acertada a la realidad según sus operaciones y controles.

6.5.5 Construcción del mapa del proceso de facturación.

Se procedió a elaborar un mapa de procesos de todos los procedimientos utilizados en el área de facturación de principio a fin, en el que se indicaron entradas, actividades, documentos generados, los programas y ERP utilizados y puntos críticos de seguridad

en cada uno de ellos, con el objeto de identificar la información sensible involucrada en cada proceso de las operaciones.

6.5.6 Elaboración del inventario de información sensible.

A partir del mapa de procesos se realizó un inventario de información diseñado en una tabla donde se concentraron los programas que se utilizan a lo largo del proceso de facturación, para detectar el tipo de información que gestionan, como datos fiscales, datos personales de los clientes, comprobantes digitales (CFDI) y registros operativos. La tabla permite visualizar el nivel de sensibilidad de la información y el uso que se le da en el proceso de facturación, siendo un pilar para el desarrollo de las demás herramientas utilizadas en el presente proyecto para garantizar la confidencialidad, disponibilidad e integridad de la información con el uso del SGSI.

6.5.7 Análisis FODA.

Para identificar el contexto actual interno y externo del área de facturación, se procedió con un análisis FODA para conocer los factores positivos y negativos que impactan en el Sistema de Gestión de Seguridad de la Información (SGSI). Se observaron las fortalezas, debilidades, amenazas y oportunidades en los procesos de gestión, resguardo, seguridad y tratamiento de la información. Se realizó a partir de entrevistas dirigidas al personal involucrado y mediante la observación de las operaciones, lo que permitió tener un panorama claro del nivel de cumplimiento de seguridad de la información con el que se cuenta. Los resultados obtenidos fueron un pilar clave para determinar las estrategias a seguir para el diseño y toma de decisiones en el SGSI.

6.5.8 Elaboración de la matriz de riesgos.

Con base en el check list y el análisis FODA se identificaron los riesgos que pueda enfrentar la seguridad de la información, se diseñó una matriz en la que se colocó el activo que puede estar en riesgo, el riesgo que podría enfrentar y la debilidad que pueda ser la causa, así como una escala de puntuación de la probabilidad de ocurrencia, el impacto que tendría si ocurriera, el nivel de riesgos que este representa

con un sistema de semáforo para medir la categoría en que se posiciona y finalmente un tratamiento para cada uno con el área que resulta responsable.

6.5.9 Integración del diagnóstico.

Se cruzaron los resultados del check list de controles de seguridad, entrevistas, mapa de procesos y matriz de riesgos que permitieron tener una visión integral del contexto actual de la organización en cuanto a la seguridad de la información. El check list facilitó la identificación de controles y grado de cumplimiento, la entrevista aclaró un panorama real de como los colaboradores perciben y operan en materia de seguridad de la información, el mapa de procesos permitió identificar los puntos críticos del proceso de facturación donde se gestiona la información sensible, por otro lado, la matriz de riesgos facilitó el análisis y evaluación de riesgos asociados con la confidencialidad, integridad y disponibilidad de la información, así como el seguimiento de un plan de tratamiento.

A partir de la recolección de información con estas herramientas se obtuvo información muy valiosa sobre las necesidades de la empresa para la creación y toma de decisiones en el diseño del SGSI.

6.5.10 Elaboración de la propuesta.

Finalmente, se formularon medidas preventivas y correctivas alineadas a ISO/IEC 27001:2022, considerando la viabilidad y necesidades de la empresa para hacer la propuesta del SGSI.

7. ANÁLISIS DE RESULTADOS Y DISCUSIÓN.

Esta sección expone los resultados obtenidos a partir de las actividades realizadas, estructurándolos conforme a los objetivos específicos del proyecto. Para facilitar su comprensión, los hallazgos se presentan en secciones que abarcan el diagnóstico del área, el nivel de cumplimiento de los controles del Anexo A de la norma ISO/IEC 27001:2022, el análisis del flujo de información mediante el mapa de procesos, la identificación de información sensible, el análisis FODA, la evaluación de riesgos.

7.1 Resultados.

7.1.1 Resultados del diagnóstico mediante entrevistas.

Se aplicaron entrevistas estructuradas y un check list basado en los requisitos de la norma, lo que facilitó una valoración objetiva del grado de implementación de políticas, controles técnicos, procedimientos operativos y medidas de protección física y digital. Asimismo, los resultados obtenidos permitieron identificar riesgos asociados al manejo de información fiscal, operativa y confidencial del proceso de facturación, considerando que la exposición o alteración de estos activos podría impactar la continuidad operativa y la confianza institucional (Pozo et al., 2025).

El análisis de las respuestas permitió identificar el funcionamiento general del área, los sistemas utilizados, las responsabilidades del personal y las prácticas actuales en materia de seguridad de la información. La tabla 2 muestra el concentrado de respuestas obtenidas:

Tabla 2.

Resultados de entrevistas con colaboradores clave del proceso de facturación.

1. Organización y políticas de seguridad (A.5, A.6)			
No.	Pregunta	Respuesta 1	Respuesta 2
1	¿Existe una política formal de seguridad de la información aplicable al área de facturación?	Existe una general, pero no enfocada al área	Existe una general, pero no enfocada al área
2	¿El personal de facturación ha firmado acuerdos de confidencialidad?	Por medio de un contrato	Por medio de un contrato
3	¿El aviso de privacidad incluye el uso de datos en facturación y aduanas?	Aduana si se mencionada, pero específicamente facturación no	Facturación no
2. Gestión de accesos y control de usuarios (A.9, A.5.17)			
No.	Pregunta	Respuesta 1	Respuesta 2
4	¿Cada usuario tiene un acceso individual y único al sistema de facturación?	Para cada plataforma se necesita ingresar usuario y contraseña	Cada usuario cuenta con sus accesos exclusivos para el ingreso a cada plataforma
5	¿Se aplican roles y permisos diferenciados (ej. quien captura no puede autorizar ni cancelar)?	No todos tienen los mismos permisos para ciertas operaciones	En cada sistema se lleva la configuración de roles y permisos para cada colaborador de la empresa

			dependiendo de su puesto es como se da la autorización
6	¿Se bloquean accesos cuando un empleado deja la empresa o cambia de puesto?	Se dejan aproximadamente dos meses por si se requiere.	Se desactivan los accesos del excolaborador y para cambios de puesto se mantienen accesos
7	¿Se revisa periódicamente la lista de usuarios activos en el sistema?	Ocasionalmente	Ocasionalmente
	3. Seguridad en operaciones y respaldos (A.8, A.12)		
No.	Pregunta	Respuesta 1	Respuesta 2
8	¿Existen controles de seguridad informática (ej. respaldo, encriptación, acceso restringido)?	Implementado	Implementado
9	¿Los respaldos están cifrados y almacenados en un sitio seguro (local o nube confiable)?	En nube y plataformas	Parcialmente
10	% de cumplimiento de respaldos realizados conforme a lo planificado.	51–75%	51–75%
	4. Protección de la información y documentos (A.7, A.8, A.11)		
No.	Pregunta	Respuesta 1	Respuesta 2
11	¿Las facturas y pedimentos se almacenan de manera segura y controlada?	Se almacenan en sistemas propios de manera digital y físico de acuerdo con la ley	Está documentación solo se encuentra dentro de los sistemas internos de los cuales estos

			mismos cuentan con seguridad en sus accesos
12	¿Se cuenta con medidas de resguardo de documentos físicos (archivadores cerrados, acceso limitado)?	Se cuentan con bodegas a las que pueden ingresar solo personal autorizado	Se tiene cierta documentación en la empresa y se cuenta con bodegas con acceso controlado a ciertas personas
13	¿Se emplean certificados digitales (ej. sellos SAT, otros certificados en sistemas web)?	Si	Cuentan con firmas digitales y certificados de seguridad implementados tanto en los sistemas internos como en las páginas web
5. Capacitación y concienciación (A.6.3, A.6.7)			
No.	Pregunta	Respuesta 1	Respuesta 2
14	¿El personal está capacitado para el uso y manejo de información sensible?	Cada dos meses	Periódicamente
15	¿El personal de facturación recibe capacitación periódica en protección de datos y confidencialidad?	Cada 4 meses	Periódicamente
6. Gestión de incidentes (A.16)			
No.	Pregunta	Respuesta 1	Respuesta 2
16	¿Se documentan y atienden incidentes de seguridad de la información?	Se registró un incidente de pérdida total de información en RITS pero estaba la información física.	se atienden en base al seguimiento de tickets y en caso de ser muy grande la incidencia también se

			involucra el área de calidad documentado todo el detalle
17	¿El personal sabe cómo reportar un incidente de seguridad de la información?	Tickets a sistemas	Sistema helpdesk donde se levantan tickets de incidencias
18	Nº de incidentes de seguridad en facturación en el último año	0	N/A
19	% de accesos no autorizados detectados	0%	N/A
20	Tiempo promedio de respuesta a incidentes	Desde minutos hasta horas	N/A
	7. Controles físicos (A.7.5, A.11)		
No.	Pregunta	Respuesta 1	Respuesta 2
21	¿El área de facturación tiene controles físicos (acceso restringido, cámaras, cerraduras)?	Cámaras y accesos a través de credenciales	N/A
22	¿Los equipos donde se emiten facturas están protegidos contra accesos no autorizados?	Bloqueo del equipo al tercer intento	N/A
	8. Relación con clientes y proveedores (A.5.7, A.5.23)		
No.	Pregunta	Respuesta 2	Respuesta 2
23	¿Cómo es el acercamiento de los clientes con la empresa?	El vendedor se acerca a la empresa en su mayoría ofreciendo el servicio de agencia aduanal para importaciones o exportaciones.	N/A

24	¿Existen filtros que utilicen para la admisión de un cliente? ¿Cuáles?	Se cuenta con un check list para cada tipo de servicio con requisitos que el cliente debe cumplir para ser parte de la cartera.	N/A
25	¿Qué tipo de datos personales solicitan a los clientes?	Celular, correo, comprobante de domicilio, INE (check list)	N/A
26	¿Existen lineamientos para el manejo de datos fiscales y aduanales sensibles?	Si existen	N/A

Nota. Elaboración propia

Del análisis se encontró lo siguiente:

- Se observó que el personal tiene claridad sobre las actividades operativas, pero no existen procedimientos formalizados ni documentados.
- Se identificó que el manejo de información fiscal y aduanal se realiza principalmente mediante plataformas ERP y repositorios en la nube.
- Se detectó una falta de capacitación formal en seguridad de la información.
- Se encontró que las prácticas de respaldo no están estandarizadas, lo que coincide con el incidente de pérdida total ocurrido en 2022.
- Se evidenció que no todos los colaboradores conocen las políticas institucionales relacionadas con la protección de datos.

Un resultado contrario a lo esperado fue que, a pesar de que la empresa utiliza plataformas tecnológicas robustas, no se cuenta con roles y permisos documentados, lo cual representa una brecha significativa.

Las entrevistas se visualizan más a detalle en los anexos A.1 y A.2.

7.1.2 Check list de cumplimiento del Anexo A.

El check list aplicado al área de facturación permitió evaluar el nivel de cumplimiento de los controles establecidos en el Anexo A de la norma ISO/IEC 27001:2022, con el fin de obtener un panorama real y verificable sobre la madurez de la seguridad de la información dentro del proceso. Este instrumento fue diseñado con base en las directrices establecidas por la norma, las cuales señalan que los controles de seguridad deben analizarse de manera objetiva mediante evidencias documentales, operativas y técnicas (UNE, 2023).

Como se observa en la tabla 3 la evaluación se realizó mediante la asignación de puntajes, los cuales permitieron clasificar el nivel de cumplimiento de los controles analizados:

- 0 = No cumple
- 1 = Cumple parcialmente
- 2 = Cumple

Tabla 3.

Resultado de cumplimiento por bloque temático

Escala de cumplimiento
0 = No implementado → No hay evidencia.
1 = Parcialmente implementado → Existe, pero no está completo o actualizado.
2 = Totalmente implementado → Existe, está documentado y se aplica de forma regular.

Nota. Elaboración propia

Los resultados se reflejan en la tabla 4, en la cual se visualizan los controles seleccionados del Anexo A de la norma ISO/IEC 27001:2022 que se utilizaron como guía para evidenciar el nivel de cumplimiento actual de la organización. Dicho nivel se determinó mediante una escala de cumplimiento aplicada a partir de una pregunta

clave de verificación para cada control. La elaboración de la tabla se apoyó en entrevistas realizadas al personal del área de facturación, con el propósito de obtener información más precisa y confiable sobre la aplicación de controles.

Tabla 4.

Resultados detallados de controles aplicables.

Nº Control	Nombre del control	Pregunta de verificación	Evidencia	Escala de cumplimiento	Observaciones
A.5.1	Políticas de seguridad de la información	¿Existe una política aprobada y comunicada al personal?	Documento de política, firma de recibo de empleados	1	Se cuenta con un documento de políticas de seguridad de la información general más no una enfocada al área de facturación
A.5.7	Seguridad en relaciones con proveedores	¿Los contratos con proveedores incluyen cláusulas de seguridad de la información?	Contratos	1	No se explica a detalle la seguridad de la información
A.7.5	Seguridad física	¿El área de facturación cuenta con acceso restringido?	Fotografías, registros de accesos, manual de seguridad	2	Cada empleado cuenta con una credencial de acceso que se utiliza para ingresar al área que le corresponde y a las oficinas
A.8.12	Protección de datos	¿Los respaldos están cifrados y almacenados en un sitio seguro?	Evidencia de cifrado, bitácora de respaldos	1	Se alamcenan en plataformas y en la nube, pero hubo un incidente en el año 2022 donde todo se perdió
A.9.4	Gestión de acceso	¿Cada usuario tiene credenciales únicas y roles definidos en el sistema de facturación?	Políticas de usuarios, bitácora de accesos	2	Se cuentan con accesos y usuarios para cada empleado con distintos permisos según su puesto
A.16.1	Gestión de incidentes	¿Se registran y documentan los incidentes de seguridad?	Reportes de incidentes, actas de seguimiento	2	Cada que hay un error en sistemas se levanta un ticket al que se le da seguimiento y queda registrado en una plataforma

Nota. Elaboración propia

En la tabla 5 se presentan los resultados agrupados por bloques temáticos: Políticas y organización, Control de accesos y Seguridad física y tecnológica. En la tabla se calculó el porcentaje de cumplimiento de la empresa para cada categoría, lo que

permitió identificar el nivel de cumplimiento alcanzado y los riesgos asociados en función de los porcentajes obtenidos.

Tabla 5.

Tabla de resultados por bloque

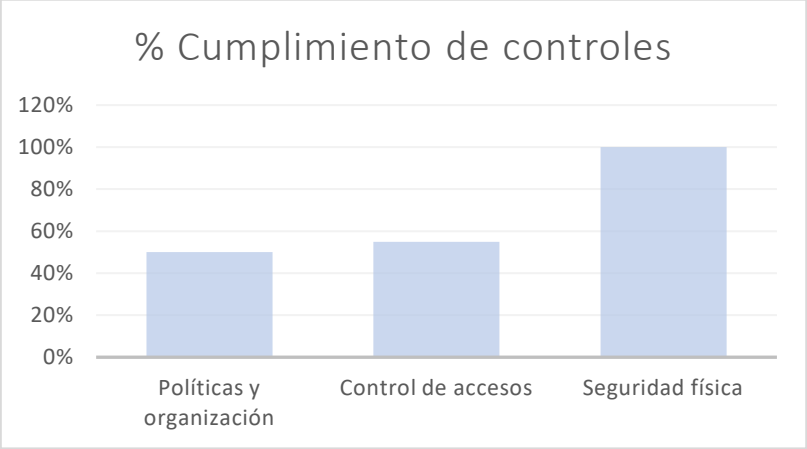
Dominio ISO 27001	% Cumplimiento	Riesgo detectado	Recomendación	Razón principal
Políticas y organización	50%	Existe documento, sin embargo no se actualiza periódicamente ni hay uno para facturación	Actualizar cada 12 meses y emplear políticas enfocadas al área de facturación	Marco de referencia para todo el SGSI
Control de accesos	55%	Los contratos no explican con detalle cláusulas de seguridad de la información. Riesgo de pérdida de información	Actualizar contratos e incluir cláusulas de confidencialidad y protección de datos conforme ISO 27001. Mantener controles de acceso físico y reforzar con auditorías periódicas. Implementar respaldos cifrados automáticos, con redundancia (local + nube confiable), y pruebas de recuperación periódicas.	Importante pero menos crítico frente a accesos digitales
Seguridad física	100%	Ninguno	Mantener la práctica, reforzar revisiones periódicas para asegurar que las cuentas inactivas se den de baja oportunamente. Continuar con tickets; analizar tendencias de incidentes para mejoras preventivas.	Riesgo más crítico en facturación (datos digitales sensibles)

Nota. Elaboración propia

En la figura 5 se presenta el gráfico correspondiente a los resultados del nivel de cumplimiento de los controles por categoría. Los resultados muestran que la categoría de Políticas y organización alcanzó un 50% de cumplimiento, mientras que el Control de accesos un 55%. Por su parte el de Seguridad física presentó un 100% de cumplimiento, lo que indica que los controles asociados a esa categoría se encuentran bien implementados en el área evaluada.

Figura 5.

Gráfica de porcentaje de cumplimiento de controles



Nota. Elaboración propia

Se evidenciaron que algunos controles presentan un nivel de cumplimiento satisfactorio, especialmente aquellos relacionados con el acceso al área física como se observa en el gráfico de la figura 5, la asignación de credenciales individuales y la gestión de incidentes mediante plataformas de registro. Estas prácticas coinciden con las recomendaciones de Pozo et al., (2025), quienes destacan que la adecuada asignación de roles y la trazabilidad de incidentes fortalecen la integridad y disponibilidad de los activos informáticos.

No obstante, el análisis reveló brechas importantes en controles relacionados con la gestión de proveedores, la protección de respaldos y la documentación formal de procedimientos. Por ejemplo, se identificó que los contratos de servicios no incorporan cláusulas específicas de seguridad de la información, lo cual representa un riesgo potencial si se consideran las exigencias normativas actuales. El propio estándar ISO/IEC 27001 señala que la relación con terceros debe incluir acuerdos formales que garanticen la protección adecuada de los datos compartidos o procesados (UNE, 2023).

Asimismo, se detectó un nivel de cumplimiento parcial en los controles de respaldo de información, ya que, aunque existen mecanismos de almacenamiento en la nube, la

empresa ha enfrentado incidentes previos de pérdida total de datos. Este tipo de situaciones se encuentra documentado en la literatura académica, donde se explica que los fallos en los respaldos constituyen una de las vulnerabilidades más críticas para las organizaciones, especialmente en áreas donde se gestionan datos fiscales y operativos (De la Cruz et al., 2023).

En términos generales, los resultados del check list permitieron identificar tres tendencias principales:

1. Controles plenamente implementados, especialmente aquellos relacionados con acceso físico y registro de incidentes.
2. Controles parcialmente implementados, como la protección de respaldos y el manejo de datos sensibles.
3. Controles no implementados o carentes de formalización, particularmente en relación con proveedores, políticas específicas y acuerdos de confidencialidad.

Este diagnóstico constituye la base para los apartados posteriores, donde se analizan los riesgos detectados y se proponen medidas correctivas orientadas a reducir vulnerabilidades, mejorar la trazabilidad y fortalecer la protección de los activos informativos conforme a las mejores prácticas internacionales.

7.1.3 Mapa de procesos del área de facturación.

A partir de la observación directa y las entrevistas, se elaboró el mapa general del proceso de facturación, donde se identificaron las actividades desde la recepción de documentos hasta la emisión y envío de los CFDI.

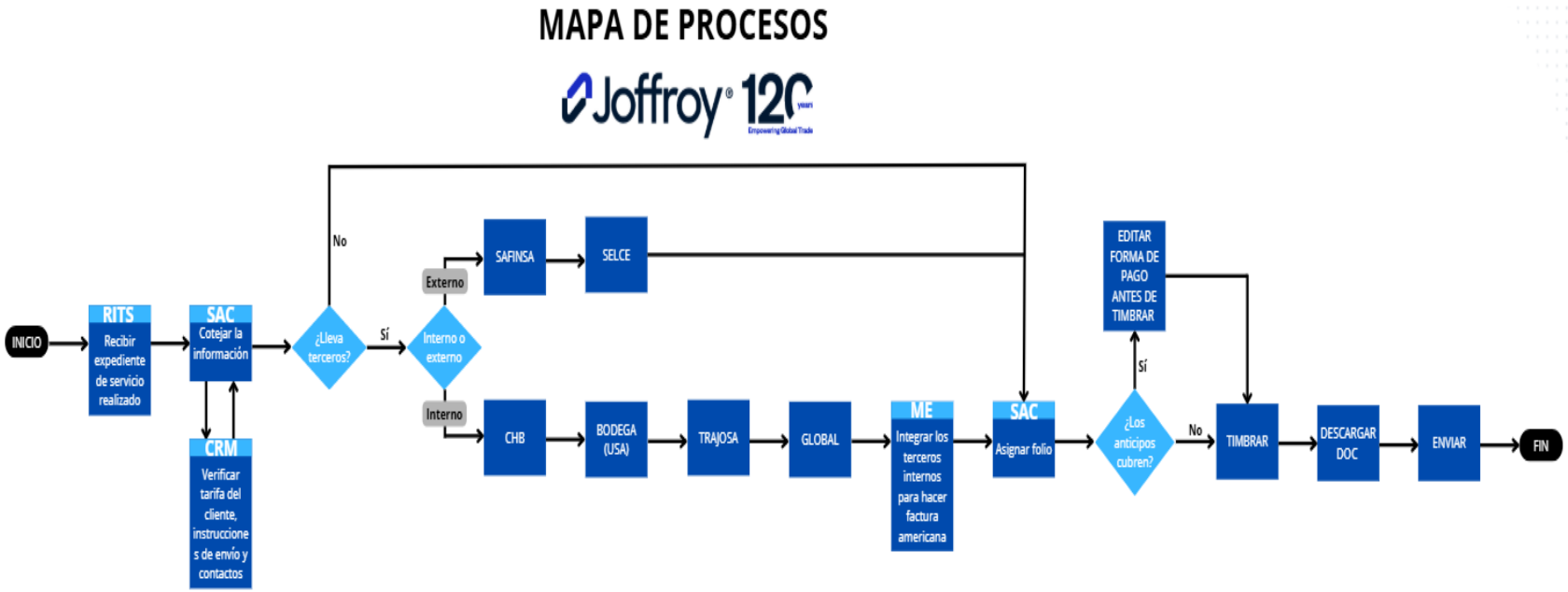
El mapa de procesos del área de facturación permitió visualizar de manera clara cómo fluye la información dentro del departamento y en qué puntos se concentran los activos más sensibles. De acuerdo con la ISO/IEC 27001, comprender la interacción entre los procesos y los activos es un paso esencial para identificar riesgos y asignar controles adecuados (UNE, 2023). Este análisis facilita reconocer cuáles actividades presentan

mayor exposición y qué sistemas o plataformas requieren medidas de protección específicas.

La Figura 6 muestra el mapa de procesos del área de facturación, donde se identifican las etapas clave del flujo operativo: recepción de datos, validación de documentos, emisión de CFDI, control de pedimentos y envío de información al cliente. Este esquema permitió analizar de forma visual los puntos donde se concentra información fiscal, operativa y aduanal, así como los momentos en los que intervienen distintos sistemas tecnológicos.

Figura 6.

Mapa de procesos del área de facturación.



Nota. Elaboración propia con información de la empresa

El análisis del mapa evidenció que las etapas con mayor manejo de información sensible son la recepción de datos, la emisión de facturas CFDI y la integración de pedimentos, ya que en estos pasos se procesan claves fiscales, documentos aduanales, RFC, datos de mercancía y registros de operaciones. Como señalan Pozo, et al., (2025), identificar estos puntos críticos permite definir controles específicos de acceso, resguardo y respaldo de la información para minimizar el riesgo de alteraciones o pérdidas.

7.1.4 Concentrado de información sensible utilizada en el proceso.

Se clasificó la información sensible manejada por plataforma tecnológica, lo cual permitió identificar qué sistemas concentran mayor volumen y datos críticos.

La Tabla 6 presenta el concentrado de la información sensible identificada durante el análisis de procesos, clasificándola según la plataforma o sistema en el que se almacena o procesa. Esta clasificación es fundamental para evaluar la superficie de exposición digital y determinar qué sistemas requieren controles más estrictos o mayor monitoreo (De la Cruz et al., 2023).

Tabla 6.

Concentrado de información sensible por plataforma

Plataforma	Uso	Información sensible que maneja
RITS	Base de datos de expediente	• Pedimento • Facturas comerciales • Cuentas americanas • Coves • Valor de la mercancía
SAC	Plataforma de concentrado de impuestos, honorarios y demás cobros que se realizan al cliente	• Anticipos • Estados de cuenta • Pagos aplicados • Datos bancarios
CRM	Verificación de tarifas e instrucciones de envío	• Dirección del cliente • Número de celular • Alianzas • Tarifas • Datos fiscales • INE • Corresponsalía

ME	Elaboración de factura americana	• Descripción de mercancía • Información de cheques • tax ID • Ubicación de traslado de mercancías

Nota. Elaboración propia.

La tabla revela que los sistemas más críticos son los generados por el sistema ERP contable, la plataforma de control aduanal y los repositorios de respaldo en la nube, debido a la cantidad y sensibilidad de los datos que manejan. Entre la información más relevante se encuentran CFDI, pedimentos, bases de clientes, datos fiscales y documentos digitalizados. De acuerdo con la UNE-EN ISO/IEC 27001:2023, estos activos deben contar con controles formales de acceso, cifrado, respaldo y seguimiento de incidentes (UNE, 2023), por lo que su supervisión se considera prioritaria.

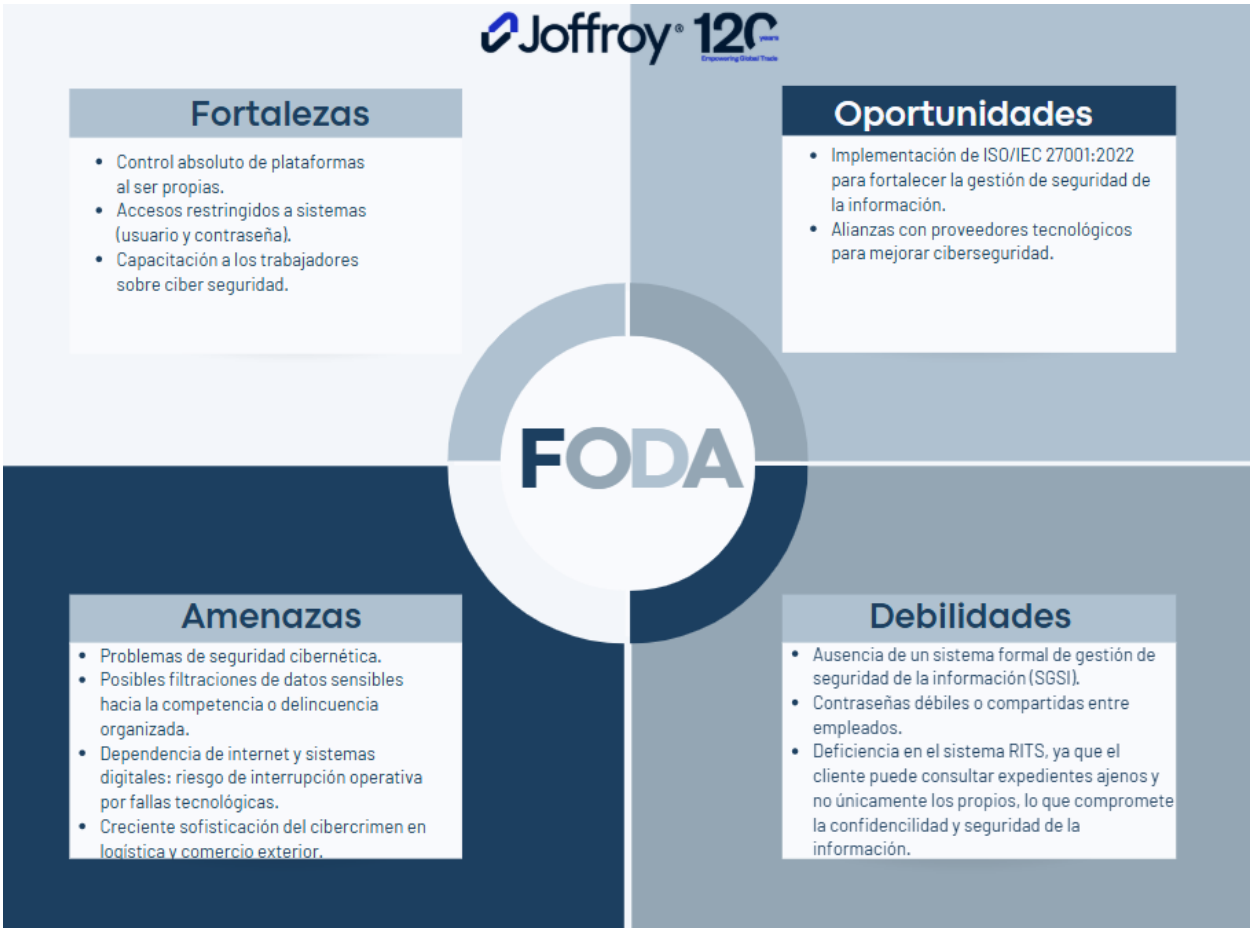
7.1.5 Análisis FODA del proceso de facturación.

La Figura 7 muestra el análisis FODA con el fin de complementar los resultados del diagnóstico, integrando tanto factores internos como externos que influyen en la seguridad de la información del área de facturación. Esta herramienta permite reconocer fortalezas que pueden aprovecharse, debilidades que deben atenderse, oportunidades provenientes del entorno tecnológico y amenazas que podrían comprometer la integridad de los datos (Pozo et al., 2025).

La norma ISO/IEC 27001 enfatiza que el análisis del contexto interno y externo es un paso esencial para la planificación del SGSI, por lo que el FODA contribuye directamente a comprender las condiciones que afectan el tratamiento de riesgos y la toma de decisiones (UNE, 2023).

Figura 7.

FODA de la empresa



Nota. Elaboración propia.

Entre las fortalezas, se identificó personal experimentado y un proceso operativo bien definido.

Las debilidades principales se relacionan con la falta de procedimientos, capacitación y controles tecnológicos avanzados.

En oportunidades, se identificaron tecnologías disponibles que la empresa aún no ha adoptado.

Entre las amenazas, destaca el riesgo constante de ataques cibernéticos y el uso de datos sensibles en comercio exterior.

7.1.6 Matriz de riesgos y tratamiento.

Se generó una matriz de riesgos considerando probabilidad, impacto y nivel de riesgo resultante. Los riesgos críticos fueron priorizados para el diseño de medidas preventivas y correctivas.

En la tabla 7 se aprecia la simbología y ponderación del sistema de semáforo que se utilizó para los criterios de la matriz de riesgos presentada en la tabla 8. Los criterios utilizados para la medición de probabilidad, impacto y nivel de riesgo (probabilidad * impacto) son los siguientes:

Probabilidad	Impacto	Resultado	Nivel de riesgo
1= Baja	1= Bajo	1–2	Bajo
2= Media	2= Medio	3–4	Medio
3= Alta	3= Alto	6–9	Alto

Tabla 7.

Simbología semáforo

Simbología semáforo		
Nivel de riesgo	**Descripción**	**Color**
Bajo (1-2)	Riesgo menor requiere monitoreo	Verde
Medio (3-4)	Riesgo moderado requiere seguimiento	Amarillo
Alto (6-9)	Riesgo significativo requiere atención prioritaria	Rojo

Nota. Elaboración propia

Tabla 8.

Matriz de riesgos y tratamientos (Parte 1)

MATRIZ DE RIESGOS Y TRATAMIENTO											
ACTIVO O PROCESO	AMENAZA	VULNERABILIDAD	VALORACIÓN DE PROBABILIDAD DE IMPACTO (1-3)	IMPACTO (1-3)	NIVEL DE RIESGO	SEMÁFORO	TRATAMIENTO SUGERIDO (Reducir/Evitar/Transferir /Aceptar)	CONTROLES ISO ASOCIADOS	RESPONSABLE	TIEMPO ESTIMADO DE IMPLEMENTACIÓN	RECOMENDACIÓN
Equipos de computo	Virus	Ausencia o mala configuración de antivirus	1	2	2	Bajo	Reducir	A.8.12	Sistemas/TI	2 semanas	Implementar y actualizar antivirus, parches, y monitoreo de sistemas
Sistemas de facturación	ccesos no autorizado	Contraseñas débiles	3	3	9	Alto	Reducir	A.9.4	Sistemas/TI	1 mes	Contar con políticas de contraseñas robustas, autentificación y limitación de permisos
Información de clientes/proveedores	Fuga de información	Accesos limitados	2	2	4	Medio	Reducir	A.5.7	Sistemas/TI	1 mes	Implementra controles de acceso y cifrado
Base de datos	erdida de informació	Configuraciones incorrectas, falta de controles de accesos, dependencia de un solo medio de almacenamiento	2	3	6	Alto	Reducir	A.8.12	Sistemas/TI	1-2 meses	Realizar copias de seguridad periodicamente, monitoreo de base de datos para detectar modificaciones no autorizadas y contar con más de un medio de almacenamiento
Documentación impresa	Mal uso, extravio o acceso no autorizado	Almacenamiento inseguro sin acceso limitado	2	1	2	Bajo	Reducir	A.7.5	Área responsable del documento	2-3 meses	Plantar controles de acceso físicos y resguardo seguro de la documentación, además de capacitación
Usuarios internos	Uso indebido	Falta de controles de acceso y restricción de permisos y licencias	3	2	6	Alto	Evitar	A.9.4 A.5.1	Sistemas/TI	2 semanas	Emplear políticas de uso de usuarios, acceos y contraseñas, restringir y delimitar permisos de aaccesos
Portal de clientes	formación ajena visib	Los clientes pueden ver en plataforma información de otros clientes porque no hay acceso restringido	3	3	9	Alto	Eliminar	A.5.7	Sistemas/TI	2 semanas	Implementar controles de ID por cliente para que solo puedan ver su información en plataforma
Correos electrónicos	Phishing	Falta de filtros	2	2	4	Medio	Reducir	A.8.12 A.16.1	Sistemas/TI	6 semanas	Implementar un sistema antiphishing, autentificación avanzada, capacitación a los usuarios sobre el pishing, políticas de uso del correo, procesos de reportes de correos sospechosos
Servidores y servicios en la nube	Malware	Software o sistemas desactualizados, configuraciones incorrectas, credenciales débiles, falta de controles y parches de seguridad	1	3	3	Medio	Reducir	A.8.12	Sistemas/TI	3-4 semanas	Implementar antimalware, actualizaciones automáticas de los sistemas, respaldos periodicos y pruebas de restauración

Nota. Elaboración propia

Tabla 9.

Matriz de riesgos y tratamientos (Parte 2)

Conexiones de internet	Hackeo, robo de información, insertar virus	Ausencia de firewall	1	3	3	Medio	Reducir	A.8.12	Sistemas/TI	2 semanas	Implementación e VLAN
Uso de USB	Robo o travío	Descuido, falta de políticas de uso, no hay un registro de inventario, falta de lugares de resguardo	1	3	3	Medio	Eliminar	A.8.12	Sistemas/TI	1 semana	Eliminar el uso de USB y bloquear puertos en los equipos de cómputo
Personal	Error humano	Falta de capacitación	3	2	6	Alto	Reducir	A.5.1	Recursos humanos Facturación	2 semanas	Crear un programa de capacitacion periodico en temas de seguridad y ciberataques, crear políticas de seguridad de la información en el área
Infraestructura TI	Falla del sistema	Falta de mantemineto preventivo, infraestructura vulnerable	1	3	3	Medio	Reducir	A.8.12	Sistemas/TI	5-6 semanas	Mantenimiento preventivo periodico, soporte técnico avanzado, servicios de conectividad segura
Facturas XML	Manipulación de datos	Archivos XML almacenados sin cifrado ni controles de seguridad, falta de validación automática	1	3	3	Medio	Reducir	A.8.12 A.9.4	Sistemas/TI Facturación	4 semanas	Limitar el acceso a sistema y archivos XML a personal autorizado, modificación al sistema para detectar accesos o modificación no autorizadas, concientización de la validación y uso correcto de los XML
Respaldo	Pérdida de datos	No se generan respaldos automáticos, equipos de almacenamiento sin actualizar, ausencia de encriptación, fallas en software	2	3	6	Alto	Reducir	A.8.12	Sistemas/TI	2 semanas	Pruebas de restauración
Impresoras	Exposición de información	Documentos olvidados	2	1	2	Bajo	Evitar	A.7.5 A.8.12	Calidad	1 semana	Reubicar impresoras que manejan información sensible a áreas controladas, reglas del manejo de información, colocar avisos y recordatorios, destruir documentos no reclamados
Equipos móviles	Robo o pérdida	Sin cifrado	1	2	2	Bajo	Reducir	A.7.5 A.8.12	Sistemas/TI	1 semana	Implementar cifrado en los equipos, activar bloqueo automático en caso de robo, registro de inventario de equipos periodicamente, un lugar de resguardo
Correo de Facturación	Suplantación	Ausencia de mecanismos de verificación y autentificación	1	3	3	Medio	Reducir	A.8.12	Sistemas/TI	1 semana	Incorporar cifrado avanzado de correo
Tokens bancarios	Robo o extravío	Descuidos por falta de resguardo	1	3	3	Medio	Evitar	A.8.12	Tesorería	1 semana	Tener un lugar especifico para resguardarlo bajo llave y clave

Nota. Elaboración propia

Un hallazgo fue la falta de controles específicos para la eliminación segura de documentos, lo cual incrementa riesgos legales y operativos. De manera general, se concluyó que:

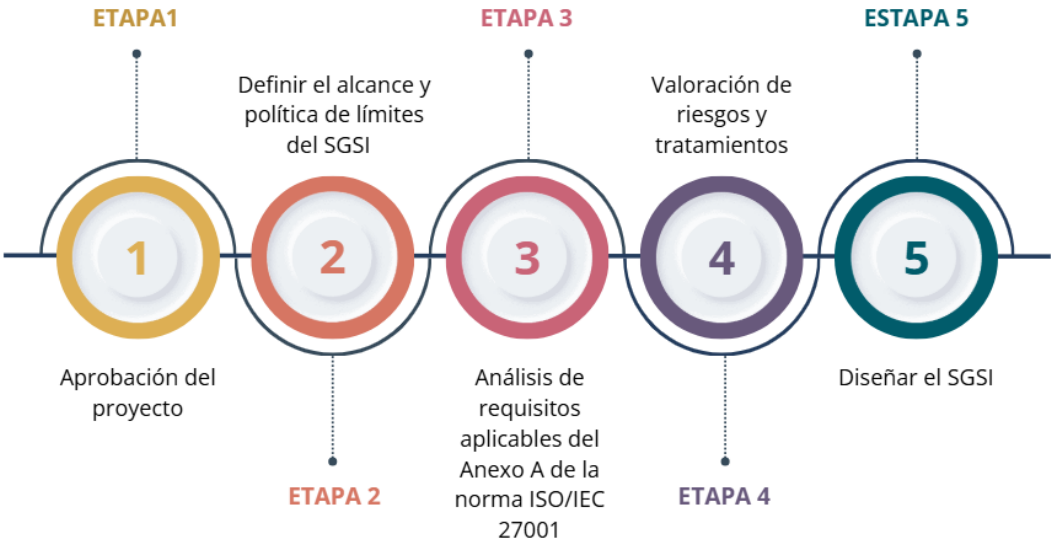
- El nivel de madurez en seguridad de la información es aún básico.
- Existen esfuerzos aislados, pero no un enfoque sistemático.
- El proceso depende de múltiples plataformas sin criterios homogéneos de seguridad.
- Los incidentes documentados no se gestionan como incidentes de seguridad.
- La empresa tiene disposición para implementar mejoras.

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

El proceso de elaboración del Sistema de Seguridad de la Información se dividió en 5 etapas como se muestra en la figura 8, en la etapa 1 se planteó la idea en la organización explicando las ventajas que tendría la ejecución del proyecto para que este sea aprobado, en la etapa 2 se definió el alcance y las políticas internas con las que contará el SGSI para delimitar y centrar el objetivo esperado, luego, en la etapa 3 se realizó una investigación sobre los controles de Anexo A de la norma ISO/IEC 27001:2022 que sean aplicables al proyecto y al área en cuestión, posteriormente en la etapa 4 con base en las actividades antes mencionadas se seleccionaron los riesgos que el área de facturación podría enfrentar en cuanto a la seguridad de la información para establecer una valoración de riesgos y tratamientos y finalmente en la etapa 5 se recopiló toda la información de cada una de las actividades para hacer una estructura y diseño para el Sistema de Gestión de Seguridad de la información.

Figura 8.

Etapas de la elaboración del SGSI



Nota. Elaboración propia

Los puntos que integran el Sistema de Gestión de Seguridad de la Información (SGSI) planteados en la figura 8 se desarrollan a continuación:

1. **Contexto de la Organización**

El Sistema de Gestión de Seguridad de la Información (SGSI) se implementa parcialmente en el área de facturación de una agencia aduanal. Dicha área es responsable del manejo de la información fiscal, operativa y financiera, incluyendo información de alta sensibilidad como Comprobantes Fiscales Digitales por Internet (CFDI), datos importantes de los clientes, credenciales de acceso a plataformas y documentación relacionadas con las operaciones aduanales.

Se llevó a cabo un diagnóstico, el cual, reflejó la situación actual del área de facturación respecto al estado real de los procesos, el manejo y protección de los datos y el nivel de cumplimiento en materia de seguridad de la información de acuerdo con el anexo A de la norma ISO/IEC 27001.

Dicho diagnostico se llevó a cabo por medio de entrevistas al personal de las áreas involucradas, revisión documental, observación directa y demás factores que permitieron analizar el contexto interno y externo de la entidad.

El contexto interno de la organización toma en cuenta la estructura organizacional, los procesos involucrados en el área de facturación, la tecnología de la información (TI), el personal involucrado y sus responsabilidades y el tratamiento de la información. Por otro lado, el contexto externo contempla los requisitos legales y normativos aplicables de acuerdo con la norma seleccionada, la ley aduanera, riesgos asociados al manejo de datos sensibles y ciberataques, imagen de la empresa ante los clientes y regulaciones del Servicio de Administración Tributaria (SAT).

Los resultados obtenidos fueron:

- Nivel de madurez medio de la seguridad de la información
- Falta de revisiones periódicas
- Falta de respaldos y cifrados
- Falta de protocolos ante incidentes
- Se observó que el personal tiene claridad sobre las actividades operativas, pero no existen procedimientos formalizados ni documentados.
- Se detectó una falta de capacitación formal en seguridad de la información.
- Se evidenció que no todos los colaboradores conocen las políticas institucionales relacionadas con la protección de datos.

El contexto de la organización fue establecido conforme a la cláusula 4 de la norma ISO/IEC 27001:2022, la cual dispone de explicar el propósito, alcance y la situación actual de la organización.

2. Liderazgo y Compromiso.

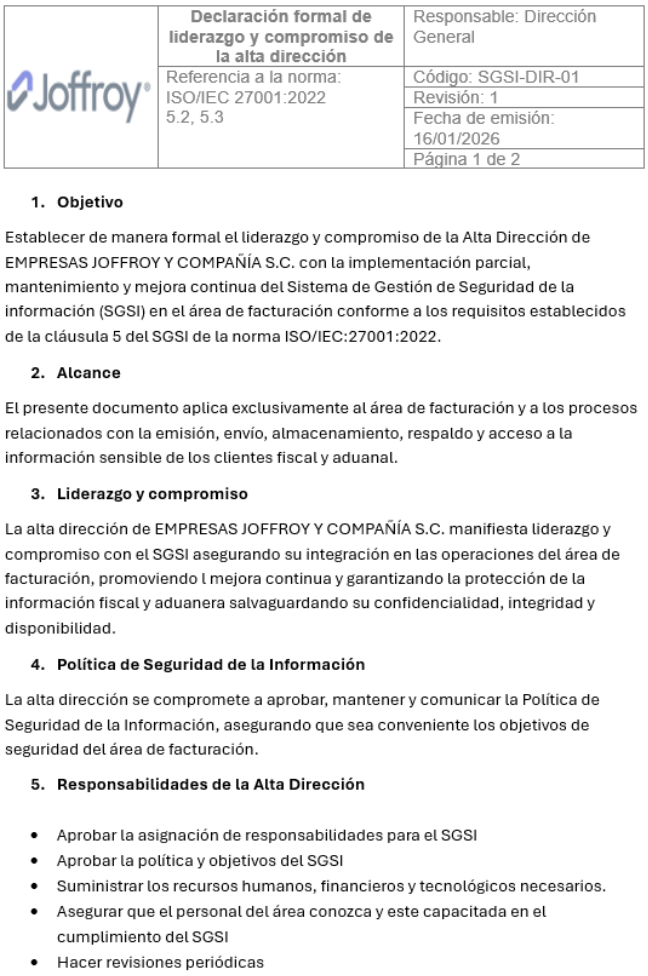
La alta dirección manifiesta liderazgo y compromiso con la seguridad de la información a través de la aceptación del SGSI y la gestión de recursos necesarios para su ejecución y mantenimiento. Por su parte, promueve la cultura organizacional

enfocada en la protección y aseguración de los datos, certificando que el personal comprenda la importancia de seguir y cumplir con las políticas internas, procedimientos y controles establecidos.

Para el respaldo del liderazgo y compromiso que asume la alta dirección y el cumplimiento de la cláusula 5 de liderazgo de la norma, se creó un documento en el que se describe el objetivo, alcance, política, responsabilidades y aprobación del SGSI tal como lo indican los controles 5.1 liderazgo y compromiso, 5.2 Política de seguridad de la información y 5.3 Roles y responsabilidades de seguridad de la información detallado en las figuras 9 y 10.

Figura 9.

Declaración formal de liderazgo y compromiso de la alta dirección (página 1).



Joffroy	**Declaración formal de liderazgo y compromiso de la alta dirección**	Responsable: Dirección General
	Referencia a la norma: ISO/IEC 27001:2022 5.2, 5.3	Código: SGSI-DIR-01
		Revisión: 1
		Fecha de emisión: 16/01/2026
		Página 1 de 2

1. **Objetivo**

Establecer de manera formal el liderazgo y compromiso de la Alta Dirección de EMPRESAS JOFFROY Y COMPAÑÍA S.C. con la implementación parcial, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la información (SGSI) en el área de facturación conforme a los requisitos establecidos de la cláusula 5 del SGSI de la norma ISO/IEC:27001:2022.

2. **Alcance**

El presente documento aplica exclusivamente al área de facturación y a los procesos relacionados con la emisión, envío, almacenamiento, respaldo y acceso a la información sensible de los clientes fiscal y aduanal.

3. **Liderazgo y compromiso**

La alta dirección de EMPRESAS JOFFROY Y COMPAÑÍA S.C. manifiesta liderazgo y compromiso con el SGSI asegurando su integración en las operaciones del área de facturación, promoviendo l mejora continua y garantizando la protección de la información fiscal y aduanera salvaguardando su confidencialidad, integridad y disponibilidad.

4. **Política de Seguridad de la Información**

La alta dirección se compromete a aprobar, mantener y comunicar la Política de Seguridad de la Información, asegurando que sea conveniente los objetivos de seguridad del área de facturación.

5. **Responsabilidades de la Alta Dirección**

- Aprobar la asignación de responsabilidades para el SGSI
- Aprobar la política y objetivos del SGSI
- Suministrar los recursos humanos, financieros y tecnológicos necesarios.
- Asegurar que el personal del área conozca y este capacitada en el cumplimiento del SGSI
- Hacer revisiones periódicas

Nota. Elaboración propia

Figura 10.

Declaración formal de liderazgo y compromiso de la alta dirección (Página 2)

Joffroy	**Declaración formal de liderazgo y compromiso de la alta dirección**	Responsable: Dirección General
	Referencia a la norma: ISO/IEC 27001:2022 5.2, 5.3	Código: SGSI-DIR-01
		Revisión: 1
		Fecha de emisión: 16/01/2026
		Página 2 de 2

- Promover una cultura organizacional orientada a la seguridad de la información

6. Vigencia y revisión

Esta declaración entra en vigor a partir de su aprobación y será revisada anualmente o cuando se presente algún cambio significativo en el SGSI o las operaciones del área de facturación.

7. Aprobación

Mediante la firma del presente documento, la Alta Dirección avala formalmente su liderazgo y compromiso con el Sistema de Gestión de Seguridad de la Información (SGSI).

Nombre y firma del Director General

Nombre y firma del responsable del SGSI

16/01/2026

Fecha de aprobación

Nota. Elaboración propia

3. Objetivos de SI (Seguridad de la Información).

Los objetivos de Seguridad de la Información (SI) se establecieron tomando como base el contexto de la organización y los riesgos identificados en el área de facturación, teniendo como fin salvaguardar la información y asegurar la continuidad de las operaciones.

Los principales objetivos de seguridad de la información son:

- Proteger la confidencialidad de la información fiscal y aduanal
- Asegurar la integridad de los datos en el proceso de facturación
- Garantizar la disponibilidad de la información y los sistemas ERP involucrados en las operaciones
- Disminuir incidentes de seguridad de la información
- Cumplir con los requerimientos legales, fiscales y normativos

Una vez definidos los objetivos que busca el Sistema de Gestión se da cumplimiento a la cláusula 6.2 objetivos de seguridad de la información impuesto por la norma ISO/IEC 27001:2022.

4. Política de SI (Seguridad de la Información).

Con base en el análisis del contexto interno y externo de la organización, el diagnóstico inicial y la evaluación de riesgos previamente realizada, se establece la presente política de seguridad de la información, tomando en cuenta las necesidades del área de facturación de la agencia aduanal, tipo de servicio que brinda y su entorno con base en la cláusula 5.2 política de seguridad de la información, estas políticas se respaldan bajo el control A.5.1 del Anexo A de la norma ISO/IEC 27001:2022.

La empresa reconoce la importancia de la información como uno de sus principales activos en la prestación de servicios, y la toma de decisiones, es por lo que se establecen las medidas necesarias para la seguridad de la información del área de facturación, con el objeto de mitigar riesgos que atenten contra la triada de la información (confidencialidad, integridad y disponibilidad).

La alta dirección se compromete a proporcionar los recursos humanos, tecnológicos, financieros y logísticos necesarios para salvaguardar la información en la prestación de sus servicios y el cumplimiento del SGSI.

La política de seguridad de la información debe ser comunicada a todo el personal de las áreas involucradas con el propósito de fortalecer la cultura organizacional orientada a la protección y seguridad de los datos.

4.1 Objetivos de la política de seguridad de la información.

Para el cumplimiento del SGSI se establecen los siguientes objetivos de la política de seguridad de la información:

- Mitigar riesgos que pongan en peligro la seguridad de la información del área de facturación
- Fomentar una cultura organizacional orientada a la seguridad de la información
- Asegurar que los sistemas utilizados en el manejo de datos se encuentren siempre disponibles
- Garantizar que la información se mantiene integra sin manipulaciones
- Certificar que la información será estrictamente confidencial sin divulgaciones no autorizadas.

4.2 Políticas específicas de la seguridad de la información.

Con el objetivo de reducir posibles causadas de riesgos o vulnerabilidades se plantean las siguientes políticas internas.

4.2.1 Seguridad física y del entorno.

Se implementan controles de seguridad en acceso físico a áreas sensibles, orientadas a la protección de equipos y prevenir daños o accesos no autorizados que pongan en riesgo la seguridad de la información.

- **Acceso controlado a los activos de información:** Se restringe el acceso a servidores y cuartos de sistemas solo a personal autorizado mediante controles físicos.
- **Protección ambiental de los sistemas de información:** Se dispone de equipos de control de temperatura y humedad para asegurar el correcto funcionamiento de los equipos.
- **Mecanismos seguros de accesos a los sistemas:** Accesos a los servidores por medio de autentificación segura con claves de seguridad para evitar accesos no autorizados.
- **Prevención de incidentes físicos:** La organización cuenta con detección y control de incendios a través de detectores de humo y extintores que permiten reducir el impacto de este tipo de eventos que pongan en riesgo la disponibilidad de la información

4.2.2 Seguridad contra virus y malware.

La empresa aplica medidas preventivas para tener un control de los sistemas utilizados para evitar virus, malware y demás ataques informáticos, entre estas medidas se encuentran:

- Des-habilitación de puertos USB para reducir riesgos
- Uso de la red de internet exclusivo para objetivos laborales
- Filtros en correos electrónicos para evitar malware y spam
- Restricción de sitios web que no sean con fines laborales
- Las instalaciones de programas a los equipos de la empresa se encentran restringidas y solo podrá realizarse por personal autorizado del área de Tecnología
- Las instalaciones de antivirus y antimalware deberán actualizarse mensualmente y monitorearse diariamente.
- Se prohíbe la apertura de enlaces o archivos adjuntos en correos electrónicos de remitentes desconocidos, sospechosos o no verificados.
- Toda aquella sospecha de virus o malware debe ser reportada inmediatamente al área de tecnología.

- La empresa fomenta la capacitación periódica al personal en temas relacionados con prevención de virus y malware.

4.2.3 Seguridad y control de usuarios.

Con el objeto de evitar manipulación de datos, uso indebido de sistemas e información, divulgación y accesos no autorizados se manifiestan las siguientes medidas.

- Restricción de información y sistemas solo a personal autorizado
- Implementación de cifrado y contraseñas seguras que se actualizan cada mes
- Los accesos de información se asignad de acuerdo con las responsabilidades de cada puesto, siguiendo el principio de mínimo privilegio
- Todos los usuarios deben contar con credenciales únicas e intransferibles para sus accesos
- Se prohíbe compartir credenciales de acceso
- En caso de cambio de puesto o baja, los accesos del colaborador deberán ser eliminados de manera inmediata
- Los sistemas de información deberán ser utilizados exclusivamente para fines laborales

4.2.4 Cultura organizacional y concienciación.

- El personal deberá ser capacitado en temas de seguridad de la información, eso de accesos, contraseñas, buenas prácticas de seguridad, prevención de virus y malware y correcto manejo de la información mínimo 2 veces al año
- Se debe capacitar e inducir en el tema de seguridad de la información al personal de nuevo ingreso antes de acceder a los sistemas de información
- Cada colaborador es responsable de proteger la información que involucran sus procesos apegándose a las políticas y buenas prácticas de la información, además de reportar cualquier incidente

- La empresa debe evaluar el nivel de concientización del personal en materia de seguridad de la información de manera periódica para identificar áreas de oportunidad y reforzar las debilidades.

4.2.5 Medios de información y respaldos.

- La empresa deberá implementar respaldos periódicos de la información
- La información deberá respaldarse y almacenarse en lugares seguros y protegidos contra accesos no autorizados
- Se debe contar con procesos de recuperación de la información respaldada para no afectar con las operaciones diarias del área
- Los respaldos deberán estar cifrados con accesos solo a personal autorizado

5. Roles, Responsabilidades y Competencias.

Con el propósito de definir y estructurar organizadamente las funciones dentro del Sistema de Gestión de Seguridad de la Información, bajo la cláusula 5.3 roles, responsabilidad y autoridades en la organización, con aplicación de los controles del Anexo A A.5.2 Roles y responsabilidades de seguridad de la información, A.5.3 Segregación de funciones y A.5.4 Responsabilidades de la dirección, se realizó una tabla de roles, responsabilidades y competencias, como se muestra en la tabla 9, esta herramienta permite asegurar el correcto funcionamiento de las actividades en el sistema de gestión, delegando responsabilidades y asegurando que se ejecuten por personas capacitadas y autorizadas para cada puesto, además de un documento formal de declaración de compromiso y aceptación de responsabilidades para reforzar de manera legal el cumplimiento por lo antes previsto, véase en la figura 11.

Cada rol dentro del marco del sistema se encuentra alienado a los procesos establecidos, lo que permite una mejor gestión de este, facilitando el correcto cumplimiento de las políticas, controles y procedimientos de seguridad de la información, siguiendo el lineamiento establecido por la norma ISO/IEC 27001:2022.

El tener una estructura sólida y definida de roles y responsabilidades disminuye la probabilidad de riesgos relacionados con controles no autorizados, divulgación y/o manipulación de información y posibles errores humanos al definir quién es el responsable de cada actividad dentro del SGSI. La tabla 10 facilita la integración del Sistema de Gestión en el área ya que proporciona una estructura organizacional clara alineada a los requisitos propuestos por la norma, promueve la participación de la alta dirección, facturación, recursos humanos y sistemas, formando un equipo integral que fortalece y asegura la seguridad de la información.

Tabla 10.

Roles, responsabilidades y competencias en el SGSI

Rol	Función en el SGSI	Responsabilidades en seguridad de la información (SI)	Competencias requeridas
Alta dirección	Liderar y apoyar	- Aprobar la política de seguridad de la información - Asignación de recursos para el SGSI - Supervisar el funcionamiento del SGSI - Promover una cultura organizacional orientada a la seguridad de la información	- Conocimientos sobre negocios - Comprensión sobre riesgos de la SI - Capacidad de toma de decisiones - Liderazgo
Responsable del SGSI/Sistemas TI	Gestionar el SGSI	- Diseñas el SGSI - Administrar los recursos - Ejecutar e implementar el SGSI - Coordinar asignaciones	- Conocimientos técnicos sobre Tecnología de la información (TI) - Gestión de riesgos

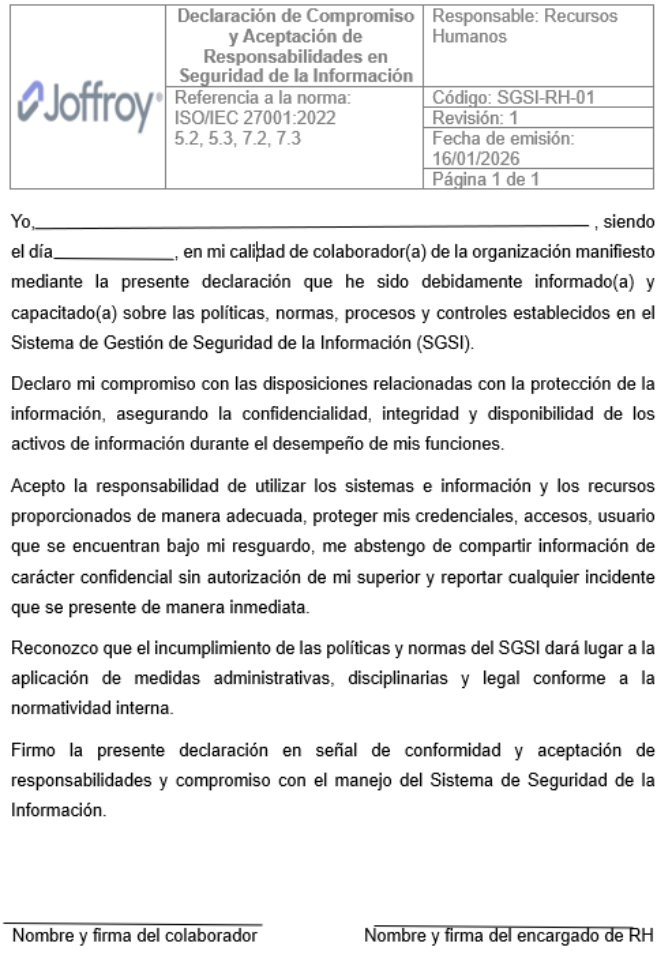
		- Actualizar y mantener el Sistema de Gestión	- Conocimientos en ISO 27001 - Gestión de proyectos - Liderazgo
Responsable del área de facturación	Control operativo en el área	- Garantizar el uso del Sistema de Gestión en las operaciones - Supervisar el cumplimiento de las políticas - Reportar incidentes	- Conocimientos en procesos de facturación aduanales - Manejo de información sensible - Conciencia en SI - Liderazgo
Personal de Facturación	Operación de SI	- Compromiso con el cumplimiento del SGSI - Proteger la información que utiliza - Uso de los sistemas con responsabilidad - No compartir accesos Reportar incidentes a su jefe inmediato	- Conocimientos en sistemas de facturación - Buenas prácticas en manejo de información - Conocimientos básicos en materia de seguridad de la información - Compromiso
Recursos Humanos	Gestión del personal	- Registrar cambios en el personal - Coordinación de inducción a personal de nuevo ingreso - Coordinación de capacitaciones periódicas	- Conocimientos en procesos administrativos - Manejo de personal - Gestión documental - Conciencia en SI

Usuarios del Sistema de Gestión	Uso autorizado de sistemas	- Cumplir con las políticas del SGSI - No compartir accesos - Reportar incidentes	- Conocimientos en buenas prácticas de SI - Uso seguro de sistemas - Responsabilidad y compromiso

Nota. Elaboración propia

Figura 11.

Declaración de compromiso y aceptación de responsabilidades en seguridad de la información.



Joffroy	**Declaración de Compromiso y Aceptación de Responsabilidades en Seguridad de la Información**	Responsable: Recursos Humanos
	Referencia a la norma: ISO/IEC 27001:2022 5.2, 5.3, 7.2, 7.3	Código: SGSI-RH-01
		Revisión: 1
		Fecha de emisión: 16/01/2026
		Página 1 de 1

Yo,_____ , siendo el día_____, en mi calidad de colaborador(a) de la organización manifiesto mediante la presente declaración que he sido debidamente informado(a) y capacitado(a) sobre las políticas, normas, procesos y controles establecidos en el Sistema de Gestión de Seguridad de la Información (SGSI).

Declaro mi compromiso con las disposiciones relacionadas con la protección de la información, asegurando la confidencialidad, integridad y disponibilidad de los activos de información durante el desempeño de mis funciones.

Acepto la responsabilidad de utilizar los sistemas e información y los recursos proporcionados de manera adecuada, proteger mis credenciales, accesos, usuario que se encuentran bajo mi resguardo, me abstengo de compartir información de carácter confidencial sin autorización de mi superior y reportar cualquier incidente que se presente de manera inmediata.

Reconozco que el incumplimiento de las políticas y normas del SGSI dará lugar a la aplicación de medidas administrativas, disciplinarias y legal conforme a la normatividad interna.

Firmo la presente declaración en señal de conformidad y aceptación de responsabilidades y compromiso con el manejo del Sistema de Seguridad de la Información.

_____ Nombre y firma del colaborador

_____ Nombre y firma del encargado de RH

Nota. Elaboración propia

6. Gestión de riesgos.

Para esta sección como parte importante del Sistema de Gestión de Seguridad de Información, bajo la cláusula 6.1 Acciones para abordar riesgos y oportunidades, con el control A.5.23 Gestión de riesgos de seguridad de la información, se elaboró una matriz de riesgos expuesta en las tablas 8 y 9 con el propósito de identificar, analizar y evaluar los riesgos que puedan comprometer la seguridad de la información del área de facturación de la agencia aduanal. La matriz se realizó a partir del contexto de la organización, identificando los activos principales de la entidad que manejan información crítica, tomando en cuenta procesos, sistemas y recursos involucrados en el área. Para cada riesgo se identificó una vulnerabilidad y su posible impacto.

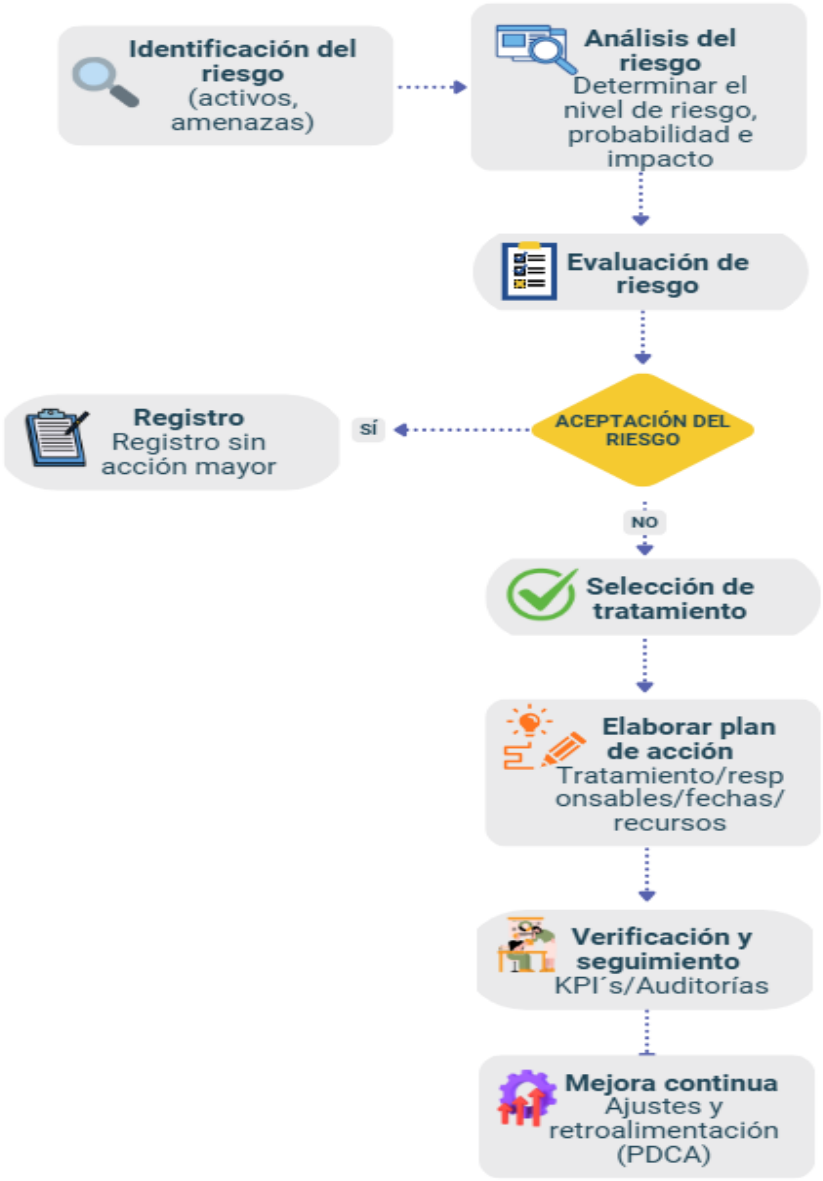
La evaluación de riesgos se realizó mediante una probabilidad de ocurrencia e impacto, clasificados por diferentes niveles (alto, medio, bajo), esta clasificación permitió facilitar la priorización de los riesgos. Igualmente se utilizó como base para generar un plan de tratamiento para cada riesgo, en el que se establecieron las acciones alineadas al Anexo A de la norma ISO/IEC 27001:2022 para mitigar, eliminar, reducir o aceptar cada uno.

Como parte del plan de tratamiento de riesgos del SGSI se desarrolló un diagrama de flujo como se observa en la figura 12, que describe secuencialmente los pasos a seguir cuando se presenta o identifica un riesgo para generar un tratamiento, en él se visualizan las decisiones y acciones que se deben ejecutar desde la identificación del riesgo hasta su control y seguimiento.

- El diagrama comienza con la identificación del riesgo y el activo que afecta, para seguir con sus correspondientes análisis apoyado de la matriz de riesgos.
- Identificar la clasificación en la matriz para considerar su nivel de riesgo e impacto que representa, además de identificar su posición en el sistema de semáforo para ubicar el grado del riesgo en caso de que se tengan otros.
- Una vez evaluado el grado del riesgo se establece un punto de decisión donde se plantea si se acepta el riesgo o no, en caso de que se acepte, se decide que el riesgo no tendrá acciones mayores y solo se hará el respectivo registro.
- Si se decide no aceptar el riesgo se tendrá que hacer una selección de tratamiento, de acuerdo con el catálogo encontrado en la matriz de riesgos, teniendo la opción de hacer un plan para mitigar, eliminar, reducir o aceptar el riesgo.
- Ya que se selecciona el tipo de tratamiento se elabora el plan a seguir, donde se deberá establecer el responsable de realizar el plan y encargado de su implementación, las fechas en las que se planea ejecutar y los recursos destinados a ese propósito.
- Cuando el plan de tratamiento se encuentre en marcha y haya cumplido con el periodo establecido se realiza un seguimiento para verificar si tuvo éxito o si existen áreas de oportunidad.
- Siguiendo con el ciclo de Deming o PDCA, se realizan las correcciones necesarias para mejorar el plan de tratamiento y buscar siempre la posible eliminación del riesgo.

Figura 12.

Diagrama de flujo de tratamiento de riesgos



Nota. Elaboración propia

El tener un plan de acción para los procesos permite tener una estructura sólida para que los colaboradores tengan conocimientos que como actuar ante un incidente, el diagrama de flujo funciona como una guía del proceso a seguir cuando se presenta un riesgo, disminuyendo las probabilidades de errores, la correcta aplicación de tratamientos y el seguimiento correspondiente.

7. **Evaluación del desempeño y KPI (monitoreo de desempeño/riesgo/cumplimiento).**

Cumpliendo con la cláusula 9.1 seguimiento, medición, análisis y evaluación, se utilizó un Balanced Scorecard (Cuadro de Mando Integral) explicado en la tabla 11, como una herramienta de apoyo para el monitoreo de desempeño del Sistema de Gestión de Seguridad de la información, permitiendo medir el nivel de cumplimento de los objetivos de seguridad, gestión de riesgos y mejora continua del SGSI alineado a los requerimientos del Anexo A de la norma ISO/IEC 27001:2022, evaluando los objetivos desde cuatro perspectivas: financiera, clientes, procesos internos y aprendizaje y crecimiento.

Tabla 11.

Balanced Scorecard

Balanced Scorecard					
Perspectiva	**Objetivo estratégico**	**Indicador (KPI)**	**Meta**	**Iniciativa estratégica**	**Alineación ISO/IEC 27001:2022**
Financiera	Reducción de pérdidas económicas por incidentes de seguridad	Costo económico por incidentes de seguridad de la información	0 incidentes críticos por año	Implementar controles y tratamiento de riesgos	A.5 Gestión de riesgos
	Evitar multas o sanciones legales y fiscales	Número de multas o sanciones por	≥95%	Cumplimiento de las normas y auditorías internas	A.5.31 Cumplimiento de requisitos legales y

		incumplimiento			contractuales
Cliente	Aumentar confianza de los clientes	Nivel de satisfacción del cliente respecto al manejo de su información	≥95%	Implementación de políticas de confidencialidad y seguridad	A.5.1 Políticas de seguridad de la información
	Protección de la información aduanal y fiscal del cliente	Número de incidentes relacionados con la información de los clientes	0 incidentes críticos por año	Control de accesos, gestión y tratamiento de riesgos	A.5.15 Control de accesos
	Continuidad del servicio de facturación	Porcentaje de disponibilidad del sistema de facturación	≥99%	Respaldos de seguridad y planes de contingencia	A.8.13 Copias de seguridad de la información
Procesos internos	Fortalecer la gestión de riesgos del SGSI	Porcentaje de riesgos identificados y evaluados	100%	Aplicación de la metodología de tratamiento de riesgos	6.1.2 Evaluación de riesgos

	Aplicación de tratamiento de riesgos efectivos	Porcentaje de riesgos tratados	≥90%	Plan de tratamiento de riesgos	6.1.3 Tratamiento de riesgos
	Mejorar la gestión de incidentes	Tiempo promedio de atención a incidentes	≤ 24 horas	Proceso de gestión de incidentes	A.5.24 Gestión de incidentes
	Certificar el cumplimiento del SGSI	Porcentaje de controles aplicados	≥90%	Auditorías internas	9.2 Auditoría interna
	Mantener la documentación actualizada	Porcentaje de documentos actualizados	100%	Control de documentos	7.5 Información documentada
Aprendizaje y crecimiento	Fortalecer las competencias de los colaboradores	Número de capacitaciones anuales	≥ 2 capacitaciones al año	Talleres, cursos y conferencias	7.2 Competencia
	Fomentar la cultura de seguridad	Nivel de cumplimiento de políticas	≥95%	Comunicación interna efectiva sobre el SGSI	7.4 Comunicación

Aumentar conciencia de la seguridad de la información	Porcentaje del personal capacitado	100%	Programas de capacitación y concientización	7.3 Conciencia

Nota. Elaboración propia

Perspectiva financiera

Desde la perspectiva financiera, los indicadores mencionados permitieron evaluar el impacto económico relacionado con los incidentes de seguridad de la información que puedan presentarse y el cumplimiento de los requisitos legales y fiscales. En los resultados se observa que la aplicación de controles y tratamientos de riesgos fomentan loa reducción de pérdidas económicas y prevención de sanciones por incumplimientos normativo.

Perspectiva del cliente

Se observa que los indicadores reflejan el nivel de confianza que los clientes tengan a la empresa en cuanto al manejo de sus datos e información, los resultados exponen que la protección de los datos y la continuación del servicio de facturación fortalecen el grado de satisfacción del cliente y la reputación de la entidad en el mercado.

Perspectiva de procesos internos

El Balanced Scorecard facilita el monitoreo de la eficacia de la gestión de riesgos, la atención de incidentes y el cumplimiento de los controles definidos a lo largo del SGSI, los indicadores permiten evaluar de manera objetiva la aplicación de los tratamientos de riesgos y como contribuye a la reducción de los niveles de riesgo identificados, fortaleciendo el control interno del área de facturación.

Perspectiva de aprendizaje y crecimiento

Permite evaluar el nivel de concientización, capacitación, compromiso y competencias del personal del área de facturación en materia de seguridad de la información, los resultados obtenidos demuestran que la capacitación continua y concientización del personal son elementos clave para la reducción de posibles riesgos por error humano, fomenta un enfoque de integridad en el SGSI.

La aplicación del Balanced Scorecard facilitó la integración de indicadores claves de desempeño que en conjunto reflejan el estado de los controles de seguridad y el impacto de la gestión de riesgos, tratamientos aplicados y nivel de cumplimiento conforme a la norma. Permite establecer objetivos de forma integral alineados al SGSI con indicadores medibles, apoyando la metodología de mejora continúa basado en el ciclo PDCA.

El uso de esta herramienta es de suma importancia para el área de facturación de la agencia aduanal, ya que permite evaluar, controlar y mejorar el desempeño de sus objetivos en cuanto a seguridad de la información, fortaleciendo y reforzando la toma de decisiones con bases sólidas para la mejora continua del SGSI y su posible apertura a otras áreas.

8. Documentación.

Parte importante de la norma es la documentación de los procesos, documentar permite tener las definiciones organizadas, establecidas y con cumplimiento normativo, además de ser un requisito obligatorio para la gestión de las auditorias tanto internas como externas, funcionan como evidencias de las imposiciones propuestas por la organización. Es un instrumento para asegurar correctamente la planeación, operación y control del sistema.

La norma establece en la cláusula 7.5 el requerimiento de mantener y controlar la información de forma documentada y asegurar que esta se encuentre disponible, actualizada y protegida en todo momento, cada documento permite estandarizar los procesos y tener una trazabilidad de los cambios según la necesidad, es por lo que en la tabla 12 se establece un inventario de documentación, donde se visualiza el

nombre del documento, código, versión, fecha de emisión y el responsable de este, dicha tabla deberá ser actualizada cada que se presente un cambio en alguno de los documentos.

Tabla 12.

Inventario de documentos

Nombre del documento	Código	Fecha de emisión	Revisión	Responsable
Declaración formal de liderazgo y compromiso de la alta dirección	SGSI-DIR-01	16-01-2026	1	Dirección General
Declaración de compromiso y aceptación de responsabilidades en seguridad de la información	SGSI-RH-01	16-01-2026	1	Recursos Humanos
Evaluación del plan de concienciación del SGSI	SGSI-RH-02	16-01-2026	1	Recursos Humanos
Acuerdo de confidencialidad de proveedores	SGSI-TEC-01	16-01-2026	1	Tecnología de la información (TI)
Plan de auditoría interna del SGSI	SGSI-AUD-01	16-01-2026	1	Auditor Interno
Check list de auditoría interna	SGSI-AUD-02	16-01-2026	1	Auditor Interno
Gestión de incidentes	SGSI-RES-01	16-01-2026	1	Responsable del SGSI

Nota. Elaboración propia.

9. Comunicación.

Con el propósito de garantizar una comunicación efectiva en el Sistema de Gestión de Seguridad de la Información y cumplir con la cláusula 7.4 comunicación, bajo el control A.5.6 Contacto con autoridades, se planteó una matriz de comunicación para llevar un control interno y transmitir de manera correcta el mensaje a comunicar, véase en la tabla 13.

Esta matriz avala que las partes interesadas como facturación, alta dirección, TI, recursos humanos y demás partes interesadas cuenten con lineamientos de organización para comunicar sus necesidades y cumplir correctamente con sus responsabilidades, promoviendo un ambiente de concienciación y compromiso con la aplicación de las políticas internas, además permite tener una trazabilidad documentada de las comunicaciones, siendo este un apoyo en las auditorías internas y mejora continua del SGSI.

Tabla 13.

Matriz de comunicación

Información para comunicar	Público objetivo	Medio/ canal	Frecuencia	Responsable	Evidencia
Política de Seguridad de la Información	Personal de facturación	Correo institucional	Semestral/ Revisión	Responsable del SGSI	Correo/Política firmada/Lista de personal informado
Roles y responsabilidades del SGSI	Personal del SGSI	Reunión	Anual	Jefe de área	Declaración de roles y responsabilidades firmada

Gestión de riesgos y tratamientos	Personal clave	Reunión	Trimestral	Responsable del SGSI	Matriz de riesgos aprobada/Minutas de reuniones
Reporte de incidentes	Todo el personal	Correo/reunión	Cuando se presente	Responsable del SGSI/TI	Registro/Tickets/Captura de correos
Resultados de auditorías	Alta dirección	Informe	Semestral	Auditor interno	Lista de verificación Informe de auditoría
Informes de seguimiento	Alta dirección	Correo/reunión	Semestral	Responsable del SGSI	Informe físico Formatos firmados
Acciones correctivas y mejoras	Personal clave	Correo/reunión	Cuando aplique	Responsable del SGSI	Minutas
Campañas de concientización	Todo el personal	Correo/reunión/carteles/muro de concientización	Semestral	Recursos Humanos	Material gráfico Evaluaciones Fotografías de actividades Capturas de correos
Cambios en el SGSI	Personal clave	Reunión	Cuando aplique	Responsable del SGSI	Solicitud de cambios firmada Versión actualizada

						de documentos Minuta

Nota. Elaboración propia.

10. Conciencia.

Con el fin de que el personal del área de facturación tenga conciencia de sus responsabilidades y comprenda la importancia del SGSI se implementan distintas herramientas plasmadas en un documento que incluyen plan de capacitación, programas de concienciación y simulación de incidentes, mismas que serán evaluadas bajo indicadores claves de desempeño (KPI) facilitando su monitoreo e identificando áreas de oportunidad, cumpliendo con la cláusula 7.3 conciencia, con los controles A.6.3 Concienciación, educación y capacitación en seguridad de la información.

La Tabla 14 indica los métodos de evaluación utilizados para las distintas actividades, a través de indicadores KPI.

Tabla 14.

Evaluación del programa de concienciación del SGSI

Método de evaluación	**Actividad evaluada**	**KPI**	**Meta**	**Frecuencia**	**Responsable**	**Evidencia**
Evaluación de conocimientos	Cuestionario para medir el nivel de comprensión de las políticas del SGSI	% de cuestionarios aprobados	≥90%	Semestral	Responsable del SGSI/RH	Resultados del cuestionario
Simulación de incidentes	Evaluación de comportamiento y acciones del	% de incidentes	≥80%	Semestral	Responsable del SGSI/TI	Reporte de simulación

	personal en los escenarios	gestionados correctamente				
Análisis de incidentes reales	Análisis de incidentes reales en el periodo	% de incidentes reportados	≥95%	Semestral	Responsable del SGSI/TI	Bitácora de incidentes/Tickets registrados
Observación operativa	Verificación de buenas prácticas de seguridad de la información	% de cumplimiento de buenas prácticas	≥95%	Semestral	Responsable del SGSI	Check list de cumplimiento
Evaluación de campañas	Impacto de campañas de concienciación	Nivel de participación	≥90%	Semestral	Responsable del SGSI/RH	Material de apoyo

Nota. Elaboración propia

Cumpliendo con la obligatoriedad de la norma, se plantea el documento mostrado en la figura 13 y 14, en el que se detalla el objetivo del documento, alcance, método de evaluación, responsables y manejo de resultados.

Figura 13.

Evaluación del plan de concienciación del SGSI (Página. 1)

Joffroy	Evaluación del plan de concienciación del SGSI	Responsable: Recursos Humanos
	Referencia a la norma: ISO/IEC 27001:2022 7.3, 9.1	Código: SGSI-RH-02
		Revisión: 1
		Fecha de emisión: 16/01/2026
		Página 1 de 2

1. Objetivo

Evaluar la efectividad del plan de concienciación del Sistema de Gestión de Seguridad de la Información (SGSI), validando el nivel de conocimiento y compromiso que presenta el personal del área de facturación frente a las políticas del SGSI.

2. Alcance

La evaluación aplica a todo el personal del área de facturación y demás involucrados en el SGSI

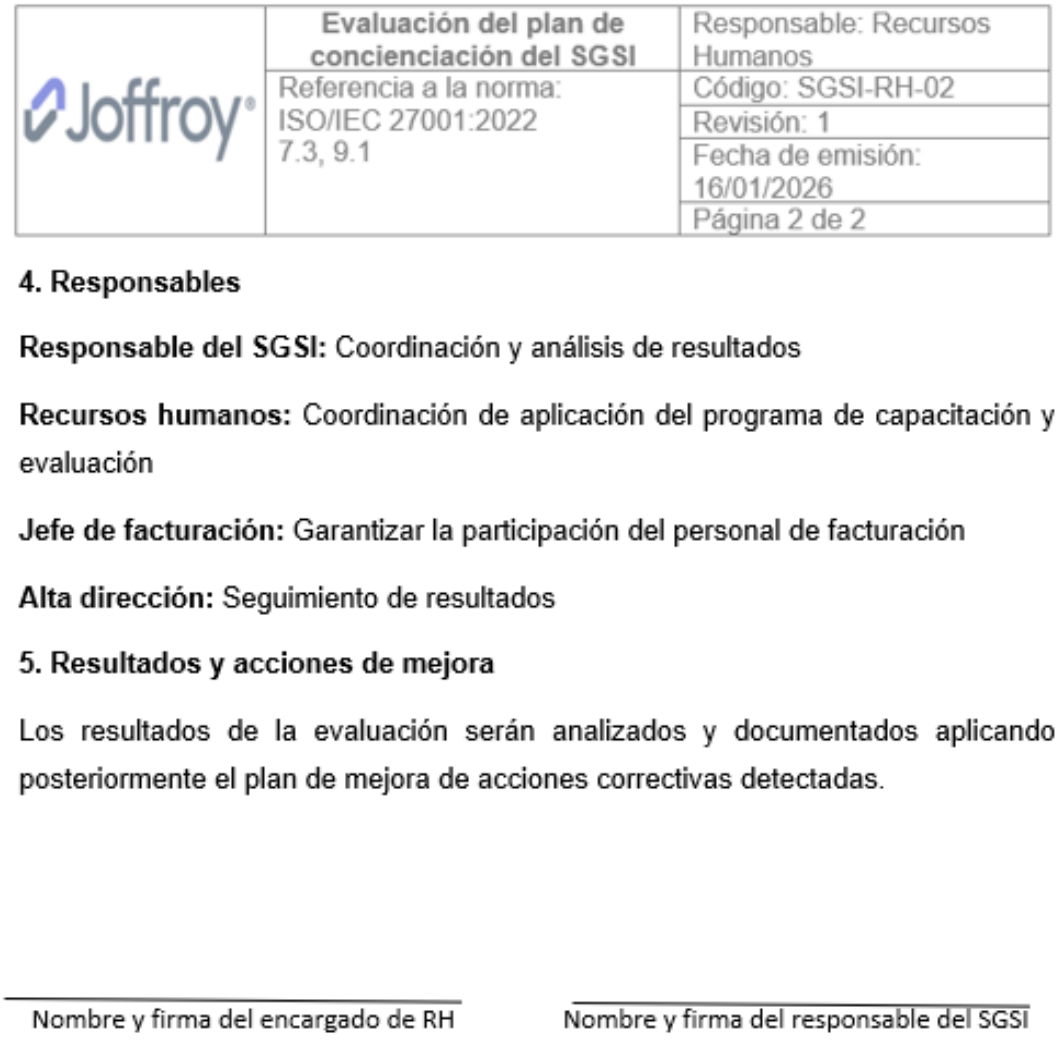
3. Evaluación por KPI

Método de evaluación	Actividad evaluada	KPI	Meta	Frecuencia	Responsable	Evidencia
Evaluación de conocimientos	Cuestionario para medir el nivel de comprensión de las políticas del SGSI	% de cuestionarios aprobados	≥90%	Semestral	Responsable del SGSI/RH	Resultados de cuestionarios
Simulación de incidentes	Evaluación del comportamiento y acciones del personal en los escenarios	% de incidentes gestionados correctamente	≥85%	Semestral	Responsable del SGSI/TI	Reporte de simulación
Exploración de incidentes reales	Análisis de incidentes reales en el periodo	% de incidentes reportados	≥95%	Semestral	Responsable del SGSI/TI	Bitácora de incidentes/ Tickets registrados
Observación operativa	Verificación de buenas prácticas de seguridad de la información	% de cumplimiento de buenas prácticas	≥90%	Semestral	Responsable del SGSI	Check list de cumplimiento
Evaluación de campañas	Impacto de campañas de concienciación	Nivel de participación	≥90%	Semestral	Responsable del SGSI/RH	Material de apoyo

Nota. Elaboración propia

Figura 14.

Evaluación del plan de concienciación del SGSI (Página. 2).



Joffroy	Evaluación del plan de concienciación del SGSI	Responsable: Recursos Humanos
	Referencia a la norma: ISO/IEC 27001:2022 7.3, 9.1	Código: SGSI-RH-02
		Revisión: 1
		Fecha de emisión: 16/01/2026
		Página 2 de 2

4. Responsables

Responsable del SGSI: Coordinación y análisis de resultados

Recursos humanos: Coordinación de aplicación del programa de capacitación y evaluación

Jefe de facturación: Garantizar la participación del personal de facturación

Alta dirección: Seguimiento de resultados

5. Resultados y acciones de mejora

Los resultados de la evaluación serán analizados y documentados aplicando posteriormente el plan de mejora de acciones correctivas detectadas.

Nombre y firma del encargado de RH

Nombre y firma del responsable del SGSI

Nota. Elaboración propia

La evaluación de programa de concienciación permite tener una visión clara del comportamiento de los colaboradores en su participación con el cumplimiento de políticas del SGSI, contar con un análisis periódico y definido fortalece las brechas de oportunidad que mejoran el SGSI, de tal forma que no solo cumple con lo establecido por la norma, sino que también valida el seguimiento continuo del SGSI.

11. Relaciones con proveedores.

La relación con los proveedores es un elemento clave en el Sistema de Gestión de Seguridad de la información, ya que de manera directa o indirecta se relacionan terceros en el proceso de facturación, entre estos se encuentran proveedores de infraestructura, mantenimiento de servidores, servidores en la nube y de instalaciones. La entidad reconoce la responsabilidad que tiene en el manejo de servicios externos, ya que pueden presentarse riesgos por su parte que pongan en peligro la confidencialidad, integridad y disponibilidad de la información, es por ello por lo que se platean procesos para llevar un control y monitoreo de estos a través de una clasificación y evaluación de proveedores, acuerdos de confidencialidad, documento de políticas y criterios de selección. Para ello se plantean las siguientes políticas:

1. Política de evaluación de proveedores

La organización estable un proceso formal de evaluación de proveedores con el objetivo de asegurar que los servicios brindados por terceros cumplan con el seguimiento de buenas prácticas de seguridad de la información, buscando un enfoque y control no solo interno, sino también externo, previo a la contratación se deberá realizar un cuestionario de buenas prácticas para conocer el nivel de cumplimiento que este tenga con el manejo de la información, dicha evaluación permitirá tener una clasificación de los proveedores existentes en la entidad según su nivel de riesgo y grado de criticidad.

La evaluación deberá ser documentada y revisada periódicamente cuando se presenta algún cambio, buscando una correcta alineación para el SGSI y su mejora continua.

El cuestionario ilustrado en la tabla 15 deberá ser enfocado a la seguridad de la información de cada uno de los proveedores para su selección y seguimiento, para evaluar las prácticas de seguridad de la información que prestan a la organización, los resultados obtenidos en su aplicación reflejan vulnerabilidades en sus controles que puedan poner en riesgo la triada de la información del área de facturación.

Dicho cuestionario tiene como base los controles del Anexo A de la norma ISO/IEC 27001:2022 que sustentan el SGSI, tomando en cuenta políticas de seguridad, control de accesos, amenazas, riesgos, gestión de incidentes, requisitos legales y demás, la aplicación de este cuestionario pone en evidencia la viabilidad de seleccionarlo y su seguimiento.

Los resultados son analizados y utilizados como punto de decisión para la clasificación del proveedor, este debe ser aplicado previo a su contratación y durante evaluaciones de seguimiento de los actuales, siendo parte de los criterios del SGSI en la gestión de riesgos externos y buscando fortalecer los lineamientos del sistema.

Tabla 15.

Cuestionario de Seguridad de la Información para proveedores

Control evaluado	Pregunta	Respuesta (Sí, No, Parcial)	Evidencia	Riesgo asociado
Política de SI	¿Cuenta con una política orientada a la seguridad de la información?		Documentación vigente	Fugas de información
Control de accesos	¿Cuenta con restricciones de accesos físicos y de información?		Evidencias como fotografías y registros	Accesos no autorizados
Gestión de usuarios	¿Lleva una gestión de altas, bajas y cambios de accesos del personal?		Registros	Usos indebidos

Protección contra malware y virus	¿Cuenta con antivirus y antimalware actualizados?	Evidencia de su existencia	Pérdida o robo de datos
Respaldo de información	¿Realiza respaldos de información periódicos?	Políticas y registros	Pérdida de información
Gestión de incidentes	¿Implementa procesos para reporte y seguimiento de incidentes?	Políticas, registros y procedimientos	Incidentes no gestionados
Mejora continua	¿Cuenta con un plan de seguimiento de mejora continua?	Documentos vigentes y políticas	Procesos planos
Confidencialidad	¿Implementa acuerdos de confidencialidad en el personal?	Documentación firmada	Mal uso de información y divulgación

Nota. Elaboración propia

Con el fin de tener una organización interna y base para herramientas relacionadas con la gestión de proveedores se plantea un inventario de proveedores relacionados al manejo y almacenamiento de información, que deberá someterse a análisis y cambios cuando se presenten nuevas actualizaciones como altas, bajas, fusiones y demás ajustes según la necesidad (Tabla 16).

Tabla 16.

Inventario de proveedores

Proveedor	Categoría	Tipo de Servicio	Modalidad
Honne	TI / Cloud	Administración de servidores en la nube (AWS)	Recurrente
Pintec	Infraestructura	Instalaciones de seguridad y cableado de red en plantas	Por proyecto
Hugo	TI / On-premise	Configuración y mantenimiento de servidores locales	Recurrente / Bajo demanda
Upwork – Equipo de desarrollo externo	TI / Desarrollo de Software	Desarrollo, mantenimiento y soporte de aplicaciones y sistemas	Recurrente / Por horas o proyecto

Nota. Elaboración propia con información de la empresa

Como punto importante del SGSI se plantea una matriz de clasificación de proveedores (Tabla 17) donde se evalúan de acuerdo con su nivel de criticidad, el impacto que tendría, clasificar de esta manera genera un panorama claro sobre que proveedores necesitan mayor atención, control y seguimiento para evitar percances. Los proveedores que se clasifican como críticos requieren una mayor atención y control, ya que tienen acceso directo a información sensible, mientras que los relevantes, aunque pueden llegar a tener contacto con la información no lo tienen de manera directa y son más fáciles de controlar, por otro lado, los de nivel no crítico se tratan con controles básicos generalmente administrativos.

Tabla 17.

Matriz de clasificación de proveedores

Tipo de proveedor	Servicio	Tipo de acceso	Nivel del proveedor	Impacto ante incidente	Tratamiento o control
TI/Cloud	Administración de servidores en la nube (AWS)	Acceso directo a información sensible de la empresa en los servidores	Crítico	Alto	Evaluación de seguridad, definición de cláusulas, control de accesos, cifrado de información, monitoreo continuo y acuerdos de confidencialidad
Infraestructura	Instalaciones de seguridad y cableado de red en plantas	Acceso parcial o indirectos	Relevante	Medio	Evaluación del proveedor, controles de accesos físicos, supervisión activa y de cumplimiento
TI/On-premise	Configuración y mantenimiento de servidores locales	Acceso parcial o indirectos	Relevante	Medio	Control de accesos, registro de actividades, accesos autorizados, supervisión y

					acuerdo de confidencialidad
TRI/Desarrollo de Software	Desarrollo, mantenimiento y soporte de aplicaciones y sistemas	Acceso directo a información sensible de la empresa en los servidores	Crítico	Alto	Control de desarrollo, revisión de códigos, monitoreo y acuerdo de confidencialidad
Servicios generales	Papelería y demás servicios generales	Sin acceso o mínimo	No crítico	Bajo	Control administrativo y supervisión general

Nota. Elaboración propia

2. Política de gestión y relación con proveedores

Buscando la certeza de que la información interna se encuentre segura de manera directa o indirecta en los proveedores que tienen estos accesos se implementa un acuerdo de confidencialidad (figura 15 y 16) entre la empresa y el proveedor donde se aclaran las obligaciones que debe cumplir, uso y resguardo seguro de la información, así como las posibles sanciones en caso de incumplimiento con la política.

Figura 15.

Acuerdo de confidencialidad de proveedores (página. 1)

Joffroy	**Acuerdo de confidencialidad de proveedores**	Responsable: Tecnología
	Referencia a la norma: ISO/IEC 27001:2022 5.19, 5.20,5.21	Código: SGSI-TEC-01
		Revisión: 1
		Fecha de emisión: 16/01/2026
		Página 1 de 2

1. **Objetivo**

Establecer las obligaciones y responsabilidades del proveedor respecto al manejo de la seguridad de la información garantizando su confidencialidad, integridad y disponibilidad.

2. **Alcance**

El presente acuerdo aplica para todos aquellos proveedores que de manera directa o indirecta tienen acceso a información, sistemas, soporte y demás servicios relacionados con el área de facturación.

3. **Información confidencial**

Se considera información confidencial a toda aquella relacionada con:

- Información financiera
- Información fiscal
- Operaciones aduaneras
- Información personal de los clientes
- Sistemas y aplicaciones
- Base de datos
- Documentación, procesos y registros

4. **Obligaciones del proveedor**

El proveedor deberá cumplir con lo previsto por las siguientes disposiciones

- Abstinencia de divulgación de datos
- Accesos autorizados a los datos de la organización
- No utilizar la información para fines que no sean del servicio prestado
- No manipular datos
- Implementar medidas para proteger la información de la empresa ante accesos no autorizados, perdida, alteración o destrucción de información
- Notificar a la empresa cualquier incidente relacionado con el servicio

Nota. Elaboración propia

Figura 16.

Acuerdo de confidencialidad de proveedores (página. 2)

Joffroy	**Acuerdo de confidencialidad de proveedores**	Responsable: Tecnología
	Referencia a la norma: ISO/IEC 27001:2022 5.19, 5.20,5.21	Código: SGSI-TEC-01
		Revisión: 1
		Fecha de emisión: 16/01/2026
		Página 2 de 2

5. Incumplimiento

El incumplimiento de lo establecido en este acuerdo podrá derivar sanciones administrativas o legales, conforme a las políticas internas de la empresa.

6. Vigencia

El presente documento tendrá vigencia durante toda la relación de la prestación de servicio y una vez finalizada.

7. Aceptación

Leído el presente acuerdo y conforme con su contenido por las partes interesadas, lo firman en señal de conformidad

Nombre y firma del contratante del servicio	Nombre y firma del representante del proveedor

Fecha

Nota. Elaboración propia

3. Política de Comunicación con proveedores

La organización debe mantener una relación controlada y documentada con los proveedores de manera formal para mantener una trazabilidad de la comunicación, asegurando que la información compartida y el mensaje se transmita de la manera que se espera. Toda comunicación relacionada con la seguridad de la información, incidentes, cambios, actualizaciones, detalles y demás temas, serán a través de canales seguros y actualizados como correos institucionales, reuniones, llamadas telefónicas por el número oficial de la empresa y documentos formales.

Con las políticas implementadas se da cumplimiento a la cláusula 8 operación, controles 4.5.7 Seguridad de la información en relación con proveedores, A.5.8 Dirección de la seguridad de la información en la cadena de suministro, A.5.9 Seguridad de la información para el uso de servicios de proveedores.

12. Auditoría Interna (Auditoría Interna).

Para una aplicación y mejora más integral se planificarán auditorías internas dirigidas al personal y evolución del SGSI para validar su correcta aplicación y cumplimiento de los requisitos especificados en la cláusula 9.2 de auditoría interna de la norma, donde se requiere de planificación, ejecución periódica, evaluación y documentación de la auditoria.

Para ello, se cuenta con un plan de auditoría interna siguiendo el esquema mostrado en la figura 17, el cual consta de 5 etapas esenciales.

Planificación: Definir los objetivos y alcance que tendrá la auditoria, se realiza un cronograma de actividades y los recursos necesarios para su implementación.

Determinaciones: Aplicación del plan de auditoría mediante instrumentos de recolección de información.

Implementación: Análisis de las observaciones y notas del auditor.

Monitoreo: Elaboración de informe documentando los hallazgos encontrados en la auditoría.

Revisión y mejora: Verificación, acciones correctivas y propuestas de mejora.

Figura 17.

Etapas de la auditoría interna

Nota. Elaboración propia

Una vez definidas las etapas se presenta el documento formal del plan de auditoria (figura 18, 19 y 20), donde se muestra el objetivo de la realización de la auditoría, lo objetivos que se pretenden cumplir, los roles y responsabilidades involucradas en el proceso para garantizar la participas de las personas involucradas en las operaciones del área, la frecuencia con la que se aplicarán las auditorias, así mismo se plantean las metodologías a seguir para la recolección de información y obtención de resultados, especialmente la aplicación de un check list que también se encuentra documentado. Se toma en cuenta un cronograma de actividades de las etapas previstas anteriormente desde la planeación hasta las acciones correctivas, para seguir con la elaboración del informe que genera el auditor con el

análisis de los resultados y conclusiones obtenidas, para finalizar con las sugerencias que propone para mejorar los aspectos de no conformidad sirviendo como base para la alta dirección en la toma de decisiones de mejora del SGSI.

Figura 18.

Plan de auditoría interna del SGSI (Página. 1)

Joffroy	Plan de auditoría interna del SGSI	Responsable: Auditor interno
	Referencia a la norma: ISO/IEC 27001:2022 9.2	Código: SGSI-AUD-01
		Revisión: 1
		Fecha de emisión: 16/01/2026
		Página 1 de 3

1. Objetivo

Evaluar el grado de cumplimiento del Sistema de Gestión de Seguridad de la información (SGSI) y la implementación de controles

2. Alcance

El plan de auditoría se centraliza en el área de facturación en los siguientes aspectos

a) Prácticas de seguridad de la información
b) Gestión de riesgos
c) Gestión de incidentes
d) Roles, responsabilidades y competencias
e) Comunicación
f) Concienciación
g) Relación con proveedores
h) Documentación
i) Evaluación de desempeño

3. Periodicidad de la auditoria

La auditoría deberá realizarse de manera anual o cuando se presente algún evento significativo para el SGSI

4. Roles y responsabilidades

Rol	Responsabilidad
Auditor interno	Planear y ejecutar la auditoría
Responsable del SGSI	Coordinar lo necesario para la auditoría
Jefe de facturación	Atender las necesidades del auditor
Personal de facturación	Estar a la disposición de las actividades y requerimientos
Alta dirección	Revisión de resultados y seguimiento

Nota. Elaboración propia

Figura 19.

Plan de auditoría interna del SGSI (Página. 2)

Joffroy	Plan de auditoría interna del SGSI	Responsable: Auditor interno
	Referencia a la norma: ISO/IEC 27001:2022 9.2	Código: SGSI-AUD-01
		Revisión: 1
		Fecha de emisión: 16/01/2026
		Página 2 de 3

5. **Metodología**

El proceso se llevará a cabo por medio de:

- Entrevistas
- Observación directa
- Revisión de documentos
- Realización check list
- Revisión de indicadores (KPI)
- Revisión de evidencias
- Revisión de gestión de incidentes

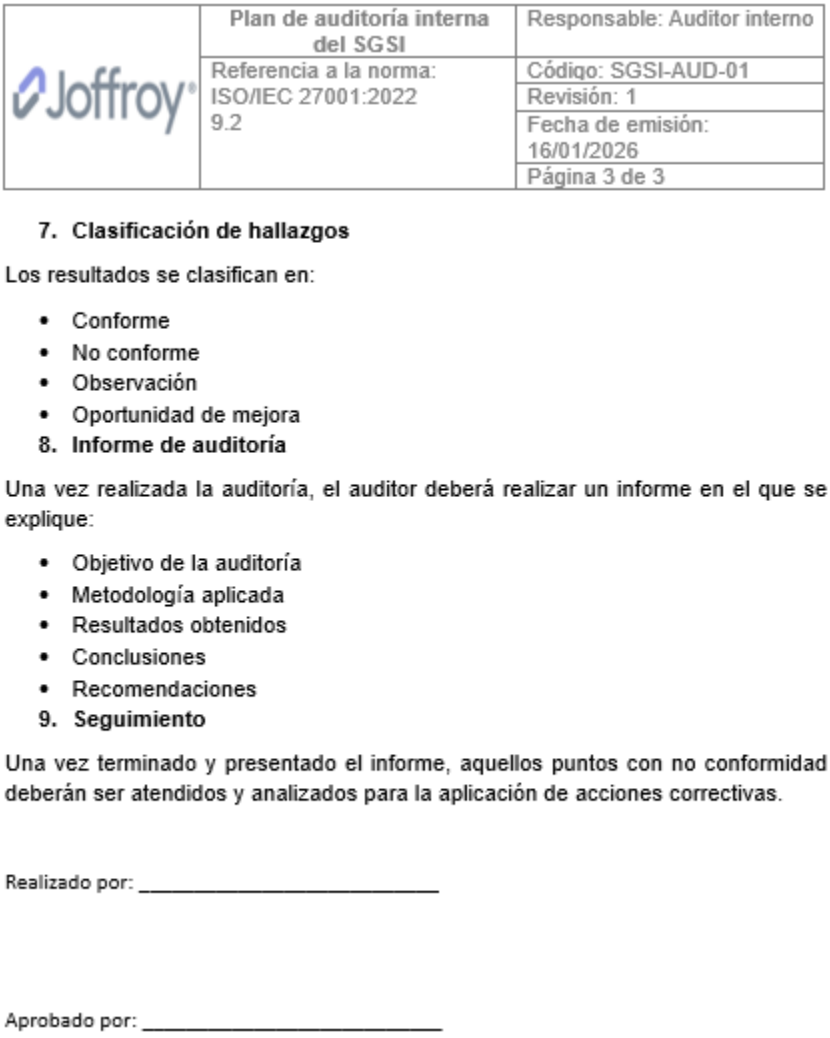
6. **Programa y cronograma**

Etapa	Actividad	Responsable	Evidencia
Planificación	Definir los criterios y alcance de la auditoría	Auditor interno/Responsable del SGSI	Planeación de la auditoria
Determinaciones	Aplicación de actividades y metodología de la auditoría	Auditor interno	Aplicación del check list
Implementación	análisis de los resultados	Auditor interno	Notas del auditor
Monitoreo	Elaboración y documentación de análisis y de hallazgos	Auditor interno	Informe
Revisión y mejora	Verificación y correcciones	Auditor interno/Responsable del SGSI	Registros

Nota. Elaboración propia

Figura 20.

Plan de auditoría interna del SGSI (Página. 3)



Joffroy	Plan de auditoría interna del SGSI	Responsable: Auditor interno
	Referencia a la norma: ISO/IEC 27001:2022 9.2	Código: SGSI-AUD-01
		Revisión: 1
		Fecha de emisión: 16/01/2026
		Página 3 de 3

7. **Clasificación de hallazgos**

Los resultados se clasifican en:

- Conforme
- No conforme
- Observación
- Oportunidad de mejora

8. **Informe de auditoría**

Una vez realizada la auditoría, el auditor deberá realizar un informe en el que se explique:

- Objetivo de la auditoría
- Metodología aplicada
- Resultados obtenidos
- Conclusiones
- Recomendaciones

9. **Seguimiento**

Una vez terminado y presentado el informe, aquellos puntos con no conformidad deberán ser atendidos y analizados para la aplicación de acciones correctivas.

Realizado por: _____

Aprobado por: _____

Nota. Elaboración propia

Brindando una herramienta de apoyo de evaluación para la auditoría se dispone del check list de evaluación presentado en las figuras 21, 22, 23 y 24, el cual está diseñado para medir el nivel de cumplimiento del SGSI con las cláusulas aplicadas en este. Este instrumento es de gran utilidad para la verificación de los elementos del sistema identificando aquellos de conformidad, no conformidad, observaciones y puntos de mejoras.

Figura 21.

Check list de auditoría interna (Página. 1)

Joffroy	**Check list de auditoria interna**	Responsable: Auditor interno
	Referencia a la norma: ISO/IEC 27001:2022 9.2	Código: SGSI-AUD-02
		Revisión: 1
		Fecha de emisión: 16/01/2026
		Página 1 de 4

No. Informe de auditoría:	**Fecha:**	
Auditor(a):	**Hora de inicio:**	
Revisado por:	**Hora de término:**	

1. Contexto de la organización				
No.	**Criterio**	**Sí**	**No**	**Observaciones**
1.1	Se identifica el contexto interno y externo de la organización			
1.2	Se define el alcance del SGSI			
1.3	Se identifica a los involucrados del SGSI			

2. Liderazgo y compromiso				
No.	**Criterio**	**Sí**	**No**	**Observaciones**
2.1	Existe una declaración documentada de liderazgo y compromiso de la alta dirección			
2.2	La alta dirección aprueba el SGSI			
2.3	Se definen las responsabilidades de la alta dirección			

3. Objetivos de SI				
No.	**Criterio**	**Sí**	**No**	**Observaciones**
3.1	Se establecen los objetivos del SGSI			
3.2	Se define el alcance del SGSI			
3.3	Se identifica a los involucrados del SGSI			

4. Política de SI				
No.	**Criterio**	**Sí**	**No**	**Observaciones**
4.1	Existen políticas documentadas de seguridad de la información			
4.2	Las políticas se comunican al personal			
4.3	Se definen los objetivos de la política			

Nota. Elaboración propia

Figura 22.

Check list de auditoría interna (Página. 2)

Joffroy	**Check list de auditoria interna**	Responsable: Auditor interno
	Referencia a la norma: ISO/IEC 27001:2022 9.2	Código: SGSI-AUD-02
		Revisión: 1
		Fecha de emisión: 16/01/2026
		Página 2 de 4

5. Roles, responsabilidades y competencias				
No.	**Criterio**	**Sí**	**No**	**Observaciones**
5.1	Los roles del personal involucrado en el SGSI se encuentran definidos			
5.2	El personal conoce sus responsabilidades			
5.3	Se definen las competencias de cada puesto			

6. Gestión de riesgos				
No.	**Criterio**	**Sí**	**No**	**Observaciones**
6.1	Se cuenta con una herramienta de gestión de riesgos			
6.2	Existe una evaluación de riesgos			
6.3	Los riesgos identificados cuentan con un tratamiento			
6.4	Se lleva un seguimiento de los riesgos			

7. Evaluación del desempeño y KPI				
No.	**Criterio**	**Sí**	**No**	**Observaciones**
7.1	Se cuenta con indicadores KPI para la evaluación del SGSI			
7.2	Se encuentran definidas las metas de los objetivos			
7.3	Se cuenta con evidencia de cada evaluación			

8. Documentación				
No.	**Criterio**	**Sí**	**No**	**Observaciones**
8.1	La documentación del SGSI se encuentra controlada			
8.2	Se registran los cambios aplicados			
8.3	Se actualizan los registros			
8.4	Se resguarda de manera segura la documentación			

Nota.

Nota. Elaboración propia

Figura 23.

Check list de auditoría interna (Página. 3)

Joffroy	**Check list de auditoria interna**	Responsable: Auditor interno
	Referencia a la norma: ISO/IEC 27001:2022 9.2	Código: SGSI-AUD-02
		Revisión: 1
		Fecha de emisión: 16/01/2026
		Página 3 de 4

9. Comunicación				
No.	**Criterio**	**Sí**	**No**	**Observaciones**
9.1	Se definen los canales seguros de comunicación			
9.2	Se cuenta con una matriz de comunicación del SGSI			
9.3	El personal conoce las políticas de comunicación			

10. Conciencia				
No.	**Criterio**	**Sí**	**No**	**Observaciones**
10.1	Existe un programa de concienciación			
10.2	Se capacita al personal mínimo dos veces al año			
10.3	Se realizan campañas internas			

11. Relaciones con proveedores				
No.	**Criterio**	**Sí**	**No**	**Observaciones**
11.1	Se clasifica a los proveedores por nivel de criticidad			
11.2	Se implementa una evaluación previa a la contratación			
11.3	Se evalúan periódicamente			
11.4	Se cuenta con acuerdos de confidencialidad			

12. Gestión de incidentes				
No.	**Criterio**	**Sí**	**No**	**Observaciones**
12.1	Se cuenta con un procedimiento de gestión de incidentes			
12.2	Se lleva un control o registro de incidentes			
12.3	El personal conoce como reportar incidentes			
12.4	Se aplican acciones correctivas ante incidentes			

Nota. Elaboración propia

Figura 24.

Check list de auditoría interna (Página. 4)

Joffroy	**Check list de auditoría interna**	Responsable: Auditor interno
	Referencia a la norma: ISO/IEC 27001:2022 9.2	Código: SGSI-AUD-02
		Revisión: 1
		Fecha de emisión: 16/01/2026
		Página 4 de 4

13. Mejora continua				
No.	**Criterio**	**Sí**	**No**	**Observaciones**
13.1	Se Realizan auditorías periódicamente			
13.2	Se plantean acciones correctivas en el SGSI			
13.3	Se realizan ajustes de mejora al SGSI			

Elaborado por: _____

Revisado por: _____

Nota. Elaboración propia

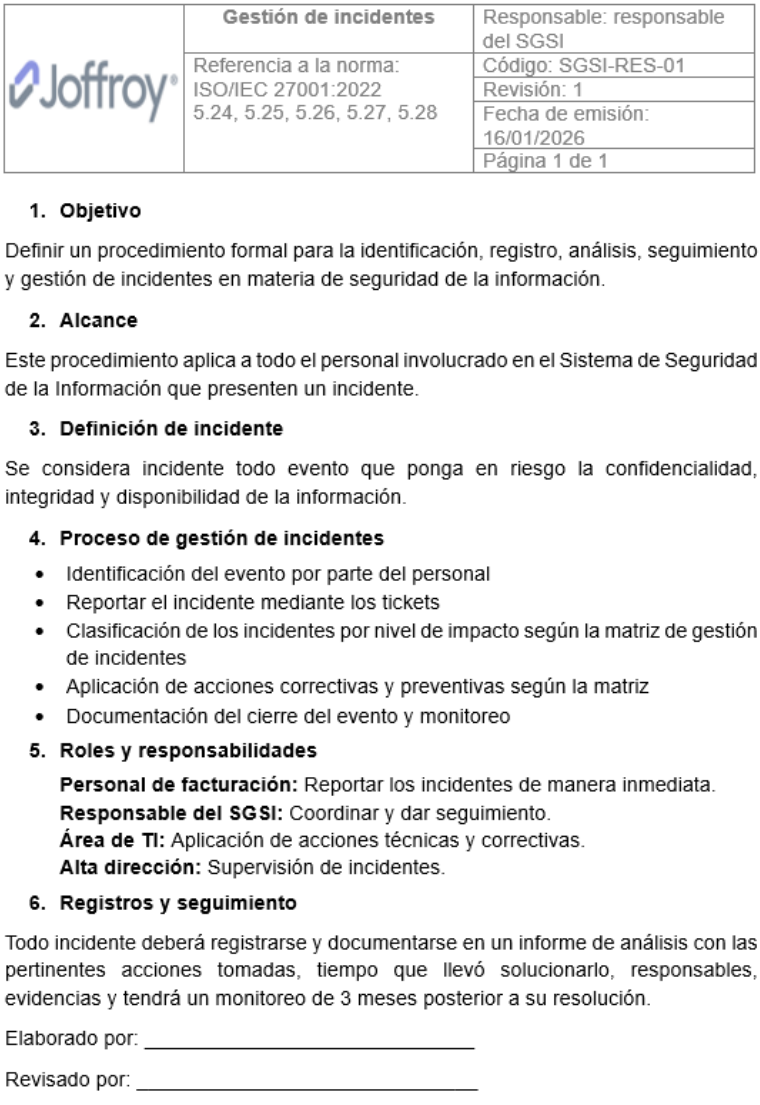
13. Gestión de incidentes.

Uno de los propósitos más importantes del SGSI es como la empresa gestiona los incidentes, es de carácter prioritario tener una estructura clara de cuáles serán las respuestas y acciones correctivas ante un evento que ponga en riesgo la seguridad de la información, es por ello, que respaldado bajo la cláusula 8.1 de control operacional de la norma ISO/IEC 27001:2022 y por los controles A.5.24 al A.5.28, se establece una planificación de respuesta ante incidentes, aprendizaje y recolección de evidencias.

Siguiendo con los controles establecidos se presenta un documento oficial donde se ilustra el procedimiento a seguir cuando se presenta un incidente, desde la detección hasta el seguimiento que debe seguir (figura 25), como herramienta de apoyo de la matriz de gestión de incidentes, siendo este un utensilio de soporte para las acciones correctivas que deben seguirse cuando se presenta un evento, además de ilustrar el nivel de impacto que representa y el responsable de darle el tratamiento y seguimiento correspondiente.

Figura 25.

Gestión de incidentes



Joffroy	**Gestión de incidentes**	Responsable: responsable del SGSI
	Referencia a la norma: ISO/IEC 27001:2022 5.24, 5.25, 5.26, 5.27, 5.28	Código: SGSI-RES-01
		Revisión: 1
		Fecha de emisión: 16/01/2026
		Página 1 de 1

1. **Objetivo**

Definir un procedimiento formal para la identificación, registro, análisis, seguimiento y gestión de incidentes en materia de seguridad de la información.

2. **Alcance**

Este procedimiento aplica a todo el personal involucrado en el Sistema de Seguridad de la Información que presenten un incidente.

3. **Definición de incidente**

Se considera incidente todo evento que ponga en riesgo la confidencialidad, integridad y disponibilidad de la información.

4. **Proceso de gestión de incidentes**

- Identificación del evento por parte del personal
- Reportar el incidente mediante los tickets
- Clasificación de los incidentes por nivel de impacto según la matriz de gestión de incidentes
- Aplicación de acciones correctivas y preventivas según la matriz
- Documentación del cierre del evento y monitoreo

5. **Roles y responsabilidades**

Personal de facturación: Reportar los incidentes de manera inmediata.
Responsable del SGSI: Coordinar y dar seguimiento.
Área de TI: Aplicación de acciones técnicas y correctivas.
Alta dirección: Supervisión de incidentes.

6. **Registros y seguimiento**

Todo incidente deberá registrarse y documentarse en un informe de análisis con las pertinentes acciones tomadas, tiempo que llevó solucionarlo, responsables, evidencias y tendrá un monitoreo de 3 meses posterior a su resolución.

Elaborado por: _____

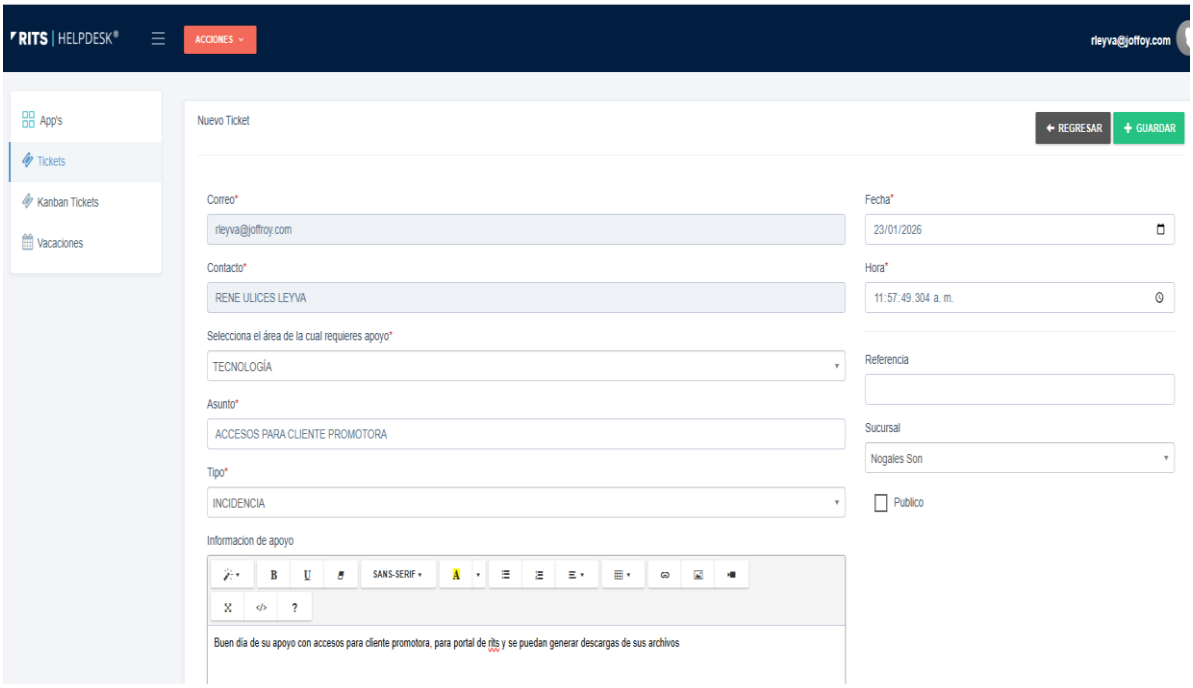
Revisado por: _____

Nota. Elaboración propia

Con el objeto de llevar un registro y monitoreo de incidentes, cumpliendo con el control A.5.25, A.5.27 y A.5.28, se muestra en las figuras 26, 27 y 28 el sistema de tickets interno que se maneja, en el cual se debe reportar de manera inmediata la incidencia que se presenta y las necesidades que requiere.

Figura 26.

Sistema de tickets



Nota. Propiedad de la empresa

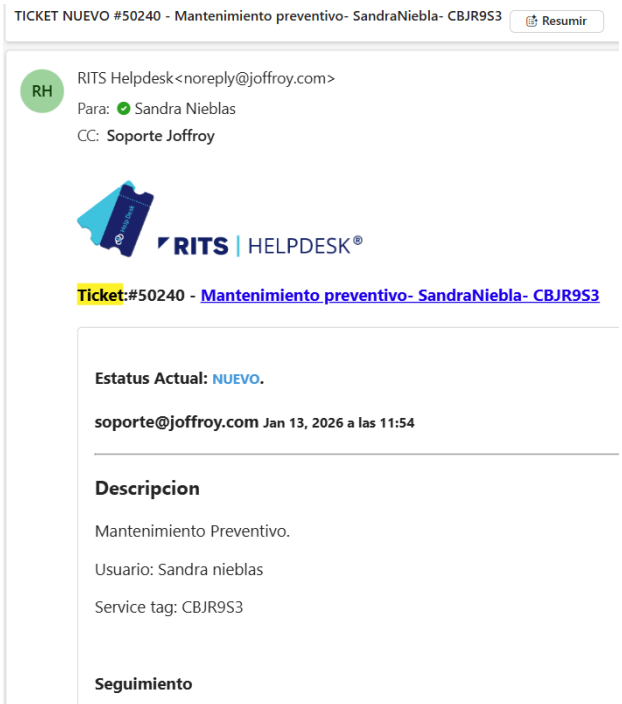
Figura 27.

Seguimiento de tickets en plataforma

Nota. Propiedad de la empresa

Figura 28.

Correo de seguimiento de ticket



Nota. Propiedad de la empresa.

Como base de la gestión de incidentes se presenta una matriz que explica las acciones inmediatas en caso de un incidente. La tabla 18 representa la simbología de los criterios de evaluación del nivel de impacto de los incidentes ilustrados en la matriz, utilizando una ponderación de alto, medio y bajo.

Tabla 18.

Criterios de evaluación del nivel de impacto de incidentes

Nivel de impacto	Descripción
Alto	Incidente con afectación crítica que requiere acción inmediata
Medio	Incidente con afectación moderado que requiere seguimiento
Bajo	Incidente con afectación menor

Nota. Elaboración propia

La tabla 19 expone la matriz de acciones correctivas a seguir en caso de que se presente un incidente, forma parte importante del SGSI, ya que permite identificar, clasificar y atender los eventos que pongan en riesgo la seguridad de la información, funciona como un instrumento operativo y de control, sirviendo como guía y plan de contingencia para el personal al momento de hacer un reporte. Facilita la toma de decisiones y trabaja como evidencia documental en las auditorías internas.

Tabla 19.

Matriz de gestión de incidentes

Incidente	Nivel de impacto	Acción inmediata	Responsable
Virus	**Medio**	Aislar el equipo infectado, bloquear accesos y aplicar antivirus	TI
Accesos no autorizados	**Alto**	Bloqueo de usuarios y cabio de credenciales	TI
Fuga de información	**Alto**	Notificar a la dirección	Responsable del SGSI
Hackeo	**Alto**	Identificar la fuente del virus que ocasiona el hackeo	TI

Mal uso, extravío o acceso no autorizados de documentación impresa	**Medio**	Recuperación del documento si es posible, reforzar accesos de seguridad y reportar a la alta dirección	TI
Uso indebido de sistemas	**Medio**	Suspensión de accesos	TI
Phishing	**Alto**	Bloqueo del correo y alertar al personal	TI/Responsable del SGSI
Malware	**Alto**	Aislar el equipo afectado, notificar, bloquear accesos del usuario del equipo	TI
Robo o extravío de información por USB	**Medio**	Bloquear todos los puertos USB, notificar	TI
Error humano en eliminación o envío erróneo de información	**Medio**	Recuperación de la información y capacitar al personal	TI/Responsable del SGSI/RH
Falla del sistema (Interrupción de servicios)	**Medio**	Investigar la fuente y notificar	TI
Manipulación de datos de XML	**Alto**	Bloqueo del archivo y revisión	TI
Pérdida de datos por falta de respaldos	**Alto**	Backup interno	TI
Exposición de información en impresoras	**Bajo**	Retirar de forma inmediata el documento	Jefe de área
Robo o pérdida de información de dispositivos móviles	**Alto**	Bloqueo automático y cambio de accesos	TI
Suplantación (Correos falsos)	**Alto**	Bloqueo de la cuenta y notificar al personal y clientes	TI/Responsable del SGSI
Robo o extravío de token bancario	**Alto**	Bloqueo del token, notificar al banco y alta dirección	Tesorería, finanzas y dirección

Nota. Elaboración propia

Mensualmente se aplica un formulario a los colaboradores para que reporten los percances que se hayan presentado durante el mes, esto con el fin de detectar

incidentes que quizás no hayan sido reportado mediante el sistema de tickets, tal como se muestra en la figura 29.

Figura 29.

Formulario de incidentes

Nota. Elaboración propia

Una vez enviado, el responsable de seguimiento de incidentes recibe la respuesta que se observa en la figura 30. Se observa que el registro se guarda con la persona que reporta el incidente, la fecha en que sucedió, una descripción del percance, evidencia de este si se cuenta con ella y finalmente la firma del coaborador.

Figura 30.

Reporte de incidentes de seguridad

Nota. Elaboración propia

14. Mejora continua.

Con el fin de que el Sistema de Gestión de Seguridad de la Información sea eficaz y eficiente de acuerdo con los objetivos establecido con el fin de mejorar constantemente se plantean las siguientes propuestas cumpliendo con la cláusula 10 de mejora.

- Auditorías al SGSI periódicas, por lo menos una vez al año
- Informes semestrales por parte de la gerencia sobre el estado del SGSI
- Revisión y actualización de la matriz de riesgos cuando se presenten cambios en los sistemas o nuevas políticas
- Análisis del Balanced Scorecard para medir si los KPI cumplen con los objetivos esperados.

8. CONCLUSIONES Y RECOMENDACIONES.

En este apartado se exponen las conclusiones el proyecto, presentadas en función de los objetivos especifico establecidos y de los resultados obtenidos. Se obtuvo un diagnóstico conciso en el que se detectaron las áreas de oportunidad para la implementación del SGSI, el nivel de cumplimiento en cuanto seguridad de la información con el que cuenta la empresa, los principales riesgos a los que se enfrenta el área de facturación y finalmente se realizó el diseño de la propuesta del SGSI.

8.1 Conclusiones por objetivo específico.

8.1.1 Conclusión del Objetivo 1: Diagnosticar el nivel de cumplimiento actual de la empresa con respecto a los controles del Anexo A de la norma ISO/IEC 27001:2022.

Como resultado de la aplicación de entrevistas, observación directa y el checklist basado en la norma ISO/IEC 27001:2022, se determinó que el área de facturación presenta un nivel de madurez bajo en cuanto a la implementación de controles formales de seguridad de la información. Se observó que los controles relacionados con la gestión de accesos y asignación de roles muestran un nivel moderado de cumplimiento, derivado del uso de credenciales individuales; sin embargo, se identificó que no existe un procedimiento formal de revisión periódica de usuarios ni de desactivación inmediata de accesos al finalizar una relación laboral.

Asimismo, se detectó que los controles relacionados con el respaldo y cifrado de la información presentan un nivel de cumplimiento limitado, lo cual ya había ocasionado incidentes previos, como la pérdida total de información histórica en 2022. Los resultados mostraron también que los procesos de gestión de incidentes no están estructurados bajo criterios específicos de seguridad de la información, sino únicamente bajo un esquema de tickets de carácter operativos. En conjunto, estos hallazgos permitieron evaluar de manera clara el grado real de cumplimiento y evidenciar las brechas existentes en el área de facturación.

8.1.2 Identificar los principales riesgos de seguridad de la información en el proceso de facturación.

A partir de la matriz de riesgos elaborada, se identificó que los riesgos más críticos están relacionados a la exposición, corrupción o pérdida de información fiscal y aduanal. Dichos riesgos se originan principalmente por:

- Respaldos sin cifrado
- Ausencia de controles formales de continuidad del negocio
- Falta de revisión periódica de accesos
- Uso de canales no seguros para el envío de documentación
- Dependencia de plataformas externas sin supervisión documental

Asimismo, se observó que los puntos vulnerables del proceso de facturación coinciden con etapas donde se concentra un elevado flujo de información sensible, tales como la integración de documentos, emisión de CFDI y el resguardo de información en plataformas de almacenamiento en la nube.
Estos hallazgos demostraron que el riesgo empresarial no se debe únicamente a amenazas externas, sino también responde a debilidades internas y a la ausencia de procedimientos formalizados para la gestión de seguridad de la información.

8.1.3 Diseñar propuesta de medidas preventivas y correctivas que reduzcan la exposición a amenazas, basado en la norma ISO/IEC 27001:2022.

Con base en los instrumentos aplicados y en la evaluación de riesgos, se diseñaron medidas orientadas a fortalecer la seguridad del proceso de facturación, mediante la implementación gradual de controles de carácter organizativo, tecnológicos y operativos. Las medidas propuestas se enfocaron en:

- Formalizar procedimientos de respaldo y cifrado
- Implementar revisiones periódicas de usuarios y permisos
- Establecer protocolos de gestión de incidentes
- Documentar roles y responsabilidades
- Proteger la información en repositorios y canales de envío

- Mejorar las prácticas de resguardo físico de documentos

Se concluyó que dichas medidas, aun cuando representan cambios progresivos en la forma de operación del área, resultan viables para la empresa y contribuyen de manera significativa a la protección de los datos fiscales y aduanales manejados por el proceso de facturación. Estas propuestas fueron desarrolladas con base en las cláusulas más relevantes del Anexo A de la norma ISO/IEC 27001:2022, con el propósito de estructurarlas de manera organizada y documentada para su integración de la propuesta de un Sistema de Seguridad de la Información.

8.2 Conclusión general.

De manera general, se concluyó que el área de facturación de la empresa aduanera requiere fortalecer sus procesos de seguridad de la información mediante la adopción de un enfoque sistemático basado en la gestión de riesgos y en la aplicación de buenas prácticas internacionales como la norma ISO/IEC 27001:2022. El diagnóstico realizado permitió identificar debilidades relevantes en temas de respaldo de información, control de accesos, continuidad operativa y cumplimiento documental, así como la presencia de riesgos críticos que podrían afectar la disponibilidad y confidencialidad de los datos. Estos resultados muestran bases para el diseño de la propuesta del Sistema de Gestión de Seguridad de la Información y para la toma de decisiones que permitan fortalecer la protección de información en el proceso de facturación.

La propuesta desarrollada presenta un conjunto de acciones concretas, viables y alineadas a la realidad operativa de la organización, lo cual constituye un avance significativo hacia la mejora continua del proceso. El SGSI permitió tener un panorama claro sobre los pasos a seguir ante una posible contingencia, así como con una metodología definida para el manejo y protección de la información en los ámbitos internos y externos de la organización. Asimismo, la propuesta contempla políticas generales basadas en buenas prácticas de seguridad de la información, mecanismos de relación, comunicación y evaluación de proveedores, así como una gestión de riesgos e incidentes estructurada. De igual forma se fortaleció la

organización del SGSI al definir los roles y responsabilidades de las personas involucradas en el sistema, así como la evaluación de los objetivos establecidos. Adicionalmente se planteó un plan de auditoría interna que busca evaluar el seguimiento y el impacto del SGSI, la cual funciona como una herramienta de mejora continua para el proyecto, buscando corregir detalles y áreas de oportunidad que se puedan presentar en su aplicación.

El diseño del SGSI evidenció la importancia de contar con una herramienta metodológica y explicativa de procedimientos a seguir para la gestión de riesgos de seguridad de la información por medio de políticas, controles, procesos y responsabilidades claras y delimitadas. La aplicación de controles funcionó para proponer medidas de mejora de acuerdo con las necesidades y contexto de la organización, identificando debilidades y teniendo una mejor preparación ante incidentes, mejorando la imagen ante los clientes y el mercado operando con bases normativas internacionales como la norma ISO/IEC 27001:2022.

8.3 Recomendaciones.

- Ampliar el alcance del SGSI a otras áreas de la empresa para ir avanzando poco a poco hasta lograr la aplicación total.
- Utilizar la propuesta del sistema de gestión como base para obtener la certificación ISO/IEC 27001 incluyendo los ajustes necesarios para obtenerla.
- Incluir más controles del Anexo A al sistema.

9. REFERENCIAS.

(ASF), A. S. (Mayo de 2024). LINEAMIENTO PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. Obtenido de https://www.asf.gob.mx/uploads/242_transp_fraccion01/2AD3RT05_Lineamiento_seguridad.pdf

(UAA), U. A. (30 de Julio de 2024). *Seguridad digital: uno de los principales desafíos en el comercio internacional.* Obtenido de https://www.uaa.mx/portal/noticias/seguridad-digital-uno-de-los-principales-desafios-en-el-comercio-internacional/

Asociación Española de Normalización (UNE). (2023). Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos (UNE-EN ISO/IEC 27001:2023). UNE.

360, R. s. (27 de Octubre de 2024). *Las Mejores Prácticas para Garantizar la Seguridad de la Información en Empresas*. Obtenido de https://revistaseguridad360.com/noticias/ciberseguridad/las-mejores-practicas-para-garantizar-la-seguridad-de-la-informacion-en-empresas/

Andrés Diaz Artunduaga, e. a. (2023). Manual de buenas prácticas en gestión de la seguridad de los datos. Obtenido de https://repositorio.uniajc.edu.co/server/api/core/bitstreams/b62fb3bc-7e7d-431f-b65a-7f68e70bd646/content

Arias, A. M. (Agosto de 2019). *PROPUESTA DE MEJORA CONTINUA EN EL PROCESO DE PRODUCCIÓN DE UNA PLANTA DE PLÁSTICOS MEDIANTE LA METODOLOGÍA PDCA Y MANUFACTURA ESBELTA .* Obtenido de file:///C:/Users/snieblas/Downloads/ESPINOZA_ARIAS_ANTHONY_PROPUESTA_MEJORA_CONTINUA.pdf

Cely, F. U. (2021). *DIAGNOSTICO DE LA IMPLEMENTACION DE LOS CONTROLES DEL ANEXO A DE LA NORMA ISO ISO/IEC 27001 ACORDE A LA POLITICA DE SEGURIDAD DE LA INFORMACION DE LA CORPORACION DE ESPECIALISTAS DEL DOLOR.* Obtenido de https://repository.libertadores.edu.co/server/api/core/bitstreams/99fde922-620c-44d1-b210-d8552383e143/content

Coello, A. A. (2024). Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano. *Journal of Economic and Social Science Research*, 140-156.

De la Cruz Rodríguez, G., De la Cruz, R. A., & Hernández, P. (2023). Seguridad de la información en el comercio electrónico basado en ISO 27001: una revisión sistemática. Revista Innovación y Software, 4(1), 219–236.

Díaz, J. E. (2017). Armas cibernéticas. Malware inteligente para ataques dirigidos. *Revista Ingenierías USBMed*, 48-57.

Erik Gremeyer, e. a. (2022). *Guía de Implementación ISO/IEC 27001:2022.* Berlín: Capítulo de ISACA Alemania e. v.

ESET. (2025, 29 de julio). 1 de cada 4 empresas de Latinoamérica sufrió un ciberataque en el último año. https://www.eset.com/pa/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/1-de-cada-4-empresas-de-latinoam

Galaván, M. (10 de Junio de 2025). México registró 59 millones de ciberataques al día en primer trimestre del 2025: Cloudflare; phishing, la amenaza más reportada. *El universal*.

Cámara Nacional de Agentes Aduanales. (2023). Manual de procedimientos y seguridad digital en operaciones aduanales.

Centro Criptológico Nacional (CCN-CERT). (2023). Guía de seguridad: Principios básicos. Gobierno de España.

Coello, A. A. (2024). Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano. Journal of Economic and Social Science Research, 140-156.

Correa Sánchez, J. (2020). Manual de buenas prácticas en seguridad de la información para entornos hospitalarios. Universidad EIA.

Group, E. (23 de Septiembre de 2022). *Ventajas de tener un sistema de gestión de seguridad de la información*. Obtenido de ISO Tools: https://www.isotools.us/2022/09/23/ventajas-de-tener-un-sistema-de-gestion-de-seguridad-de-la-informacion/

Guacanés Castro, M. V. (2022). Propuesta de diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001: Caso de estudio de la empresa ULTRALINK [Tesis de licenciatura, Escuela Politécnica Nacional]. Repositorio Institucional EPN.

https://bibdigital.epn.edu.ec/bitstream/15000/22812/1/CD%2012289.pdf

Hernández Cabecera, M. R. (2025). Transformación digital en la aduana mexicana. Caleidoscopio, Revista de investigación en la Universidad Autónoma del Estado de Hidalgo. https://repository.uaeh.edu.mx/revistas/index.php/caleidoscopi/article/download/13789/12145/93207

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2019). Guía para la implementación del enfoque basado en procesos en los sujetos obligados.

ISO (2015). ISO 9000:2015. Quality management systems — Fundamentals and vocabulary. International Organization for Standardization. https://qpsolutions.vn/cgi-bin/document/iso9000-2015.pdf

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

ISO/IEC. (2016). *ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)*.

ISO/IEC (2022). *ISO/IEC 27001:2022. Information technology — Security techniques — Information security management systems — Requirements.* International Organization for Standardization. https://ia801902.us.archive.org/28/items/iso-iec-27001-2022-standard/ISO%20IEC%2027001%202022%20Standard.pdf

Jimenez, K. A. (2022). *IMPORTANCIA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) Y SU INCIDENCIA EN MATERIA DE CONTROL INTERNO.* Bogotá D.C.: Universidad Militar Nueva Granada.

Martinez, M. y. (2020). *CONOCER EL VALOR DE LA INFORMACIÓN (ACTIVO ECONÓMICO) PARA VALORAR LA NECESIDAD DE LA CIBERSEGURIDAD.* Obtenido de Tecnológico de Antioquia, Institución Universitaria.

Microsoft. (s.f.). *¿Qué es la seguridad de la información (InfoSec)?* Obtenido de https://www.microsoft.com/es-co/security/business/security-101/what-is-information-security-infosec?msockid=0571c6752258652e2244d006237e64e5

Muñoz, A. M. (2018). DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA AGENCIA DE ADUANAS MOVE CARGO S.A. NIVEL 1. *UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD ESCUELA DE CIENCIAS BASICAS, TECNOLOGICAS E INGENIERÍA ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA*.

NMK-I-27002-NYCE-2015, N. M. (s.f.). *Tecnologías de la información, Técnicas de seguridad, Código de buenas prácticas para el control de la seguridad de la información.* Obtenido de

https://it.uat.edu.mx/TSI/Documents/legislaciones/NMX-I-27002-NYCE-2015_UAT.pdf

Peña, R. L. (2016). *Diseño de un Sistema de Gestión de Seguridad de la Información basado en las Normas ISO/IEC 27001 e ISO/IEC 27002 para proteger los activos de información en el proceso de suministros de medicamentos de la Red de Salud de Lambayeque 2015.* Lambayeque: UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO.

Pérez, P. y. (2021). Gestión estratégica del riesgo y su importancia en las buenas prácticas empresariales. *ERUDITUS*, 9-24.

Pozo Hernández, C. G., Reascos Pinchao, R. S., & Minaya Macías, R. W. (2025). Fundamentos de seguridad informática y ciberseguridad. Ediciones GESICAP.

Salvador Montesinos González, e. a. (2020). Mejora Continua en una empresa en México: estudio desde el ciclo Deming. Revista Venezolana de Gerencia (RVG), 1863-1883.

Sánchez, J. J. (2020). *MANUAL DE BUENAS PRÁCTICAS EN SEGURIDAD DE LA INFORMACIÓN PARA ENTORNOS HOSPITALARIOS.* Obtenido de file:///C:/Users/snieblas/Downloads/CorreaJuan_2020_ManualBuenasPracticas.pdf

SAT. (22 de Junio de 2017). Obtenido de http://omawww.sat.gob.mx/informacion_fiscal/factura_electronica/Paginas/requisitos_factura_electronica_cfdi.aspx

SAT. (s.f.). *Guía de llenado de los comprobantes fiscales digitales por Internet*. Obtenido de http://omawww.sat.gob.mx/tramitesyservicios/Paginas/documentos/GuiaAnexo20.pdf

Secretaría de Economía. (2016). NMX-R-026-SCFI-2016, servicios aduanales—calidad de los servicios proporcionados por el agente aduanal (calidad del

agente aduanal)—requisitos. https://www.claa.org.mx/phocadownload/nmx-r-026-scfi-2016.pdf

Servicio de Administración Tributaria (SAT). (2023). Guía de llenado del Comprobante Fiscal Digital por Internet (CFDI) 4.0. SAT México.

STIC. (8 de Mayo de 2023). *Confidencialidad, Integridad y Disponibilidad*. Obtenido de https://ciberseguridad.comillas.edu/confidentiality-integrity-and-availability/

UNIÓN, C. D. (22 de Diciembre de 2020). *LEY ADUANERA.* Obtenido de https://www.diputados.gob.mx/LeyesBiblio/pdf/LAdua.pdf

Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security. Cengage Learning.

10. ANEXOS.

A.1 Entrevista 1

Objetivo: Identificar prácticas actuales de seguridad de la información.

Dimensiones: Gestión de accesos, respaldo de datos, controles físicos, políticas internas.

Escala: Preguntas abiertas más preguntas dicotómicas.

Nombre: René Leyva

Puesto: Analista de facturación

1. Organización y políticas de seguridad (A.5, A.6)

1. ¿Existe una política formal de seguridad de la información aplicable al área de facturación?

Escala: 0 = No existe | **1 = Existe, pero no se aplica** | 2 = Existe y se aplica regularmente.

Existe una general, más no una enfocada al área de facturación

2. ¿El personal de facturación ha firmado acuerdos de confidencialidad?

Escala: **Sí** / No.

Por medio de un contrato

3. ¿El aviso de privacidad incluye el uso de datos en facturación y aduanas?

Escala: Sí / No / **Parcialmente**.

Aduana si se mencionada, pero específicamente facturación no

2. Gestión de accesos y control de usuarios (A.9, A.5.17)

4. ¿Cada usuario tiene un acceso individual y único al sistema de facturación?

Escala: **Sí** / No.

Para cada plataforma se necesita ingresar usuario y contraseña

5. ¿Se aplican roles y permisos diferenciados (ej. quien captura no puede autorizar ni cancelar)?

Escala: 0 = No | 1 = Parcial | 2 = **Sí, completamente**.

No todos tienen los mismos permisos para ciertas operaciones

6. ¿Se bloquean accesos cuando un empleado deja la empresa o cambia de puesto?

Escala: **Sí** / No.

Se dejan aproximadamente dos meses por si se requiere.

7. ¿Se revisa periódicamente la lista de usuarios activos en el sistema?

Escala: Nunca / **Ocasionalmente** / Regularmente.

3. Seguridad en operaciones y respaldos (A.8, A.12)

8. ¿Existen controles de seguridad informática (ej. respaldo, encriptación, acceso restringido)?

Escala: 0 = No implementado | 1 = Parcial | **2 = Implementado**.

9. ¿Los respaldos están cifrados y almacenados en un sitio seguro (local o nube confiable)?

Escala: **Sí** / No / Parcialmente.

Se tienen en la nube y plataformas.

10. % de cumplimiento de respaldos realizados conforme a lo planificado.

Escala: (0–25% / 26–50% / **51–75%** / 76–100%).

4. Protección de la información y documentos (A.7, A.8, A.11)

11. ¿Las facturas y pedimentos se almacenan de manera segura y controlada?

Si, porque se almacenan en sistemas propios de manera digital y físico de acuerdo con la ley.

12. ¿Se cuenta con medidas de resguardo de documentos físicos (archivadores cerrados, acceso limitado)?

Si, se cuentan con bodegas a las que pueden ingresar solo personal autorizado.

13. ¿Se emplean certificados digitales (ej. sellos SAT, otros certificados en sistemas web)?

Escala: **Sí** / No / En proceso.

5. Capacitación y concienciación (A.6.3, A.6.7)

14. ¿El personal está capacitado para el uso y manejo de información sensible?

Escala: Nunca / Una vez / **Periódicamente**.

Cada dos meses.

15. ¿El personal de facturación recibe capacitación periódica en protección de datos y confidencialidad?

Escala: **Sí** / No.

Cada 4 meses.

Las sesiones que se manejan se enfocan más al seguimiento de lo visto, más no se brinda información nueva.

6. Gestión de incidentes (A.16)

16. ¿Se documentan y atienden incidentes de seguridad de la información?

Escala: **Sí** / No / Parcialmente.

Hubo un incidente donde toda la información digital se perdió de la plataforma RITS, tanto del sistema como de la nube, no se pudo recuperar, pero se contaba con la información física.

17. ¿El personal sabe cómo reportar un incidente de seguridad de la información?

Escala: **Sí** / No.

Se reporta mediante un ticket al área de sistemas para darle seguimiento al problema.

18. Nº de incidentes de seguridad en facturación en el último año.

Escala: Numérica. 0

19. % de accesos no autorizados detectados.

Escala: Numérica. 0%

20. Tiempo promedio de respuesta a incidentes.

Escala: Minutos / **Horas** / Días.

7. Controles físicos (A.7.5, A.11)

21. ¿El área de facturación tiene controles físicos (acceso restringido, cámaras, cerraduras)? Si, se cuenta con cámaras y accesos a través de credenciales.

22. ¿Los equipos donde se emiten facturas están protegidos contra accesos no autorizados?

Escala: **Sí** / No / Parcial.

Se bloquea el equipo al tercer intento si no es el correcto.

8. Relación con clientes y proveedores (A.5.7, A.5.23)

23. ¿Cómo es el acercamiento de los clientes con la empresa?

El vendedor se acerca a la empresa en su mayoría ofreciendo el servicio de agencia aduanal para importaciones o exportaciones.

24. ¿Existen filtros que utilicen para la admisión de un cliente? ¿Cuáles?

Se cuenta con un check list para cada tipo de servicio con requisitos que el cliente debe cumplir para ser parte de la cartera.

Filtros:

-Información preliminar (incluir datos como razón social, RFC, dirección fiscal, contacto principal y página web)

-Verificación (antisoborno, anticorrupción, certificaciones)

-Criterios de exclusión (se excluyen automáticamente empresas que: 1. Atenúen contra derechos humanos o laborales, 2. Estén involucrados en actividad ilícitas, 3. No textiles

Se anexan dos check list de ejemplo.

25. ¿Qué tipo de datos personales solicitan a los clientes?

Celular, correo, comprobante de domicilio, INE (check list)

26. ¿Existen lineamientos para el manejo de datos fiscales y aduanales sensibles?

Escala: **Sí** / No.

1. Protección de datos en pedimentos y transmisiones eléctricas

2. los datos contenidos en los pedimentos deben ser transmitidos electrónicamente media te sistemas autorizados.

A.2 Entrevista 2

Objetivo: Identificar prácticas actuales de seguridad de la información.

Dimensiones: gestión de accesos, respaldo de datos, controles físicos, políticas internas.

Escala: Preguntas abiertas más preguntas dicotómicas.

Nombre: Melissa Cota

Puesto: (IT Project Leader & Automation)

1. Organización y políticas de seguridad (A.5, A.6)

4. ¿Existe una política formal de seguridad de la información aplicable al área de facturación?

   Escala: 0 = No existe | 1 = Existe, pero no se aplica | **2 = Existe y se aplica regularmente.**

   Existe una política de seguridad en la información solo que es general, no está basado en un área en específico.

5. ¿El personal de facturación ha firmado acuerdos de confidencialidad?

   Escala: **Sí** / No.

   En cada contrato laboral se firma un acuerdo de confidencialidad

6. ¿El aviso de privacidad incluye el uso de datos en facturación y aduanas?

   Escala: Sí / No / **Parcialmente**.

Facturación no

2. Gestión de accesos y control de usuarios (A.9, A.5.17)

8. ¿Cada usuario tiene un acceso individual y único al sistema de facturación?

   Escala: **Sí** / No.

Cada usuario cuenta con sus accesos exclusivos para el ingreso a cada plataforma

9. ¿Se aplican roles y permisos diferenciados (ej. quien captura no puede autorizar ni cancelar)?

   Escala: 0 = No | 1 = Parcial | **2 = Sí, completamente.**

   En cada sistema se lleva la configuración de roles y permisos para cada colaborador de la empresa dependiendo de su puesto es como se da la autorización

10. ¿Se bloquean accesos cuando un empleado deja la empresa o cambia de puesto?

    Escala: **Sí** / No.

    Cuando el usuario deja la empresa se desactivan los accesos del excolaborador y en otros casos incluso aplica cambios de contraseñas en sistemas.

    Para cambios de puesto se mantienen accesos ya que aún es colaborador en la empresa más sin embargo se cambian los roles.

11. ¿Se revisa periódicamente la lista de usuarios activos en el sistema?

    Escala: Nunca / **Ocasionalmente** / Regularmente.

3. Seguridad en operaciones y respaldos (A.8, A.12)

11. ¿Existen controles de seguridad informática (ej. respaldo, encriptación, acceso restringido)?

    Escala: 0 = No implementado | 1 = Parcial | **2 = Implementado**.

    Se tiene un control de accesos restringido para información más confidencial, así como también se realizan respaldos de la información de los diferentes sistemas con los que se cuentan

12. ¿Los respaldos están cifrados y almacenados en un sitio seguro (local o nube confiable)?

    Escala: Sí / No / **Parcialmente.**

13. % de cumplimiento de respaldos realizados conforme a lo planificado.

    Escala: (0–25% / 26–50% / **51–75%** / 76–100%).

4. Protección de la información y documentos (A.7, A.8, A.11)

11. ¿Las facturas y pedimentos se almacenan de manera segura y controlada?

    Si, está documentación solo se encuentra dentro de los sistemas internos de los cuales estos mismos cuentan con seguridad en sus accesos.

12. ¿Se cuenta con medidas de resguardo de documentos físicos (archivadores cerrados, acceso limitado)?

    Si, se tiene cierta documentación en la empresa y se cuenta con bodegas con acceso controlado a ciertas personas.

13. ¿Se emplean certificados digitales (ej. sellos SAT, otros certificados en sistemas web)?

    Escala: **Sí** / No / En proceso.

    Si, Cuentan con firmas digitales y certificados de seguridad implementados tanto en los sistemas internos como en las páginas web.

5. Capacitación y concienciación (A.6.3, A.6.7)

15. ¿El personal está capacitado para el uso y manejo de información sensible?

    Escala: Nunca / Una vez / **Periódicamente.**

    Si, se realizan cursos periódicamente sobre la seguridad de la información creando conciencia en el personal.

16. ¿El personal de facturación recibe capacitación periódica en protección de datos y confidencialidad?

Escala: **Sí** / No.

Si, son capacitaciones periódicas donde se refuerza la información brindada anteriormente y en caso de alguna actualización se notifica.

6. Gestión de incidentes (A.16)

17. ¿Se documentan y atienden incidentes de seguridad de la información?

    Escala: **Sí** / No / Parcialmente.

    Si, se atienden en base al seguimiento de tickets y en caso de ser muy grande la incidencia también se involucra el área de calidad documentado todo el detalle.

18. ¿El personal sabe cómo reportar un incidente de seguridad de la información?

    Escala: **Sí** / No.

Si, se cuenta con un sistema llamado helpdesk donde se levantan tickets de incidencias y el equipo de tecnología es quien apoya en solventarlas.