UNIVERSIDAD DEL PACÍFICO | Contabilidad
Facultad de Ciencias Empresariales

EL ANÁLISIS DE LOS RIESGOS DE SEGURIDAD DURANTE LA ENTRADA DE DATOS EN EL SISTEMA CONTABLE QUICKBOOKS PARA LA EMPRESA SOUTH STAR BATTERY METALS CORP.

Trabajo de Suficiencia Profesional
presentado para optar al Título Profesional de
Contadora Pública

Presentado por
Melissa Fernanda Berrocal Bendezú

Asesor: Mario Alberto Yáñez Quiroz
0009-0009-1615-1237

Lima, junio de 2025

UNIVERSIDAD DEL PACÍFICO

REPORTE DE EVALUACIÓN DEL SISTEMA ANTIPLAGIO

FACULTAD DE CIENCIAS EMPRESARIALES

A través del presente, la Facultad de Ciencias Empresariales deja constancia de que el Trabajo de Suficiencia Profesional titulado: "El análisis de los riesgos de seguridad durante la entrada de datos en el Sistema Contable QuickBooks para la empresa South Star Battery Metals Corp"; presentado por doña MELISSA FERNANDA BERROCAL BENDEZU, con DNI N° 72472522, para optar al Título Profesional de Contadora Pública, fue sometido al análisis del sistema antiplagio Turnitin el 9 de abril de 2025. El siguiente fue el resultado obtenido:

Visualizador de documentos

Turnitin Informe de Originalidad

Procesado el: 23-jun-2025 19:08 -05
Identificador: 2704998133
Número de palabras: 22475
Entregado: 1

Berrocal, Melissa_Trabajo de suficiencia prof... Por Melissa Fernanda Berrocal Bendezu

Índice de similitud	Similitud según fuente	
11%	Fuentes de Internet:	10%
	Publicaciones:	1%
	Trabajos del estudiante:	2%

De acuerdo con la política vigente, el porcentaje obtenido de similitud con otras fuentes está dentro de los márgenes permitidos.

Se emite el presente documento para los fines estipulados en el Reglamento de Grados y Títulos de Pregrado.

Lima, 2 de julio de 2025

Karen Weinberger
Decana
Facultad de Ciencias Empresariales

RESUMEN

Esta investigación, enfocada en la empresa South Star Battery Metals Corp., tuvo como objetivo analizar los riesgos de seguridad durante la fase de entrada de datos en el sistema contable QuickBooks Online y proponer estrategias de mitigación efectivas. Se empleó una metodología cualitativa con enfoque descriptivo, adecuada ante la limitada disponibilidad de estudios previos sobre esta problemática.

La recolección de información se basó en tres técnicas principales: una encuesta aplicada a 10 contadores con experiencia directa en el uso de QuickBooks Online, entrevistas semiestructuradas, y el análisis de 114 incidencias extraídas de plataformas oficiales de soporte y foros de usuarios.

Los resultados evidenciaron que la fase de entrada de datos representa el punto más vulnerable del sistema, debido a su elevada exposición a amenazas como el phishing, la suplantación de identidad y el fraude digital. Entre los riesgos más reportados se encuentran: (1) correos electrónicos manipulados que contienen enlaces maliciosos o solicitudes fraudulentas; (2) llamadas telefónicas de individuos que se hacen pasar por personal técnico de QuickBooks, con el fin de obtener credenciales o realizar cobros indebidos; y (3) ventanas emergentes fraudulentas dentro del sistema, diseñadas para inducir al usuario a ejecutar acciones perjudiciales.

ABSTRACT

This research, focused on South Star Battery Metals Corp., aimed to analyze security risks during the data entry phase in the QuickBooks Online accounting system and to propose effective mitigation strategies. A qualitative methodology with a descriptive approach was applied, appropriate given the limited availability of prior studies addressing this specific issue.

Information was gathered using three main techniques: a survey administered to 10 accountants with direct experience using QuickBooks Online, semi-structured interviews, and an analysis of 114 incident reports extracted from official support platforms and user forums.

The findings revealed that the data entry phase is the most vulnerable point within the system, primarily due to its exposure to threats such as phishing, identity theft, and digital fraud. The most frequently reported risks include: (1) manipulated emails containing malicious links or fraudulent requests; (2) phone calls from individuals posing as QuickBooks support staff to obtain credentials or execute unauthorized charges; and (3) fraudulent pop-up windows within the system, designed to deceive users into taking harmful actions.

TABLA DE CONTENIDO

RESUMEN iii

ABSTRACT iv

ÍNDICE DE TABLAS viii

ÍNDICE DE FIGURAS ix

ÍNDICE DE ANEXOS x

INTRODUCCIÓN 1

CAPÍTULO I. planteamiento del problema 2

1.1 La empresa 2

1.1.1 Valores 3

1.1.2 Políticas 4

1.1.3 Estructura organizacional 4

1.2 Planteamiento del problema 6

1.3 Objetivos 8

1.3.1 Objetivo general: 8

1.3.2 Objetivos específicos: 8

1.4 Alcance 8

1.4.1 Alcance teórico 8

1.4.2 Alcance práctico 9

1.5 Metodología 9

CAPÍTULO II. marco de referencia 9

2.1 Los Sistemas de Información Contable 9

2.1.1 Definición de los Sistemas de Información 9

2.1.2 Etapas de los Sistemas de Información 10

2.1.3 Importancia de los Sistemas de Información Contable (SIC) en la gestión contable y tributaria 12

2.2 QuickBooks Online en el entorno empresarial 13

2.2.1 Características técnicas de QuickBooks Online.....13

2.2.2 Uso de QuickBooks Online para pequeñas y medianas empresas 15

2.3 Riesgos en la entrada de datos en sistemas contables 16

2.3.1 Errores humanos que incrementan la vulnerabilidad en la fase de entrada de datos 17

2.3.2 Errores técnicos, procedimentales y de gestión que incrementan la vulnerabilidad en la fase de entrada de datos 18

2.3.3 Datos que evidencian la debilidad en la fase de entrada de datos en los Sistemas Informáticos Contables.....19

2.4 Amenazas de seguridad de los Sistemas Informáticos Contables en la nube como QuickBooks Online 20

2.5 Principios de Seguridad de la Información: Tríada CIA 22

CAPÍTULO III. propuesta.....24

3.1 Fase 1: Selección de los riegos específicos asociados a la interacción del usuario durante el proceso de ingreso de datos.....24

3.1.1 Documentación y fuentes secundarias 24

3.1.2 Entrevistas 25

3.1.3 Encuestas 26

3.1.4 Matriz de riesgos.....28

3.1.5 Resultados.....31

3.2 Fase 2: Diseñar un plan de contingencia que incluya estrategias específicas para mitigar las vulnerabilidades y riesgos vinculados a la etapa de ingreso de datos por parte del usuario en el sistema contable QuickBooks.....32

3.2.1 Manual de procedimientos.....33

3.2.2 Normas de gestión y seguridad de la información 36

3.2.3 Norma para la Gestión de Incidentes de Seguridad de la Información...40

3.2.4 Norma para medidas de respaldo y recuperación de información 46

3.2.5 Norma para la gestión del recurso humano en relación con el uso de activos de información 48

CONCLUSIONES 51

RECOMENDACIONES 53

Bibliografía 55

ANEXOS 69

ÍNDICE DE TABLAS

Tabla 1. Plan comercial con proyección de oferta de productos de grafito en 5 a 7 años 2
Tabla 2. Clasificación de riesgos en QuickBooks Online y sus impactos 21
Tabla 3. Verificación de la tríada CIA en el Sistema Contable en línea QuickBooks ..23
Tabla 4. Los riesgos más relevantes en QuickBooks Online 25
Tabla 5. Riesgos reportados por usuarios de QuickBooks 26
Tabla 6. Profesionales que realizaron la encuesta 27
Tabla 7. Nivel de probabilidad.....28
Tabla 8. Nivel de impacto 28
Tabla 9. Clasificación 29
Tabla 10. Matriz de riesgo de los riesgos de QuickBooks Online 29
Tabla 11. Nivel de riesgo y clasificación 30
Tabla 12. Planificar, Hacer, Verificar, y Actuar 34
Tabla 13 Roles y responsabilidades para el manual de procedimientos 36
Tabla 14. Alineación de la norma de gestión y seguridad de la información y la tríada CIA.....39
Tabla 15. Alineación de la norma Gestión de incidentes de seguridad con la tríada CIA 41
Tabla 16. Alineación de la norma medidas de respaldo y recuperación de información contable con la tríada CIA 47
Tabla 17 Alineación de la norma Gestión del recurso humano y activos de información con la tríada CIA.....49

ÍNDICE DE FIGURAS

Figura 1. Junta Directiva de South Star Battery Metals Corp. 5
Figura 2. Área administrativa de South Star Battery Metals Corp. 5
Figura 3. Etapas del proceso del Sistema de Información.....11
Figura 4. Área administrativa de South Star Battery Metals Corp. 35
Figura 5. Flujograma de acciones a tomar si se reciben correos sospechosos 43
Figura 6. Flujograma de acciones a tomar si se reciben llamada sospechosa de falsos técnicos de soporte.....44
Figura 7. Flujograma de acciones a tomar si se reciben llamada ventana emergente en la plataforma de QuickBooks 45
Figura 8. Proceso para restauración automatización 47
Figura 9. Proceso para restauración manual 47

ÍNDICE DE ANEXOS

Anexo 1. Términos y condiciones relevantes de QuickBooks en línea.....70
Anexo 2. Errores y factores que incrementan la vulnerabilidad de la entrada de datos .71
Anexo 3. Riesgos encontrados en la página oficial de soporte de QuickBooks.....71
Anexo 4. Persona comparte una experiencia de estafa por parte de un trabajador de la plataforma de QuickBooks 74
Anexo 5. Cliente en Reddit comparte su molestia respecto a una ventana emergente producida por QuickBooks 75
Anexo 6. Cliente en Reddit comparte una transacción fraudulenta de la nómina de sueldos de QuickBooks.....75
Anexo 7. Riesgos cuantificados.....76
Anexo 8 Guías de entrevistas 77
Anexo 9. Transcripción resumida de entrevistas semiestructuradas 78
Anexo 10. Perfil de usuario 79
Anexo 11. Riesgos de seguridad y fraude 80
Anexo 12. Riesgo de visualización y reportes.....80
Anexo 13. Riesgos en la plataforma y automatizaciones 81
Anexo 14.¿Cómo calificarías tu experiencia general con QuickBooks?.....81
Anexo 15. Ejemplo de información bancaria de clientes de South Star Battery Metals Corp. 82
Anexo 16. Estado de Posición Financiera de South Star Battery Metals Corp a Setiembre 2024 83
Anexo 17. Estado de Flujo de Caja de South Star Battery Metals Corp a Setiembre 2024 84
Anexo 18 Ejemplo de Acuerdo de Confidencialidad entre South Star Mining Corp. y los usuarios 85
Anexo 19. Exportar automática o manualmente información de respaldo de QuickBooks en línea.....86

INTRODUCCIÓN

En un contexto empresarial cada vez más digitalizado, las organizaciones requieren herramientas contables que no solo optimicen la gestión financiera, sino que también garanticen la protección de la información registrada. Una de las soluciones más empleadas por pequeñas y medianas empresas es QuickBooks Online, debido a su facilidad de uso, capacidad de integración con otras plataformas y disponibilidad en la nube. Según Latimer (2024), aproximadamente el 82 % de las pymes en Estados Unidos utilizan esta herramienta, lo que evidencia su fuerte penetración en el mercado. Sin embargo, esta creciente adopción también ha expuesto vulnerabilidades críticas en materia de seguridad de la información.

Diversos estudios (Action1 Corporation, 2025; Proofpoint, 2024) advierten que una parte significativa de los incidentes registrados en plataformas contables se origina durante la interacción del usuario con el sistema, en especial durante la fase de entrada de datos. Esta etapa, que constituye el primer punto de contacto entre el usuario y el software, implica la recopilación, validación y registro de la información financiera. Por tanto, errores humanos, ataques de phishing y accesos no autorizados se consolidan como riesgos persistentes en organizaciones que no disponen de políticas claras de ciberseguridad.

En particular, se ha identificado que las amenazas más frecuentes en QuickBooks Online incluyen: (1) correos electrónicos manipulados, diseñados para engañar a los usuarios mediante enlaces maliciosos o solicitudes fraudulentas; (2) llamadas telefónicas realizadas por falsos técnicos, que simulan ser personal de soporte para obtener credenciales o generar cobros indebidos; y (3) ventanas emergentes fraudulentas, que aparecen dentro del sistema con enlaces o contactos alterados que inducen a realizar acciones perjudiciales.

Este trabajo se fundamenta en el marco normativo ISO/IEC 27001 y en principios de ciberseguridad como la tríada CIA (Confidencialidad, Integridad y Disponibilidad), con el fin de ofrecer una propuesta de mejora aplicable y realista para empresas de tamaño y complejidad similares. Asimismo, se destaca el rol del contador como figura clave en la protección de la información financiera, en un entorno donde la seguridad digital no es una opción, sino una exigencia estratégica.

CAPÍTULO I. PLANTEAMIENTO DEL PROBLEMA

1.1 La empresa

South Star Battery Metals Corp. es una empresa que tiene como finalidad seleccionar y desarrollar proyectos de corto plazo que crean valor en el sector de metales industriales y baterías (South Star Battery Metals Corp. , s.f.). Opera en el sector de materiales dentro de la industria minera, clasificada como de pequeño tamaño dada su nómina promedio de 12 colaboradores (TMX Money, 2025). La organización se dedica al desarrollo de proyectos de metales para baterías localizados en el continente americano, mediante una estrategia de selección adquisitiva y el desarrollo de proyectos a corto plazo (OTC Markets, 2025). Fundada en 1984 en Vancouver, Columbia Británica, la empresa fue listada en el TSX Venture Exchange (TSXV: STS) en Canadá en 2017 y, posteriormente, en el OTC Bulletin Board (OTC: STSBF) en los Estados Unidos en 2018 (SEDAR+, 2025) Actualmente, cuenta con dos proyectos principales ubicados en Bahía, Brasil, y Alabama, Estados Unidos.

El proyecto Santa Cruz Graphite Mine, localizado en Brasil, se proyecta como pionero en la producción de grafito en las Américas desde 1996 y se sitúa en el segundo país con mayor producción de grafito a nivel mundial (South Star Battery Metals Corp., 2025). La fase de producción se inició en el cuarto trimestre de 2024, con planes de completar la segunda fase en 2027 y la última en 2028. La empresa posee un plan comercial que ofrece un portafolio diversificado para distintos sectores, con el objetivo de satisfacer la demanda global de grafito en aplicaciones como refractarios, lubricantes, productos de fricción, láminas y aceros de alta resistencia, con un valor estimado entre 500 y 3000 USD por tonelada. Adicionalmente, los productos destinados a baterías tradicionales y de litio (LiB), dispersiones y grafeno se valorizan entre 3500 y 12000 USD por tonelada (South Star Battery Metals, 2024).

Tabla 1. Plan comercial con proyección de oferta de productos de grafito en 5 a 7 años

Aplicación industrial	Aplicaciones con valor agregado
Aceros de alta resistencia	Baterías tradicionales
Refractarios	Baterías de ion de litio
Productos de fricción	Expansibles
Lubricantes	Polvos/Dispersiones

Nota. South Star Battery Metals Corp. (2025). *Plan comercial de 5 a 7 años de venta de productos de grafito: febrero 2025*. Obtenido de https://www.southstarbatterymetals.com/ydihapto/2025/03/STS-02_2025_ND_R1.pdf

Se proyecta que Santa Cruz Graphite experimentará un crecimiento en sus ingresos de 15 millones de USD a finales de 2025 a 90 millones de USD para 2029 (500%) (South Star Battery Metals, 2024). De acuerdo con el Banco Mundial (2020), la demanda global de grafito crecerá en promedio un 400% debido a la transición de baterías convencionales a baterías de litio y al aumento en la demanda de vehículos eléctricos. Se estima un incremento en la demanda de 1,100,000 toneladas en 2022 a 7,210,000 toneladas en 2035 (South Star Battery Metals, 2024).

Por otro lado, el proyecto BamaStar, ubicado en Alabama, Estados Unidos, se encuentra aún en fase exploratoria, donde se llevarán a cabo diversas pruebas como perforación diamantina, ensayos metalúrgicos y estimación de recursos. Al igual que Santa Cruz Graphite, se anticipa el hallazgo de cantidades significativas de grafito, con una producción promedio estimada de 25,000 toneladas para 2027 y 50,000 toneladas para 2029 (South Star Battery Metals, 2024). Además, se planea una inversión en la planta de ánodo en los Estados Unidos entre 2027 y 2029. Actualmente, la empresa continúa fortaleciendo y desarrollando relaciones con las comunidades locales y las agencias gubernamentales.

1.1.1 Valores

South Star Battery Metals Corp. integra los Objetivos de Desarrollo Sostenible (ODS) en su proyecto Santa Cruz Graphite. Su compromiso se manifiesta en la erradicación de la pobreza mediante la contratación equitativa, salarios dignos y la generación de empleo directo e indirecto. Adicionalmente, promueve la seguridad alimentaria a través de la provisión de comidas y la redistribución de excedentes a la comunidad local. En el ámbito de la salud, la empresa ofrece exámenes médicos, seguros de salud y apoyo para abordar problemas de salud mental (South Star Mining Corp., 2015).

En relación con la sostenibilidad, la organización fomenta el acceso a energía limpia, minimiza el uso de agua y promueve el reciclaje. Asimismo, busca reducir las desigualdades mediante la inclusión en cadenas de suministro y la contratación

equitativa. En cuanto a infraestructura, comparte recursos como carreteras y energía con la comunidad. La compañía mantiene una política de transparencia, cumplimiento normativo y monitoreo ambiental continuo. Finalmente, refuerza su compromiso con la justicia, la gobernanza ética y la colaboración con organizaciones clave para la consecución de los ODS (South Star Mining Corp., 2015).

1.1.2 Políticas

South Star Battery Metals Corp. alinea sus operaciones mineras con los Objetivos de Desarrollo Sostenible (ODS) mediante la implementación de prácticas de contratación equitativa, la adopción de salarios justos y la generación de empleo. La empresa asegura la seguridad alimentaria para sus empleados y las comunidades circundantes, promueve el acceso a la salud y fortalece la educación a través de programas de capacitación. Adicionalmente, prioriza la sostenibilidad mediante el uso de energías renovables, el reciclaje de agua y la minimización del impacto ambiental. Cabe destacar que Brasil obtiene el 80% de su electricidad de fuentes renovables, lo que favorece la demanda de grafito en sectores clave como baterías de alta tecnología, siderurgia, fundiciones, lubricantes, electrónica y la industria automotriz (South Star Battery Metals, 2024).

Para reforzar su compromiso con la responsabilidad social y el desarrollo sostenible, la empresa ha implementado políticas integrales de ética, diversidad, anticorrupción, denuncia de irregularidades y seguridad laboral. Su código de conducta empresarial promueve un comportamiento ético en todas sus operaciones, mientras que la política anticorrupción prohíbe de manera explícita el soborno (South Star Battery Metals Corp., 2022a). La política de diversidad fomenta la inclusión en los procesos de contratación y en los niveles de liderazgo (South Star Battery Metals Corp., 2022b), y la política de denuncias establece mecanismos para proteger a aquellos que reportan malas prácticas (South Star Battery Metals Corp., 2022c). Asimismo, la política de salud y seguridad enfatiza la prevención de accidentes laborales y el estricto cumplimiento de las normativas vigentes. Estas políticas, en su conjunto, consolidan el compromiso de la empresa con la responsabilidad social y el desarrollo sostenible.

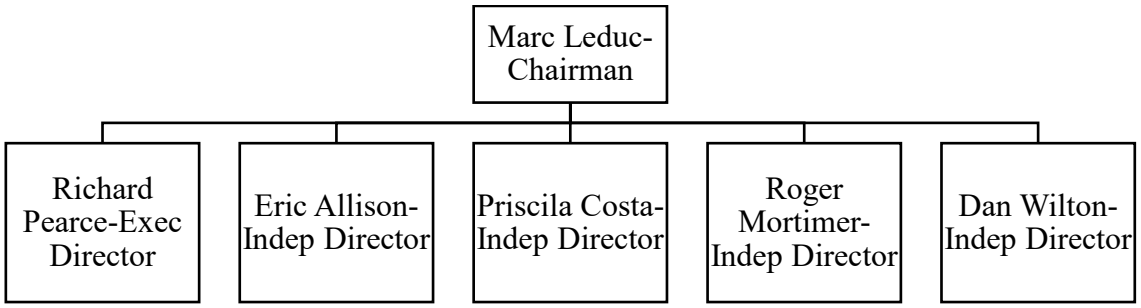
1.1.3 Estructura organizacional

La estructura organizacional de South Star Battery Metals Corp. se divide en dos categorías principales: la junta directiva y la parte administrativa. Cabe resaltar que

ambos equipos se involucran constantemente en la toma de decisiones empresariales para impulsar los proyectos mencionados. La planilla está compuesta por únicamente por el área administrativa,

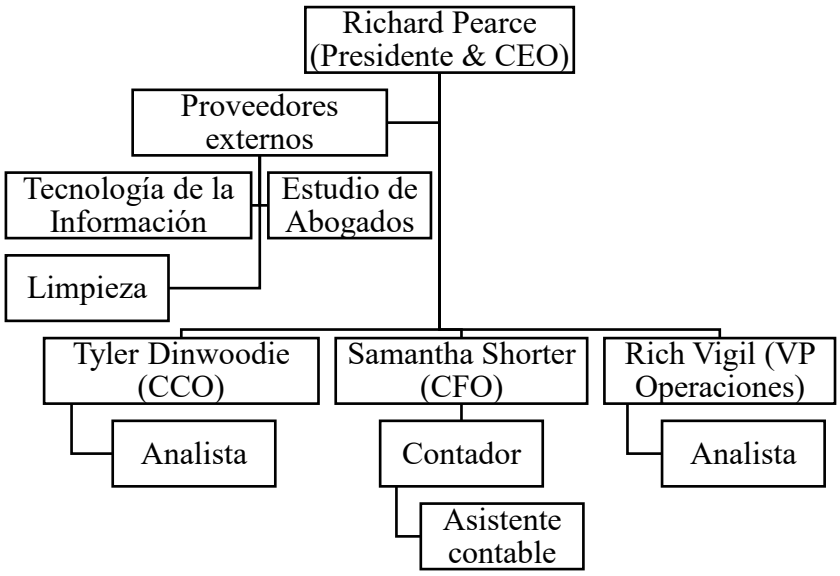
Por otro lado, la empresa cuenta con una limitada dotación de personal, particularmente en la parte administrativa, la cual se enfoca principalmente en labores operativas. Se anticipa que, una vez iniciada la fase de producción a gran escala, la empresa podrá considerar la expansión de sus diversas áreas para hacer frente al aumento de las operaciones y la contratación de nuevo personal.

Figura 1. Junta Directiva de South Star Battery Metals Corp.



Nota. Adaptado de Estructura organizacional de South Star Battery Metals Corp: Febrero 2025, por South Star Battery Metals Corp., 2025, https://www.southstarbatterymetals.com/ydihapto/2025/03/STS-02_2025_ND_R1.pdf. Copyright 2025 por South Star Battery Metals Corp.

Figura 2. Área administrativa de South Star Battery Metals Corp.



Nota. Adaptado de Estructura organizacional de South Star Battery Metals Corp: Febrero 2025, por South Star Battery Metals Corp., 2025,

https://www.southstarbatterymetals.com/ydihapto/2025/03/STS-02_2025_ND_R1.pdf. Copyright 2025 por South Star Battery Metals Corp.

Por último, es importante señalar que la empresa cuenta con proveedores externos para atender casos puntuales vinculados a asuntos legales, servicios tecnológicos y limpieza. La tercerización de estos servicios permite a la organización reducir costos operativos y obligaciones laborales, ya que el tamaño actual de la empresa no justifica la contratación de personal adicional para funciones administrativas (Shorter, 2025).

1.2 Planteamiento del problema

En la actualidad, las empresas requieren sistemas contables confiables que garanticen una clara diferenciación entre los gastos personales y los empresariales, aspecto esencial para una adecuada gestión tributaria. Entre los diversos softwares contables disponibles, QuickBooks se ha consolidado como una de las herramientas más utilizadas a nivel mundial, especialmente por pequeñas y medianas empresas. De acuerdo con Ha (2024), la plataforma mantiene una participación de mercado cercana al 60%; en Estados Unidos, el 82% de las pequeñas empresas la utilizan (Latimer, 2024), y a nivel global el 56% de los trabajadores autónomos también optan por este sistema (Yoder & Ruiz, 2024).

A pesar de su popularidad y facilidad de uso, QuickBooks Online enfrenta desafíos sustanciales en materia de seguridad, especialmente debido a la exposición de información financiera en entornos digitales. Según Fuesz (2023), aproximadamente el 85 % de los incidentes de seguridad en plataformas contables se deben a errores humanos, omisión de actualizaciones o fraudes de tipo phishing, lo que constituye una amenaza persistente para la integridad de los datos financieros. Además, las vulnerabilidades críticas de los softwares, tanto en ataque a base de datos y sistemas operativos, se han incrementado en un promedio de 37% respecto al 2024 (Action1 Corporation, 2025).

La página oficial de Intuit QuickBooks reportó que, entre 2020 y 2024, aproximadamente el 27% de los incidentes registrados en su plataforma de soporte estuvieron relacionados con ataques de phishing, hacking y fraudes digitales (Intuit QuickBooks, 2025). Estas amenazas incluyen suplantación de identidad, accesos no autorizados y transacciones ilícitas. Además, los entornos en la nube conllevan riesgos inherentes como errores humanos, vulnerabilidades de conexión y escasez de controles de validación robustos (Deemer, 2024; SentinelOne, 2024; Vij, 2023).

South Star Battery Metals Corp. utilizó inicialmente el sistema contable QuickBooks Desktop para gestionar sus operaciones financieras. Sin embargo, el incremento de actividades comerciales, la necesidad de accesibilidad remota y la colaboración simultánea entre usuarios motivaron a la empresa a migrar hacia QuickBooks Online a finales del año 2023. La versión en línea ofrece ventajas funcionales relevantes, como la actualización automática del sistema, disponibilidad desde cualquier dispositivo conectado a internet y mayor interoperabilidad.

No obstante, tras la migración a QuickBooks Online, la empresa ha enfrentado diversos problemas, tales como el ingreso erróneo de información, duplicación de datos, falta de autenticación de usuarios y contraseñas, así como filtración de información confidencial. La falta de mecanismos eficaces que mitiguen los riesgos asociados a la etapa de ingreso de datos compromete la integridad de la información financiera de la empresa. Dichos fallos pueden derivar en pérdidas económicas, errores contables, vulneración de datos sensibles y deterioro de la confiabilidad interna de los registros.

Según Tinoco, Rivera, Navarrete y Alarcón (2022), QuickBooks Online carece de mecanismos de protección considerados avanzados, como la rotación periódica de contraseñas, autenticación biométrica o validación basada en patrones de comportamiento. Además, el sitio oficial de la plataforma indica que la seguridad se basa en el uso de certificados SSL (Secure Sockets Layer) y la autenticación por contraseña como medidas principales de protección del acceso a los datos (Intuit Quickbooks, 2025). La ausencia de controles más sofisticados incrementa el riesgo frente a amenazas comunes como el phishing, acceso no autorizado, y software malicioso.

Como sostienen Laudon y Laudon (2016), la fase de entrada de datos representa un punto crítico, ya que constituye el primer contacto del usuario con el sistema, y cualquier error en esta etapa incrementa la probabilidad de acceso no autorizado, robo de información, o pérdida de datos. En este contexto, resulta necesario identificar las debilidades de seguridad asociadas a dicha fase, ya que, según hallazgos preliminares, constituye el momento de mayor exposición dentro del sistema contable. Esta problemática justifica el presente estudio, cuyo propósito es analizar los riesgos vinculados a la entrada de datos en QuickBooks Online y diseñar estrategias de mitigación que garanticen la integridad de la información financiera de la empresa.

1.3 Objetivos

1.3.1 Objetivo general:

Analizar los riesgos de seguridad asociados a la entrada de datos en el sistema contable QuickBooks Online utilizado por South Star Battery Metals Corp., y desarrollar estrategias de mitigación eficaces que reduzcan su impacto en la integridad de la información financiera de la empresa.

1.3.2 Objetivos específicos:

- Objetivo específico 1: Evaluar las características del sistema contable QuickBooks e identificar las vulnerabilidades relacionadas con la entrada y seguridad de datos en South Star Battery Metals Corp.
- Objetivo específico 2: Analizar los riesgos específicos asociados a la interacción del usuario durante el proceso de ingreso de datos y determinar su impacto en la vulnerabilidad del sistema contable QuickBooks.
- Objetivo específico 3: Diseñar un plan de contingencia que incluya estrategias específicas para mitigar las vulnerabilidades y riesgos vinculados a la etapa de ingreso de datos por parte del usuario en el sistema contable QuickBooks.

1.4 Alcance

1.4.1 Alcance teórico

Tras una revisión exhaustiva de la literatura disponible sobre las ventajas y desventajas del sistema contable QuickBooks, no se han identificado estudios que analicen de manera específica los riesgos asociados a este sistema durante la interacción del usuario en la etapa de entrada de datos. En contraste, existe una amplia disponibilidad de artículos que destacan los beneficios de su versión en línea. En este sentido, el presente estudio busca aportar información que permita tomar decisiones más informadas al momento de seleccionar un sistema contable en la nube, ofreciendo una visión equilibrada que contemple tanto los posibles riesgos como sus ventajas operativas.

1.4.2 Alcance práctico

El objetivo es proporcionar recomendaciones de seguridad a las empresas que deseen implementar sistemas contables en línea, como QuickBooks, con el fin de prevenir posibles impactos financieros, legales y reputacionales. La seguridad en los sistemas contables constituye un campo de investigación relativamente poco explorado, pero fundamental para mitigar los riesgos asociados a la gestión de datos sensibles. Las recomendaciones formuladas en este estudio pueden ser aplicables a organizaciones de tamaño y giro similares a South Star Battery Metals Corp., una empresa de pequeña escala perteneciente al sector minero.

1.5 Metodología

El presente estudio adopta un enfoque exploratorio con elementos descriptivos. Se optó por esta modalidad debido a que el tema presenta escasa investigación previa o no ha sido abordado con la profundidad necesaria (Universidad Latinoamericana, 2017). Asimismo, se empleará un enfoque cualitativo, a través de la aplicación de encuestas a usuarios de QuickBooks Online y el análisis de incidencias reportadas, con el propósito de describir los riesgos asociados al sistema contable durante la interacción del usuario con el Sistema de Información (Salazar-Escorcia, 2020).

CAPÍTULO II. MARCO DE REFERENCIA

2.1 Los Sistemas de Información Contable

2.1.1 Definición de los Sistemas de Información

Para obtener información significativa, es necesario manipular los datos mediante sistemas diseñados para organizar, analizar y procesarlos de forma estructurada (Oz, 2008). Un sistema bien configurado asegura que los datos sean tratados de manera coherente y eficaz, maximizando su valor en la toma de decisiones y en la generación de conocimiento (Stair & Reynolds, 2017). A su vez, el desarrollo tecnológico ha impulsado la creación de sistemas cada vez más sofisticados, capaces de adaptarse con rapidez a las necesidades del entorno empresarial. En este contexto, los Sistemas de Información (SI) desempeñan un papel fundamental, ya que permiten organizar y procesar datos de manera continua y eficiente.

Un sistema puede entenderse como un conjunto de elementos interrelacionados que funcionan conforme a un plan o reglas determinadas, con el fin de alcanzar objetivos específicos (Encyclopedia Britannica, s.f.). También puede concebirse como la interacción de múltiples subsistemas, donde cada uno cumple una función específica dentro del sistema global (Romney & Steinbart, 2018). En esencia, un sistema recibe datos de entrada, los somete a un proceso determinado y genera salidas alineadas con sus objetivos (McNamara, 2020).

Los datos, por sí solos, representan elementos individuales que reflejan características o eventos, sin haber sido procesados. En cambio, la información es el resultado de transformar esos datos en un formato significativo y útil para la toma de decisiones (Laudon & Laudon, 2016). Por ello, resulta esencial contar con un sistema que procese estos datos dispersos y los convierta en información precisa y oportuna: los Sistemas de Información.

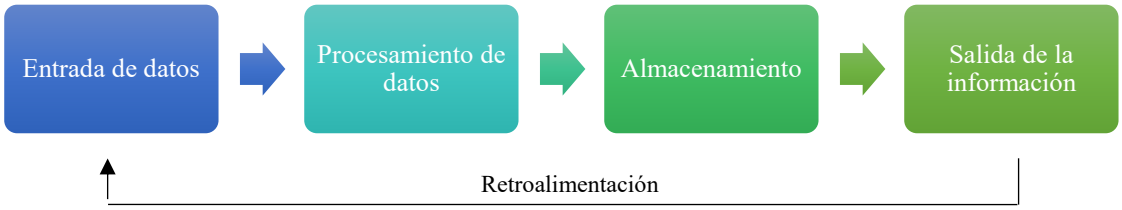
Según Sousa y Oz (2017), los Sistemas de Información son "un conjunto de componentes que participan en el procesamiento de datos y la producción de información". Estos sistemas son fundamentales para el éxito organizacional, ya que permiten gestionar datos de manera eficaz, apoyar la toma de decisiones y resolver problemas en tiempo real (Rodríguez-Cruz & Pinto, 2018). Pangestu y Akwila (2024) señalan que los Sistemas de Información tienen como objetivo apoyar a las empresas en la planificación, el control y la toma de decisiones, al transformar datos individuales, que por sí solos no generan beneficio, en información que aporte valor al proceso decisional. Para ello, se involucran componentes como hardware, software, procedimientos y personas que trabajan de manera conjunta (Pérez, 2024).

2.1.2 Etapas de los Sistemas de Información

Conocer las etapas que conforman el procesamiento de un Sistema de Información (SI) resulta importante para comprender el flujo de datos. Además, el presente trabajo se enfoca en los riesgos de seguridad del sistema contable QuickBooks Online. Por lo que se considera prioritario analizar cómo opera dicha etapa dentro del ciclo completo del sistema. Este análisis permitirá no solo describir el funcionamiento de cada fase, sino también sustentar, con base teórica, que cuál es el punto más vulnerable del proceso.

Las cuatro etapas principales son: entrada de datos, procesamiento, almacenamiento y salida de información (Sousa & Oz, 2017). Asimismo, es importante destacar que los SI están conformados por subsistemas interdependientes que cooperan para alcanzar los objetivos organizacionales (Romney & Steinbart, 2018). Estos subsistemas interactúan de forma dinámica: pueden generar salidas que actúan como entradas para otros, formando así una estructura integrada y adaptable (Sousa & Oz, 2017).

Figura 3. Etapas del proceso del Sistema de Información



Nota. Adaptado de Administración de los sistemas de información (7.ª ed.), por K. J. Sousa & E. Oz, 2017, Cengage Learning. Copyright 2017 por Cengage Learning.

- Entrada de datos

La entrada de datos es la actividad mediante la cual se recopila, captura y almacena información proveniente de diversas fuentes internas o externas (Stair & Reynolds, 2017; Piccoli & Pigni, 2019). Esta etapa busca organizar y validar los datos para su correcto uso en fases posteriores del sistema. Los usuarios involucrados pueden ser colaboradores, clientes, proveedores u otros actores que interactúan con la organización y acceden al sistema a través de interfaces, como formularios digitales o el ingreso manual de datos (Trasobares, 2003; Lenis, 2023).

- Procesamiento de datos

En esta etapa, los datos capturados se transforman en información significativa. Esto puede implicar operaciones como cálculo, análisis, normalización, limpieza y conversión (Romney & Steinbart, 2018). Según Laudon y Laudon (2020), el procesamiento permite interpretar los datos sin alterar su originalidad, convirtiéndolos en conocimiento útil para la organización.

- Almacenamiento

El almacenamiento se refiere a la conservación de la información procesada en repositorios digitales. Este puede realizarse en bases de datos relacionales (SQL) o no relacionales (NoSQL), dependiendo de la estructura y finalidad de los datos (Elmasri &

Navathe, 2015). Según Amazon (2024). e IBM (2022), el uso de tecnologías diversas permite preservar la información, facilitar su recuperación y replicarla como medida preventiva ante riesgos, vulnerabilidades o fallos en el sistema.

- Salida de información

Esta fase consiste en presentar la información de forma comprensible, accesible y oportuna para la toma de decisiones (Stair & Reynolds, 2017). Las salidas pueden presentarse mediante reportes, alertas, gráficos o la transferencia de datos hacia otros sistemas a través de APIs, que permiten la integración entre diferentes plataformas (Grolinger, Higashino, Tiwari, & Capretz, 2013).

Comprender el funcionamiento de las etapas del procesamiento de un Sistema de Información permite identificar con mayor precisión los puntos más susceptibles a vulnerabilidades, especialmente en entornos donde operan Sistemas Contables. A continuación, se procederá a definir y analizar estos sistemas en el contexto organizacional.

2.1.3 Importancia de los Sistemas de Información Contable (SIC) en la gestión contable y tributaria

Los usuarios internos como externos requieren información sobre la salud financiera de cualquier la empresa para tomar decisiones correctivas, en caso de que no se alcancen los objetivos financieros, o para verificar que las decisiones adoptadas se alinean con las expectativas empresariales (Warren, Reeve, & Duchac, 2016). Para ello, requieren de un sistema integrado que recopile y analice los datos provenientes de distintas fuentes para comprender la situación actual de la entidad.

El área contable es responsable de registrar las operaciones diarias de la empresa —como compras, ventas, pagos de salarios y costeo de productos, entre otras— por lo que requiere de un Sistema de Información Contable capaz de procesar los datos financieros y transformarlos en información útil y significativa (Sousa & Oz, 2017). Un Sistema de Información Contable (SIC) se define como una asociación de diferentes agentes involucrados como el personal, registros y procedimientos para convertir datos financieros en información (Horngren, Smith Bamber, & Harrison, 2003).

Diversas fuentes señalan que los Sistemas de Información Contable (SIC) influyen de manera positiva en la gestión tributaria, al optimizar el trabajo operativo, reducir los

errores manuales, facilitar los procesos relacionados con las declaraciones fiscales y fortalecer los lazos de confianza entre la empresa y la administración tributaria (Mohammed et al.; Al-Khasawneh, 2020).

Es importante destacar que, en el pasado, los SIC se desarrollaban de forma manual; sin embargo, con el avance de la tecnología, hoy se dispone de herramientas más sofisticadas, como sistemas contables de escritorio o en línea, que permiten registrar las operaciones cotidianas de manera más eficiente (Turner, Weickgenannt, & Copeland, 2017). Asimismo, la incorporación de tecnología en los SIC contribuye a la evaluación continua de los procesos clave de la organización (Prasad & Green, 2015).

2.2 QuickBooks Online en el entorno empresarial

QuickBooks es una herramienta contable diseñada principalmente para pequeñas y medianas empresas, con el objetivo de facilitar el manejo y control de su información financiera. Se estima que aproximadamente el 82 % de las pequeñas empresas en Estados Unidos utilizan QuickBooks como su sistema contable principal (Latimer, 2024). A nivel mundial, en promedio, el 56 % de las pequeñas empresas y trabajadores por cuenta propia también hacen uso de esta herramienta (Yoder & Ruiz, 2024).

Por su parte, la versión en línea de QuickBooks posee una participación de mercado promedio del 5 % (Cook, 2025). De este grupo, el 81 % de los usuarios se encuentran en Estados Unidos, y el 63 % corresponde a pequeñas empresas (Enlyft, 2024). Aunque esta versión presenta una cuota de mercado reducida en comparación con sus competidores, tiene un alto potencial de crecimiento debido a la creciente tendencia global hacia soluciones basadas en la nube.

Dado que South Star Battery Metals Corp. emplea la versión en línea de QuickBooks, a continuación, se presenta una descripción detallada de su infraestructura y funcionalidades.

2.2.1 Características técnicas de QuickBooks Online

- Infraestructura en la nube de QuickBooks

QuickBooks Online opera sobre la infraestructura de Amazon Web Services (AWS), complementada por su propia arquitectura tecnológica. AWS proporciona servicios en la nube como almacenamiento, bases de datos, migraciones, análisis de datos y procesamiento multimedia (AWS, 2025).

- Inteligencia artificial y aprendizaje automático

QuickBooks ha integrado funcionalidades de inteligencia artificial a través de la herramienta Intuit Assist que permite generar informes, gráficos comparativos e informes en segundos. Además, ofrece retroalimentación personalizada con el fin de incrementar la rentabilidad y asegurar la continuidad del negocio (Intuit QuickBooks, 2025).

La plataforma también identifica patrones de comportamiento para automatizar tareas como recordatorios de pago o la clasificación de transacciones (Intuit, 2023). Asimismo, facilita la conciliación bancaria y emite alertas ante movimientos inusuales (Hargrave, 2023).

- Integraciones mediante API

QuickBooks Online permite la integración con aplicaciones externas mediante interfaces de programación de aplicaciones (API) (QuickBooks, 2025). Las API actúan como puentes entre diferentes softwares, permitiendo su interoperabilidad sin importar su arquitectura o lenguaje de programación (SAP, 2024).

- Seguridad en QuickBooks Online
    - Autenticación multifactor (MFA)

QuickBooks Online utiliza autenticación multifactor (MFA) para reforzar la seguridad del acceso de los usuarios. Este sistema requiere una verificación adicional, como el ingreso de un código enviado por SMS o a través de una llamada telefónica, antes de acceder a la cuenta (QuickBooks, 2024).

    - Encriptación de datos

El sistema emplea encriptación SSL de 128 bits para proteger la transmisión de datos entre el usuario y los servidores de QuickBooks Online, garantizando la seguridad de la información confidencial (QuickBooks, 2024). SSL (Secure Sockets Layer) es un protocolo que cifra los datos enviados a través de páginas web para evitar accesos no autorizados (Sectigo, 2025).

    - Protocolos de seguridad adicionales

- Controles de acceso: Los administradores pueden configurar permisos basados en roles, asegurando que cada usuario acceda únicamente a la información relevante para sus funciones.

- Protección contra amenazas: La plataforma cumple con estándares de seguridad de la industria, implementando actualizaciones periódicas para protegerse frente a nuevas amenazas.

    - Service Level Agreement (SLA)

El Service Level Agreement (SLA) es un contrato celebrado con un proveedor en el que se especifican el nivel y la calidad del servicio que el usuario espera recibir. Asimismo, establece las acciones que se tomarán en caso de incumplimiento de lo estipulado (Goodwin, 2024). En el caso de QuickBooks Online, los términos y condiciones del SLA se encuentran disponibles en su sitio web como respaldo para comprender el nivel de servicio ofrecido. Un resumen de los puntos más relevantes puede consultarse en el Anexo 1.

A pesar de contar con medidas avanzadas de protección, QuickBooks Online no detalla públicamente sus procedimientos específicos de monitoreo, auditoría ni respuesta ante incidentes. Esta falta de transparencia genera inquietudes, especialmente entre usuarios que gestionan información financiera crítica, ya que el uso de soluciones en la nube exige mayor claridad en cuanto a los protocolos de mitigación de riesgos.

2.2.2 Uso de QuickBooks Online para pequeñas y medianas empresas

QuickBooks Online tiene dos principales segmentos de clientes: las pequeñas empresas, con menos de 50 colaboradores, representan en promedio el 63 % de su base de usuarios, mientras que las empresas medianas constituyen aproximadamente el 21 % (Enlyft, 2025). Además, sus clientes se concentran principalmente en tres sectores: construcción (17 %), contabilidad (13 %) y servicios de tecnología de la información (12 %) (Yaqub, 2024).

Otro informe indica que QuickBooks Online es el software contable preferido frente a otras alternativas del mercado, como Xero y FreshBooks. En 2023, QuickBooks generó ingresos por 8 mil millones de dólares, mientras que FreshBooks reportó apenas 113 millones, es decir, aproximadamente 71 veces menos (Ruiz & Yoder, 2024).

Las pequeñas y medianas empresas (Pymes) prefieren QuickBooks Online debido a su formato intuitivo, que facilita el registro contable sin necesidad de experiencia previa en

Sistemas de Información Contable (SIC). Asimismo, la plataforma incorpora funciones de automatización en la entrada de datos, lo que contribuye a minimizar errores manuales. Te brinda reportes en tiempo real y contribuye a cálculo de impuesto en pocos minutos. Adicionalmente, permite personalizar ciertas funcionalidades según las necesidades específicas de cada empresa (Abacus, 2024).

En el caso específico de South Star Battery Metals Corp., la adopción de QuickBooks Online respondió a la necesidad de contar con una plataforma accesible desde múltiples ubicaciones y con capacidad para colaborar entre distintos usuarios en tiempo real, lo cual facilitó el crecimiento de sus operaciones contables a partir de 2023.

QuickBooks Online es el Sistemas de Información Contable (SIC) preferido por pequeñas y medianas empresas. El crecimiento se debe a las ventajas operativas, accesibilidad en la nube y diseño intuitivo para usuarios no especializados. Sin embargo, esta misma facilidad de acceso y descentralización introduce nuevos desafíos, particularmente en lo que respecta a la seguridad de la información financiera.

A medida que las organizaciones delegan tareas críticas como el ingreso de datos a distintos usuarios y dispositivos, aumentan también los riesgos asociados a errores, fraudes o accesos no autorizados. En este contexto, resulta indispensable analizar las vulnerabilidades que se presentan durante la interacción del usuario con el sistema, especialmente en la etapa de entrada de datos, la cual será abordada a continuación.

2.3 Riesgos en la entrada de datos en sistemas contables

Los Sistemas de Información Contable (SIC) dependen de datos ingresados por usuarios internos o provenientes de fuentes externas que, en muchos casos, no han sido completamente verificados o autenticados (O'Brien & Marakas, 2011). En otras palabras, la integridad y seguridad de la información financiera dependen en gran medida de los mecanismos de captura y registro implementados. Además, la entrada de datos constituye el primer punto de contacto entre el usuario y el sistema (Mehta, 2022). Por ello, en ausencia de medidas de protección robustas contra agentes externos, la información valiosa podría perderse, ser destruida o interceptada por terceros, lo cual pondría en riesgo datos sensibles, secretos comerciales o incluso la privacidad personal (Laudon & Laudon, 2016).

Forbes (2024) informó que, a nivel mundial, el robo de información genera pérdidas promedio de 1.23 millones de dólares para grandes empresas y de 120,000 dólares para pequeñas empresas. En Estados Unidos, los ciberataques han ocasionado pérdidas superiores a los 12.5 mil millones de dólares, relacionadas con estafas, fraudes de inversión y filtraciones de información (Hamel, 2024). En el caso de Perú, la incidencia de ataques cibernéticos aumentó del 10 % en 2018 al 32 % a fines de 2024 (CEPLAN, 2024).

Tanto QuickBooks Online como otros sistemas contables basados en la nube deben incorporar mecanismos que mitiguen los riesgos asociados a la fase de entrada de datos dentro del procesamiento de los SIC. A continuación, se presentará un análisis de los factores que inciden en la vulnerabilidad de esta etapa, así como evidencia teórica y empírica que respalda su carácter crítico dentro del funcionamiento de los Sistemas de Información Contable.

2.3.1 Errores humanos que incrementan la vulnerabilidad en la fase de entrada de datos

Durante el proceso de entrada de datos, la interacción del usuario con el Sistema de Información Contable (SIC) puede dar lugar a errores humanos, ya sea por acciones no intencionadas o por omisiones, las cuales pueden causar, propagar o facilitar la aparición de vulnerabilidades dentro del sistema (Ahola, s.f.). Según la norma ISO 14224 (2016), el error humano se relaciona con tres tipos de fallas: la pérdida de desempeño, el conjunto de causas que conducen a la falla, y los mecanismos o procesos que la desencadenan.

En esa línea, el informe de investigación de Verizon (2025) señala que los errores humanos representan el 68 % de las vulnerabilidades de datos de los SIC. Por su parte, IBM (2024) reporta una cifra aún más elevada, estimando que el 74 % de los incidentes están vinculados a factores humanos. Ambos informes destacan como causas recurrentes el phishing, la mala configuración de sistemas y la entrega incorrecta de información.

- Errores en la ejecución de tareas
    - Entrega indebida de información. En otras palabras, enviar información confidencial a personas incorrectas (Coker, 2025).

- Duplicar u omitir ingreso de data a los Sistemas de Información Contable (SIC) (Ceballo, 2024).

- Errores de decisión en entornos operativos

  - Uso de contraseñas débiles y reutilización de la misma clave en múltiples plataformas en línea (Haan & Watts, 2024).

  - La desactualización o mala configuración de los SIC pueden permitir el acceso no autorizado de terceros a los datos almacenados. Esta situación puede derivar en el robo de información confidencial contenida en discos duros o en la asignación errónea de privilegios excesivos a usuarios dentro de la red (Kosinski, 2024).
  - Omitir los protocolos de seguridad establecidos por la organización, como dejar dispositivos desbloqueados, posponer actualizaciones del sistema, compartir contraseñas o conectarse a redes Wi-Fi no seguras, incrementa significativamente los riesgos de seguridad informática (Tamari, 2025).

2.3.2 Errores técnicos, procedimentales y de gestión que incrementan la vulnerabilidad en la fase de entrada de datos

Si bien el usuario es responsable del ingreso de los datos, la fiabilidad de la captura también depende del diseño del Sistema de Información Contable (SIC), de los controles automáticos incorporados y del medio a través del cual se realiza el registro. A continuación, se presentan los factores que incrementan la vulnerabilidad en la fase de entrada de datos:

- Errores del diseño de los SIC

  - Cuando la actualización del sistema no se realiza de forma completa o adecuada, se incrementa la exposición a accesos no autorizados por parte de agentes externos (Luettmann & Bender, 2007). Del mismo modo, una configuración incorrecta del sistema puede generar errores en el registro de la información (Nor, Jalil, & Manan, 2012).

- Cuando no se cuenta con mecanismos para identificar al autor o la fecha de ingreso de los datos, se dificulta la detección de errores o fraudes (ASOCEX, 2015).
    - Incluye el acceso compartido sin restricciones de rol.
- Cuando el sistema presenta integraciones débiles con otras plataformas a través de APIs, se incrementa el riesgo de que datos confidenciales sean transmitidos a terceros o de que la información transferida resulte inconsistente (DIMTEC, 2025).

- Errores en la gestión y política de los procesos de los SIC
    - Permitir el uso de los SIC a personas o usuarios que no cuentan con habilidad en el área contable conlleva a que la data sea registrada de manera incorrecta, se pierda o sea compartida con terceros (Charbonneau, 2011).
    - Compartir credenciales sin restricciones o utilizar un único usuario para múltiples colaboradores impide realizar un seguimiento adecuado y controlar quién manipula los datos (ISO/IEC 27001:2013).
    - Si los SIC permiten el ingreso libre de datos sin aplicar filtros de formato, rangos o control de duplicidad, se incrementa significativamente el riesgo de errores. En otras palabras, los sistemas carecen de validaciones automáticas de datos.

En el Anexo 2 se muestra como los factores humanos y los aspectos técnicos y de gestión se combinan para incrementar la exposición al riesgo durante la entrada de datos. Por lo que esta clasificación permitirá establecer estrategias de mitigación alineadas a cada tipo de falla identificada.

2.3.3 Datos que evidencian la debilidad en la fase de entrada de datos en los Sistemas Informáticos Contables

Diversos informes y estudios coinciden en que la fase de entrada de datos en los Sistemas de Información Contable (SIC) está expuesta a inseguridades y errores operativos. Borgeaud (2025) reportó que el 66 % de los Gerentes de Seguridad de la Información en Estados Unidos consideran que los errores humanos inciden directamente en la vulnerabilidad de sus sistemas. Por su parte, el World Economic Forum (2022) concluyó que el 95 % de los problemas de ciberseguridad pueden atribuirse a errores humanos, y que el 43 % de estos corresponden a amenazas internas —intencionadas o no— que ocurren durante la interacción inicial con el sistema.

Adicionalmente, el informe Verizon DBIR (2025) reveló que el 60 % de las vulnerabilidades en los Sistemas de Información Contable (SIC) se deben a factores humanos. Por su parte, un estudio realizado por la Universidad de Stanford señaló que aproximadamente el 88 % de los colaboradores generan incidentes en los sistemas que facilitan el ingreso de agentes externos no autorizados, así como la modificación o eliminación de datos (CISOMAG, 2020).

Por último, un informe de Thales Data (2023) documentó que, en promedio, el 55 % de las empresas consideran que una gestión inadecuada de los usuarios en los sistemas contribuye a la filtración de datos confidenciales a terceros. Además, mencionan que las contraseñas débiles, compartir información sin cifrar, y no realizar las actualizaciones requeridas, permiten que terceros intercedan.

En el caso de South Star Battery Metals Corp., se ha identificado que, tras la migración a QuickBooks Online, los incidentes más frecuentes estuvieron asociados a fallos en la entrada de datos, como registros duplicados, ingreso incorrecto de montos y uso compartido de accesos. Esta evidencia interna, junto con la literatura revisada, justifica la necesidad de centrar el análisis de riesgos en esta etapa específica del procesamiento contable. A continuación, se explicarán otros factores que inciden sobre los Sistemas de Información Contable (SIC), derivados de acciones humanas que, de forma directa o indirecta, comprometen la seguridad, integridad y detección de los datos financieros.

2.4 Amenazas de seguridad de los Sistemas Informáticos Contables en la nube como QuickBooks Online

Los Sistemas de Información Contable (SIC) que han migrado a medios digitales, aquellos que están alojados en la nube y son accesibles a través de internet (Microsoft

Azure, 2024; AWS Amazon, 2024), comienzan a enfrentar desafíos que pueden comprometer la seguridad de la información financiera. El uso de herramientas en la nube conlleva riesgos relevantes, entre los que se destacan la falta de protección de los datos, la posibilidad de errores humanos y la dependencia de la conectividad (Deemer, 2024; SentinelOne, 2024; Vij, 2023). También, Hernández et al. (2019) advierten que este tipo de sistemas en línea puede ser más vulnerable a ataques informáticos si no se implementan los protocolos de seguridad.

Según el World Economic Forum (2025), el 42 % de los usuarios de sistemas contables en línea han reportado ataques que comprometieron la seguridad de sus plataformas. Asimismo, Cortés (2025) informa un incremento global del 57 % en los ciberataques. En particular, Verizon (2023) señala que el 44 % de los incidentes están relacionados con *phishing*, y el 25 % involucran el uso de identidades robadas. Finalmente, PricewaterhouseCoopers (2024), en su informe sobre ciberseguridad, reveló que el 31 % de las empresas consideran que el uso de software en línea incrementa la probabilidad de errores.

QuickBooks Online ofrece características como accesibilidad desde cualquier dispositivo en cualquier momento, funciones colaborativas y servicios de almacenamiento en la nube (Intuit QuickBooks, 2025). Sin embargo, las fuentes secundarias indican que pueden presentar vulnerabilidades significativas. A partir de ellos, se han clasificado los riesgos en SIC digitales en cuatro categorías principales, para comprender la naturaleza de las amenazas y poder establecer protocolos para mitigarlos.

Tabla 2. Clasificación de riesgos en QuickBooks Online y sus impactos

Categoría de riesgo	Descripción	Impactos
Procesamiento de datos	Errores en cálculos contables, conciliaciones bancarias, duplicación u omisión de registros.	Estados financieros inexactos, errores tributarios, sanciones fiscales, reprocesos.
Seguridad y fraude	Phishing, accesos no autorizados, robo de identidad, uso de credenciales compartidas, llamadas fraudulentas, ventanas emergentes falsas y cuentas hackeadas.	Confusión entre intentos legítimos y posibles ataques. También, fraude dentro de un canal oficial. Pérdida de datos, fraudes contables y financieros, pérdidas económicas, daños a la reputación.

Visualización y reportes	Informes incompletos, errores en filtros, dificultades para obtener data en tiempo real.	Errores en la presentación de impuestos, la interfaz de usuario.
Operativos y de plataforma	Base de datos corruptas, pérdida de información contable, migración de datos entre cuentas con dificultades operativas, e inaccesibilidad a los reportes por fallos en los servidores.	Retraso de decisiones financieras e interrupción de operaciones. Propagación de errores, falta de control interno, imposibilidad de auditar registros.

Nota. La información fue obtenida del Anexo 3 y de la página de soporte de QuickBooks (2025)

2.5 Principios de Seguridad de la Información: Tríada CIA

- Confidencialidad

El acceso a la información se puede dar de dos formas: física y técnica. Por ello, este principio busca procedimientos que controle y limiten estos tipos de acceso no autorizados (Cabric, 2015).

- Integridad

Este principio establece que la información del sistema debe mantenerse sin modificaciones accidentales o intencionales por agentes internos y externos no autorizados. Además, que la información ingresada sea tan precisa y exacta, que se pueda confiar en ella sin problemas (Cabric, 2015).

- Disponibilidad

Impedir que los usuarios autorizados accedan a los sistemas cuando lo necesitan es una forma de ataque a la seguridad. En otras palabras, la pérdida de acceso puede ser costosa por la falta de capacidad de realizar pagos o, en caso de accidentes o desastres, se pierde el acceso (Harjinder, Thompson, Titis, & Stephens, 2025).

- Relacionando QuickBooks Online y tríada CIA

Tabla 3. Verificación de la tríada CIA en el Sistema Contable en línea QuickBooks

CIA	Cumple	No cumple
Confidencialidad	Autenticación multifactorial [a].	Llamadas de personal de soporte técnico falso [b].
		Correos con mensajes alterados [d].
	Encriptación 128-bit SSL [c].	Ventanas emergentes fraudulentas [e].
	Manejo y control de usuarios [a].	Mensajes de texto engañosos [f].
Integridad	Automatización de ciertos procesos.	Introducir cierta información manualmente (datos, importes) [a].
	Integración del banco con el software [a].	Se han reportado problemas con las APIs [g].
	Generación reportes en tiempo real [a].	Fallos en la migración de datos [e].
	Colaboración simultanea con otros usuarios al mismo tiempo [a].	Reporte de alteración de datos por terceros [h].
Disponibilidad	Acceso en la nube [a].	Fallas de la conexión continua a internet [i].
	Disponible en dispositivos móviles y computador [a].	Interrupción del servicio por fallas de los dispositivos [e].
	Actualizaciones automáticas [c].	

Nota. Se procedió a comparar las características más relevantes de QuickBooks Online con las vulnerabilidades identificadas en los sistemas contables en línea. La información se obtuvo de las siguientes fuentes: QuickBooks Support (2025), Intuit QuickBooks (2024), Redacción EC (2023), Proofpoint (2024), Hayes (2020), Cortés (2025), Hassan (2025) y Secureframe (2024). La lista de problemas identificados en QuickBooks proviene de quejas registradas por usuarios en la página oficial de soporte de QuickBooks (https://quickbooks.intuit.com/learn-support/en-us).

Con base en lo expuesto, el sistema no cumple con ninguno de los principios evaluados, lo que evidencia que la seguridad actual no es suficiente. En consecuencia, South Star Battery Metals Corp. debe asumir un rol proactivo en la protección de la privacidad y la seguridad de su información confidencial.

No es suficiente confiar únicamente en las medidas de seguridad que ofrece QuickBooks; es imprescindible que la empresa implemente estrategias adicionales para fortalecer la protección de sus datos al utilizar un sistema de contabilidad en línea. Estas estrategias pueden incluir el desarrollo de políticas internas de seguridad, la capacitación continua

del personal en prácticas seguras y la incorporación de soluciones de seguridad complementarias.

CAPÍTULO III. PROPUESTA

3.1 Fase 1: Selección de los riegos específicos asociados a la interacción del usuario durante el proceso de ingreso de datos

En cada una de las categorías de riesgo descritas en el capítulo anterior, se identificaron múltiples riesgos. No obstante, para efectos del presente análisis, se han seleccionado aquellos que resultan más relevantes y que afectan directamente la fase de entrada de datos. Esta decisión responde al hecho de que, conforme se ha demostrado previamente, dicha fase constituye el punto más vulnerable dentro del ciclo de procesamiento del sistema contable.

3.1.1 Documentación y fuentes secundarias

Para identificar los riesgos asociados al uso de QuickBooks Online, se analizó una muestra de 114 quejas recopiladas desde la página oficial de QuickBooks Support y foros especializados como Reddit (véase Anexo 3,4,5, y 6).

Con el objetivo de cuantificar los hallazgos, se procedió a agrupar y contabilizar los reportes repetidos, calculando su proporción respecto al total de la muestra. Los resultados evidenciaron que el 52 % de los usuarios reportaron incidentes relacionados con seguridad y fraude, mientras que un 22 % refirió fallas vinculadas a la visualización de reportes. El porcentaje restante se distribuyó entre problemas operativos y de plataforma (véanse Anexos 3 y 7). A continuación, se realizará un resumen de los riesgos más relevantes y comunes.

El 43 % de los usuarios reporta que QuickBooks Online presenta problemas relacionados con seguridad y fraude, principalmente debido a la recepción de correos electrónicos con enlaces maliciosos, llamadas de personas que se hacen pasar por personal de soporte técnico, y mensajes de texto engañosos. Estos riesgos se vinculan directamente con la fase de entrada de datos, ya que, al interactuar con estas amenazas, los usuarios pueden comprometer el sistema al proporcionar información confidencial.

Las consecuencias más comunes incluyen: pérdida de datos, accesos no autorizados, fraude financiero y confusión entre comunicaciones legítimas y ataques cibernéticos.

Cabe señalar que, en algunos casos, los fraudes han ocurrido incluso dentro de canales considerados oficiales, lo que aumenta el nivel de exposición y vulnerabilidad.

El 22 % se encuentra categorizado dentro de los riesgos de visualización y reportes, los cuales incluyen errores del sistema como el cálculo incorrecto de montos y fallas en los procesos automatizados. Estos problemas pueden derivar en errores en la presentación de impuestos, así como en costos adicionales y consecuencias negativas en la productividad. Por último, el 20% se generar por errores operativos ya que fallas en los servidores no permiten descargar reportes ni contar con información completa.

Tabla 4. Los riesgos más relevantes en QuickBooks Online

Categoría	Descripción del riesgo reportado	% estimado
Seguridad y fraude	Recepción de correos electrónicos maliciosos con enlaces fraudulentos.	43%
	Llamadas falsas de personal de soporte técnico.	
	Ventanas emergentes fraudulentas dentro del navegador.	
	Correos con alertas falsas sobre hackeo de cuenta.	
	Mensajes de texto con alertas de fraude.	
Visualización y reportes	Errores en el cálculo automático de montos (como impuestos o nóminas).	10%
	Fallas en automatizaciones: conciliaciones, facturación, invoicing, y pagos recurrentes.	12%
Operativo y plataforma	Inaccesibilidad a reportes financieros por fallos en servidores.	12%
	Reportes contables con información incompleta o incorrecta.	8%

Nota. Los datos fueron obtenidos del portal oficial de soporte de QuickBooks: Hola, te damos la bienvenida al soporte de QuickBooks (QuickBooks, 2025). Recuperado de https://quickbooks.intuit.com/global/es/learn-and-support/

3.1.2 Entrevistas

Para corroborar los riesgos identificados en la revisión de la literatura, se optó por realizar tres entrevistas semiestructuradas dirigidas a usuarios con experiencia directa en el uso

de QuickBooks Online. Se eligió esta técnica debido a su flexibilidad para adaptarse al entrevistado, su capacidad para profundizar en temas relevantes y su valor para aclarar situaciones prácticas, tal como lo explican Díaz-Bravo & et. (2013). Las entrevistas se estructuraron en torno a tres categorías clave de riesgo: seguridad y fraude, visualización y reportes, y problemas operativos y de plataforma (Anexo 8 y 9). Esta clasificación permitió recoger percepciones específicas sobre situaciones reales enfrentadas por los usuarios.

Tabla 5. Riesgos reportados por usuarios de QuickBooks

Entrevistada	Riesgos identificados	Acciones preventivas
Samantha Shortert	• Ataques de phishing por correo y SMS. • Facilidad de acceso no autorizado. • Mensajes maliciosos haciéndose pasar por QuickBooks.	• Activó doble verificación. • No guarda su contraseña en Google. • Envía alertas al equipo.
Whitney Sham	• Recibió llamadas fraudulentas simulando soporte técnico. • Pagó por una "actualización" que nunca ocurrió (fraude).	• Reportó a su proveedor. • Solicitó reembolso e implementó validación de proveedores.
Julie Sisks	• Uso de QuickBooks Desktop con actualizaciones constantes. • Detectó movimientos contables sospechosos. • Cree que el sistema puede ser alterado sin aviso.	• -Cambia su contraseña cada 3 meses. • Revisa los registros contables manualmente.

Nota. Elaboración propia en base a las entrevistas semiestructuradas realizadas

De estas encuestas se encontró que correos electrónicos con mensajes alterados, llamadas de falsos técnicos, ventanas emergentes fraudulentas, hackeo de cuenta y manipulación de la data, y, por último, reportes financieros que muestran información incorrecta o incompleta fueron los riesgos más comunes que presentaron los entrevistados.

3.1.3 Encuestas

Posteriormente, se aplicó una encuesta a usuarios de QuickBooks Online con el objetivo de corroborar la identificación de riesgos de seguridad durante la fase de entrada de datos. La muestra estuvo conformada por 10 participantes, debido a que no fue posible acceder

a una población más amplia de usuarios con experiencia comprobada en el uso operativo del sistema.

Tabla 6. Profesionales que realizaron la encuesta

Nombre	Profesión	Empresa	Usuario QuickBook en línea	Usuario QuickBook deskopt
Anu Thomas	Contador	RedFern Consulting	x	
Jonathan Richards	Manager	RedFern Consulting	x	x
Samantha Shorter	CFO	RedFern Consulting-South Star Mining Corp	x	
Whitney Sham	Contador	RedFern Consulting-South Star Mining Corp	x	x
Alastair Brownlow	CPA	RedFern Consulting-South Star Mining Corp	x	x
Alonso Ulloa	Contador	REF International	x	x
Julie Sisks	Contador	REF International-REF USA	x	x
Kimberly Hibler	CEO	*REF International-REF USA*		x
Jasmine Lau	CPA	RedFern Consulting	x	x
Sofia Figueiroa	Contador	RedFern Consulting	x	x

Nota. Diseño propio.

A pesar del número reducido, los encuestados cumplieron con los criterios establecidos de conocimiento técnico, y sus respuestas permitieron confirmar los principales riesgos detectados en la revisión teórica. Además, se constató que no emergieron nuevas categorías de riesgo vinculadas a la entrada de datos, lo que refuerza la validez del análisis realizado.

A partir de los resultados de la encuesta, se identificó que, dentro de la categoría de riesgos de seguridad y fraude, los tres incidentes más frecuentes fueron: la recepción de correos electrónicos con mensajes alterados (30 %), llamadas telefónicas de personas que se hacen pasar por personal de QuickBooks (24 %) y la aparición de ventanas emergentes fraudulentas al ingresar a la plataforma (véase Anexo 11). En cuanto a los riesgos de visualización, el 36 % de los encuestados reportó haber detectado informes financieros con información incorrecta o incompleta (véase Anexo 12). Finalmente, respecto a los riesgos operativos y de plataforma, el 60 % señaló haber enfrentado fallas en procesos automatizados, y el 40 % indicó haber perdido información contable tras una actualización del sistema o migración de datos (véase Anexo 13).

3.1.4 Matriz de riesgos

Con el objetivo de evaluar la vulnerabilidad en cada etapa del sistema de información, se identificaron y clasificaron los riesgos más relevantes. Para ello, se empleó una escala de evaluación basada en la probabilidad y el impacto, con el fin de calcular el nivel de riesgo asociado a cada amenaza. En otras palabras, se estableció una clasificación del nivel de riesgo con el propósito de determinar cuáles representan un mayor potencial de generar deficiencias o fallas en los procesos durante la entrada de datos de South Star Battery Metals Corp (Rodríguez, 2011).

Tabla 7. Nivel de probabilidad

Nivel de probabilidad	Explicación
Baja	El riesgo ocurre rara veces
Media	El riesgo ocurre algunas veces
Alta	El riesgo ocurre siempre o casi siempre

Nota. Adaptado de Manual para identificación de peligros y evaluación de riesgo de determinación de controles IPERC, por SUNAFIL, 2020.

Tabla 8. Nivel de impacto

Nivel de Impacto	Explicación
Nivel catastrófico	Incluye incidentes como hackeos, pérdida de información crítica, robo de dinero o de identidad.
Nivel significativo	Se refiere a la pérdida temporal de datos o accesos no autorizados que no generan consecuencias graves.
Nivel moderado	Comprende fallas técnicas, errores contables sin repercusiones económicas significativas e interrupciones menores del servicio.
Nivel bajo	Agrupa incidentes que provocan confusión, generación de *spam* o alertas falsas, pero que no comprometen información ni implican pérdidas económicas

Nota. Adaptado de Prevención y gestión de riesgos, por Revista de Contabilidad y Dirección, 2019.

Para desarrollar la matriz de riesgos, la probabilidad fue determinada mediante la cuantificación de la frecuencia de quejas registradas en el Anexo 6, y se asignó una escala porcentual del 1 % al 100 % para representar el nivel de percepción del riesgo por parte de los usuarios. Posteriormente, el impacto fue clasificado utilizando una escala ordinal del 1 al 5, de acuerdo con criterios previamente establecidos. Cabe destacar que esta evaluación se fundamentó en el juicio del investigador, sustentado en la información

obtenida de fuentes secundarias y en los resultados recopilados a través de la entrevista y encuesta aplicadas.

Tabla 9. Clasificación

Impacto	Valor	Especificaciones
No genera impacto	1	Errores de formato o numéricos que no generan consecuencias financieras ni reputacionales para la empresa.
Menor	2	Incidentes que generan confusión en los usuarios, como correos con mensajes fraudulentos, sin implicancias financieras ni reputacionales. Solo generan alertas.
Mediano	3	Incluye pérdidas temporales de conexión con el proveedor, interrupciones o fallas técnicas que no conllevan pérdidas económicas.
Mayor	4	Casos en los que se filtran o modifican datos, o se otorga acceso a terceros no autorizados, generando un impacto reputacional —como la pérdida de confianza—, sin afectar aspectos legales o económicos.
Genera gran impacto	5	Incidentes que implican robo de datos, extracción de fondos, pérdida de información sensible y confidencial, hackeos o filtraciones graves. Afectan de manera significativa los ámbitos legal, reputacional y económico de la empresa.

Nota. Diseño propio

Finalmente, el nivel de riesgo se ha obtenido multiplicando la probabilidad del riesgo con el impacto que puede generar para la empresa (Dumoy, 1999). También, se clasifico el nivel de riesgo entre 0 a 100% con el fin de determinar qué riesgos generar más nivel de riesgo y tomar acciones inmediatas para evitar daños que generen pérdidas de confianza con sus clientes, información prestigiosa y sensible, y monetaria.

Tabla 10. Matriz de riesgo de los riesgos de QuickBooks Online

Categoría del riesgo	Riesgo	Probabilidad	Impacto	Nivel de Riesgo	Clasificación
Seguridad y fraude	Recepción de correos electrónicos maliciosos con enlaces fraudulentos.	0.6	3	1.8	Catastrófico
	Llamadas falsas de personal de soporte técnico.	0.24	4	0.96	Catastrófico

	Ventanas emergentes fraudulentas dentro del navegador.	0.24	4	0.96	Catastrófico
	Correos con alertas falsas sobre hackeo de cuenta.	0.1	2	0.2	Moderado
	Mensajes de texto con alertas de fraude.	0.1	2	0.2	Moderado
Visualización y reportes	Errores en el cálculo automático de montos (como impuestos o nóminas).	0.3	1	0.3	Significativo
	Fallas en automatizaciones: conciliaciones, facturación, invoicing, y pagos recurrentes.	0.3	2	0.6	Catastrófico
Operativo y plataforma	Inaccesibilidad a reportes financieros por fallos en servidores.	0.4	2	0.8	Catastrófico
	Reportes contables con información incompleta o incorrecta.	0.36	1	0.36	Significativo

Nota. Datos obtenidos de Hola, te damos la bienvenida al soporte de QuickBooks, QuickBooks, 2025 (https://quickbooks.intuit.com/global/es/learn-and-support/) y de Análisis y evaluación de riesgos: aplicación de una matriz de riesgo en el marco de un plan de prevención contra el lavado de activos, por Albanese, Revista de Administração e Contabilidade da Unisinos, 2012 (https://doi.org/10.4013/base.2012.93.01).

Tabla 11. Nivel de riesgo y clasificación

Nivel de Riesgo	Clasificación
< 0.10	Bajo
0.10 – < 0.30	Moderado
0.30 – < 0.60	Significativo
≥ 0.60	Catastrófico

Nota. Diseño propio.

3.1.5 Resultados

Finalmente, con base en el análisis de fuentes secundarias y los resultados obtenidos de la encuesta, se concluye que la fase de entrada de datos representa el área más vulnerable dentro del sistema QuickBooks. Esta vulnerabilidad se debe, principalmente, a la facilidad con la que los atacantes pueden engañar a los usuarios para que proporcionen información confidencial. Entre ellos destacan:

- Correos electrónicos manipulados, que evidencian intentos de phishing, mediante los cuales los usuarios de QuickBooks son expuestos a enlaces maliciosos o solicitudes fraudulentas.

- Llamadas de falsos técnicos, en las que los estafadores se hacen pasar por personal de soporte de QuickBooks con el objetivo de obtener credenciales o efectuar cobros indebidos.

- Ventanas emergentes fraudulentas, que aparecen dentro del sistema con enlaces sospechosos o números de contacto alterados, diseñadas para inducir a los usuarios a realizar acciones perjudiciales.

Estos riesgos comprometen la seguridad de los datos financieros y operativos, incrementando la probabilidad de filtraciones de información, robo de identidad y pérdidas económicas para los usuarios de QuickBooks. En consecuencia, se deben proponer estrategias de mitigación, considerando que la entrada de datos constituye la primera capa de protección para salvaguardar la integridad de la información.

Adicionalmente, se identificaron otros eventos de riesgo considerados catastróficos, como las fallas en automatizaciones (por ejemplo, en conciliaciones bancarias, facturación, invoicing o pagos recurrentes), así como la inaccesibilidad a reportes financieros causada por fallos en los servidores. No obstante, a pesar de su gravedad potencial, estos incidentes fueron clasificados con un nivel de ocurrencia significativamente menor en comparación con los riesgos vinculados a la entrada de datos, y por tanto no se consideran los más críticos en términos de frecuencia.

Riesgo	Impacto Económico	Impacto Legal	Impacto Reputacional
Correos electrónicos con mensajes	Robo de datos bancarios de clientes: La	Responsabilidad legal de la empresa: South Star Battery Metals	Pérdida de confianza del cliente: Un incidente relacionado

alterados, llamadas de falsos técnicos y ventanas emergentes fraudulentas	empresa almacena información de tarjetas de crédito del 90 % de su base de clientes (ver Anexo 15). En caso de filtración o acceso no autorizado, los atacantes podrían comprometer un promedio mensual de hasta $250,000 USD en transacciones fraudulentas (ver Anexo 16). Asimismo, existe el riesgo de pérdida de información bancaria corporativa, lo cual podría derivar en operaciones no autorizadas con un impacto financiero estimado en $2,472,442 USD en promedio.	Corp. está obligada a garantizar la confidencialidad de los datos de sus clientes conforme a la *Personal Information Protection and Electronic Documents Act (PIPEDA)*. En caso de un incidente que genere un riesgo significativo, la empresa podría enfrentar sanciones de hasta 25 millones de dólares canadienses o el 3 % de sus ingresos anuales, lo que resulte mayor **Fuente especificada no válida.**.	con *phishing* puede deteriorar significativamente la percepción de seguridad entre los clientes, disminuyendo su disposición a compartir información confidencial y afectando negativamente la reputación corporativa de South Star Battery Metals Corp.

Nota. La información fue obtenida por La página de Justicia de Canadá, 2025. & Sedar+, 2025.

3.2 Fase 2: Diseñar un plan de contingencia que incluya estrategias específicas para mitigar las vulnerabilidades y riesgos vinculados a la etapa de ingreso de datos por parte del usuario en el sistema contable QuickBooks.

Durante el desarrollo del presente trabajo, se verificó, como se muestra en el anexo 1, que la plataforma QuickBooks no asume responsabilidad alguna ante pérdidas de información, fallos técnicos ni errores derivados del uso de servicios de terceros integrados. En este contexto, se recomienda que South Star Battery Metals Corp. adopte herramientas y mecanismos adecuados dentro de sus procedimientos internos, a fin de mitigar dichos riesgos de manera efectiva.

Asimismo, es importante subrayar que la propuesta planteada en este Trabajo de Suficiencia Profesional tiene como objetivo reducir las vulnerabilidades identificadas en la fase de entrada de datos.

Dicha propuesta se estructura en torno a los tres pilares fundamentales que conforman la gestión de los Sistemas de Información Contable:

- Procesos y organización: Se refiere a los procedimientos estructurados que aseguran eficiencia y coherencia en el manejo de la información (Urquhart, Hamad, Tbaishat, & Yeoman, 2018).

- Personas: Comprende a los usuarios y responsables de operar, supervisar y tomar decisiones en relación con el sistema contable QuickBooks Online (Urquhart, Hamad, Tbaishat, & Yeoman, 2018).

- Tecnología: Incluye las herramientas y plataformas que facilitan la automatización, el almacenamiento y el análisis de datos (Urquhart, Hamad, Tbaishat, & Yeoman, 2018).

3.2.1 Manual de procedimientos

South Star Battery Metals Corp. no cuenta con un área especializada en Tecnología de la Información; por ello, se propone la elaboración de un manual de procedimientos dirigido al equipo de contabilidad, con el propósito de facilitar la mitigación de riesgos operacionales. El manual de procedimientos se entiende como un documento que presenta, de forma ordenada y sistemática, las etapas necesarias para la ejecución de una determinada actividad (Vivanco Vergara, 2017). Además, cumple una función clave como instrumento de control interno, al incluir de manera detallada las políticas, responsabilidades e instrucciones que deben seguirse en las distintas operaciones de la organización (Molina, Torres, Zambrano, & Martínez, 2016).

Para su elaboración, se tomarán como referencia los lineamientos del Sistema de Gestión de Seguridad de la Información (SGSI) establecidos en la norma ISO/IEC 27001. Este sistema tiene como objetivo proteger la información sensible frente a riesgos derivados de accesos no autorizados, alteraciones indebidas de datos y pérdida de disponibilidad de la información. Asimismo, la norma proporciona una guía estructurada para la elaboración de manuales que cumplan con el ciclo de mejora continua Planificar, Hacer,

Verificar y Actuar (PHVA) (Pinango-Bayas, Méndez-Naranjo, Caiza-Méndez, & Barreno-Naranjo, 2022).

Tabla 12. Planificar, Hacer, Verificar, y Actuar

Ciclo	Descripción
Planificar	Se han identificado los principales riesgos asociados a la etapa de entrada de datos, entre los cuales destacan: correos electrónicos con contenido malicioso, llamadas de personas que se hacen pasar por técnicos de soporte, y ventanas emergentes fraudulentas. A partir de este diagnóstico, se diseñarán estrategias específicas para mitigar cada uno de estos riesgos.
Hacer	Se procederá a la asignación de responsabilidades concretas a los colaboradores del área contable. Asimismo, se establecerán normativas internas y se elaborarán flujogramas detallados para la gestión de cada riesgo previamente identificado.
Verificar	Los responsables asignados deberán supervisar de forma continua el cumplimiento de las políticas implementadas. Además, tendrán la obligación de asegurar que los procedimientos sean aplicados correctamente por todo el personal a su cargo.
Actuar	Se elaborarán informes sistemáticos sobre las incidencias detectadas, y con base en ello, se definirán acciones correctivas que permitan optimizar los controles implementados y fomentar la mejora continua.

Nota. Diseño propio

- Política de Seguridad de la Información

    - Definición:

La presente Política de Seguridad de la Información establece los lineamientos y medidas que deben considerarse para gestionar adecuadamente los riesgos durante la etapa de entrada de datos, especialmente frente a incidentes como correos electrónicos con contenido fraudulento, llamadas de falsos técnicos de soporte y ventanas emergentes maliciosas en la plataforma contable QuickBooks Online.

    - Objetivo:

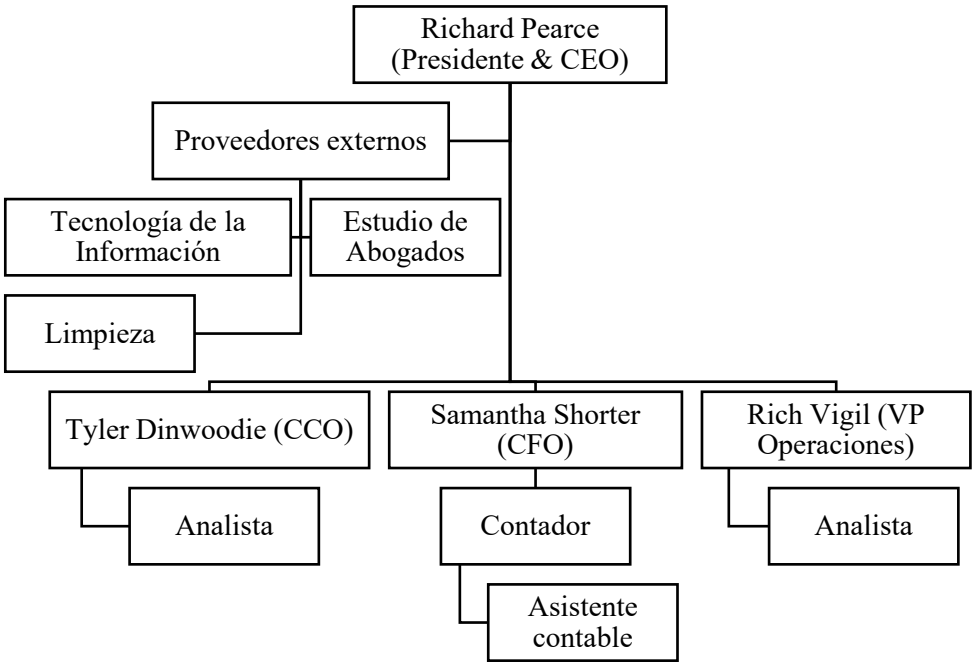
Establecer principios, prácticas y directrices que permitan a la organización asegurar una gestión eficaz y segura del proceso de entrada de datos en el sistema contable. El propósito es salvaguardar la información registrada y prevenir la ocurrencia de riesgos como ataques de phishing, pérdida de datos sensibles y accesos no autorizados.

- Alcance

Esta política está dirigida al área de Contabilidad de South Star Battery Metals Corp. y es de aplicación obligatoria para todos los colaboradores que tengan acceso a la plataforma QuickBooks Online. Comprende las actividades relacionadas con el registro de compras y ventas, la emisión de facturas, la gestión de cobranzas y la conciliación bancaria. La política aplica a todos los procesos, activos de información y personas involucradas directa o indirectamente en estas funciones, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información contable de la organización.

- Roles y responsabilidades:

Figura 4. Área administrativa de South Star Battery Metals Corp.



Nota. Adaptado de Estructura organizacional de South Star Battery Metals Corp: febrero 2025, por South Star Battery Metals Corp., 2025, https://www.southstarbatterymetals.com/ydihapto/2025/03/STS-02_2025_ND_R1.pdf.

Dado que la empresa se encuentra actualmente en una etapa de expansión, no se contempla, al menos en el corto plazo, la incorporación de personal especializado en el área de Tecnologías de la Información. En este escenario, el rol del Chief Financial Officer (CFO) adquiere especial relevancia, al asumir la responsabilidad directa de garantizar el cumplimiento y la supervisión de la presente Política de Seguridad de la

Información. Esta designación responde a la necesidad de centralizar el control de los riesgos vinculados al sistema contable en un cargo con capacidad de decisión estratégica, velando por la protección de los datos financieros de la organización.

Tabla 13 Roles y responsabilidades para el manual de procedimientos

Rol	Responsabilidades
CFO y Responsable de Seguridad de la Información	• Establecer los lineamientos y políticas de seguridad aplicables a los sistemas de información. • Autorizar el acceso y la creación de usuarios en QuickBooks Online. • Supervisar que los registros contables sean precisos y libres de movimientos no autorizados. • Reportar incidentes al área contable y al soporte técnico externo, así como gestionar las acciones correctivas correspondientes. • Coordinar actividades de capacitación en seguridad informática dirigidas al equipo contable. • Supervisar el cumplimiento de la política de seguridad en su totalidad.
Contador	• Velar por la correcta aplicación de la presente política en el área contable. • Implementar medidas de seguridad tales como la verificación de copias de respaldo, uso de antivirus, y aplicación oportuna de actualizaciones. • Registrar las operaciones contables de manera íntegra y precisa. • Asegurar la confidencialidad de la información financiera. • Cumplir con las buenas prácticas de seguridad establecidas en este documento.
Asistente Contable	• Apoyar en la digitación y revisión de información contable. • Garantizar que los datos ingresados en QuickBooks Online sean completos y correctos. • Informar de inmediato a su superior ante cualquier error o anomalía detectada.
Soporte Técnico Externo	• Asesorar en la definición e implementación de las políticas de seguridad, evaluando su viabilidad técnica. • Coordinar y ejecutar capacitaciones para el equipo contable. • Brindar soporte inmediato ante cualquier situación que comprometa la seguridad de la información. • Verificar que se cumplan los lineamientos establecidos en la política de seguridad. • Implementar medidas correctivas urgentes en caso de riesgo inminente. • Proponer acciones de mejora continua en materia de ciberseguridad.

Nota. Adaptado de Pasos para hacer una política de seguridad de la información, por Universidad Internacional SEK, 2019, Repositorio Digital Universidad Internacional SEK.

3.2.2 Normas de gestión y seguridad de la información

- Gestión y control de accesos y perfiles

Esta norma regula el acceso a la plataforma QuickBooks Online, garantizando que solo el personal autorizado del área contable de South Star Battery Metals Corp. tenga acceso al sistema. La Chief Financial Officer (CFO) será la responsable de asignar los usuarios

correspondientes, así como de gestionar y supervisar los accesos, los cuales deberán contar con su autorización previa.

- Niveles de acceso autorizados

  - Colaboradores del área de contabilidad:

1. **CFO**: Titular de la cuenta principal de QuickBooks Online. Posee acceso total a todas las funciones, configuraciones y módulos del sistema. Además, tiene la facultad de agregar, eliminar y modificar los roles de los usuarios secundarios, así como de administrar la suscripción y la configuración general de la cuenta (QuickBooks, 2025).
2. **Contador:** Usuario con perfil de **administrador**. Dispone de privilegios similares a los del propietario de la cuenta, con la salvedad de que no puede modificar los roles de otros usuarios ni acceder a configuraciones administrativas avanzadas (QuickBooks, 2025).
3. **Asistente contable y soporte técnico externo:** Usuarios con perfil **estándar**, con acceso limitado a funciones específicas según sus responsabilidades. Este perfil permite restringir el acceso a determinados procesos y tareas, asegurando el principio de mínimo privilegio (QuickBooks, 2025).

- Credenciales y contraseñas

  - Normas generales de uso:

    - Queda estrictamente prohibido compartir nombres de usuario y contraseñas con personas, tanto internas como externas a la organización.

    - No se permite almacenar credenciales utilizando la función de "recordar contraseña" en navegadores o dispositivos. Asimismo, está prohibido compartirlas a través de aplicaciones no seguras, como WhatsApp.

    - Es obligatorio activar la autenticación multifactor (MFA) que ofrece QuickBooks Online.

1. Esta puede incluir el envío de un código de verificación a través de SMS o correo electrónico.

        - Recomendaciones para la creación de contraseñas (Microsoft, 2025).

1. La contraseña debe tener una longitud mínima de 12 caracteres.
2. Debe incluir al menos una letra mayúscula, una letra minúscula, un número y un símbolo del conjunto ASCII estándar.
3. Se recomienda utilizar una frase fácil de recordar, que no esté relacionada con información personal (como fechas de nacimiento, número de DNI, etc.) y que evite el uso de caracteres consecutivos.
4. Se sugiere el uso de herramientas seguras para la generación de contraseñas encriptadas:
    1. Navegadores como Google Chrome y Microsoft Edge incluyen generadores automáticos de contraseñas seguras.
    2. Tutoriales disponibles en: Chrome – acesse.one/DEARX y Edge – acesse.one/CbDT9

- Buenas prácticas

    - Acuerdo de confidencialidad:

Todo usuario deberá firmar un acuerdo de confidencialidad como requisito previo para acceder al sistema. Este documento formaliza el compromiso de no compartir credenciales de acceso, cumplir con los protocolos de creación de contraseñas seguras y abstenerse de almacenarlas en plataformas no verificadas o poco seguras. Además, establece la obligación de proteger y no divulgar información confidencial de la empresa, incluyendo registros contables, cifras de ventas e información bancaria (ver Anexo 18).

    - Cierre de sesión obligatorio:

Se deberá cerrar sesión en QuickBooks al finalizar la jornada laboral, con el fin de evitar accesos no autorizados.

    - Cambio periódico de contraseña:

Las contraseñas deberán actualizarse cada seis (6) meses.

- Reporte de incidentes:

Cualquier incidente, anomalía o sospecha de riesgo deberá ser reportado inmediatamente al CFO.

- Control y vigilancia

  - Gestión de accesos por parte del CFO:

La CFO será responsable de mantener un registro actualizado de los usuarios, especificando el tipo de acceso, fechas de alta, modificación y baja. También deberá desactivar de manera inmediata los accesos de aquellos colaboradores que ya no formen parte de la organización.

  - Verificación de cambios de contraseña:

El personal externo de soporte TI, en conjunto con la CFO, deberá garantizar que las contraseñas de todos los usuarios se modifiquen semestralmente.

Tal como se explicó en el capítulo anterior, se debe verificar la seguridad de los Sistemas Informáticos Contables (SIC) bajo el cumplimiento de la tríada CIA.

Tabla 14. Alineación de la norma de gestión y seguridad de la información y la tríada CIA

Principio (CIA)	Aplicación en la norma
Confidencialidad	- Asignación de accesos diferenciados por perfil (CFO, contador, asistente). - Prohibición de compartir credenciales. - Firma obligatoria de acuerdos de confidencialidad. - Activación de autenticación multifactor. - Restricciones de almacenamiento inseguro de contraseñas.
Integridad	- Registro y control centralizado de accesos por parte del CFO. - Control de cambios de contraseña cada seis meses. - Obligación de reportar incidentes o anomalías. - Supervisión del historial de accesos y roles activos.
Disponibilidad	- Asignación clara de usuarios según función para evitar bloqueos o conflictos de acceso. - Uso de herramientas de generación de contraseñas para prevenir bloqueos por contraseñas inseguras. - Participación del soporte TI para mantener la operatividad del sistema de autenticación.

Nota. Diseño propio

3.2.3 Norma para la Gestión de Incidentes de Seguridad de la Información

Esta sección establece las acciones a seguir ante amenazas internas o externas, basadas en tres fases: detección, acción inmediata y seguimiento del incidente.

- Riesgos identificados:
    - Correos electrónicos con contenido fraudulento.
    - Llamadas de falsos técnicos que simulan provenir de QuickBooks o utilizan números enmascarados.
    - Ventanas emergentes fraudulentas dentro de la plataforma de QuickBooks.
- Procedimiento de actuación:

Ante la sospecha o detección de un riesgo, este deberá ser reportado de inmediato al CFO, quien será responsable de: Evaluar la gravedad del incidente, determinar las acciones correctivas necesarias, documentar el incidente en el registro correspondiente, y notificar, si corresponde, a otros miembros del equipo o proveedores afectados.

Se recomienda seguir los pasos descritos en el protocolo de respuesta definido para minimizar el impacto y garantizar la trazabilidad de cada evento:

- El CFO será responsable de clasificar el nivel de riesgo de los incidentes reportados. Posteriormente, deberá coordinar las acciones correctivas correspondientes, documentar el incidente y comunicarlo a las partes involucradas.
- En caso de haber compartido información confidencial, se deberá proceder inmediatamente a modificar las contraseñas comprometidas.
- Se debe contactar al equipo de soporte de TI para verificar si hubo accesos no autorizados a la plataforma o alteración de datos.
- Si el equipo de soporte de TI confirma la detección de un programa malicioso, será necesario retener los dispositivos tecnológicos

involucrados (laptop y/o celular) para su revisión y descartar infiltraciones en el sistema contable.

- Buenas prácticas:

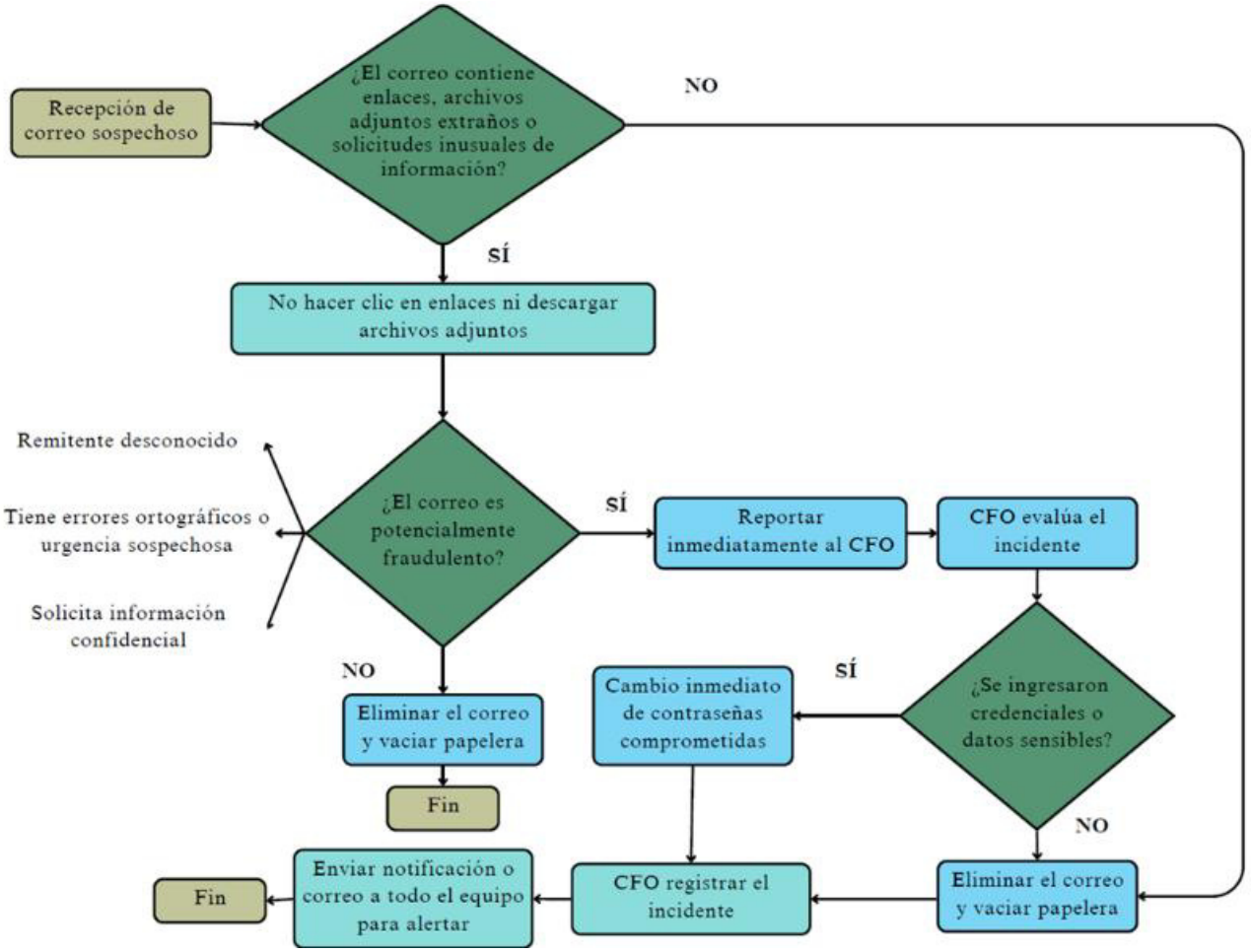
    - El CFO llevará un registro documentado de todos los incidentes de seguridad**.** Además, será responsable de comunicar estos eventos al equipo correspondiente con el fin de generar conciencia y reforzar las medidas de prevención ante futuras recurrencias.

Tabla 15. Alineación de la norma Gestión de incidentes de seguridad con la tríada CIA

Principio (CIA)	Aplicación en la norma
Confidencialidad	- Modificación inmediata de contraseñas comprometidas. - Retención de equipos potencialmente vulnerados. - Comunicación restringida y dirigida sobre el incidente solo a las partes necesarias. - Prevención del acceso no autorizado tras detección de suplantación o phishing.
Integridad	- Registro documentado de incidentes que garantiza trazabilidad. - Verificación por parte del soporte TI ante sospechas de alteración de datos. - Clasificación de nivel de riesgo y acciones correctivas coordinadas por el CFO. - Evaluación de impacto sobre la información contable.
Disponibilidad	- Activación de un protocolo de respuesta rápida para minimizar interrupciones. - Coordinación con soporte técnico para restablecer el sistema si hubo afectaciones. - Documentación de incidentes para prevenir recurrencias que afecten el acceso continuo a QuickBooks Online.

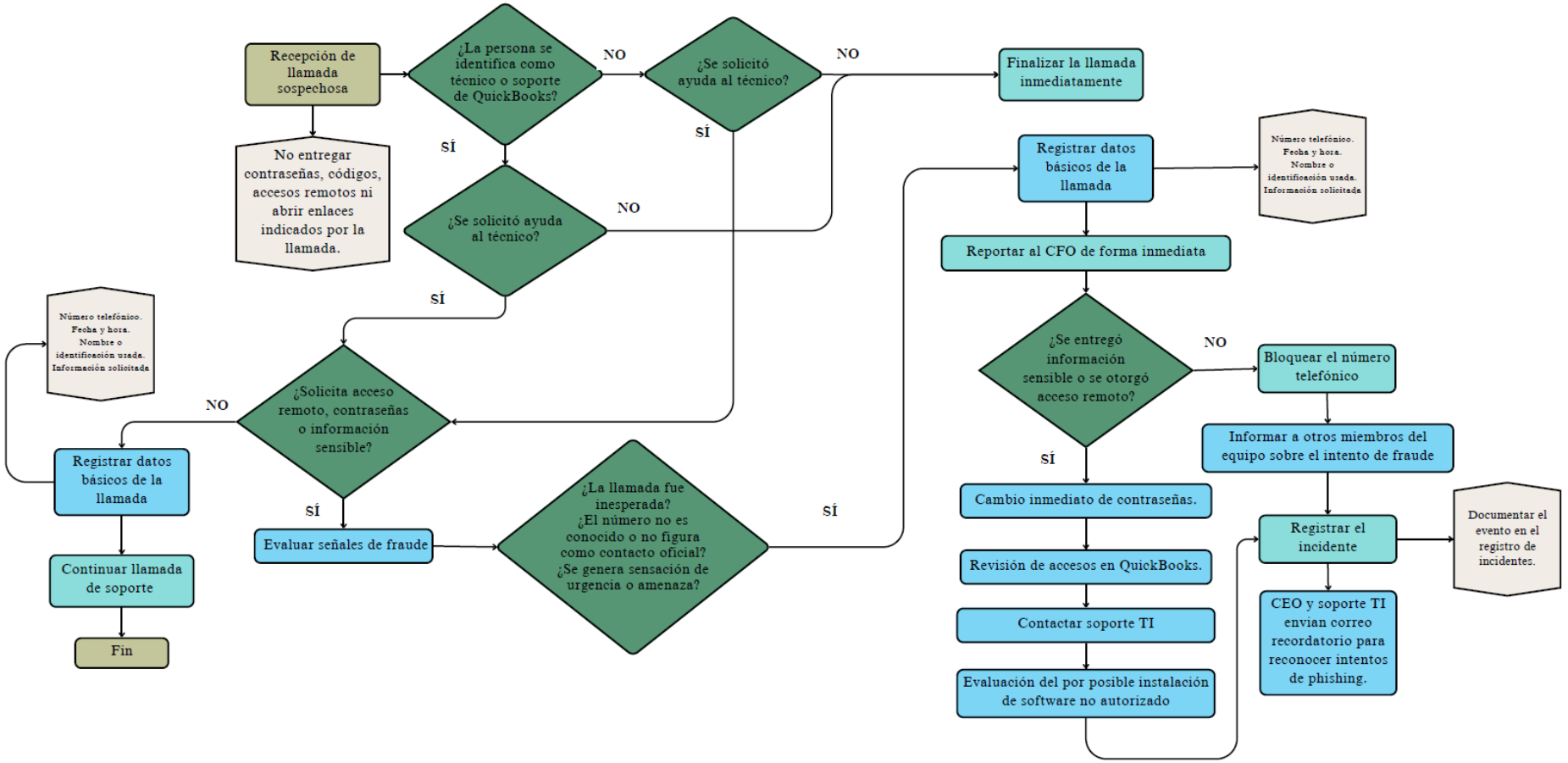
Nota. Diseño propio

Figura 5. Flujograma de acciones a tomar si se reciben correos sospechosos



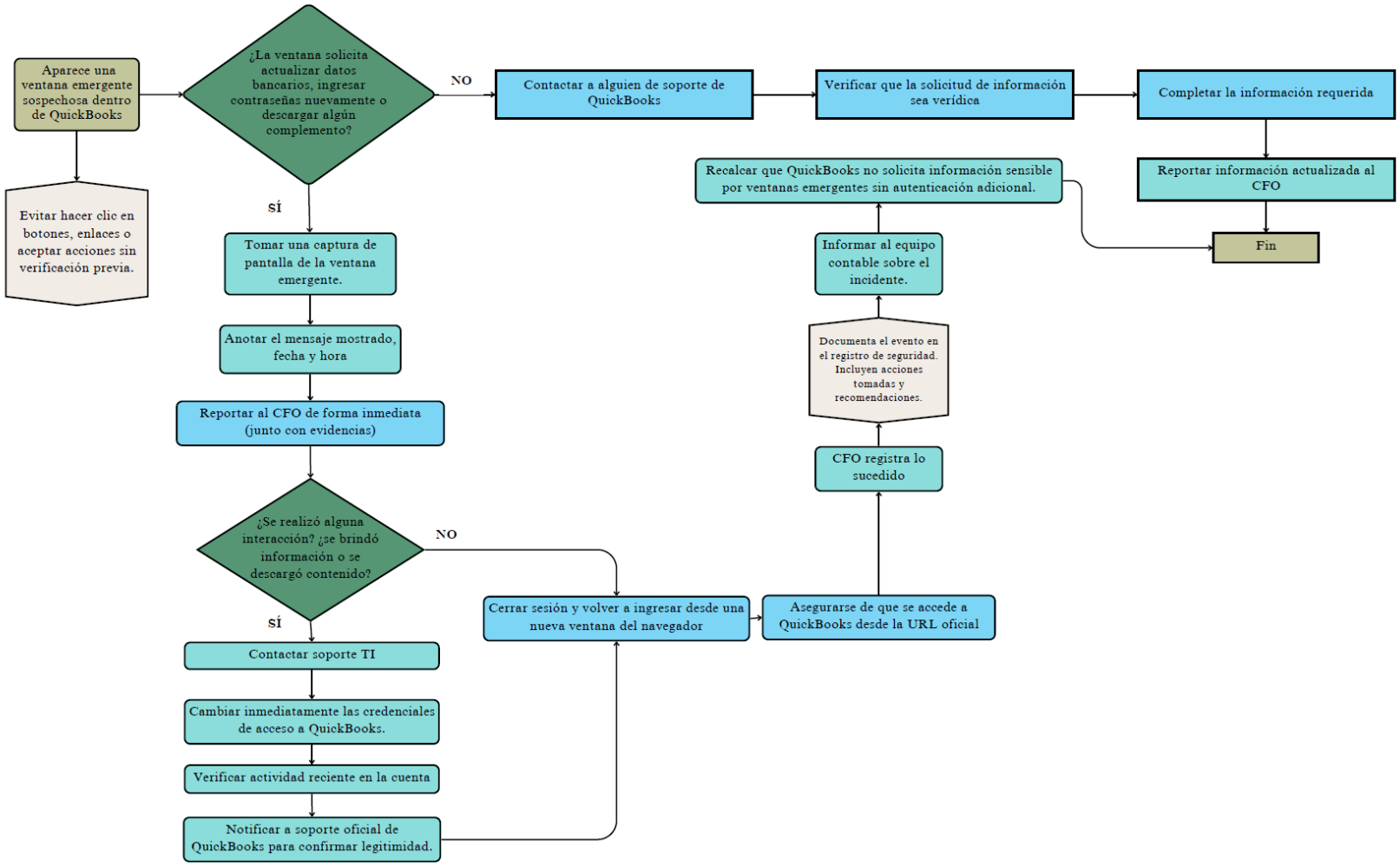
Nota. Diseño propio.

Figura 6. Flujograma de acciones a tomar si se reciben llamada sospechosa de falsos técnicos de soporte



Nota. Diseño propio.

Figura 7. Flujograma de acciones a tomar si se reciben llamada ventana emergente en la plataforma de QuickBooks



Nota. Diseño propio.

3.2.4 Norma para medidas de respaldo y recuperación de información

South Star Mining Corp. gestiona información confidencial relacionada con clientes, precios de venta de metales y costos de producción. En caso de que un agente externo, mediante técnicas de *phishing* —como correos electrónicos, llamadas o ventanas emergentes fraudulentas— acceda a QuickBooks y altere o robe la información registrada, será fundamental contar con un respaldo actualizado.

- Generación de copias de seguridad

El contador será responsable de realizar y resguardar los archivos de respaldo correspondientes a las operaciones diarias de la empresa.

- Respaldo mensual de datos:

Cada fin de mes, el contador deberá realizar una copia de seguridad de la información almacenada en QuickBooks Online. Este respaldo puede efectuarse de manera manual o automática (ver procedimiento en el Anexo 19). Se recomienda la configuración manual, dado que la información será requerida trimestralmente.

- Los datos deberán almacenarse siguiendo los criterios siguientes:
  - Guardar los archivos en una carpeta específica creada en el disco local C del equipo de trabajo, con el fin de asegurar mayor control y protección local.
  - Subir una copia adicional a la nube corporativa (Google Drive o OneDrive), asegurándose de que la cuenta cuente con una contraseña segura y autenticación multifactor.

- Reportes contables requeridos:

- Mensualmente, deberán descargarse y respaldarse los siguientes documentos contables: Libro mayor, Balance general, Estado de resultados, Registro de compras y ventas, y Cuentas por cobrar y por pagar

Los archivos deberán guardarse conforme a las medidas de almacenamiento indicadas anteriormente.

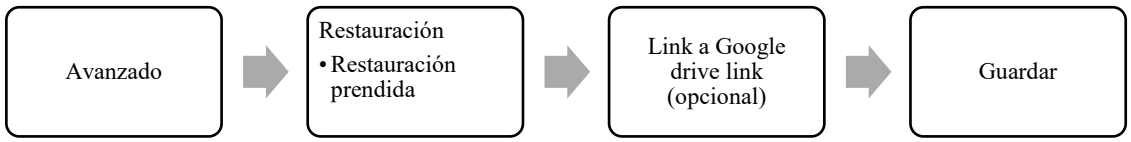
- Plan de recuperación

En caso de producirse un incidente que comprometa la integridad de la información contable, el contador será responsable de coordinar el proceso de recuperación, en estrecha colaboración con el soporte técnico externo asignado.

  - Restauración de datos:

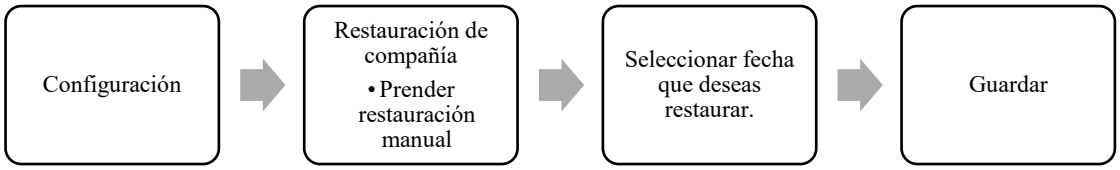
QuickBooks Online cuenta con una funcionalidad que permite restaurar transacciones registradas, definiendo una fecha y hora específica para la recuperación.

Figura 8. Proceso para restauración automatización



Nota. Diseño propio. Adaptado de *How to back up and restore your data | QuickBooks Online Advanced* [Video], por Intuit QuickBooks, 2025, 21 de marzo, YouTube. https://www.youtube.com/watch?v=0EDRlFSV6NY

Figura 9. Proceso para restauración manual



Nota. Diseño propio. Adaptado de *How to back up and restore your data | QuickBooks Online Advanced* [Video], por Intuit QuickBooks, 2025, 21 de marzo, YouTube. https://www.youtube.com/watch?v=0EDRlFSV6NY

Tabla 16. Alineación de la norma medidas de respaldo y recuperación de información contable con la tríada CIA

Principio (CIA)	Aplicación en la norma
Confidencialidad	- Los respaldos son almacenados en ubicaciones controladas: disco local C y nube corporativa con MFA. - Se exige que las cuentas de almacenamiento cuenten con contraseñas seguras. - Se restringe el acceso únicamente al contador y personal autorizado.

Integridad	- Se establece la descarga mensual de libros contables oficiales (libro mayor, balance, etc.), garantizando la conservación exacta de los registros. - Se detalla el procedimiento de restauración en caso de incidentes. - El respaldo asegura la no alteración de los datos.
Disponibilidad	- La información respaldada puede recuperarse manual o automáticamente según necesidad. - Existe un plan definido de recuperación en caso de pérdida o manipulación de información. - Se garantiza el acceso continuo a los datos contables pese a fallos o incidentes.

Nota. Diseño propio

3.2.5 Norma para la gestión del recurso humano en relación con el uso de activos de información

La empresa proporciona a cada colaborador una laptop para fines laborales. No obstante, no restringe su uso exclusivo al ámbito profesional, permitiendo que los empleados utilicen tanto dicha laptop como sus dispositivos móviles personales para actividades laborales y personales de forma simultánea. En este contexto, se establece una política interna alineada con los lineamientos del modelo *Bring Your Own Device (BYOD)* del Gobierno de Canadá (Office of the Privacy Commissioner of Canada, 2025).

- Protección de dispositivos
    - Activación de BitLocker (sistema operativo Windows):

Se deberá activar BitLocker en todas las laptops corporativas. Esta función permite cifrar las unidades de almacenamiento, protegiendo la información frente a accesos no autorizados, especialmente en casos de pérdida o robo del equipo. El cifrado puede aplicarse al disco completo o a unidades específicas, como el disco local C (Microsoft, 2025).

- Contraseñas y métodos de autenticación
    - Verificación en dos pasos para el acceso a los equipos:
        - Se deberá habilitar la autenticación multifactor para todas las computadoras corporativas.
            - Métodos de autenticación recomendados:
                - Bloqueo mediante huella dactilar

- PIN de al menos ocho dígitos
- Contraseña segura, conforme a las directrices de esta política

- Almacenamiento de datos

  - Información sensible:

Toda información sensible y confidencial deberá almacenarse exclusivamente en el disco local C de la laptop corporativa, evitando la combinación de datos personales con información empresarial.

  - Eliminación de información sensible:

El personal de soporte técnico estará facultado para eliminar información confidencial en caso lo considere necesario para preservar la seguridad de los datos corporativos.

- Instalación de antivirus

  - Gestión de protección antivirus:

El contador será responsable de mantener un registro actualizado de los dispositivos que cuentan con antivirus instalado. Asimismo, deberá asegurarse, en coordinación con el soporte técnico, de que todos los equipos corporativos dispongan de protección activa.

  - Configuración de firewall

    - Activación del firewall de Windows Defender:

Tanto el contador como el soporte técnico deberán garantizar que el firewall de Windows Defender se encuentre activo en todos los dispositivos. Esta herramienta alerta ante intentos de conexión no autorizados y permite configurar el bloqueo o autorización de aplicaciones específicas según criterios de seguridad.

Tabla 17 Alineación de la norma Gestión del recurso humano y activos de información con la tríada CIA

Principio (CIA)	Aplicación en la norma
Confidencialidad	- Se exige el cifrado de discos mediante BitLocker para restringir accesos no autorizados en caso de pérdida o robo del equipo. - La información sensible debe almacenarse exclusivamente en el disco local C, evitando su exposición.

Integridad	- Se establece la eliminación controlada de datos sensibles por parte del soporte técnico cuando haya riesgo de exposición. - Se recomienda autenticación fuerte para prevenir modificaciones no autorizadas de los activos digitales.
Disponibilidad	- La protección con antivirus y firewall garantiza que los dispositivos se mantengan operativos y protegidos contra malware o bloqueos del sistema. - El uso de métodos de autenticación evita interrupciones por accesos indebidos.

Nota. Diseño propio

CONCLUSIONES

QuickBooks Online es un software contable que destaca por su interfaz intuitiva y accesibilidad operativa, permitiendo su uso por usuarios con distintos niveles de experiencia. Al operar en la nube, facilita el acceso remoto y la colaboración simultánea, lo que agiliza el trabajo en equipo. Su integración con aplicaciones bancarias y otros sistemas permite la automatización de transacciones y la generación de reportes en tiempo real. Además, la incorporación de funciones basadas en inteligencia artificial optimiza procesos contables rutinarios y reduce la carga operativa.

No obstante, el presente estudio ha identificado riesgos significativos asociados a su uso, particularmente en la fase de entrada de datos. Entre los principales se encuentran el fraude, accesos no autorizados, errores en el procesamiento de información y generación de reportes, así como suplantación de identidad. Estos riesgos se traducen en eventos como pagos indebidos, hackeo de cuentas, pérdida de datos sensibles y fallas en los reportes financieros, con posibles impactos económicos, reputacionales y legales.

Los resultados de las entrevistas, encuesta y el análisis de quejas en plataformas oficiales revelan que los ataques de phishing, las ventanas emergentes fraudulentas y la falta de control en los accesos representan amenazas críticas. Estas podrían causar pérdidas económicas de hasta USD 2,473,442, evidenciando la necesidad urgente de adoptar medidas de seguridad. Además, se comprobó que el soporte técnico de QuickBooks no garantiza la protección de datos ni asume responsabilidad ante pérdidas de información, lo que hace indispensable la realización periódica de respaldos.

La investigación se centró en la empresa South Star Battery Metals Corp., la cual no cuenta con un área de Tecnología de la Información ni protocolos formales de seguridad. Esta ausencia incrementa su exposición a ataques informáticos y errores operativos. Por ello, se propuso la implementación de un manual de seguridad basado en la norma ISO/IEC 27001, con políticas sobre acceso, contraseñas seguras, cifrado de datos y protocolos de respuesta ante incidentes. Esta medida representa una solución viable para reducir significativamente las amenazas detectadas.

Las propuestas desarrolladas en esta investigación pueden ser replicadas en otras pequeñas y medianas empresas del sector, sin requerir grandes inversiones ni complejidad en su implementación. Su éxito radica en la formación del personal y en la adecuada aplicación de controles administrativos y tecnológicos.

Finalmente, este estudio pone en valor el rol del contador en la era digital. El profesional contable del siglo XXI no solo debe interpretar información financiera, sino también velar por su integridad, seguridad y disponibilidad. Para ello, debe estar capacitado en el manejo de sistemas de información, análisis de riesgos y seguridad digital, participando activamente en la selección, evaluación y auditoría de plataformas contables, con el fin de garantizar su confiabilidad, eficiencia y resiliencia ante amenazas emergentes.

RECOMENDACIONES

South Star Battery Metals Corp. debe establecer un manual de seguridad de la información alineado con la norma ISO/IEC 27001, el cual contemple medidas preventivas frente a los riesgos detectados. Entre las prioridades se encuentra la implementación de políticas de acceso restringido y autenticación multifactor, ya que la ausencia de barreras de protección básicas facilita el acceso no autorizado y la posible pérdida de datos sensibles. Asimismo, se recomienda incorporar la encriptación de la información contable y un sistema de respaldo automatizado de datos, con claves robustas que imposibiliten su descifrado por parte de terceros. Este respaldo debe permitir la recuperación rápida ante escenarios de pérdida, alteración o robo de información.

En paralelo, se sugiere establecer protocolos de monitoreo continuo para la detección de accesos sospechosos o intentos de fraude, así como procedimientos de respuesta ante incidentes que aseguren una actuación oportuna y documentada.

El riesgo de fraude y acceso no autorizado puede mitigarse de forma significativa mediante la capacitación periódica del personal. Se recomienda implementar talleres trimestrales enfocados en temas como: identificación de ataques de phishing y ventanas emergentes fraudulentas; uso correcto de contraseñas seguras; buenas prácticas de acceso en entornos en la nube; y pasos a seguir ante un incidente de seguridad. Esta estrategia permitirá no solo fortalecer la conciencia del riesgo, sino también fomentar una cultura organizacional orientada a la ciberseguridad.

Asimismo, se recomienda la incorporación de herramientas tecnológicas como software de monitoreo, firewalls especializados, antivirus y sistemas UTM (Unified Threat Management), que refuercen las capacidades de seguridad del sistema QuickBooks. En caso de ciberataques o fallas del sistema, la empresa deberá contar con un plan de recuperación ante desastres, en el cual se detallen responsabilidades por área, protocolos de recuperación de datos, y estrategias de comunicación ante filtraciones que involucren información financiera crítica.

Finalmente, se propone la realización de auditorías semestrales para evaluar la eficacia de los controles implementados, identificar nuevas vulnerabilidades y ajustar las medidas según la evolución del entorno digital. Aunque QuickBooks ofrece una solución accesible para pequeñas y medianas empresas, su nivel de seguridad podría resultar limitado frente a las demandas de una organización en etapa operativa dentro del sector minero.

De forma complementaria, se sugiere que futuras investigaciones exploren la comparación de riesgos y medidas de seguridad entre distintas plataformas contables, como SAP, Oracle NetSuite, Xero y Microsoft Dynamics 365. Este enfoque contribuiría a generar un marco más amplio y robusto para la selección e implementación de sistemas contables digitales con altos estándares de seguridad.

BIBLIOGRAFÍA

Abacus. (2024). *QuickBooks for SMBs: Is It Worth It?* Retrieved from Go Abacus: https://goabacus.com/quickbooks-for-smbs-is-it-worth-it/

ACCID. (2019). Prevención y gestión de riesgos. *Revista de Contabilidad y Dirección, 28*.

Action1 Corporation. (2025). *Software vulnerability ratings report 2025.* Retrieved from https://www.action1.com/wp-content/uploads/2025/06/Software-Vulnerability-Ratings-Report-2025.pdf

Ahola, M. (n.d.). *The Role of Human Error in Successful Cyber Security Breaches*. Retrieved from Usecure: https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches

Al- Khasawneh, R. O. (2020). *Role of Electronic Accounting Information Systems in Reducing the Phenomenon of Tax Evasion in Facilities Subject to Income and Sales Tax in the Hashemite Kingdom of Jordan* (2 ed., Vol. 10). International Journal of Accounting and Financial Reporting. doi:https://doi.org/10.5296/ijafr.v10i2.17298

Amazon. (2024). *¿Qué es SQL (lenguaje de consulta estructurada)?* Retrieved from Herramientas para desarrolladores: https://aws.amazon.com/es/what-is/sql/

ASOCEX. (2015). GPF OCEX 1500: Evidencia de auditoría. Asociación de Órganos de Control Externo Autonómicos (ASOCEX). *Grupo de Trabajo de Procedimientos de Fiscalización.* Retrieved from https://asocex.es/wp-content/uploads/2017/02/GPF-OCEX-1500_Evidencia-de-auditoria.pdf

AWS. (2024). *Nivel gratuito de AWS.* Retrieved from AWS: https://aws.amazon.com/es/free/?gclid=Cj0KCQjwm7q-BhDRARIsACD6-fWC2OW_fG2M2e0DgAlX65-jKx27XBIFaiBkuBQ7iHbKAqAIjo6Z2ggaAjTkEALw_wcB&trk=8fa18207-f2c2-4587-81a1-f2a3648571b3&sc_channel=ps&ef_id=Cj0KCQjwm7q-BhDRARIsACD6-fWC2OW_fG2M2e0DgAlX65-jKx27XBIFaiBkuBQ

AWS. (2025). *Servicios en la nube de AWS.* Retrieved from AWS: https://aws.amazon.com/es/products/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-

order=asc&awsf.re%3AInvent=*all&awsf.Free%20Tier%20Type=*all&awsf.tech-category=*all

AWS Amazon. (2024). *What is SaaS (Software as a Service)?* Retrieved from https://aws.amazon.com/what-is/saas/

Borgeaud, A. (2025, March 10). *Share of CISOs in companies in the United States in agreement that human error is their organization's biggest cyber vulnerability from 2021 to 2024*. Retrieved from Statista: https://www.statista.com/statistics/1448350/ciso-human-error-organization-cyber-vulnerability-global/

Cabric, M. (2015). *Corporate security management : Challenges, risks, and strategies.* Elsevier Science & Technology. doi:http://dx.doi.org/10.1016/B978-0-12-802934-3.00011-1

Ceballo, M. (2024, Noviembre 15). *Estos son los errores contables más comunes en una empresa*. Retrieved from Areandina: https://www.areandina.edu.co/blogs/estos-son-los-errores-contables-mas-comunes-en-una-empresa

CEPLAN. (2024, Julio). *Incremento del ciberdelito*. Retrieved from Presidencia de Consejo de Ministros: https://observatorio.ceplan.gob.pe/ficha/t85

CertiSur. (2024). *¿Qué es el cifrado?* Retrieved from CertiSur S.A.: https://www.certisur.com/shop/faq/ssl/what-is-encryption

Charbonneau, S. (2011). The role of user-driven security in data loss prevention. *Computer Fraud & Security*, 5-8. doi:https://doi.org/10.1016/S1361-3723(11)70112-9

CISOMAG. (2020, September 12). *"Psychology of Human Error" Could Help Businesses Prevent Security Breaches.* Retrieved from CISOMAG: https://cisomag.com/psychology-of-human-error-could-help-businesses-prevent-security-breaches/

Coker, J. (2025, Marzo 11). *95% of Data Breaches Tied to Human Error in 2024*. Retrieved from InfoSecurity: https://www.infosecurity-magazine.com/news/data-breaches-human-error/

Cook, B. (2025, Febrero 27). *QuickBooks Online vs. Desktop: ¿Qué solución de contabilidad QuickBooks es adecuada para su negocio?* Retrieved from Tipalti: https://tipalti.com/blog/quickbooks-online-vs-desktop/

Cortés, M. (2025, Marzo 21). *El phishing creció un 86% en 2024 y marca un nuevo desafío.* Retrieved from CIO EDIWorld: https://iworld.com.mx/el-phishing-crecio-un-86-en-2024-y-marca-un-nuevo-desafio/?utm_source=chatgpt.com

Cortés, M. (2025, Marzo 21). *El phishing creció un 86% en 2024 y marca un nuevo desafío.* Retrieved from CIO Ediworld: https://iworld.com.mx/el-phishing-crecio-un-86-en-2024-y-marca-un-nuevo-desafio/?utm_source=chatgpt.com

Deemer, B. (2024, Julio 17). *existen riesgos asociados con el uso de herramientas en la nube, como la seguridad de los datos, errores humanos, la dependencia de la conectividad (internet y servidores externos) y la vulnerabilidad del sistema debido a la necesidad de mantener actuali*. Retrieved from AuditBoard: https://www.auditboard.com/log/what-are-the-security-risks-of-cloud-computing/

Díaz-Bravo, L., Torruco-García, U., Martínez-Hernández, M., & VarelaRuiz, M. (2013). La entrevista, recurso flexible y dinámico. *Investigación en Educación Médica*. Retrieved from La entrevista, recurso flexible y dinámico

Digicert. (2025). *¿Qué Es SSL, TLS & HTTPS?* Retrieved from Digicert: https://www.digicert.com/es/what-is-ssl-tls-and-https

DIMTEC. (2025, Marzo 13). *¿Por qué las APIs son un objetivo atractivo para los atacantes?* Retrieved from Digital Media Technologies: https://www.dimtec.com/blog/apis-inseguras-la-amenaza-oculta-que-puede-exponer-los-datos-de-tu-empresa-y-como-protegerlos

Dumoy, J. S. (1999). Los factores de riesgo. *Revista Cubana de Medicina General Integral, 15*(4), 446-452. Retrieved from http://scielo.sld.cu/pdf/mgi/v15n4/mgi18499.pdf

Elmasri, R., & Navathe, S. (2015). *Fundamentals of Database Systems* (7th ed. ed.). Pearson.

Enabl. (2023). *The Human Factor in Cybersecurity: How to Mitigate Human Errors*. Retrieved from Enabl: https://www.enabl.work/blog/the-human-factor-in-cybersecurity-managing-human-errors

Encyclopedia Britannica. (n.d.). *System*. Retrieved from Encyclopedia Britannica: https://www.britannica.com/dictionary/system

Enlyft. (2024). *Companies using QuickBooks Online*. Retrieved from Enlyft: https://enlyft.com/tech/products/quickbooks-online

Enlyft. (2025). *Companies using QuickBooks Online*. Retrieved from QuickBooks Online: https://enlyft.com/tech/products/quickbooks-online#:~:text=QuickBooks%20Online%20is%20most%20often,1M%2D10M%20dollars%20in%20revenue.

Forbes Staff. (2024, Abril 9). *La pérdida de datos le puede costar más de 1 millón de dólares a las empresas*. Retrieved from Forbes Perú: https://forbes.pe/tecnologia/2024-04-09/la-perdida-de-datos-le-puede-costar-mas-de-1-millon-de-dolares-a-las-empresas

Fortinet. (2024). *Tríada CIA: confidencialidad, integridad y disponibilidad*. Retrieved from Fortinet: https://www.fortinet.com/lat/resources/cyberglossary/cia-triad

Fuesz, B. (2023, Junio 16). *Security and information sharing: what you should know about QuickBooks*. Retrieved from Technology & Innovation: https://www.sage.com/en-us/blog/security-and-information-sharing-what-you-should-know-about-quickbooks/?utm_source=chatgpt.com

Goodwin, M. (2024). *What is an SLA?* Retrieved from IBM: https://www.ibm.com/think/topics/service-level-agreement

Grolinger, K., Higashino, W. A., Tiwari, A., & Capretz, M. A. (2013). *Data management in cloud environments: NoSQL and NewSQL data stores* (Vol. 2). Journal of Cloud Computing.

Ha, J. (2024, Mayo 16). *What is QuickBooks? Updated 2024 – Simplify Your Business Finances*. Retrieved from Beehexa: https://www.beehexa.com/blog/what-is-quickbooks/

Haan, K., & Watts, R. (2024, Junio 3). *America's Password Habits: 46% Report Having their Password Stolen Over the Last Year*. Retrieved from Forbes: https://www.forbes.com/advisor/business/software/american-password-habits/

Hamel, L. (2024, Marzo 18). *FBI's IC3 Report: Losses from Cybercrime Surpass $12.5 Billion—a New Record* . Retrieved from ProofPoint: https://www.proofpoint.com/us/blog/email-and-cloud-threats/fbis-ic3-report-losses-cybercrime-surpass-125-billion-new-record

Hargrave, M. (2023, Octubre 31). *Artificial intelligence (AI) for small business: 8 ways to use artificial intelligence as a business owner*. Retrieved from Running a Business: https://quickbooks.intuit.com/r/running-a-business/ai-for-small-business/#determine

Harjinder, S. L., Thompson, A., Titis, E., & Stephens, P. (2025). Analysing cyber attacks and cyber security vulnerabilities in the university sector. *Computers, 14*(2), 49. doi:https://doi.org/10.3390/computers14020049

Hassan, D. (2025, Febrero 13). *6 errores de API que ocurren con frecuencia y cómo evitar que sucedan.* Retrieved from Astera: https://www.astera.com/es/type/blog/api-errors/

Hayes, S. M. (2020). *El Impacto de los delitos financieros.* Retrieved from KPMG: https://assets.kpmg.com/content/dam/kpmg/mx/pdf/2020/06/El-impacto-de-los-delitos-financieros.pdf?utm_source=chatgpt.com

Hernández, H. M., Cantero, L. G., Vidal, D. M., & Villadiego, L. R. (2019). Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia. *Revista Venezolana de Gerencia, 2*, 528-541. Retrieved from https://www.redalyc.org/journal/290/29063446029/html/

Hernández, H. M., Cantero, L. G., Vidal, D. M., & Villadiego, L. R. (2019). Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia. *Revista Venezolana de Gerencia, 2*.

Horngren, C. T., Smith Bamber, L., & Harrison, W. T. (2003). *Contabilidad.* Retrieved from Pearson Educación: https://www-ebooks7-24-com.up.idm.oclc.org/?il=4409

Hund, K., Porta, D. L., Fabregas, T. P., Laing, T., & Drexhage, J. (2020). *Minerals for Climate Action:The Mineral Intensity of the Clean Energy Transition.* Retrieved from Banco Mundial: https://documents1.worldbank.org/curated/en/099052423172525564/pdf/P16627806f5aa400508f8c0bdcba0878a3e.pdf

IBM. (2022, Diciembre 12). *¿Qué es una base de datos NoSQL?* Retrieved from IBM: https://www.ibm.com/es-es/think/topics/nosql-databases

IBM. (2024, Agosto 15). *CISOs list human error as their top cybersecurity risk*. Retrieved from IBM: https://www.ibm.com/think/insights/cisos-list-human-error-top-cybersecurity-risk#:~:text=Proofpoint's%202024%20Voice%20of%20the,the%20reasons%20for%20the%20reduction.

Intuit. (2023, Setiembre 6). Intuit Assist for QuickBooks.

Intuit QuickBooks. (2024). *Security*. Retrieved from Intuit QuickBooks: https://quickbooks.intuit.com/global/security/

Intuit QuickBooks. (2025). *Grow confidently with automations by your side*. Retrieved from Intuit QuickBooks: https://quickbooks.intuit.com/ai-accounting/

Intuit QuickBooks. (2025). *QuickBooks Support*. Retrieved from Intuit Quickbooks: https://quickbooks.intuit.com/learn-support/en-us/help-search/34?filter=location&q=hack

Intuit Quickbooks. (2025). *Security*. Retrieved from Intuit Quickbooks: https://quickbooks.intuit.com/global/security/?utm_source=chatgpt.com

ISO 14224. (2016). *Petroleum, petrochemical and natural gas industries collection and exchange of reliability and maintenance data for equipment.* International Standard Organisation. Retrieved from International Standard Organisation.

ISO/IEC 27001:2013. (2013). Information technology — Security techniques — Information security management systems — Requirements. *International Organization for Standardization*.

ITRC. (2024, Enero). *2023 Data Breach Report.* Retrieved from Identity Theft Resource Center: https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf

Kosinski, M. (2024, Mayo 24). *What is a data breach?* Retrieved from IBM: https://www.ibm.com/think/topics/data-breach

Latimer, J. (2024, Julio 25). *Do Large Companies Use QuickBooks?* Retrieved from Medium: https://medium.com/@jakemlatimer/do-large-companies-use-quickbooks-e9435be0607e

Laudon, K. C., & Laudon, J. P. (2016). *Sistemas de información gerencial.* Retrieved from Pearson Educación: https://www-ebooks7-24-com.up.idm.oclc.org/?il=3300

Laudon, K. C., & Laudon, J. P. (2020). *Management Information Systems: Managing the Digital Firm.* Pearson.

Lenis, A. (2023, Mayo 17). *Qué es la interfaz de usuario, qué tipos existen y ejemplos*. Retrieved from Hubspot: https://blog.hubspot.es/website/interfaz-usuario#que-es

Luettmann, B. M., & Bender, A. C. (2007). Man-in-the-middle attacks on auto-updating software. *Bell Labs Technical Journal, 3*, 131-138. doi:10.1002/bltj.20255

McNamara, C. (2020). *Field Guide to Consulting and Organizational Development.* Authenticity Consulting LLC.

Mehta, P. (2022, Julio 22). *Stages of Data Vulnerability and the Risks*. Retrieved from BitRaser: https://www.bitraser.com/article/stages-of-data-vulnerability-risks.php?srsltid=AfmBOooBvdnrQwqHXb6Szce3ATS_5Ncd969BdjfdUC7pPSw5jzzTMUhI

Microsoft. (2025). *Crear y usar contraseñas seguras*. Retrieved from Microsoft Support: https://support.microsoft.com/es-es/windows/crear-y-usar-contrase%C3%B1as-seguras-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb

Microsoft. (2025). *Device Encryption in Windows*. Retrieved from Windows security, safety, and privacy: https://support.microsoft.com/en-us/windows/device-encryption-in-windows-cf7e2b6f-3e70-4882-9532-18633605b7df

Microsoft Azure. (2024). *What is SaaS?* Retrieved from https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-saas#:~:text=Software%20as%20a%20service%20(SaaS,from%20a%20cloud%20service%20provider.

Mohammed, K. S., Kadem Hamed, Q., Ahmed, M. A., Mohammed, K. S., & Ahmed, Q. K. (2024). *The Impact of Accounting Information Systems on Tax Performance* (Vol. 12). American Journal of Economics and Business Management. doi:https://n9.cl/wypohs

Molina, M. A., Torres, M. M., Zambrano, R. O., & Martínez, J. E. (2016). Manual de procedimiento en la empresa. *Revista Caribeña de Ciencias Sociales*. Retrieved from http://www.eumed.net/rev/caribe/2016/11/manual.html

Nor, F. B., Jalil, K. A., & Manan, J.-L. A. (2012). Mitigating man-in-the-browser attacks with hardware-based authentication scheme. *International Journal of Cyber-Security and Digital Forensics, 3*.

O'Brien, J. A., & Marakas, G. M. (2011). *Management Information Systems.* McGraw-Hill. Retrieved from McGraw-Hill.

Office of the Privacy Commissioner of Canada. (2025). *Is a Bring Your Own Device (BYOD) Program the Right Choice for Your Organization?* Retrieved from Mobile devices and online services at work: https://www.priv.gc.ca/en/privacy-topics/employers-and-employees/mobile-devices-and-online-services-at-work/gd_byod_201508/#heading-0-0-0-18

OTC Markets. (2025, Marzo 8). *South Star Battery Metals Corp.* Retrieved from Company Profile: https://www.otcmarkets.com/stock/STSBF/profile

Oz, E. (2008). Sistemas de información de las empresas. In E. Oz, *Administración de los Sistemas de Información* (Vol. Quinta edición, pp. 7-19). Great Valley: Cengage Learning Editores.

Pangestu, J. C., & Akwila, K. (2024). *Improving MSME Performance: Strategic Management Accounting, Accounting Information Systems, And Management Control Systems Moderated By Financial Technology* (3 ed., Vol. 5). Journal of

Accounting and Finance Management. doi:https://doi.org/10.38035/jafm.v5i3.691

Pérez, A. (2024, Julio 15). *Tipos de sistemas de información más utilizados por las empresas.* Retrieved from OBS Business School: https://www.obsbusiness.school/blog/tipos-de-sistemas-de-informacion-mas-utilizados-por-las-empresas

Piccoli, G., & Pigni, F. (2019). *Information Systems for Managers with cases.* Prospect Press, Inc.

Pinango-Bayas, Á., Méndez-Naranjo, P., Caiza-Méndez, D., & Barreno-Naranjo, D. (2022). Plan de seguridad para plataformas web empleando normas ISO-27001 y considerando el OWASP top 10-2017. *Revista Ciencia UNEMI, 15*(40), 01-15. doi:https://doi.org/10.29076/issn.2528-7737vol15iss40.2022pp1-15p

Prasad, A., & Green, P. (2015). *Organizational competencies and dynamic accounting information system capability: impact on AIS processes and firm performance* (3 ed., Vol. 29). Journal of Information Systems. doi:10.2308/isys-51127

PricewaterhouseCoopers. (2024). *Enfrentar los desafíos del futuro y abordar los riesgos con inteligencia.* Retrieved from Encuesta Global de Crimen y Fraude Económico de PwC Colombia 2024: https://www.pwc.com/co/es/publicaciones/gecs/2024/global-economic-crime-survey-2024.pdf

Proofpoint. (2024). *¿Qué es el email spoofing?* Retrieved from Proofpoint: https://www.proofpoint.com/es/threat-reference/email-spoofing?utm_source=chatgpt.com

QuickBooks. (2024, Febrero 28). *QuickBooks Online or Desktop: Which offers real-time data safeguards, accessibility, and collaboration for your small business?* Retrieved from QuickBooks: https://quickbooks.intuit.com/r/product-update/quickbooks-online-or-desktop-data-security/

QuickBooks. (2025). *Manage your team*. Retrieved from Intuit QuickBooks: https://quickbooks.intuit.com/team-management/

QuickBooks Support. (2025, Marzo). *Secure your Intuit Account and prevent lockout with extra verification methods*. Retrieved from QuickBooksHelp: https://quickbooks.intuit.com/learn-support/en-us/help-article/security-risk/verify-account-multi-factor-authentication/L2Xp0GNiT_US_en_US

Redacción EC. (2023). *"Tu dispositivo se encuentra en peligro": alertan que estafadores se hacen pasar por "soporte técnico" para engañar a usuarios*. Retrieved from Actualidad: https://elcomercio.pe/tecnologia/actualidad/alertan-que-estafadores-se-hacen-pasar-por-soporte-tecnico-para-enganar-a-usuarios-ciberseguridad-fbi-espana-mexico-colombia-usa-noticia/

Reddit. (2022). *QuickBooks internal Pop Up SCAM*. Retrieved from Reddit: https://www.reddit.com/r/QuickBooks/comments/wzzzg0/quickbooks_internal_pop_up_scam/

Reddit. (2023). *Fraudulent payroll transaction*. Retrieved from Reddit: https://www.reddit.com/r/QuickBooks/comments/1144eul/fraudulent_payroll_transaction/

Reddit. (2023). *Is this a scam?* Retrieved from Reddit: https://www.reddit.com/r/QuickBooks/comments/1hdklpp/is_this_a_scam/

Reddit. (2025). *QuickBooks*. Retrieved from Reddit: https://www.reddit.com/r/QuickBooks/

Rodríguez, C. P. (2011). ¿Cómo construir una matriz de riesgo operativo? *Ciencias Económicas 29*, 629-635. doi:https://doi.org/10.15517/rce.v29i1.7061

Rodríguez-Cruz, Y., & Pinto, M. (2018). Modelo de uso de información para la toma de decisiones estratégicas en organizaciones de información. *Transinformação, 30*(1), https://doi.org/10.1590/2318-08892018000100005.

Romney, M. B., & Steinbart, P. J. (2018). *Accounting Information Systems*. Retrieved from Pearson: https://library.iti.ac.id/opac/repository/EB2020002-1-151.pdf

Ruiz, E. G., & Yoder, T. (2024, Marzo 11). *12 QuickBooks Statistics You Need To Know*. Retrieved from Fit Small Business: https://fitsmallbusiness.com/quickbooks-statistics/#:~:text=3.,%25%20and%209%25%2C%20respectively.

Salazar-Escorcia, L. S. (2020, Enero 24). Investigación Cualitativa: Una respuesta a las Investigaciones Sociales Educativas. *Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología*, 101-110. doi:10.35381/cm.v6i11.327

SAP. (2024). *¿Qué es una API (interfaz de programación de aplicaciones)?* Retrieved from SAP Integration Suite: https://www.sap.com/latinamerica/products/technology-platform/integration-suite/what-is-api.html

Sectigo. (2025, Enero 9). *Preguntas frecuentes sobre certificados SSL: Su guía completa desde los principios básicos hasta los más avanzados*. Retrieved from Sectigo Limited: https://www.sectigo.com/es/recursos/preguntas-frecuentes-certificados-ssl

Secureframe. (2024, Marzo 19). *101 de las últimas estadísticas de violaciones de datos para 2024.* Retrieved from Secureframe: https://secureframe.com/es-es/blog/data-breach-statistics?utm_source=chatgpt.com

SEDAR+. (2025, Marzo 8). *Condensed Consolidated Interim Financial Statements for the year endend 2024 and 2023.* Retrieved from SEDAR: https://www.sedarplus.ca/

SentinelOne. (2024). *17 riesgos de seguridad de la computación en la nube en 2025* . Retrieved from SentinelOne: https://www.sentinelone.com/cybersecurity-101/cloud-security/security-risks-of-cloud-computing/

Shorter, S. (2025, Marzo 15). Consultas sobre estructura organizacional de South Star Battery Metals Corp. (M. Berrocal, Interviewer)

Sousa, K. J., & Oz, E. (2017). *Administración de los sistemas de información.* Retrieved from Cengage Learning: https://www-ebooks7-24-com.up.idm.oclc.org/?il=3234

South Star Battery Metals. (2024, Diciembre). *Corporate Presentation: Feb. 2025.* Retrieved from South Star Battery Metals Highlights: https://www.southstarbatterymetals.com/ydihapto/2025/03/STS-02_2025_ND_R1.pdf

South Star Battery Metals. (2024). *Sustainability.* Retrieved from South Star Battery Metals: https://www.southstarbatterymetals.com/sustainability/

South Star Battery Metals Corp. . (n.d.). *South Star Battery Metals Corp.* . Retrieved from Company Overview: https://www.southstarbatterymetals.com/about-us/

South Star Battery Metals Corp. (2025, Marzo 8). *Company Overview.* Retrieved from South Star Battery Metals Corp.: https://www.southstarbatterymetals.com/about-us/

South Star Mining Corp. (2015). *Meeting Sustainable Development Goals.* Retrieved from South Star Mining Corp.: https://www.southstarbatterymetals.com/ydihapto/2021/05/STS-Meeting-Sustainable-Development-Goals.pdf

Stair, R. M., & Reynolds, G. W. (2017). *Principios de sistemas de información.* Retrieved from Cengage Learning: https://www-ebooks7-24-com.up.idm.oclc.org/?il=3979

Stair, R. M., & Reynolds, G. W. (2017). *Principios de Sistemas de Información* (10a ed.). México D.F: CENGAGE Learning.

SUNAFIL. (2020). *Manual para Identificación de Peligros y Evaluación de Riesgos y Determinación de Controles (IPERC).* Retrieved from SUNAFIL: https://cdn.www.gob.pe/uploads/document/file/3929426/Manual%20para%20Identificaci%C3%B3n%20de%20Peligros%20y%20Evaluaci%C3%B3n%20de%20Riesgos%20y%20Determinaci%C3%B3n%20de%20Controles%20-%20IPERC.pdf.pdf

Tamari, A. (2025, Marzo 3). *Por qué el error humano es la mayor debilidad de la ciberseguridad en el diseño electrónico.* Retrieved from Altium: https://resources.altium.com/es/p/human-error-cybersecurity-electrical-engineering

Thales Data. (2023). Data Threat Report 2023. *Global Edition*. Retrieved from https://www.thalesgroup.com/es/el-mundo/group/press_release/el-informe-2023-thales-sobre-amenazas-seguridad-los-datos-revela

Tinoco, L. E., Rivera, B. B., Navarrete, J. I., & Alarcón, C. H. (2022, Agosto). Seguridad informática aplicando la Autentificación por Doble factor para la plataforma HomeOfi. *Ciencias Técnicas y Aplicadas Artículo de Investigación, 8*(3), 503-523. doi:http://dx.doi.org/10.23857/dc.v8i3

TMX Money. (2025, Marzo 8). *South Star Battery Metals Corp.* Retrieved from TMX Money: https://money.tmx.com/en/quote/STS

Trasobares, A. H. (2003). Los Sistemas de Información: evolución y desarrollo. *Proyecto social: Revista de relaciones laborales*(1133-3189), 149-165.

Turner, L., Weickgenannt, A., & Copeland, M. K. (2017). *Accounting Information System*. (C. a. Processes, Producer, & Third Edition) Retrieved from Wiley: https://www.homeworkforyou.com/static_media/uploadedfiles/AIS%20Book.pdf

Universidad Latinoamericana. (2017). *Investigacion exploratoria: Fundamento basicos*. Retrieved from HRM558 | Investigación Exploratoria: https://practicasprofesionales.ula.edu.mx/documentos/ULAONLINE/Maestria/MAN/HRM558/Publicaci%C3%B3n/Semana_3/Estudiante/HRM558_S3_E_Inv_explo.pdf

Urquhart, C., Hamad, F., Tbaishat, D., & Yeoman, A. (2018). *Information System Process and Practice.* Londo: iResearch.

Verizon. (2023). *Data Breach Investigations Report.* Retrieved from DBIR: https://www.verizon.com/business/resources/Tf91/reports/2023-data-breach-investigations-report-dbir.pdf

Verizon. (2025). *2025 Data Breach Investigations Report*. Retrieved from Verizon Business: https://www.verizon.com/business/resources/reports/dbir/

Verizon Business. (2025). *2025 Data Breach Investigations Report.* Retrieved from Verizon Business: https://www.verizon.com/business/resources/T248/reports/2025-dbir-data-breach-investigations-report.pdf

Vij, L. (2023, Junio 28). *Las ventajas de la computación en la nube y sus desventajas*. Retrieved from Open Institute Technology: https://www.opit.com/magazine/advantages-of-cloud-computing/

Vivanco Vergara, M. E. (2017). Los manuales de procedimientos como herramientas de control interno de una organización. *Universidad y Sociedad, 9*(2), 247-252. Retrieved from http://rus.ucf.edu.cu/index.php/rus

Warren, C. S., Reeve, J. M., & Duchac, J. E. (2016). *Contabilidad financiera.* Retrieved from Cengage Learning: https://www-ebooks7-24-com.up.idm.oclc.org/?il=2151

World Economic Forum. (2022). *The Global Risks Report 2022* (17 ed.). (N. U. Singapore, U. o. Oxford Martin School, & U. o. Wharton Risk Management and Decision Processes Center, Eds.) Retrieved from https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

World Economic Forum. (2025, Enero). *Global Cybersecurity Outlook 2025.* Retrieved from Insight report.

Yaqub, M. (2024, Octubre 27). *7 Quickbooks Statistics: A Must-Know in 2024*. Retrieved from BusinessDasher: https://www.businessdasher.com/quickbooks-statistics/

Yoder, T., & Ruiz, E. G. (2024, Marzo 11). *12 QuickBooks Statistics You Need To Know*. Retrieved from Fit Small Business: https://fitsmallbusiness.com/quickbooks-statistics/

ANEXOS

Anexo 1. Términos y condiciones relevantes de QuickBooks en línea

Tema	Descripción del término y condiciones
Uso de dispositivos móviles	No se garantiza un servicio continuo en dispositivos móviles (General Terms A.4). QuickBooks no asume responsabilidad por problemas de seguridad o pérdida de datos en dichos dispositivos (General Terms A.4).
Responsabilidad sobre el contenido	El usuario es responsable del contenido que registre en la plataforma. No obstante, el proveedor posee una licencia global, gratuita y no exclusiva para su uso (General Terms 6.1). Se recomienda realizar copias de seguridad, ya que QuickBooks no se responsabiliza por la pérdida de datos (General Terms 6.4).
Restricciones en el uso de los servicios	El proveedor puede utilizar cualquier sugerencia aportada por los usuarios sin obligación de compensación. También está facultado para controlar o eliminar contenido si lo considera necesario (Product Specific Terms 13.1). No se permite compartir accesos no autorizados, revender, modificar ni desensamblar el software (General Terms 2.1).
Términos adicionales	El usuario es responsable de la seguridad de su contraseña y debe reportar cualquier acceso no autorizado (General Terms 7.4). Los servicios pueden recibir actualizaciones automáticas que incluyan nuevas funcionalidades, herramientas o mejoras de seguridad (General Terms 9).
Exclusión de garantías	No se garantiza que los servicios estén libres de errores, virus o interrupciones (General Terms 9). El uso de la plataforma se realiza bajo riesgo del usuario, y no se asegura el cumplimiento con todas las regulaciones locales (General Terms 13).
Limitación de responsabilidad e indemnización	QuickBooks no se responsabiliza por daños indirectos, especiales, incidentales o punitivos. Esto incluye pérdidas relacionadas con telecomunicaciones, fallos de seguridad, virus, interrupciones en internet, pérdida de datos o fallas en software/hardware (General Terms 9).
Modificación de los servicios	El proveedor se reserva el derecho de modificar los servicios en cualquier momento, con notificación previa en caso de cambios relevantes (General Terms 1.9).
Productos de terceros	QuickBooks puede ofrecer productos de terceros, pero no asume responsabilidad por su funcionamiento ni por conflictos con sus proveedores (Product Specific Terms 3.3.2).

Nota. Adaptado de *Terms of Service for QuickBooks Online…, QuickBooks Time and QuickBooks Sole Trader in UK,* QuickBooks, 2025 (https://www.intuit.com/legal/terms/en-gb/quickbooks/online/).

Anexo 2. Errores y factores que incrementan la vulnerabilidad de la entrada de datos

Tipo de error o factor	Descripción	Referencia
Errores en la ejecución de tareas	Ingresar, omitir o duplicar información contable por descuido, o enviarla a destinatarios no autorizados.	Coker (2025); Ceballo (2024)
Errores de decisión en entornos operativos	Uso de contraseñas débiles, repetidas o configuración deficiente del sistema, lo que facilita accesos indebidos o privilegios excesivos.	Haan & Watts (2024); Kosinski (2024)
Deficiencias en el diseño del SIC	Sistemas desactualizados, sin trazabilidad ni filtros automáticos; fallos de integración con APIs o registros sin control de autoría.	Luettmann & Bender (2007); ASOCEX (2015); DIMTEC (2025)
Deficiencias en la gestión y política de procesos	Usuarios sin formación contable, credenciales compartidas, registros sin validaciones de formato ni control de duplicidad.	Charbonneau (2011); ISO/IEC 27001:2013

Anexo 3. Riesgos encontrados en la página oficial de soporte de QuickBooks

Clasificación del riesgo	Descripción del Problema
Riesgos de procesamiento de Datos	¿Cómo agrego la tarifa de procesamiento de tarjeta de crédito que QuickBooks me está cobrando?
	Dinero perdido
Riesgos de Seguridad y Fraude	Recibí unos 40 correos electrónicos diciendo que la información de mi cuenta de procesamiento de QuickBooks Money se modificó. Nada ha cambiado. ¿Es un error? No veo ningún cambio.
	Hace un tiempo, el banco LiveOak cambió su sistema de inicio de sesión y desde entonces no puedo acceder a QuickBooks Online.
	Mi cuenta ha sido hackeada y ahora QuickBooks no la reconoce.
	Bloqueo de cuenta bancaria después de demasiados intentos de inicio de sesión.
	¿Puedo obtener un reembolso de mi cuenta de Etsy que fue hackeada?
	La tarjeta de crédito de un cliente con la que realizó un pago fue hackeada. ¿Debo estar en alerta?
	¡Mi tarjeta de crédito fue hackeada después de 3 años y medio! Tengo un nuevo número de tarjeta, pero no puedo hacer que QuickBooks se conecte a Chase nuevamente.
	¿Alguien sabe cómo descongelar mi cuenta? Mi cuenta ha estado bloqueada debido a un hackeo durante 3 semanas y no he podido obtener ayuda.
	¿Alguien ha tenido un cliente que informó que su cuenta fue hackeada después de pagar a través del enlace de correo electrónico?
	¿QuickBooks ha sido hackeado? Me han estado dando vueltas y no me dicen por qué mi cuenta ha estado bloqueada por más de una semana.
	¿Cómo gestionan la contabilidad de fraude bancario?
	¡EXIJO HABLAR CON ALGUIEN! ¡MI CUENTA HA SIDO HACKEADA! ¡LO HE INTENTADO DURANTE 2 DÍAS E INTUIT SE NIEGA A AYUDARME!
	Recibí una alerta de fraude por mensaje de texto anoche. También tengo un cargo de Hulu que no hice. No sé cómo proteger mi cuenta ni detener otros pagos; QuickBooks no funciona.
	Tuve que cerrar una cuenta porque fue hackeada y abrí otra. ¿Cómo puedo empezar a conciliar la nueva cuenta porque el saldo inicial no es el mismo?
	Me hackearon y sufrí una filtración de datos. ¿Alguien tiene alguna sugerencia? No soy muy bueno con las computadoras.
	¡Me hackearon!
	He recibido unos 80 correos electrónicos sobre la actualización de mi cuenta de procesamiento de dinero. No sé si me han pirateado o si hay algún fallo. ¿Alguien más recibe estos correos?

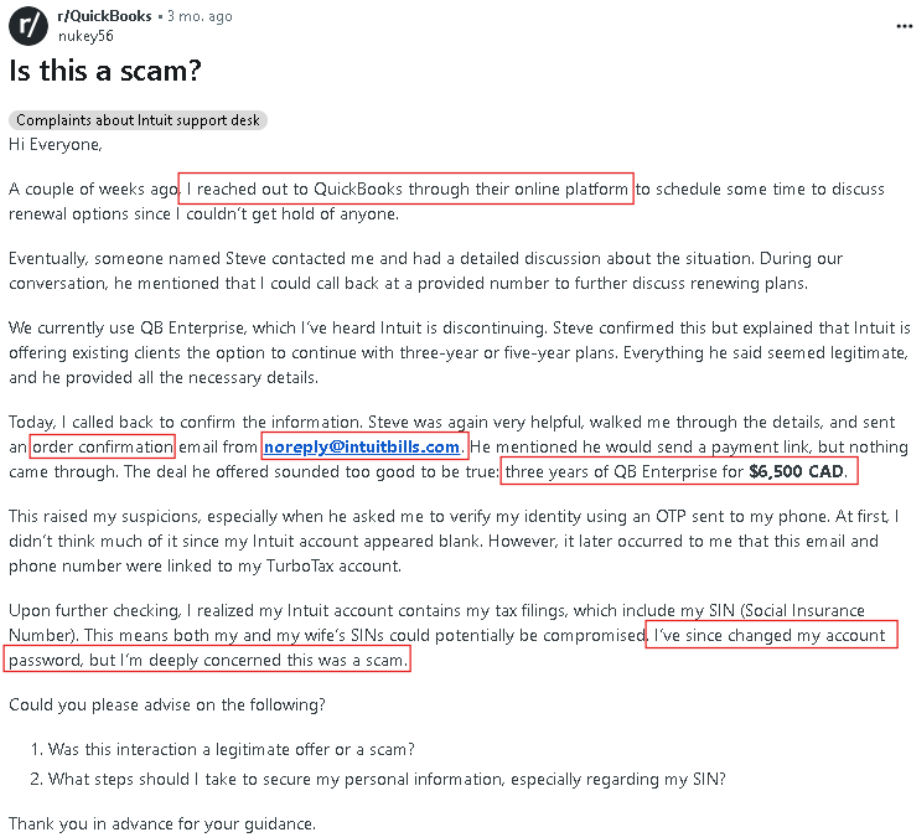
	Si estoy creando una factura de 6000, ¿por qué QuickBooks me enviaría una cantidad diferente, como 500? ¿Están pirateando el sistema? Me pasó dos veces esta semana.
	Si han pirateado mi cuenta y me han robado dinero, ¿qué hago?
	¿Alguien en esta comunidad está siendo víctima de hackers? Sigo recibiendo correos electrónicos fraudulentos y me pregunto si esto le está pasando a alguien más. QuickBooks no parece ser útil.
	Iniciar sesión con anuncio
	Fraude de cuenta mercantil
	Mi cuenta fue pirateada y se contrataron nuevos empleados que no contraté y viven en un estado completamente diferente.
	Mi tarjeta de débito comercial fue pirateada y tengo cargos no autorizados, además de la reversión de cargos del banco para registrar. ¿Cómo categorizo y concilio?
	Mi cuenta corriente fue pirateada fuera del horario de atención al cliente, ¿cómo puedo pausar mis gastos?
	Mi computadora fue pirateada recientemente y mi cuenta y mi información de QuickBooks en línea han desaparecido. ¿Cómo las recupero? Tampoco tengo acceso a ningún correo electrónico en esta cuenta... también lo perderé.
	Mi cuenta de QBO fue pirateada y me dejó debiendo $9,000.00 a QB.
	Mi cuenta de QBO fue pirateada el sábado 24/7/21. He estado intentando resolverlo desde entonces y me siguen dando largas. ¿Alguna sugerencia?
	Nos hackearon la cuenta en septiembre. Los hackers nos bloquearon y abrieron una cuenta corriente QB. Se hicieron cargos fraudulentos de hasta $245,000. Necesitamos ayuda lo antes posible.
	La nómina fue hackeada y una transferencia ha sido programada por un desconocido.
	Cuenta de QuickBooks Online hackeada.
	Reportar fraude ahora.
	Alguien hizo una "prueba" de $0 desde mi cuenta esta mañana. ¿Mi cuenta fue hackeada o fue alguien de Intuit haciendo una prueba?
	¿Alguien hackeó mi cuenta?
	Alguien hackeó mi cuenta e hizo una transacción. ¿Cómo puedo cancelarla?
	Alguien hackeó mi cuenta y creo que acabo de recuperarla.
	Alguien está usando intuit.com para falsificar facturas de Geek Squad. Creo que podrían haber hackeado Intuit.
	Alguien o algo ha hackeado el plan de cuentas, lista de productos/servicios, reportes de conciliación, facturas y más
	Alguien intentó hackear mi cuenta bancaria a través de QuickBooks Online.
	Este es el segundo intento de hackeo en mi cuenta de QuickBooks, ¿qué puedo hacer para mantener mi información segura y evitar que esto vuelva a suceder?
	Solución alternativa/Hack para los pagos anticipados de impuestos sobre ventas.
	¿Podemos rastrear una entrada a una fuente no autorizada? Quiero saber si podemos identificar su ubicación.
	Conversión desde servicios falsos de QuickBooks.
	Llamada de estafa.
	¿Estafa?
	Violación de seguridad.
	Security Metrics envió un correo electrónico sobre cumplimiento de PCI. ¿Es legítimo?
	ADVERTENCIA: ESTO ES UNA ESTAFA, ¡AYUDA AL SOPORTE!
	Seguridad de QuickBooks.
	Posible estafa sospechosa.
Riesgos de Visualización y Reportes	Se ha enviado una factura falsa desde mi cuenta. No se puede contactar con QuickBooks.
	Cambio de la dirección de correo electrónico desde la que se envían las facturas.
	¿Cómo puedo calcular la ganancia por factura para pagar comisiones sobre la ganancia?
	¿Cómo puedo obtener la factura de mi suscripción a QuickBooks Online?
	¿Cómo pueden mis clientes pagar automáticamente sus facturas en QuickBooks Online?
	¿Cómo creo un informe de Pérdidas y Ganancias que muestre todas las cuentas activas, incluso si no tienen actividad durante el período?
	¿Cómo asigno el campo de depósito que aparece en las facturas a una cuenta de pasivo? La opción se encuentra en la pantalla "Contenido del formulario de ventas". Actualmente, se contabiliza en efectivo
	¿Cómo elimino el texto de vista previa del correo electrónico que dice "Puede pagar su factura ahora"? Nuestros clientes lo consideran spam.
	¿Cómo configuro mi dirección de correo electrónico para enviar facturas?
	¿Cómo gestionar una factura con pagos parciales realizados, pero que luego deja de recibir pagos?

	¿Cómo desactivar la línea sobre nuestro logotipo en el correo electrónico de la factura que dice "¡Hola Jeffrey! ¿Ahora puedes pagar tu factura a [nombre del remitente] por un monto de $?
	Estoy intentando generar un informe 1099. He probado todos los pasos de las sugerencias de ayuda, pero no genera un informe que incluya montos. No hay filtro para los montos. ¡Ayuda!
	Tengo un cliente nuevo en el extranjero que quiere pagar por adelantado mediante transferencia bancaria. ¿Puedo enviar una factura para que pueda pagar sin ver mi información bancaria?
	He añadido artículos de diferentes categorías a mi presupuesto y factura. Quiero que se les apliquen diferentes tasas de impuestos en lugar de esta para todos. ¿Puedo hacer esto en QBO?
	Las facturas ya no se muestran en la pantalla. Tengo que descargar un PDF y luego verlo e imprimirlo desde Acrobat.
	Informes de pagos y depósitos.
	Informe de cuentas por pagar que incluye la cuenta de gastos y la clase.
	Los precios no se muestran correctamente en los presupuestos.
	Se necesita un informe de facturas de proveedores y números de cheques asociados.
	¿Qué es este bloque con "Books By Bessie" alrededor del botón "Crear Factura" en mis presupuestos?
	Al hacer entradas de diario, el NOMBRE no aparece en los reportes. ¿Hay alguna explicación para esto?
	¿De dónde salió el texto "Puedes pagar ahora" en mi correo electrónico de factura? Esto comenzó con mi última ronda de facturación.
	¿Por qué las empresas de cumplimiento de PCI me están enviando correos electrónicos? Todas mis transacciones con tarjeta de crédito se manejan a través de facturas electrónicas en Intuit.
	Cambiar el producto/servicio en una línea de factura sin eliminar la descripción.
	Personalización y ejecución de informes personalizados.
	¿QuickBooks tiene una opción para un botón de aprobación en los presupuestos?
	¿Cómo puedo generar un informe para el kilometraje de donaciones benéficas?
	¿Cómo puedo eliminar facturas antiguas que siguen apareciendo como abiertas de años anteriores?
	¿Existe una manera de ejecutar un informe de presupuesto vs real utilizando este año...?
	Informe sobre artículo/producto.
	Resuelto: ¿Cómo guardar cambios en un informe personalizado como un nuevo informe?
	La nueva plantilla para crear facturas es realmente mala. NECESITO AYUDA PARA MODIFICARLA.
	El informe P&L por clase muestra dos nóminas como "No especificadas" en lugar de.
	Usamos "subproyectos" para la facturación, ¿cómo puedo ejecutar un informe de ventas...?
	¿Estará disponible nuevamente la funcionalidad para importar facturas alguna vez?
	¿Alguien más se siente invadido por los molestos anuncios emergentes de audio con marketing de QuickBooks Online? ¿Cómo se pueden detener? ¿Puedo solicitar un reembolso? ¿Por qué me están tratando como un objetivo para más ventas?
	¿Cómo puedo bloquear los anuncios de Intuit que siguen apareciendo mientras uso QuickBooks?
	¿Cómo puedo eliminar los anuncios emergentes?
	¿Cómo desactivo todos los molestos anuncios emergentes dentro de QuickBooks Online?
Riesgos Operativo y de Plataforma	La nueva tarjeta de débito no funciona.
	Problemas de acceso a QuickBooks.
	¿Alguien más está teniendo problemas con las actualizaciones del TD Bank?
	¿Puedo transferir mis datos entre dos cuentas de QuickBooks Online? Ingresé todos mis datos en una cuenta de prueba, pero cuando compré QuickBooks, se creó una nueva cuenta. Necesito recuperar mis datos.
	Borrar actividades de tiempo facturable.
	¿Cómo importo mis datos de QuickBooks Online a TurboTax Business Desktop?
	¿Cómo configuro mi computadora como "de confianza" para no tener que recibir un mensaje de texto con un código para iniciar sesión cada vez?
	¿Cómo se solicita un financiamiento de nómina más rápido? Al parecer, el enlace no funciona. Ya lo hemos hecho antes y nunca recibimos respuesta. ¿Alguien ha tenido suerte? Gracias.
	¿A cuántas líneas está limitado al crear una sola entrada de diario?
	¿Cómo hacer que la transacción de depósito bancario se muestre en la pestaña de donantes?
	Estoy harto de que Intuit me obligue a iniciar sesión con mi cuenta personal de Google. ¡No quiero eso! ¿Cómo lo detengo?
	No puedo agregar a mi contador; me lleva a un proceso que me pide que verifique mi identidad.
	Olvidé mi contraseña

	Detesto el soporte de QuickBooks; es inexistente.
	Necesito instalar QuickBooks en línea desde mi portátil actual a otro portátil.
	Necesito reembolsar el depósito de seguridad a un inquilino. Quiero hacer una transferencia bancaria, no emitir un cheque. Al igual que con la factura del proveedor, quiero pagar directamente a través de la cuenta bancaria.
	Necesito actualizar y eliminar dos cuentas en QBO que cerré en el banco. ¿Cómo lo hago?
	Ejecutar QuickBooks Online en paralelo con QuickBooks Desktop, ¿todavía no es posible?
	Resuelto: ¿Puedo editar o administrar los tipos de detalles?
	Resuelto: Fondos no depositados en el balance general.
	¿Por qué los depósitos de mi cliente que ingreso directamente en el libro mayor no aparecen...?
	¿Cómo configuro la aplicación de autenticación multifactorial en varios dispositivos?
	Desde esta mañana, ya no tengo la opción de Producto/Servicio visible…

Nota. Los datos son proporcionados por la página de soporte de *QuickBooks*, 2025.

Anexo 4. Persona comparte una experiencia de estafa por parte de un trabajador de la plataforma de QuickBooks



r/QuickBooks • 3 mo. ago
nukey56

Is this a scam?

Complaints about Intuit support desk

Hi Everyone,

A couple of weeks ago, I reached out to QuickBooks through their online platform to schedule some time to discuss renewal options since I couldn't get hold of anyone.

Eventually, someone named Steve contacted me and had a detailed discussion about the situation. During our conversation, he mentioned that I could call back at a provided number to further discuss renewing plans.

We currently use QB Enterprise, which I've heard Intuit is discontinuing. Steve confirmed this but explained that Intuit is offering existing clients the option to continue with three-year or five-year plans. Everything he said seemed legitimate, and he provided all the necessary details.

Today, I called back to confirm the information. Steve was again very helpful, walked me through the details, and sent an order confirmation email from noreply@intuitbills.com. He mentioned he would send a payment link, but nothing came through. The deal he offered sounded too good to be true: three years of QB Enterprise for **$6,500 CAD**.

This raised my suspicions, especially when he asked me to verify my identity using an OTP sent to my phone. At first, I didn't think much of it since my Intuit account appeared blank. However, it later occurred to me that this email and phone number were linked to my TurboTax account.

Upon further checking, I realized my Intuit account contains my tax filings, which include my SIN (Social Insurance Number). This means both my and my wife's SINs could potentially be compromised. I've since changed my account password, but I'm deeply concerned this was a scam.

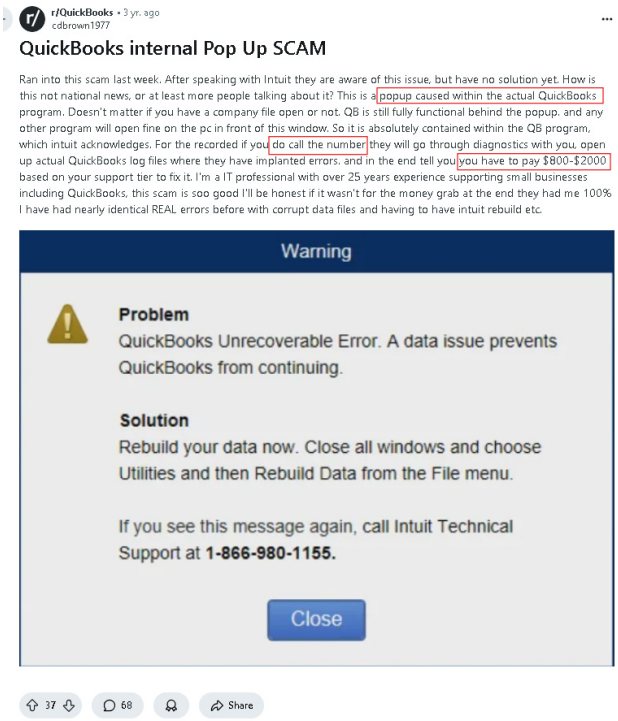
Could you please advise on the following?

1. Was this interaction a legitimate offer or a scam?
2. What steps should I take to secure my personal information, especially regarding my SIN?

Thank you in advance for your guidance.

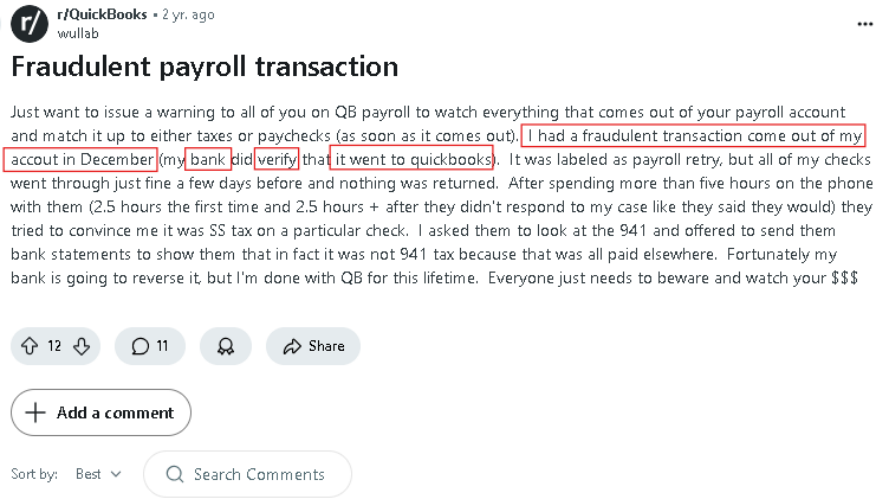
Nota: Adaptado de *Is this a scam?*, Reddit, 2023. Estafa por parte de un trabajador de la plataforma de *QuickBooks*.

Anexo 5. Cliente en Reddit comparte su molestia respecto a una ventana emergente producida por QuickBooks



Nota: Adaptado de *QuickBooks internal pop up scam*, Reddit, 2023. Estafa por ventana emergente interna de *QuickBooks*.

Anexo 6. Cliente en Reddit comparte una transacción fraudulenta de la nómina de sueldos de QuickBooks



Nota: Adaptado de *Fraudulent payroll transaction*, Reddit 2023. Transacción fraudulenta de la nómina de sueldos de QuickBooks.

Anexo 7. Riesgos cuantificados

Tipo	Riesgos	Porcentaje
Seguridad y fraude	Recepción de correos electrónicos maliciosos con enlaces fraudulentos.	43%
	Llamadas falsas de personal de soporte técnico.	
	Ventanas emergentes fraudulentas dentro del navegador.	
	Correos con alertas falsas sobre hackeo de cuenta.	
	Mensajes de texto con alertas de fraude.	
	Hackeo de cuentas: pagos no autorizados, robo de datos y filtración de información confidencial.	2%
	Manipulación de datos contables o contratación indebida desde cuentas comprometidas.	
	Alertas de ingreso indebido a cuentas de QuickBooks.	1%
	Pagos automáticos redirigidos a cuentas fraudulentas mediante ataques.	3%
	Emisión de facturas falsas desde cuentas comprometidas.	3%
Visualización y reportes	Errores en el cálculo automático de montos (como impuestos o nóminas).	10%
	Fallas en automatizaciones: conciliaciones, facturación, invoicing, y pagos recurrentes.	12%
Operativo y de Plataforma	Corrupción de bases de datos con solicitudes de pago para reparación.	0.5%
	Pérdida de información contable posterior a una actualización.	0.5%
	Dificultades en la migración de datos entre versiones de QuickBooks.	
	Inaccesibilidad a reportes financieros por fallos en servidores.	12%
	Reportes contables con información incompleta o incorrecta.	8%
	Discrepancias entre montos estimados e importes reflejados en facturación final.	5%
	Total	**100%**

Nota. Los datos son *Hola, te damos la bienvenida al soporte de QuickBooks,* QuickBooks, 2025 (https://quickbooks.intuit.com/global/es/learn-and-support/).

Anexo 8 Guías de entrevistas

Objetivo general: Analizar los riesgos de seguridad asociados a la entrada de datos en QuickBooks Online y desarrollar estrategias de mitigación.	**Bloque A – Experiencia general y uso**	¿Desde cuándo utiliza QuickBooks Online y con qué frecuencia lo emplea para tareas contables?
		¿Qué tipo de tareas realiza usted en el sistema relacionadas con el ingreso de datos contables?
	Bloque B – Riesgos de seguridad (Confidencialidad y acceso)	¿Alguna vez ha recibido correos o mensajes sospechosos relacionados con QuickBooks? ¿Cómo actuó frente a ellos?
		¿Ha notado intentos de acceso no autorizado o actividad inusual en su cuenta de QuickBooks?
		¿Qué medidas de seguridad aplica usted personalmente (por ejemplo, contraseñas, autenticación de dos factores)?
	Bloque C – Riesgos de integridad de la información	¿Ha identificado errores o alteraciones en la información contable después de ingresar los datos?
		¿Ha tenido problemas con procesos automatizados como conciliación, facturación o reportes financieros?
	Bloque D: Riesgos y disponibilidad y fallos técnicos	¿En qué momentos el sistema ha estado inaccesible o ha fallado durante operaciones importantes?
		¿Ha perdido información por errores del sistema, actualizaciones fallidas o migración de datos?
	Bloque E: Percepción de riesgos y recomendaciones	¿Cuáles considera que son los mayores riesgos al ingresar información en QuickBooks Online y qué sugerencias tendría para mitigarlos?

Nota. Elaboración propia en base a las entrevistas semiestructuradas realizadas

Anexo 9. Transcripción resumida de entrevistas semiestructuradas

Tema: Validación de riesgos de seguridad en el uso de QuickBooks Online

Tipo de instrumento: Entrevista semiestructurada

Entrevistadas: Samantha Shortert, Whitney Sham, Julie Sisks

Categorías: Seguridad y fraude / Visualización y reportes / Plataforma y operaciones

1. Entrevista 1 – Samantha Shortert (CFO)

Pregunta guía: ¿Ha identificado situaciones de riesgo o seguridad durante el uso del sistema?

Respuesta:

"Sí, varias veces me han llegado correos y mensajes de texto sospechosos, con enlaces que supuestamente eran de QuickBooks, pero en realidad eran intentos de phishing. Incluso algunas veces parecían tan reales que tuve que verificar con otras personas. Por eso, activé la verificación en dos pasos y nunca guardo la contraseña en el navegador."

"South Star no tiene área de TI, así que yo misma me encargo de reenviar estos mensajes fraudulentos a los demás para que estén alertas. También estoy redactando un pequeño manual de seguridad para el equipo."

Entrevista 2 – Whitney Sham (Contadora)

Pregunta guía: ¿Ha enfrentado intentos de fraude o confusiones operativas usando QuickBooks?

Respuesta:

"Una vez me llamaron diciendo que eran de soporte técnico de QuickBooks, me pidieron datos y luego intentaron acceder a la cuenta. También pagué por una supuesta actualización del sistema, y después me di cuenta de que era falso. Fue un error que me costó dinero y confianza."

"Desde entonces, aprendí a validar todo contacto que recibo, y a no responder llamadas que no haya solicitado. Además, instruyo a mis clientes sobre cómo identificar estas amenazas."

Entrevista 3 – Julie Sisks (Contadora)

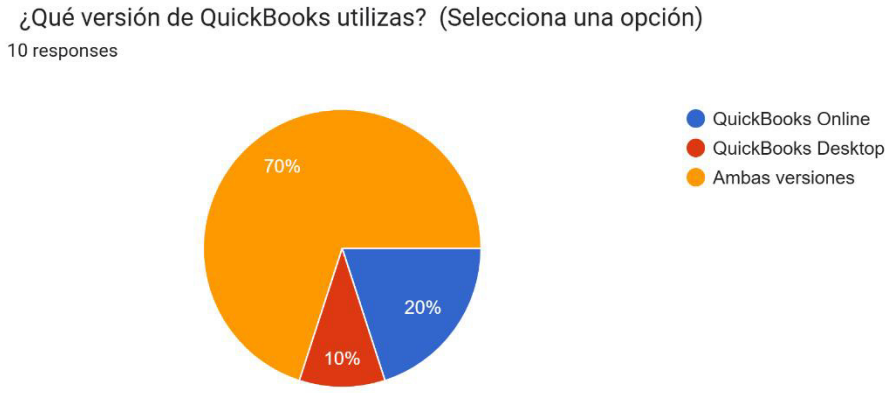
Pregunta guía: ¿Ha perdido información por errores del sistema, actualizaciones fallidas o migración de datos?

Respuesta:

"Uso QuickBooks Desktop, y si bien no he tenido problemas graves, mantenerlo actualizado es muy tedioso. A veces las actualizaciones interrumpen el trabajo. Hace poco encontré movimientos extraños en mis registros contables y no supe de inmediato si fue un error humano o del sistema."

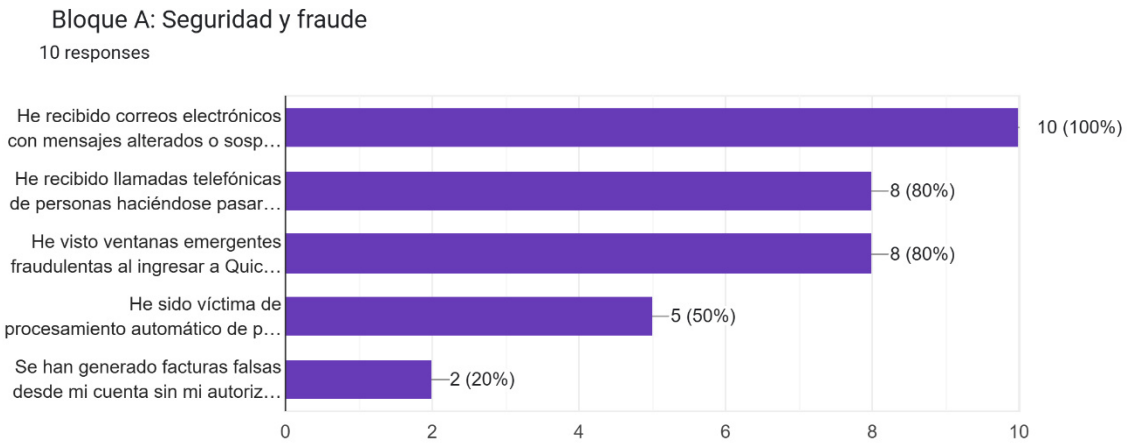
"Como medida, ahora cambio la contraseña cada tres meses y reviso los registros manualmente una vez por semana."

Anexo 10. Perfil de usuario



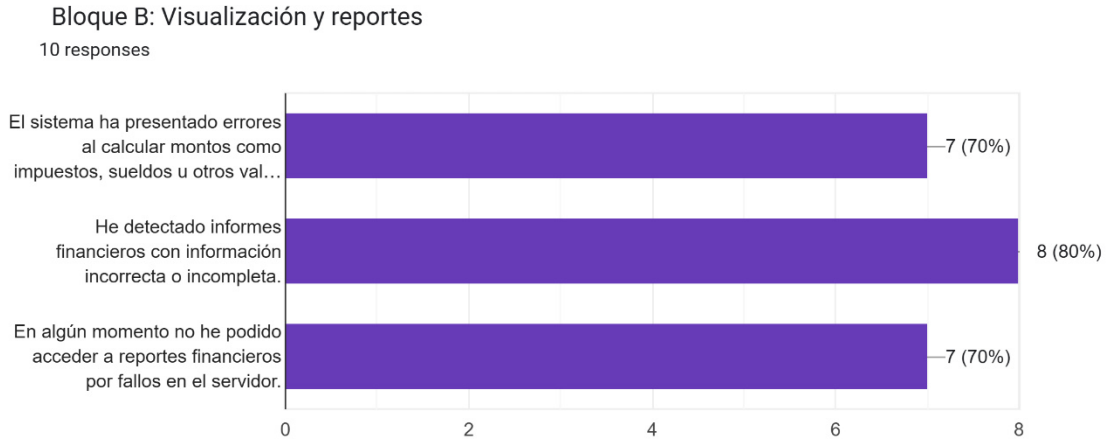
Nota. Encuesta realización propia de *QuickBooks*, 2025.

Anexo 11. Riesgos de seguridad y fraude



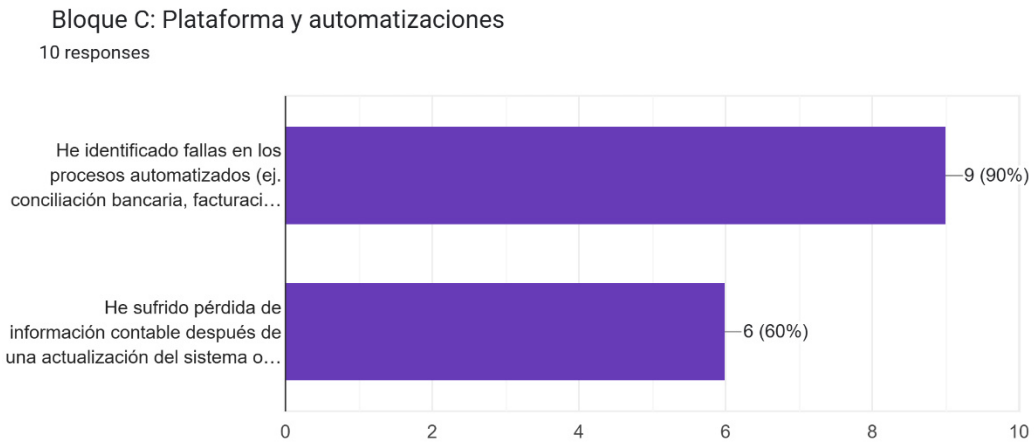
Nota. Encuesta realización propia de *QuickBooks*, 2025.

Anexo 12. Riesgo de visualización y reportes



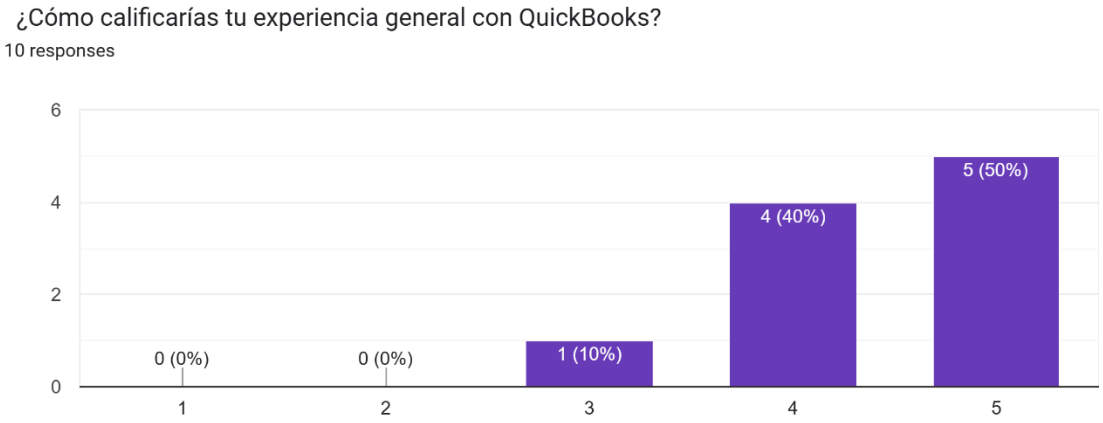
Nota. Encuesta realización propia de *QuickBooks*, 2025.

Anexo 13. Riesgos en la plataforma y automatizaciones



Nota. Encuesta realización propia de *QuickBooks*, 2025

Anexo 14.¿Cómo calificarías tu experiencia general con QuickBooks?



Nota. Encuesta realización propia de *QuickBooks*, 2025

Anexo 15. Ejemplo de información bancaria de clientes de South Star Battery Metals Corp.

Nota. Información personal borrada por confidencialidad.

Anexo 16. Estado de Posición Financiera de South Star Battery Metals Corp a Setiembre 2024

SOUTH STAR BATTERY METALS CORP.
CONDENSED CONSOLIDATED INTERIM STATEMENTS OF FINANCIAL POSITION
(Unaudited)
(Expressed in Canadian Dollars)
AS AT

	September 30, 2024	December 31, 2023
ASSETS		
Current		
Cash and cash equivalents	$ 3,226,442	$ 6,451,034
Receivables	79,210	17,373
Prepaid expenses	126,714	95,986
Inventory (Note 4)	458,527	-
	3,890,893	6,564,393
Property, plant and equipment (Note 5)	23,212,253	18,922,553
Land (Note 5)	2,068,805	2,179,827
Non-current advances (Note 5)	-	1,557,571
	$ 29,171,951	$ 29,224,344
LIABILITIES AND SHAREHOLDERS' EQUITY		
Current		
Accounts payable and accrued liabilities (Note 11)	$ 1,584,204	$ 1,563,302
Land purchase liability (Note 5)	-	625,962
Lease liabilities	-	10,335
Deferred revenue (Note 7)	1,433,713	585,363
	3,017,917	2,784,962
Deferred revenue (Note 7)	15,080,625	14,397,340
	18,098,542	17,182,302
Shareholders' equity		
Share capital (Note 8)	46,579,948	39,657,239
Reserves	5,464,557	5,374,211
Accumulated other comprehensive income (loss)	(983,287)	1,151,466
Deficit	(39,987,809)	(34,140,874)
	11,073,409	12,042,042
	$ 29,171,951	$ 29,224,344

Nature of operations and going concern (Note 1)

Nota. La información fue obtenida por SEDAR+, archivo Condensed Consolidated Interim Financial Statements, 2024. https://www.sedarplus.ca/landingpage/

Anexo 17. Estado de Flujo de Caja de South Star Battery Metals Corp a Setiembre 2024

SOUTH STAR BATTERY METALS CORP.
CONDENSED CONSOLIDATED INTERIM STATEMENTS OF CASH FLOWS
(Unaudited)
(Expressed in Canadian Dollars)
FOR THE NINE MONTHS ENDED SEPTEMBER 30,

	2024	2023
CASH FROM OPERATING ACTIVITIES		
Net loss for the period	$ (5,846,935)	$ (3,685,822)
Items not affecting cash:		
Share-based payments	226,787	58,315
Depreciation	24,612	37,401
Finance expense	1,225,966	1,209,895
Settlement of management bonus with equity	-	(137,573)
Changes in non-cash working capital items:		
Receivables	(64,334)	(29,962)
Prepaid expenses	(33,388)	(89,021)
Inventory	(482,332)	-
Accounts payable and accrued liabilities	668,235	(14,257)
Net cash used in operating activities	(4,281,389)	(2,651,024)
CASH FROM INVESTING ACTIVITIES		
Purchase of property, plant and equipment	(6,357,817)	(6,876,641)
Purchase of land	(642,274)	(669,950)
Non-current advances, net	1,487,573	(901,291)
Net cash used in investing activities	(5,512,518)	(8,447,882)
CASH FROM FINANCING ACTIVITIES		
Proceeds on issuance of common shares	6,697,103	4,590,748
Share issuance costs	(228,835)	(96,176)
Exercise of warrants	318,000	-
Lease payments	(10,154)	(15,729)
Net cash provided by financing activities	6,776,114	4,478,843
Effects of foreign exchange on cash	(206,799)	562,310
Change in cash and cash equivalents during the period	(3,017,793)	(6,620,063)
Cash and cash equivalents, beginning of the period	6,451,034	17,257,618
Cash and cash equivalents, end of the period	$ 3,226,442	$ 11,199,865
Supplemental cash flow information:		
Depreciation capitalized to construction in progress	$ -	$ 5,554
Purchase of property, plant, and equipment in accounts payable	511,523	2,142,180
Shares issued as finders' fees	122,338	-
Restricted share units exercised	136,441	-
Finder warrants issued as share issuance costs	-	4,005

The Company did not pay any cash for income taxes during the periods ended September 30, 2024 and 2023.

The accompanying notes are an integral part of these condensed consolidated interim financial statements.

Nota. La información fue obtenida por SEDAR+, archivo Condensed Consolidated Interim Financial Statements, 2024 (https://www.sedarplus.ca/landingpage/).

Anexo 18 Ejemplo de Acuerdo de Confidencialidad entre South Star Mining Corp. y los usuarios

ACUERDO DE CONFIDENCIALIDAD

Entre: South Star Mining Company Corp. (en adelante, "la Empresa").
Y: Nombres y Apellidos del Usuario, DNI o Identificación del Usuario (en adelante, "el Usuario")

OBJETO DEL ACUERDO

El presente Acuerdo de Confidencialidad tiene como finalidad proteger la información sensible, contable, financiera y estratégica a la que el Usuario pueda tener acceso en el marco de sus funciones dentro de la Empresa, y establecer lineamientos de uso seguro de credenciales y sistemas de gestión contable, como QuickBooks Online.

CLÁUSULAS

Primera – Confidencialidad de la Información:
El Usuario se compromete a mantener estricta confidencialidad respecto a toda información a la que tenga acceso durante su relación con la Empresa, incluyendo, pero no limitada a:

- Registros contables y financieros
- Información de ventas, compras y reportes internos
- Datos bancarios de la Empresa o de sus clientes/proveedores
- Credenciales de acceso a sistemas (usuarios y contraseñas)
- Información estratégica, operativa o de cualquier otro tipo que no sea de dominio público

Segunda – Uso de Credenciales y Seguridad Informática:
El Usuario declara haber sido informado sobre las políticas internas de seguridad y se compromete a:

- No compartir con terceros sus credenciales de acceso a sistemas (usuario y contraseña).
- Cumplir con los protocolos de creación y uso de contraseñas seguras exigidos por la Empresa.
- No almacenar contraseñas en navegadores, plataformas no verificadas, ni aplicaciones de mensajería instantánea (por ejemplo, WhatsApp).
- Activar y utilizar autenticación multifactor (MFA) cuando sea requerida por el sistema.
- Notificar de inmediato a la Empresa cualquier sospecha de acceso no autorizado.

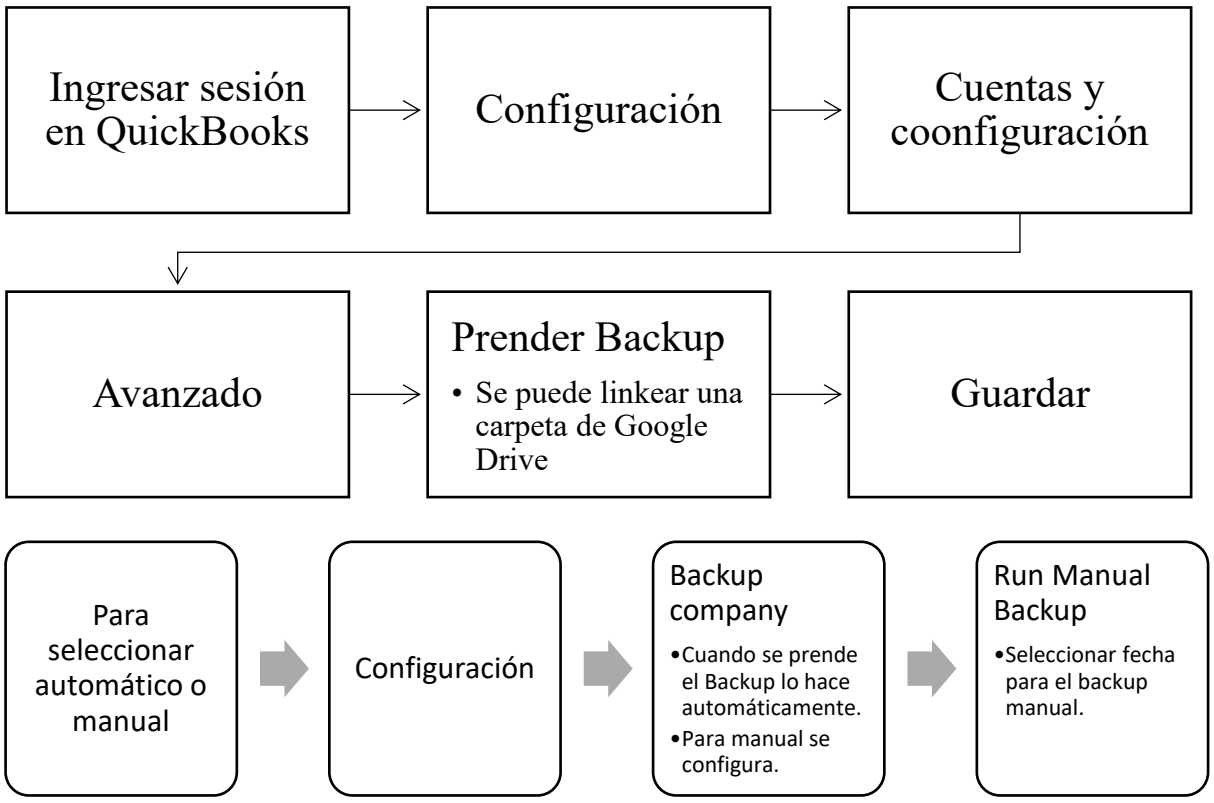
Tercera – Alcance Temporal:
La obligación de confidencialidad se mantendrá vigente incluso después del término de la relación laboral, contractual o comercial con la Empresa, por un período de [X] años.
Cuarta – Consecuencias del Incumplimiento:
El incumplimiento de lo establecido en este acuerdo facultará a la Empresa a tomar las medidas legales correspondientes, incluyendo acciones civiles o penales, según la gravedad del caso.
Fecha: [Día / Mes / Año]
Lugar: [Ciudad, País]

_____
[Nombre del Usuario]
DNI: [Número]

_____
[Nombre del Representante Legal de la Empresa]
Cargo: [Cargo]

Nota. Creación propia.

Anexo 19. Exportar automática o manualmente información de respaldo de QuickBooks en línea



Nota. Los datos fueron obtenidos de un tutorial de la página oficial de *QuickBooks* en YouTube, 2025. https://youtu.be/0EDRlFSV6NY.