UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD CONTABILIDAD Y AUDITORÍA

CARRERA DE CONTABILIDAD Y AUDITORÍA

Proyecto Integrador, previo a la obtención del Título de Licenciada en Contabilidad y Auditoría

Tema:

"Auditoría al sistema de información de la empresa Demaco Cía. Ltda. Sur Ambato"

Autora: Sánchez Ibarra, Melanie Salomé

Tutora: Dra. Jiménez Estrella, Patricia Paola

Ambato – Ecuador

2023

APROBACIÓN DEL TUTOR

Yo, Dra. Patricia Paola Jiménez Estrella con cédula de ciudadanía No. 180293423-0, en mi calidad de Tutora del proyecto integrador sobre el tema: **"AUDITORÍA AL SISTEMA DE INFORMACIÓN DE LA EMPRESA DEMACO CÍA. LTDA. SUR AMBATO"**, desarrollado por Melanie Salomé Sánchez Ibarra, de la Carrera de Contabilidad y Auditoría, modalidad presencial, considero que dicho informe investigativo reúne los requisitos, tanto técnicos como científicos y corresponde a las normas establecidas en el Reglamento de Graduación de Pregrado, de la Universidad Técnica de Ambato y en el normativo para presentación de Trabajos de Graduación de la Facultad de Contabilidad y Auditoría.

Por lo tanto, autorizo la presentación del mismo ante el organismo pertinente, para que sea sometido a evaluación por los profesores calificadores designados por el H. Consejo Directivo de la Facultad.

Ambato, Agosto 2023

TUTORA

.....

Dra. Patricia Paola Jiménez Estrella

C.C. 180293423-0

DECLARACIÓN DE AUTORÍA

Yo, Melanie Salomé Sánchez Ibarra con cédula de ciudadanía No. 180530976-0, tengo a bien indicar que los criterios emitidos en el proyecto integrador, bajo el tema: **"AUDITORÍA AL SISTEMA DE INFORMACIÓN DE LA EMPRESA DEMACO CÍA. LTDA. SUR AMBATO"**, así como también los contenidos presentados, ideas, análisis, síntesis de datos, conclusiones, son de exclusiva responsabilidad de mi persona, como autora de este Proyecto Integrador.

Ambato, Agosto 2023

AUTORA

...Melanie Sánchez.....

Melanie Salomé Sánchez Ibarra

C.C. 180530976-0

CESIÓN DE DERECHOS

Autorizo a la Universidad Técnica de Ambato, para que haga de este proyecto integrador, un documento disponible para su lectura, consulta y procesos de investigación.

Cedo los derechos en línea patrimoniales de mi proyecto integrador, con fines de difusión pública; además apruebo la reproducción de este proyecto integrador, dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica potencial; y se realice respetando mis derechos de autora.

Ambato, Agosto 2023

AUTORA

.....Melanie Sánchez.....

Melanie Salomé Sánchez Ibarra

C.C. 180530976-0

APROBACIÓN DEL TRIBUNAL DE GRADO

El Tribunal de Grado, aprueba el proyecto integrador, sobre el tema: **"AUDITORÍA AL SISTEMA DE INFORMACIÓN DE LA EMPRESA DEMACO CÍA. LTDA. SUR AMBATO"**, elaborado por Melanie Salomé Sánchez Ibarra, estudiante de la Carrera de Contabilidad y Auditoría, el mismo que guarda conformidad con las disposiciones reglamentarias emitidas por la Facultad de Contabilidad y Auditoría de la Universidad Técnica de Ambato.

Ambato, Agosto 2023

Dra. Tatiana Valle PhD
PRESIDENTE

Dr. Jaime Fabián Diaz
MIEMBRO CALIFICADOR

Dr. Mauricio Arias
MIEMBRO CALIFICADOR

DEDICATORIA

A mi padre celestial, por brindarme sabiduría y la fortaleza necesaria para no desistir y permitirme lograr con éxito este objetivo.

A mi madre y mejor amiga María Ibarra, mi mayor ejemplo de lucha y perseverancia, por su apoyo y amor incondicional, gracias a sus sabios consejos que formaron en mí una mujer de principios morales y espirituales.

A mi padre Fausto Sánchez, por ser guía y apoyo durante mi etapa universitaria brindándome su amor e incentivarme a alcanzar mis metas.

A mi esposo y compañero de vida David Medina, por confiar en mis capacidades y motivarme en todo momento, brindándome su amor y paciencia.

A mi amado hijo Stefano Medina, mi mayor tesoro y mi principal motivación, por alegrar mis días y permitirme ser cada día mejor madre.

Melanie Salomé Sánchez Ibarra

AGRADECIMIENTO

Agradezco a mi padre celestial por guiarme en el camino de lo prudente y brindarme sabiduría y fortaleza, a mi madrecita por protegerme y guiar mi camino, por ser la voz de aliento y demostrarme que con amor y dedicación todo es posible.

A mis hermanos Ronald y Jean Carlos, por cuidar de mí y permitir disfrutar mi infancia llena de alegrías y juegos, enseñándome el verdadero significado de amor y superación.

A mi tutora, Dra. Patricia Jiménez amiga y maestra, por compartir su experiencia y conocimientos, inculcando en mi responsabilidad y rigor académico, docente digna de admiración y lealtad.

Melanie Salomé Sánchez Ibarra

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE CONTABILIDAD Y AUDITORÍA

CARRERA DE CONTABILIDAD Y AUDITORÍA

TEMA: "AUDITORÍA AL SISTEMA DE INFORMACIÓN DE LA EMPRESA DEMACO CÍA. LTDA. SUR AMBATO**"**

AUTORA: Melanie Salomé Sánchez Ibarra

TUTORA: Dra. Patricia Paola Jiménez Estrella

FECHA: Agosto 2023

RESUMEN EJECUTIVO

El siguiente proyecto integrador se lo realizó en la empresa Demaco Cía. Ltda. Ubicado en la ciudad de Ambato y tuvo por objetivo realizar una auditoría al sistema de información del área informática. Para evaluar el control interno fue necesario aplicar el marco de referencia COSO ERM 2017 y para la evaluación de activos y tratamiento de los riesgos aplicamos las normas ISO/IEC 27000. Metodologías que ayudaron a tener una visión clara del estado actual de la entidad y a mejorar el tratamiento de la información y las tecnologías. Se obtuvieron resultados donde la entidad no cuenta con planes y estrategias adecuadas para una correcta gestión de los riesgos, en cuanto a los activos la mayoría de estos están protegidos y cumplen con criterios de confidencialidad, disponibilidad e integridad. La entidad tiene falencias para prevenir y eliminar los riesgos identificados en los activos, por lo que es necesario que la entidad en general maneje controles y supervise de manera constante para evitar grandes problemas que podría poner en riesgo la información o la entidad.

PALABRAS DESCRIPTORAS: AUDITORÍA, SISTEMA, COSO ERM, ISO, RIESGOS

TECHNICAL UNIVERSITY OF AMBATO

FACULTY OF ACCOUNTING AND AUDITING

ACCOUNTING AND AUDITING CAREER

TOPIC: "AUDIT OF THE INFORMATION SYSTEM OF THE COMPANY DEMACO CIA. LTDA. SUR AMBATO"

AUTHOR: Melanie Salomé Sánchez Ibarra

TUTOR: Dra. Patricia Paola Jiménez Estrella

DATE: August 2023

ABSTRACT

The next integrating project was carried out in the company Demaco Cía. Ltda. Located in the city of Ambato and aimed to perform an audit of the information system of the computer area. To evaluate internal control, it was necessary to apply the COSO ERM 2017 reference framework and for the evaluation of assets and risk treatment we apply the ISO/IEC 27000 standards. Methodologies that helped to have a clear vision of the current state of the entity and to improve the treatment of information and technologies. Results were obtained where the entity does not have adequate plans and strategies for proper risk management, in terms of assets most of these are protected and comply with criteria of confidentiality, availability and integrity. Despite this, the entity has shortcomings to prevent and eliminate the risks identified in the assets, concluding that it is important that the entity in general manages controls and supervises constantly to avoid major problems or that may endanger it.

KEYWORDS: AUDIT, SYSTEM, COSO ERM, ISO, RISKS

ÍNDICE GENERAL

CONTENIDO **PÁGINA**

PÁGINAS PRELIMINARES

PORTADA i
APROBACIÓN DEL TUTOR ii
DECLARACIÓN DE AUTORÍA iii
CESIÓN DE DERECHOS iv
APROBACIÓN DEL TRIBUNAL DE GRADO v
DEDICATORIA vi
AGRADECIMIENTO vii
RESUMEN EJECUTIVO viii
ABSTRACT ix
ÍNDICE GENERAL x
ÍNDICE DE TABLAS xiii
ÍNDICE DE ILUSTRACIONES xiv
CAPÍTULO I 1
MARCO TEÓRICO 1
1.1. Introducción 1
1.1.1. Antecedentes del proyecto integrador **1**
1.1.1.1. Historia de la empresa **1**
1.1.1.2. Detalles estratégicos **1**
1.1.1.3. Estructura organizacional **3**
1.1.1.4. Detalles de operación **4**
1.1.1.5. Detalle legales leyes, reglamentos o normativas que se rige la empresa **5**
1.1.1.6. Marca y logos **5**
1.1.1.7. Ubicación **5**
1.1.2. Descripción del entorno **6**
1.1.2.1. Auditoría informática en las organizaciones **6**
1.1.2.2. Auditoría al sistema de información de las empresas ecuatorianas **7**
1.1.2.3. Sistema de Información de la empresa DEMACO **8**
1.1.3. Justificación **9**
1.1.4. Objetivos **10**
1.1.4.1. Objetivo general **10**
1.1.4.2. Objetivos específicos **10**
1.2. Revisión de la literatura 11

1.2.1. Teoría de sistemas **11**
1.2.2. Normas internacionales de auditoría **11**
1.2.3. Normas ISO 27000 ..... **12**
1.2.4. Introducción a la informática **13**
1.2.4.1. Definición **13**
1.2.4.2. Auditoría informática **13**
1.2.4.3. Tipos y clases de Auditoría Informática **13**
1.2.4.4. Fases de auditoría **14**
1.2.4.5. Las tecnologías de la información y comunicación **15**
1.2.5. Sistema informático **15**
1.2.6. Seguridad de la información **15**
1.2.7. Control interno informático **15**
1.2.8. Clasificación general de los controles **16**
1.2.9. Ciberseguridad **16**
1.2.10. Amenaza, vulnerabilidad y riesgo **16**
CAPÍTULO II **17**
METODOLOGÍA **17**
2.1 Descripción de la metodología 17
2.1.1 Unidad de análisis **17**
2.1.2 Fuentes, técnicas e instrumentos de recolección de información **17**
2.1.3 Fases del desarrollo **19**
CAPÍTULO III **25**
DESARROLLO **25**
3.1 Resultado 25
3.1.1 Fase de planificación **25**
3.1.1.1 Marco de referencia COSO ERM 2017 ..... **32**
3.1.2 Fase de ejecución **37**
3.1.2.1 NORMAS ISO/IEC 27000 Evaluación a los activos de información **37**
3.1.2.2 Flujogramas de procedimientos informatizados de transacciones **43**
3.1.2.3 Evaluación e identificación de controles de riesgos **54**
3.1.2.4 Evaluación e identificación de riesgos **59**
3.1.3 Informe general **63**
3.1.3.1. Resultado del examen **65**
3.1.3.2. Matriz de Seguimiento y Monitoreo **89**

CAPÍTULO IV 94
CONCLUSIONES Y RECOMENDACIONES..... 94
4.1 Conclusiones 94
4.2 Recomendaciones 95
REFERENCIAS BIBLIOGRÁFICAS 96

ÍNDICE DE TABLAS

CONTENIDO **PÁGINA**

Tabla 1. Productos DEMACO.....4
Tabla 2. Cuadro de las Normas Internacionales de Auditoría.....11
Tabla 3. Normas ISO 27000.....12
Tabla 4. Fases de una Auditoría.....14
Tabla 5. Tipos de control.....16
Tabla 6. Persona entrevistada.....18
Tabla 7. Preguntas del cuestionario COSO ERM 2017.....18
Tabla 8. Fases para el desarrollo de la Auditoría.....19
Tabla 9. Medición de confianza y riesgo.....20
Tabla 10. Criterios de confidencialidad.....20
Tabla 11. Criterios de integridad.....21
Tabla 12. Criterio de disponibilidad.....22
Tabla 13. Nivel de tasación.....22
Tabla 14. Valoración del control de los activos.....23
Tabla 15. Criterios de probabilidad de riesgos.....23
Tabla 16. Criterios de ocurrencia de riesgos.....24

ÍNDICE DE ILUSTRACIONES

CONTENIDO **PÁGINA**

Ilustración 1. Organigrama DEMACO 3
Ilustración 2. Marcas y Logos 5
Ilustración 3. Sucursal DEMACO CIA. LTDA 5
Ilustración 4. Clases de Auditoría Informática 14
Ilustración 5. Sistema Informático 15
Ilustración 6. Amenaza, Vulnerabilidad y Riesgo 16
Ilustración 7. Guía de visita previa 25
Ilustración 8. Archivo Permanente 26
Ilustración 9. Autoridades de DEMACO 27
Ilustración 10. Matriz FODA 27
Ilustración 11. Memorando de Planificación 28
Ilustración 12. Programa de Auditoría 31
Ilustración 13. Marco de referencia COSO ERM 2017 33
Ilustración 14. Resultados de los componentes del COSO ERM 2017 36
Ilustración 15. Evaluación de Activos de información 38
Ilustración 16. Evaluación del Activo de Información Software 40
Ilustración 17. Evaluación del Activo de Información Hardware 40
Ilustración 18. Evaluación del Activo Redes de Comunicación 41
Ilustración 19. Evaluación del Activo Personas (Trabajadores) 42
Ilustración 20. Flujograma de ventas de contado 44
Ilustración 21. Flujograma propuesto de ventas de contado 45
Ilustración 22. Flujograma de Ventas a crédito 46
Ilustración 23. Flujograma propuesto para ventas a crédito 47
Ilustración 24. Flujograma de cuentas por cobrar 48
Ilustración 25. Flujograma propuesto de Cuentas por cobrar 49
Ilustración 26. Flujograma de pedidos para adquisiciones 50
Ilustración 27. Flujograma de Inventarios 51
Ilustración 28. Flujograma de Cotización 52
Ilustración 29. Flujograma propuesto de Cotización 53

Ilustración 30. Evaluación de controles de riesgos de los Activos 54
Ilustración 31. Valoración de los controles del Activo Software 56
Ilustración 32. Valoración de los controles del Activo Hardware 56
Ilustración 33. Valoración de los controles del Activo Redes de Comunicación 57
Ilustración 34. Valoración de los controles del Activo Personas (Trabajadores) 57
Ilustración 35. Evaluación de riesgos de los Activos 59
Ilustración 36. Mapa de calor de los riesgos 61
Ilustración 37. Valoración de los riesgos de los Activos 61
Ilustración 38. Informe general 63
Ilustración 39. Criterios de controles 90
Ilustración 40. Matriz de seguimiento y monitoreo 91

CAPÍTULO I

MARCO TEÓRICO

1.1. Introducción

1.1.1. Antecedentes del proyecto integrador

1.1.1.1. Historia de la empresa

A continuación, se presenta la historia de la empresa DEMACO CIA. LTDA., (2023):

DEMACO es una compañía de Responsabilidad limitada fundada en el mes de octubre de 1982. Esta empresa está dedicada a la distribución de todo lo que respecta a materiales construcción, ferretería, productos hidráulicos, productos eléctricos, electrodomésticos y acabados.

La mayoría de los productos que comercializan son importados principalmente de Brasil, China, Japón, Italia, Estados Unidos e Indonesia. Esta compañía es reconocida por parte de sus clientes como una de las mejores en su categoría por su excelente calidad y precios de sus productos.

Para el desarrollo de sus operaciones cuenta con cinco oficinas, locales de exhibición, ventas y bodegas ubicadas en ciudades como Guayaquil, Quito, Ambato y Portoviejo.

1.1.1.2. Detalles estratégicos

Misión

- Trabajar con entusiasmo diariamente para entregar las mayores ventajas a nuestros clientes.
- Ofrecer productos de la más alta calidad a los mejores precios.
- Buscar constantemente productos que posean las mejores tecnologías, escuchando atentamente la opinión de los usuarios antes de seleccionarlas para ponerlas a disposición de la comunidad.
- Desarrollar en el grupo de trabajo voluntad para calificarse permanentemente y desarrollar hábitos de servicio para satisfacer las necesidades de nuestros clientes oportuna y eficientemente

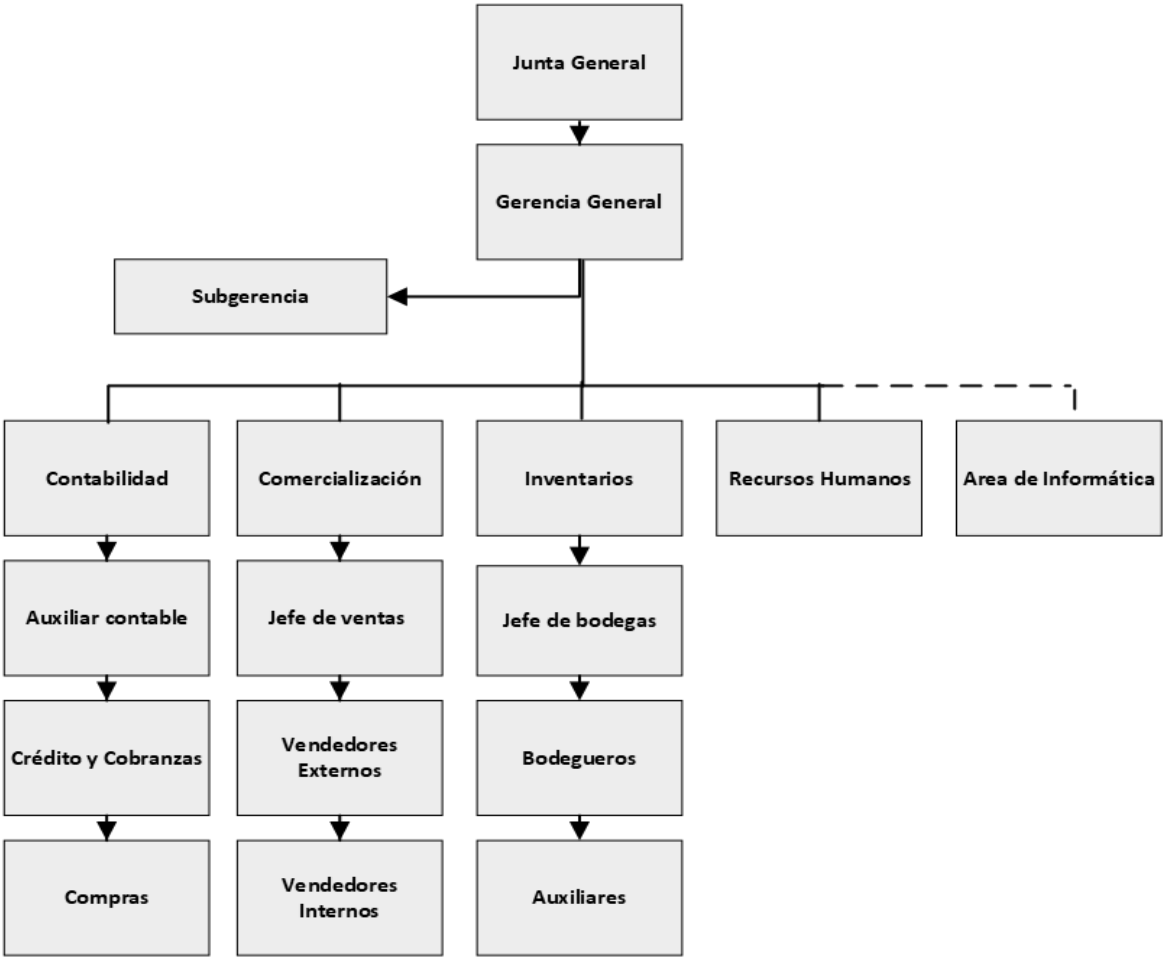
- Realizar las acciones necesarias para lograr el equilibrio necesario para lograr la rentabilidad que la empresa necesita para mantener un crecimiento sostenido.

Visión

Ser un espacio de desarrollo técnico económico y moral de los miembros que participan en la empresa, esforzándose para generar métodos y tecnología para que la comunidad tenga facilidades y pueda ejecutar con calidad y eficiencia sus obras, aportando al mantenimiento del equilibrio ecológico.

1.1.1.3. Estructura organizacional

Ilustración 1. *Organigrama DEMACO*

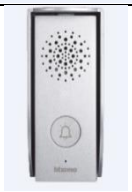
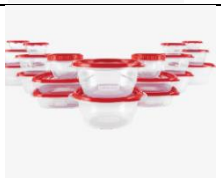


Fuente: DEMACO (2023)

1.1.1.4. Detalles de operación

La empresa DEMACO, (2023) ofrece una gran variedad de productos para el mercado, en los cuales se destacan: Materiales de construcción, ferretería, productos hidráulicos, productos eléctricos, electrodomésticos y acabados.

Tabla 1. *Productos DEMACO*

Denominación del Producto	Descripción	
Construcción	Taladro de Rotación Especial de 1/2″ Dewalt	
Ferretería	Arco de Sierra de 12″ Tramontina	
Productos hidráulicos	Calefón de 26 Litros RCA	
Productos eléctricos	Frente de Calle para Kit de Audio Zamak Bticino	
Electrodomésticos	Dispensador de Agua con Botellón Oculto TCL Blanco	
Acabados y Menaje de Casa	Contenedores de alimentos Juego de 40 piezas Rubbermaid	

Fuente: DEMACO (2023)
Elaborado por: Sánchez (2023)

1.1.1.5. Detalle legales leyes, reglamentos o normativas que se rige la empresa

La empresa DEMACO, (2023) cumple la siguiente normativa:

- Constitución de la República del Ecuador
- Ley de Compañías
- Ley de Seguridad Social
- Código de trabajo
- Ley de régimen tributario Interno

Fuente: DEMACO (2023)

1.1.1.6. Marca y logos

Ilustración 2. *Marcas y Logos*

Fuente: DEMACO (2023)

1.1.1.7. Ubicación

Sucursal Ambato- Julio Jaramillo Lourido y Julio Cesar Cañar

Ilustración 3. *Sucursal DEMACO CIA. LTDA.*

Fuente: DEMACO (2023)
Elaborado por: Sánchez (2023)

1.1.2. Descripción del entorno

1.1.2.1. Auditoría informática en las organizaciones

La auditoría informática juega un papel importante en las organizaciones ya que asegura que los objetivos se estén cumpliendo tanto en el presente como a futuro, además de verificar que los sistemas de información presten el apoyo suficiente para poder alcanzar dichos objetivos (Arcentales & Caycedo, 2017). Así que hoy en día es esencial que las tecnologías estén siempre presentes en las organizaciones porque representa un gran apoyo y facilitar la realización de actividades.

La auditoría de sistemas tiene por objetivo mejorar y fortalecer proyectos empresariales y organizacionales acompañados de herramientas afianzadas a la buena práctica aplicando modelos como COSO siendo una estrategia que ayude a la adaptación del entorno (Díaz , 2020). Por otro lado, en la actualidad se cuenta con varias herramientas informáticas las cuales tiene por objetivo identificar problemas informáticos que tienen las entidades, las ISO/IEC 27000 normas que ayudan a gestionar y proteger los activos de información digital o físicos, es una norma auditable orientada al sistema de gestión de la seguridad de la información (SGSI) garantizando la elección de controles adecuado para la seguridad (Andrade & Chávez, 2018). Es por ello que, es necesario que las entidades establezcan mecanismo de seguridad para proteger los activos y la información.

La auditoría informática también se encarga del manejo de la seguridad de la información, ya que es importante reconocer las necesidades, vulnerabilidades y proteger la información de la entidad que puede verse comprometida (Albarracin, Marín, Lozada, & Martinez , 2021). Es por ello que, actualmente las entidades u organizaciones consideran sumamente elemental resguardar los activos informáticos y poner en práctica medidas de seguridad, pero a pesar del gran esfuerzo que conlleva realizar esto, es ineludible que existan violaciones de la ciberseguridad, por lo cual en las Auditorias de TI se considera implementar la ciberseguridad (Sabillón & Cano, 2019). Finalmente, es necesario que todas las entidades conozcan que a medida que la tecnología evoluciona y trae grandes beneficios también esta puede desencadenar grandes problemas que podría poner en riesgo la información de las entidades.

1.1.2.2. Auditoría al sistema de información de las empresas ecuatorianas

En la actualidad la ausencia de auditoría a los sistemas de información en las empresas no permite evaluar de una manera adecuada la información, evitando realizar mejoras en las áreas afectadas haciendo que la problemática cada vez sea mayor y difícil de contrarrestarla (Ávila & Zambrano, 2022). En el Ecuador se puede observar que la mayoría de las empresas pequeñas no tiene la obligación de realizar auditorías por lo tanto no le dan importancia, pero al no conocer a profundidad las ventajas de esta herramienta, arrastrara consigo problemas que habrían podido evitarse (Esucomex, 2017). Por lo tanto, es necesario ampliar el conocimiento de la aplicación de una auditoria de sistemas en las entidades, la cual podría demostrar resultados efectivos.

La auditoría de los sistemas de información resulta una herramienta valiosa en la empresa públicas o privadas mejorando la eficiencia y productividad, sin embargo, surge la necesidad que estos sistemas sean precisos y confiables principalmente asegurando la información financiera (Dominguez & Solis, 2004). Además, se considera importante que las empresas mejoren los sistemas de infraestructuras informáticas en las medidas de protección para un mejor desarrollo de sus actividades (Alvarez, 2005). Así que es importante que toda empresa se encargue se asegurar su información para evitar posibles vulnerabilidades (Alonso, 2023).

En la actualidad una de las principales preocupaciones de las empresas es que han realizado la implementación de tecnología de la información es que no ven una solución inmediata, pero esto es a causa de la mala administración o la poca capacitación que existe acerca de esta herramienta (Ramirez & Alvarez, 2003). Finalmente, es importante que al implementar nuevas herramientas tecnológicas exista una previa capacitación al personal administrativo a las áreas correspondientes, con la finalidad de evitar riesgos a futuro.

1.1.2.3. Sistema de Información de la empresa DEMACO

DEMACO CIA. LTDA. facilitó acceder a su información en la cual se observó la historia y creación de la empresa, misión, visión, estructura organizacional, comercializan y la base legal. Es una empresa dedicada a la distribución de materiales para construcción especialmente ferretería y opera en las principales provincias del ecuador tanto costa como sierra.

Al ser una empresa reconocida a nivel nacional y contando con una gran cantidad de clientes en el sector ferretero y constructoras grandes, es importante manejar de una manera adecuada y responsable la información financiera mediante controles y planes. Se conoce que la empresa no ha sido sometida a auditorias de sistemas, por lo que nace la necesidad de realizar una la cual ayudará a ampliar conocimientos y controlar las diversas áreas que existen.

La Auditoría al sistema de información comprende la evaluación del control interno y del sistema de información además del análisis de los riesgos y amenazas que se presentan en la empresa DEMACO CIA LTDA. Para finalizar, se presentará un informe en el cual se encontrarán recomendaciones ante observaciones encontradas en la empresa, también una matriz de seguimiento y monitoreo que podrá evaluar y controlar.

1.1.3. Justificación

Las tecnologías de información juegan un papel fundamental, ya que facilita la realización de las actividades optimizando tiempo, recursos sea esto en el mundo laborar o en la vida cotidiana. Además, ayuda a tomar decisiones más acertadas, reducir errores humanos y generar habilidades con la utilización de herramientas informáticas para un mejor desempeño (Prieto & Martínez , 2004). En la actualidad, la auditoría de sistemas de información ha causado un gran impacto y notablemente mayor importancia en empresas o instituciones las cuales buscan poder llevar una prevención y control de riesgos, mediante análisis, evaluaciones (Solano, 2011). Por lo que hoy en día la utilización de nuevas tecnologías de información en las empresas ha traído beneficios, pero también riesgos, ya que en la actualidad las empresas consideran la información como un activo valioso por lo cual es necesario proteger de cualquier amenaza.

Mediante la auditoría de sistemas, el auditor ha adquirido experiencias en áreas de procesamiento electrónico de datos PED, sistema de información SI, tecnologías de la información y comunicación TICS, lo cual resulta importante para la seguridad de la información en empresas tanto privadas como públicas, ya que la información que genera la empresa se convirtió en un bien en riesgo que debe ser resguardado y protegido (Dávalos, 2013). Hoy en día para las organizaciones es vital que se evalúen constante y regularmente todos los procesos que en ellas se llevan a cabo, para verificar la calidad y suficiencia en cuanto a requerimiento del negocio como: control, integridad, confidencialidad y disponibilidad, además de considerar que la información representa uno de sus activos más importantes (Arcentales & Caycedo, 2017).

Hoy en día resulta necesario realizar una revisión al sistema informático de la entidad, mediante la auditoría de sistemas se podrá identificar posibles problemas que podría poner en peligro a la empresa, es por eso que nace la necesidad de realizar una evaluación al sistema de información de la empresa, que contempla activos de información, software, hardware, redes de comunicación, personal a cargo (usuarios) de la áreas operativas, con el fin de identificar amenazas, vulnerabilidades y riesgos

proporcionando soluciones inmediatas. Evaluando el cumplimiento de las normas ISO 27000 en el sistema de gestión de la seguridad de la información (SGSI) en los principios de confidencialidad, integridad y disponibilidad de la información.

1.1.4. Objetivos

1.1.4.1. Objetivo general

Realizar la Auditoría al sistema de información en la empresa DEMACO CIA. LTDA. Sur Ambato para la evaluación de la eficiencia y eficacia de los procesos.

1.1.4.2. Objetivos específicos

- Planificar procesos, procedimientos y técnicas para preparar la auditoría.
- Ejecutar las matrices preestablecidas con los datos recolectados para procesarlos y evaluarlos.
- Elaborar el informe de auditoría recomendando acciones para una mejora empresarial.

1.2. Revisión de la literatura

1.2.1. Teoría de sistemas

"La tecnología ha acabado pensando no ya en términos de máquinas sueltas si no de sistemas" (Bertalanffy, 1986). Es así que, en la actualidad toda empresa tiene por objeto manipular la información mediante equipos informáticos.

La auditoría informática evalúa informes sobre actividades económicas con el fin de determinar el grado de correspondencia y si se cumplen con los requerimientos necesarios para la empresa (Martinez, Blanco, & Loy, 2012). Puesto que, la auditoria informática es aquella que evalúa procedimientos y sugiere apoyo o modificaciones para un mejor desempeño de la empresa.

1.2.2. Normas internacionales de auditoría

Las normas Internacionales de Auditoría (NIA) son reglas establecidas por la Federación Internacional de Contadores (IFAC). Normas que garantizan la calidad de los procedimientos y los objetivos que se deben alcanzar durante la auditoría. (Westreicher, 2021)

NIA 401 Auditoría en un ambiente de sistemas de información por computadora. Esta norma tiene por objetivo establecer lineamientos sobre los procedimientos que se llevan a cabo en los sistemas de información computarizado SIC, esta norma contempla un SIC cuando de por medio se encuentra una computadora en el procesamiento de la información y que resulte importante para la auditoría. (Normas Internacionales de Auditoría, 2016)

Tabla 2. *Cuadro de las Normas Internacionales de Auditoría*

Normas Internacionales de Auditoría	
NIA 300	Planificación de la Auditoría
NIA 315	Identificación y valoración de los riesgos de incorreción material mediante el conocimiento de la entidad y de su entorno.
NIA 500	Evidencia de Auditoría
NIA 700	Formación de la opinión y emisión del informe de Auditoría

NIA 706	Párrafos de énfasis sobre asuntos y párrafos en el informe de auditoría.
NIA 720	La responsabilidad del auditor en relación a otra información.

Fuente: Adaptado de Normas Internacionales de Auditoría (2016)
Elaborado por: Sánchez (2023)

1.2.3. Normas ISO 27000

Las normas ISO establecen niveles reconocidos de cumplimiento de calidad, eficiencia y seguridad en las diferentes áreas y actividades de cada norma. Se componen de estándares y guías que son herramientas específicas de gestión aplicables en toda entidad (León & Guerra, 2016). Por otro lado, las normas ISO/IEC 2700 son normas orientadas a las buenas prácticas en relación del Sistema de Gestión de Seguridad de la Información orientadas a la mejora continua y mitigación de riesgos (Organización internacional de Normalización , 2018).

Tabla 3. *Normas ISO 27000*

Normas ISO 27000	
ISO 27000	Vocabulario y definiciones
ISO 27001:2005	Requisitos del sistema de gestión de seguridad de información
ISO 27002:2005	Código de prácticas para la gestión de la seguridad de la información
ISO 27003	Directrices de implantación
ISO 27004	Métricas y mediciones
ISO 27005	Gestión de Riesgos
ISO 27006	Requisitos para Organizaciones auditoras y certificadoras sobre los sistemas de Gestión de seguridad de la información.

Fuente: Adaptado de Normas ISO 27000 (2016)
Elaborado por: Sánchez (2023)

1.2.4. Introducción a la informática

1.2.4.1. Definición

La informática es la ciencia de la información, que permite el manejo y procesamiento de datos a través de ordenadores automatizados (Villazán, 2010). En este sentido, cabe recalcar que la informática va de la mano con la automatización y los equipos tecnológicos lo cual resulta un componente importante para las empresas.

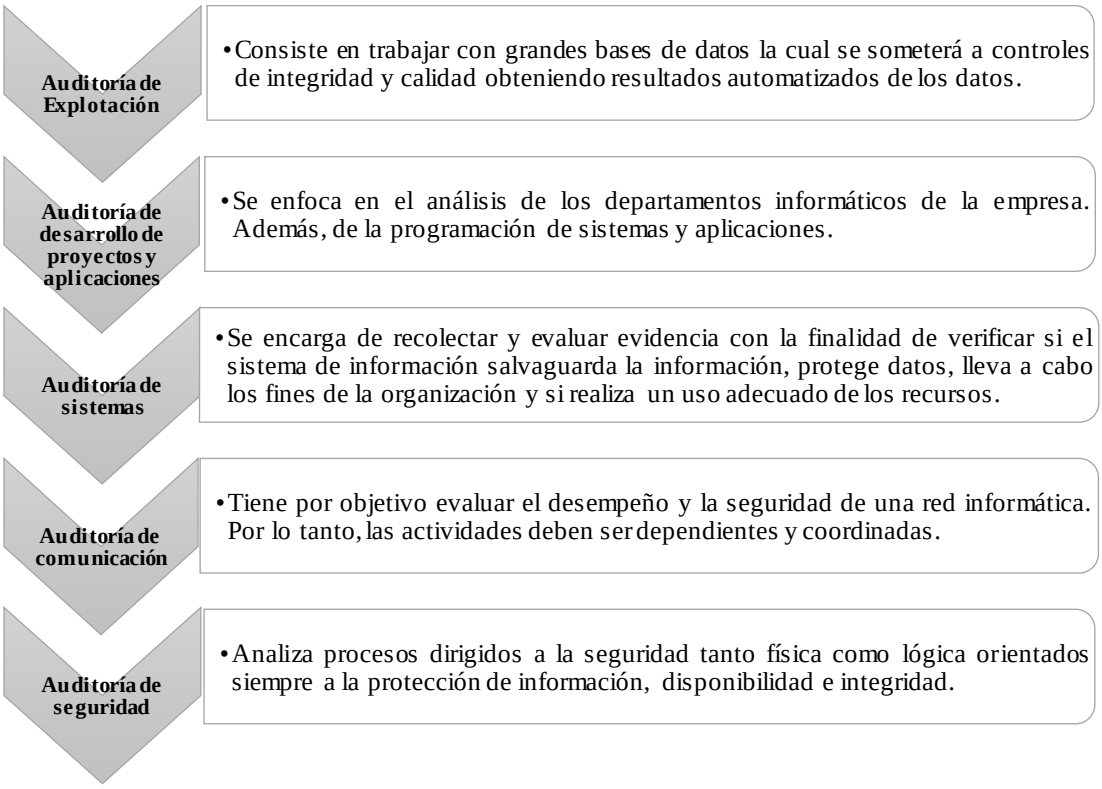
1.2.4.2. Auditoría informática

La auditoría informática tiene por objetivo realizar una evaluación completa a una empresa con la finalidad de determinar y mejorar métodos y controles. Además, de definir una correcta utilización de recursos físicos y humanos (Piattini & Del Peso, 2001). Es decir, en toda empresa será siempre fundamental llevar a cabo una Auditoria informática ya que trae consigo grandes ventajas que ayudaran a la empresa a ser más competitiva y rentable.

1.2.4.3. Tipos y clases de Auditoría Informática

En el siguiente grafico podemos observar los tipos de auditoría informática y su definición:

Ilustración 4. *Clases de Auditoría Informática*



Fuente: Adaptado de Espinosa, Mora, & Lopez (2014)
Elaborado por: Sánchez (2023)

1.2.4.4. Fases de auditoría

En este caso, se pueden apreciar las tres fases de una auditoría:

Tabla 4. *Fases de una Auditoría*

FASES DE AUDITORÍA	DEFINICIÓN
PLANIFICACIÓN	Se obtendrá información y datos importantes de la entidad. Además de determinar los procedimientos a ejecutar durante el proceso de revisión.
EJECUCIÓN	Es la recopilación, evaluación y elaboración de pruebas de las cuales se obtendrán un resultado que dará paso a la opinión del auditor.
COMUNICACIÓN	Es el informe en el cual se presentan resultados y conclusiones obtenidos mediante la aplicación de procedimiento de auditoria sustentados con la información de la entidad.

Fuente: Adaptado de Vargas (2020)
Elaborado por: Sánchez (2023)

1.2.4.5. Las tecnologías de la información y comunicación

Están compuestas por tecnologías que comprenden el acceso, producción, tratamiento y comunicación de la información representada mediante texto, imágenes, sonido y videos (Ayala & Gonzales, 2015).

1.2.5. Sistema informático

El sistema informático consta de dos elementos como el hardware un equipo electrónico formado por elementos físicos y el Software que son componentes no físicos que ayudan al funcionamiento los equipos electrónicos (Hernádez, 2003).

Ilustración 5. *Sistema Informático*

Fuente: Adaptado de Hernández (2003)
Elaborado por: Sánchez (2023)

1.2.6. Seguridad de la información

Hace referencia a la protección de la información y de los sistemas, al acceso, uso y divulgación no autorizada de datos. Además de proteger de amenazas con el objetivo de resguardar todo tipo de información de una empresa (Avenía, 2017). Es decir, en toda empresa es vital controlar y supervisar la seguridad de la información ya que esta puede poner en peligro y presentar amenaza para a la empresa.

1.2.7. Control interno informático

El control interno informático es un subsistema del sistema de control que comprende procesos administrativos y sistematizados con el fin de garantizar seguridad y control de los recursos informáticos (Brito & Solis, 2004).

1.2.8. Clasificación general de los controles

A continuación, se detallan los tres tipos de control:

Tabla 5. *Tipos de Control*

TIPOS DE CONTROL		
PREVENTIVO	**DETECTIVO**	**CORRECTIVO**
Son aquellos que anticipan a una acción, impidiendo que esta se realice, evitando el acceso a los sistemas.	Son aquellos que detectan errores, funcionan como guía para que el auditor evalué la efectividad de los controles preventivos.	Son aquellos que tiene por objetivo ayudar a corregir errores, fallos o fraudes.

Fuente: Adaptado de Carrión (2005)
Elaborado por: Sánchez (2023)

1.2.9. Ciberseguridad

La Ciberseguridad tiene la finalidad de prevenir, proteger de ataques y amenazas ya que cuenta con la capacidad de controlar el acceso a redes y sistemas informáticos (Leiva, 2015). Es así que, la ciberseguridad tiene por objetivo salvaguardar y proteger la información y no poner en riesgo su confidencialidad.

1.2.10. Amenaza, vulnerabilidad y riesgo

El siguiente recuadro tiene por objetivo describir cada uno de los siguientes términos:

Ilustración 6. *Amenaza, Vulnerabilidad y Riesgo*

RIESGO	AMENAZA	VULNERABILIDAD
• Daños o pérdidas potenciales causados por eventos fisicos de origen natural.	• Peligro latente de un evento fisico de origen natural o por acción humana.	• Fragilidad Física, económica, social, ambiental o institucional que puede ser afecta o sufrir efectos adversos ante un evento físico peligroso.

Fuente: Adapatado de Rojas & Martínez (2011)
Elaborado por: Sánchez (2023)

CAPÍTULO II

METODOLOGÍA

2.1 Descripción de la metodología

2.1.1 Unidad de análisis

Para el desarrollo del proyecto integrador se consideró como unidad de análisis a la empresa DEMACO CIA. LTDA. SUR ubicada en la ciudad de Ambato provincia de Tungurahua, la cual se dedica a la comercialización de productos de construcción. Al ser una empresa que funciona a nivel nacional y que cuenta con varias sucursales nace la necesidad de realizar una auditoría de sistemas.

Para el presente estudio se extrajo información en el área de informática, con la finalidad de identificar posibles vulnerabilidad, riesgos y amenazas que existan en el sistema de información de la entidad.

2.1.2 Fuentes, técnicas e instrumentos de recolección de información

Fuentes de información primaria. - La información fue tomada de la empresa DEMACO del área de informática, información que se refiere a: Activos de información, software, hardware, redes de comunicación y usuarios de la información informatizada.

Encuesta. - La encuesta se llevó a cabo a finales del mes Mayo en la empresa DEMACO CIA. LTDA. y se la realizó a los responsables del área de informática de manera presencial utilizando preguntas estructuradas sobre el control interno y los sistemas de información para detectar posibles riegos y controlarlos.

Cuestionario. - Para el desarrollo del proyecto integrador se utilizó el marco de referencia COSO ERM 2017 cuestionario compuesto por 62 preguntas con respuestas de SI y NO y las normas ISO-IEC 27000 y 31000.

Tabla 6. *Persona entrevistada*

Nombre	Cargo	Departamento
Cesar Caicedo	Ingeniero encargado del área.	Área de informática

Elaborado por: Sánchez (2023)

Tabla 7. *Preguntas del cuestionario COSO ERM 2017*

DEMACO CIA. LTDA. ***CUESTIONARIO DE CONTROL INTERNO*** ***COSO ERM 2017***			
COMPONENTES	**PREGUNTAS**	**SI**	**NO**
Gobierno y cultura	¿Existen reuniones con el personal del área de informática para actualizar las prácticas de gestión de riesgos? ¿Se asigna la responsabilidad del seguimiento y control de procesos en el departamento informático? Cuando se toma la decisión de usar o aplicar TI, ¿Hay un responsable que informe el proceso? ¿El área de informática tiene buenas prácticas para la gestión de riesgos? ¿Existen acciones correctivas de incidentes para determinar qué hacer?		
Estrategia y Objetivos	¿El área de informática cumple con normativas y leyes de control interno y seguridad de la información? ¿Existe conocimiento y aplicación acerca del marco de referencia COSO ERM 2017? ¿Hay escalas de medición para la evaluación de riesgos? ¿Se identifican rápidamente riesgos informáticos? ¿Se identifica el peligro que se corre ante la aparición de riesgos en los sistemas de información?		

Fuente: Adaptado de COSO ERM 2017 (2017)
Elaborado por: Sánchez (2023)

2.1.3 Fases del desarrollo

A continuación, se detallará en un cuadro resumen las fases para el desarrollo de la Auditoría:

Tabla 8. *Fases para el desarrollo de la Auditoría*

Fases	Evidencia	Desarrollo
Fase I Planificación	Aplicación de encuesta y entrevista Información necesaria de la entidad Determinar el alcance de auditoría Elaboración de guía de visita previa, memorando de planificación y programa de auditoría.	Diagnóstico previo al área de informática.
Fase II Ejecución	Evaluación de control interno mediante COSO ERM 2017 Aplicación de normas ISO 27000 Y 31000. Detección de puntos débiles de control a través de los flujogramas de los procedimientos informatizados de las transacciones de la empresa.	Evaluación del control interno. Evaluación de los Activos de información Análisis de vulnerabilidades, riesgos y amenazas. Evaluación de riesgos de los Activos de información.
Fase III Comunicación	Elaboración del informe de auditoría al sistema de información Matriz de seguimiento y monitoreo.	Comunicación de resultados Matriz de seguimiento y monitoreo para la evaluación continua.

Elaborado por: Sánchez (2023)

Descripción de cada una de las fases:

Fase I Planificación

Para la planificación de la auditoría se hizo una revisión a los activos de información de la empresa, específicamente en el área de informática. Fase en la que se identificó el alcance, se elaboró la guía de visita previa, memorando y programa de auditoría, procedimientos que tienen por objetivo conocer de mejor manera la parte interna la empresa y diagnosticar su situación actual.

Además, se realizó la recolección de información de la empresa para la aplicación del marco de referencia COSO ERM 2017 para analizar los controles con el fin de conocer el nivel de confianza y riesgo.

En la tabla 9 se puede visualizar las ponderaciones respecto al nivel de confianza y nivel de riesgo:

Tabla 9. *Medición de confianza y riesgo*

Valor de Confianza		
Bajo	**Moderado**	**Alto**
5 - 50%	51 - 75%	76 - 95%
		
95 - 50%	49 - 25%	24 - 5%
Alto	**Moderado**	**Bajo**
Valor de Riesgo		

Fuente: Adaptado de COSO ERM 2017 (2017)
Elaborado por: Sánchez (2023)

Fase II Ejecución

De igual manera se aplicó las Normas ISO/IEC 27000 para evaluar los activos de la empresa considerando los criterios de confidencialidad, integridad y disponibilidad.

Tabla 10. *Criterios de Confidencialidad*

Valor del Activo	***Confidencialidad***
5 (Muy alto)	La información del activo es solo accedida por el personal de alto rango, la divulgación seria irreparable en la empresa.

4 (Alto)	La información del activo es restringida y solo un personal especifico tiene acceso a ella, la divulgación sería grave en la empresa.
3 (Medio)	La información del activo es confidencial y solo personal de áreas internas tiene acceso a ella, la divulgación afectaría considerablemente en la empresa.
2 (Bajo)	La información del activo es de uso interno y solo el personal de ABC tiene acceso a ella, la divulgación afectaría parcialmente a la empresa.
1 (Muy bajo)	La información del activo es pública y cualquiera tiene acceso a ella, no tiene ningún impacto en la empresa.

Fuente: Adaptado de ISO/IEC 27001 (2023)
Elaborado por: Sánchez (2023)

Tabla 11. *Criterios de integridad*

Valor del Activo	***Integridad***
5 (Muy alto)	El activo tolera un máximo de pérdida o alteración de sus componentes en un 0%, la vulneración de su integridad sería irreparable para la empresa.
4 (Alto)	El activo tolera un máximo de pérdida o alteración de sus componentes en un 15%, la vulneración de su integridad sería grave en la empresa.
3 (Medio)	El activo tolera un máximo de pérdida o alteración de sus componentes en un 50%, la vulneración de su integridad afectaría considerablemente en la empresa.
2 (Bajo)	El activo tolera un máximo de pérdida o alteración de sus componentes en un 85%, la vulneración de su integridad afectaría parcialmente a la empresa.
1 (Muy bajo)	El activo tolera un máximo de pérdida o alteración de sus componentes en un 100%, la vulneración de su integridad no tiene ningún impacto en la empresa.

Fuente: Adaptado de ISO/IEC 27001 (2023)
Elaborado por: Sánchez (2023)

Tabla 12. *Criterio de disponibilidad*

Valor del Activo	***Disponibilidad***
5 (Muy alto)	Se requiere que el activo no se esté indisponible, su falta afectaría irreparablemente a la empresa.
4 (Alto)	Se considera que el activo pueda estar indisponible máximo por una hora, su falta sería grave para la empresa.
3 (Medio)	Se considera que el activo pueda estar indisponible máximo por un día, pues su falta afectaría considerablemente a la empresa.
2 (Bajo)	Se considera que el activo pueda estar indisponible máximo por una semana, su falta afectaría parcialmente a la empresa.
1 (Muy bajo)	Se considera que el activo pueda estar indisponible por tiempo indefinido, su falta no tiene ningún impacto en la empresa.

Fuente: Adaptado de ISO/IEC 27001 (2023)
Elaborado por: Sánchez (2023)

También se calcula el nivel de tasación:

Tabla 13. *Nivel de tasación*

Valor del Activo	***Nivel de tasación***
4.001 – 5.000	Muy Alto
3.001 – 4.000	Alto
2.001 – 3.000	Medio
1.001 – 2.000	Bajo
1.000 – 1.000	Muy bajo

Fuente: Adaptado de ISO/IEC 27001 (2023)
Elaborado por: Sánchez (2023)

Además, se evaluó los controles que lleva a cabo la institución ante los riesgos mediante el siguiente criterio:

Tabla 14. *Valoración del control de los Activos*

Valoración del Control de los Activos			
Frecuencia del Control	**Valores**	**Interpretación**	**Descripción**
Bajo	1	El control es mínimo, la empresa puede seguir operando con normalidad, aunque el riesgo se materialice	> 1 año
Medio	2	Existe algún control, la empresa puede continuar operando, pero posiblemente tenga un impacto en algún proceso, retraso en actividades o errores	>= a 2 meses < 1 año
Alto	3	El control está en su máximo esplendor es decir no existen anomalías ni fallas	< 2 meses

Elaborado por: Sánchez (2023)

También se evaluó la probabilidad, impacto, ocurrencia de los riesgos mediante los siguientes criterios y aplicando un mapa de calor:

Tabla 15. *Criterios de Probabilidad de riesgos*

Valores de la frecuencia de Riesgos Probabilidad		
Frecuencia del riesgo	**Valores**	**Criterios**
Bajo	1	Puede ocurrir al menos 1 vez en periodos superiores a 5 años.
Moderado	2	Puede ocurrir al menos 1 vez en 1 y 5 años
Medio	3	Puede ocurrir al menos 1 vez al año
Alto	4	Puede ocurrir varias veces en un mes
Muy Alto	5	Puede ocurrir varias veces en una semana

Elaborado por: Sánchez (2023)

Tabla 16. *Criterios de ocurrencia de riesgos*

Valores de Impacto de ocurrencia por riesgo			
Nivel del riesgo	**Valores**	**Criterios**	**Criterios**
Bajo	1	Ocurre raras veces o casi nunca.	1 <= 3
Moderado	2	Ocurre una vez al año.	>=4 Y <=7
Medio	3	Ocurre una vez en cinco meses.	>=8 Y <=12
Alto	4	Ocurre una vez al mes.	>=13 Y <=18
Muy Alto	5	Ocurre una vez a la semana.	>=19 Y <=25

Elaborado por: Sánchez (2023)

Fase III Comunicación

Una vez realizada las evaluaciones de control interno y el análisis de los activos en el área de informática, se procedió a la elaboración del informe de auditoría en el cual se detallan los resultados obtenidos concluyendo con las respectivas recomendaciones. Por otro lado, se elaboró una matriz de seguimiento y monitoreo que servirá para evaluar de manera constante si se están cumpliendo con las observaciones.

CAPÍTULO III

DESARROLLO

3.1 Resultado

3.1.1 Fase de planificación

El presente proyecto tuvo por objetivo realizar una Auditoría al sistema de información de la empresa DEMACO CIA. LTDA. Ambato aplicando las tres fases correspondientes de la auditoría.

A continuación, se mostrará el desarrollo de la **Fase I de Planificación** en la cual se recopilo toda la información necesaria de la empresa para realizar los análisis respectivos y así conocer más a fondo su situación actual y poder plantear soluciones inmediatas.

Ilustración 7. *Guía de visita previa*

C.S & A	***"CONSULTORA SÁNCHEZ & ASOCIADOS"*** ***AUDITORES - CONSULTORES***	**GVP**

Fase I Planificación
Guía de visita previa

1. Información General	
1.1 Entidad	DEMACO CIA. LTDA.
1.2 N. RUC	990621691001
1.3 Dirección de la entidad	Av. Julio Jaramillo y Av. Julio Cesar
1.4 Correo electrónico de la entidad	huachi@demaco.ec
1.5 Visita	28 de mayo del 2023
1.6 Entrevistado	Ingeniero en sistemas
1.7 Entrevistador	Melanie Sanchez

2. Información del departamento

El area informatica está encargado de dirigir y controlar actividades que esten relacionadas con el tratamiento de la información, software, Hardware, redes de comunicsción y usuarios con acceso a los sistemas y realizar un constante mantenimiento y revisión de los componentes que incluyen el sistema de información procurando prevenir posibles amenazas que puedan poner en riesgo la información como activo vital de la empresa.

Elaborado por: Sánchez (2023)

Ilustración 8. *Archivo Permanente*

C.S & A	***"CONSULTORA SÁNCHEZ & ASOCIADOS"*** ***AUDITORES - CONSULTORES***	**A.P**

ARCHIVO PERMANENTE

DATOS DE LA EMPRESA	
Nombre de la empresa:	DEMACO CIA. LTDA. Sucursal Ambato
Tipo de Examen:	Auditoría de Sistemas
Periodo Auditado	Año 2023

A.P.1 INFORMACIÓN DE LA ENTIDAD	
A.P.1.1 Breve historia de la entidad	Vease Capítulo I, pag 1
A.P.1.2 Certificado RUC	Vease Anexos, pag
A.P.1.3 Base legal	Vease Capítulo I, pag 5
A.P.1.4 Funcionarios de la entidad	Vease Capítulo III, pag 23
A.P.1.5 Organización de la entidad	Vease Capítulo I, pag 3

A.P.2 VISIÓN ESTRATEGICA DE LA ENTIDAD	
A.P.2.1 Misión, Visión	Vease Capítulo I, pag 1 y 2
A.P.2.2 Actividad empresarial	Vease Capítulo I, pag 4
A.P.2.3 Detalle FODA	Vease Capítulo III, pag 24
A.P.2.4 Marcas y Logos	Vease Capítulo I, pag 5
A.P.2.5 Ubicación de la sucursal	Vease Capítulo I, pag 5

Elaborado por: Sánchez (2023)

Ilustración 9. *Autoridades de DEMACO*

"CONSULTORA SÁNCHEZ & ASOCIADOS" AUDITORES - CONSULTORES	A.P.24.4

Autoridades de Demaco	
Cargo	**Nombres**
Gerente	Ing. Tannia Ochoa
Contabilidad	Lcda. Jenny Orellana
Créditos y cobranzas	Tec. David Ruiz
Compras y Ventas	Lcdo. Jhonathan Ulloa
Bodega	Tec. David Ruiz
Informática	Ing. Cesar Caicedo
RRHH	Ing. Jessica Rodriguez

Elaborado por: Sánchez (2023)

Ilustración 10. *Matriz FODA*

"CONSULTORA SÁNCHEZ & ASOCIADOS" AUDITORES - CONSULTORES	A.P.24.3

MATRIZ FODA	
FORTALEZAS	**OPORTUNIDADES**
Ofrecer variedades de productos Experiencia en el mercado Precios competitivos Ubicación estrategica Empleados capacitados y con experiencia	Expansión Aceptación en el mercado ferretero Profesionales en constante capacitación Apertura en nuevas marcas y proveedores Crecimiento poblacional
DEBILIDADES	**AMENAZAS**
Comercializar productos similares a los de la competencia Poco control de inventarios Politicas conservadoras de remuneración	Alta competencia en el sector Incertidumbre política Inseguridad

Elaborado por: Sánchez (2023)

Ilustración 11. *Memorando de Planificación*

C.S & A	*"CONSULTORA SÁNCHEZ & ASOCIADOS"* *AUDITORES - CONSULTORES*	**M.M**

MEMORANDO DE PLANIFICACIÓN

PERIODO DEL AÑO 2023

DEMACO CIA. LTDA.

Auditoría al sistema de información de la empresa DEMACO CIA. LTDA.

Periodo 2023

1. REQUERIMIENTO DE LA AUDITORÍA

2. FECHA DE INTERVENCIÓN

Cronograma	***Fecha estimada***
Marco de Referencia COSO ERM 2017	30/05/2023
Aplicación normas ISO 27000	01/06/2023
Mapa de calor para la administración de riesgos	10/06/2023

3. EQUIPO MULTIDISCIPLINARIO

Nombre	***Iniciales***
Melanie Salomé Sánchez Ibarra	MSSI

4. RECURSOS

Para la elaboración del proyecto integrado se contó con la parcticipación de la Doctora Patricia Paola Jimenez Estrella como tutora y mi persona, Melanie Salomé Sánchez Ibarra estudiante de la Facultad de contabilidad y Auditoria, de la Carrera de Contabilidad y Auditoría de la Universidad Técnica de Ambato.

Materiales		
Hardware y Software	$	300,00
Gastos de Transporte	$	100,00
Oficios	$	50,00
Copias	$	100,00
	$	550,00

5. ENFOQUE DE AUDITORÍA

5.1 Información general de la entidad auditada

Misión

•Trabajar con entusiasmo diariamente para entregar las mayores ventajas a nuestros clientes.
•Ofrecer productos de la más alta calidad a los mejores precios.
•Buscar constantemente productos que posean las mejores tecnologías, escuchando atentamente la opinión de los usuarios antes de seleccionarlas para ponerlas a disposición de la comunidad.
•Desarrollar en el grupo de trabajo voluntad para calificarse permanentemente y desarrollar hábitos de servicio para satisfacer las necesidades de nuestros clientes oportuna y eficientemente
•Realizar las acciones necesarias para lograr el equilibrio necesario para lograr la rentabilidad que la empresa necesita para mantener un crecimiento sostenido.

Visión

Ser un espacio de desarrollo técnico económico y moral de los miembros que participan en la empresa, esforzándose para generar métodos y tecnología para que la comunidad tenga facilidades y pueda ejecutar con calidad y eficiencia sus obras, aportando al mantenimiento del equilibrio ecológico.

Actividad Empresarial

N	***Denominación del producto***
1	Construcción
2	Ferretería
3	Productos hidráulicos
4	Productos electricos
5	Electrodomesticos
6	Acabados y Menaje de casa

Base Legal

La empresa DEMACO CIA. LTDA. cumple con la siguiente normativa:

- Constitución de la República del Ecuador
- Ley de Compañías
- Ley de Seguridad Social
- Código de trabajo
- Ley de régimen tributario Interno

5.2 Motivo de la auditoría

La Auditoria está direccionada al sistema de información de la empresa DEMACO CIA. LTDA. Para recopilar información, identificar y evaluar los activos de información, software, hardware, redes de comunicación, personal a cargo con el fin de reconocer amenazas, vulnerabilidades y riesgos, orientando a la aplicación de controles como soluciones inmediatas para la seguridad de la información y politicas para el SGSI

5.3 Enfoque a:

Auditoría al sistema de información de la empresa DEMACO CIA. LTDA.

5.4 Objetivos

.Objetivo General

Realizar la Auditoría al sistema de información en la empresa DEMACO CIA. LTDA. Sur Ambato para la evaluación de la eficiencia y eficacia de las politicas al sistema de gestión de la seguridad de la información.

.Objetivos Específicos

Planificar procesos, procedimientos y técnicas para preparar la auditoría.

Ejecutar las matrices preestablecidas con los datos recolectados para la evaluación de las amenazas, riegos

Comunicar los resultados obtenidos a través de la presentación del informe final, recomendando politicas para el sistema de gestión de la seguridad de la información, su seguimiento y monitoreo contribuyendo a

5.5 Alcance

Es una metodología innovadora que busca ser un apoyo en el sistema de gestión de la seguridad de la información para la toma de decisiones, resguardando los activos de información, previniendo posibles riesgos y amenazas que atenten al sistema de información.

5.6 Resumen de los resultados de la Evaluación de Control Interno

Se aplicó el Marco de referencia COSO ERM 2017 en el cual se evaluaron 5 componentes con sus respectivas preguntas que ayudaron a conocer esado de el área a ser auditada. Se realizaron preguntas de si o no, preguntas que dieron como resultado la identificación del nivel de reisgo y confianza, mistrando un nivel de confianza de 74,19% y un nivel de riesgo de 25,81% dando como resultado un rango moderado.

5.7 Grado de confianza y controles claves

∞ ***GOBIERNO Y CULTURA***

Se alcanzó un grado de confianza de **71,43%** y un riesgo de **28,57%** dando como resultado Moderado, con con un enfoque de auditoría Mixto doble propósito.

€ ***ESTRATEGIA Y OBJETIVOS***

Se alcanzó un grado de confianza de **70,00%** y un riesgo de **30,00%** dando como resultado moderado, con con un enfoque de auditoría mixto doble propósito.

£ ***DESEMPEÑO***

Se alcanzó un grado de confianza de **61,54%** y un riesgo de **38,46%** dando como resultado moderado, con con un enfoque de auditoría mixto doble propósito.

¥ ***REVISIÓN***

Se alcanzó un grado de confianza de **75,00%** y un riesgo de **25,00%** dando como resultado Moderado, con con un enfoque de auditoría de Mixto doble propósito.

© ***INFORMACIÓN, COMUNICACIÓN Y REPORTE***

Se alcanzó un grado de confianza de **80,00%** y un riesgo de **20,00%** dando como resultado bajo, con un enfoque de auditoría pruebas de cumplimiento.

Ω ***SISTEMA DE SEGURIDAD DE LA INFORMACIÓN***

Se alcanzó un grado de confianza de **100,00%** y un riesgo de **0%** dando como resultado bajo, con con un enfoque de auditoría pruebas de cumplimiento.

6. FASE DE EJECUCIÓN
6.1 Elaboración de los auditores en la fase de ejecución
Analisis de riesgos vulnerabilidades y amenezas Evaluación de los riesgos bajo el enfoque del Marco de referencia COSO ERM 2017 Evaluación al sistema de información y controles bajo el enfoque de las normas ISO/IEC 27001, 31000
7. COLABORACIÓN DE LA ENTIDAD AUDITADA
7.1 Ingenieros encargados del departamento
Ing. Cesar Caicedo
8. OTROS ASPECTOS
Se realizó por primera vez la auditoria al sistema de información de la empresa DEMACO CIA. LTDA. Permitiendo definir politicas del SGSI como un documento que concentre las bases sobre las que se

Elaborado por: Sánchez (2023)

Ilustración 12. *Programa de Auditoría*

C.S & A

"CONSULTORA SÁNCHEZ & ASOCIADOS" AUDITORES - CONSULTORES

P.A

PROGRAMA DE AUDITORÍA

OBJETIVOS

1. Evaluar el sistema de información de la entidad con apoyo especificamente del area informatica.
2. Delimitar los niveles de riesgos en los activos de información
3. Aplicar los marcos de referencia COSO ERM 2017 y normas ISO/IEC 27000 y 31000

Alcance

Evaluación a los componentes del sistema de información de la empresa resguardando los activos de información, previniendo posibles riesgos y amenazas que atenten al SGSI y la continuidad del negocio.

N.	*PROCEDIMIENTOS*	*TIPOS DE PROCEDIMIENTOS*	*TÉCNICA*	*ELABORADO POR*	*FECHA*
1	Levantamiento de los activos de información	Pruebas de cumplimiento	Observación y verificación	MSSI	22/5/2023
2	Evaluación del control interno informatico	Pruebas de cumplimiento	Cuestionario COSO ERM	MSSI	23/5/2023
3	Identificación de Activos de información, riesgos y amenazas	Pruebas sustantivas	Matriz de evaluación ISO/IEC 27000	MSSI	24/5/2023
4	Detección de putos debiles en procesos informatizados de las transaciones de la empresa	Pruebas de cumplimiento	Observación	MSSI	10/6/2023
5	Evaluación de riesgos de activos de información	Pruebas sustantivas	Matriz de evaluación	MSSI	10/6/2023

Elaborado por: Sánchez (2023)

3.1.1.1 Marco de referencia COSO ERM 2017

Se aplicó el marco de referencia COSO ERM 2017 para la evaluación de control interno, sus estrategias y la seguridad de la información. La información se obtuvo del área de informática en base al sistema de información.

Está conformado por 6 componentes y 20 principios que se relacionan entres si, se elaboró un total de 62 preguntas relacionadas directamente con cada principio y componente, preguntas que nos ayudaron a cuantificar y medir el nivel de riego y confianza en el área de informática para poder proponer soluciones inmediatas a los problemas encontrados.

Ilustración 13. *Marco de referencia COSO ERM 2017*

"CONSULTORA SÁNCHEZ & ASOCIADOS"
AUDITORES - CONSULTORES

DEMACO CIA. LTDA.

MATRIZ DE NIVEL DE CONFIANZA Y NIVEL DE RIESGO INHERENTE

COMPONENTE : CONTROL INTERNO
AÑO 2023

MNCNR

COMPONENTE	N.	PREGUNTA	CALIFICACIÓN		CALIFICACIÓN TOTAL
			SI	NO	
Gobierno y cultura	1	¿Existen reuniones con el personal del area de informatica para actualizar las prácticas de gestión de riesgos?	1		**1**
	2	¿Se asigna la responsabilidad del seguimiento y control de procesos en el departamento informático?		0	**0**
	3	Cuando se toma la decisión de usar o aplicar TI, ¿Hay un responsable que informe el proceso?		0	**0**
	4	¿El área de informática tiene buenas prácticas para la gestión de riesgos?	1		**1**
	5	¿Existen acciones correctivas de incidentes para determinar qué hacer?	1		**1**
	6	¿El software utilizado apoya los procesos institucionales?	1		**1**
	7	¿Hay políticas que cubran los controles de TI?		0	**0** §
	8	¿Promueven una cultura de inteligencia ante riesgos?		0	**0**
	9	¿El área de informática comprende los objetivos a ejecutarse?	1		**1**
	10	¿El área de informática no filtrado información confidencial?	1		**1**
	11	¿El personal tiene el deber de no manipular los datos del área de informática?	1		**1**
	12	¿El personal conoce las consecuencias que trae la corrupción en la seguridad cibernética?	1		**1**
	13	¿El personal se encuntra capacitado en gestión de riesgos?	1		**1**
	14	¿El departamento promueve el desarrollo del conocimiento y anima a los empleados a mejorar su desempeño?	1		**1**

Estrategia y objetivos	15	¿El área de informática cumple con normativas y leyes de control interno y seguridad de la información?	1		**1**
	16	¿Existe conocimiento y aplicación acerca del marco de referencia COSO ERM 2017 ?		0	**0** §
	17	¿Hay escalas de medición para la evaluación de riesgos?		0	**0**
	18	¿Se identifican rápidamente riesgos informáticos?	1		**1**
	19	¿Se identifica el peligro que se corre ante la aparición de riesgos en los sistemas de información?	1		**1**
	20	¿El área de informática tiene políticas de control interno ante la gestión de riesgos informáticos?	1		**1**
	21	¿La máxima autoridad del área de informática se encuentra infromado acerca de los planes estratégicos para la toma de decisiones?	1		**1**
	22	¿Hay personal apto para el desarrollo de estrategias y alternativas ante riesgos del sistema de información?	1		**1**
	23	¿El área de informática tiene estrategias adecuadas para prevenir posibles riesgos?		0	**0** §
	24	¿Poseen planes que puedan mitigar posibles riesgos?	1		**1**
Desempeño	25	¿Estan correctamente identificados los riesgos relacionados con los controles internos informáticos?		0	**0**
	26	¿Existen riesgos legales relacionados a las actividades que se ejecutan en el área informática que pudieran comprometer el logo de la entidad?	1		**1**
	27	¿El area informatica cuenta con procedimientos para detectar riesgos de gran magnitud en las actividades que realizan?	1		**1**
	28	¿El area Informatica es encargada de evaluar riesgos de fraudes?	1		**1**
	29	¿Existen procedimientos que garanticen el cumplimiento de disposiciones reglamentarias sobre el manejo de activos de información?	1		**1**
	30	¿El área de informática detecta y previene fraudes en procecos establecidos?	1		**1**
	31	¿El área de informática es consciente del riesgo del incumplimiento de las normas y leyes aplicables en sus actividades?	1		**1**
	32	¿Existen criterios claros para determinar los riesgos y probabilidad de que estos ocurran?		0	**0** §
	33	¿El área de informática cuenta con un plan de riesgos para determinar la probabilidad de ocurrencia e impacto?		0	**0**
	34	¿El área informática clasifica los riegos como aceptables o que requieren de acciones?		0	**0** §
	35	¿El área de informática toma acciones para determinar factores críticos de riesgos en las actividades?	1		**1**
	36	¿El área de informática lleva a cabo medidas de mitigación ante riesgos observado?		0	**0** §
	37	¿En el área de informática existen procedimientos que ayuden a mitigar riesgos por fraudes?	1		**1**

Revisión	38	¿El área de informática determina los cambios significativos que deben realizase?	1		**1**
	39	¿El área de informática evalúa los cambios significativos que se hayan efectuado?	1		**1**
	40	¿El área de informática analiza el funcionamiento de la gestión de los riesgos informáticos?	1		**1**
	41	¿Se controla con frecuencia el desempeño y el riesgo?		0	**0**
	42	¿El personal sabe acerca de las revisiones que se deben realizar en el área de informática ?	1		**1**
	43	¿El área de informática realiza adecuadamente las revisiones necesarias?	1		**1**
	44	¿El área informática plantea mejoras en la gestión de riesgos informáticos identificados?	1		**1**
	45	¿En el área informática se toma en cuenta el dinamismo profesional?		0	**0**
Información, comunicación y reporte	46	¿Se utiliza la tecnologia en beneficio del área de informática?	1		**1**
	47	¿La entidad cuenta con base de datos con información que soporta la toma de decisiones?	1		**1**
	48	¿En la entidad se cuenta con la seguridad de la información?	1		**1**
	49	¿La entidad cuenta con Firewalls para evitar intrusos o usuarios malicioso?	1		**1**
	50	¿Existen estrategias basadas en riesgos informáticos identificados?	1		**1**
	51	¿Se examina el impacto de los riesgos en las estrategias ya definidas?	1		**1**
	52	¿Se considera el riesgo para estrategia y desempeño departamental?	1		**1**
	53	¿Se ha establecido alguna filosofía de gestión de riesgos de sistemas de informacion?	1		**1**
	54	¿En el área informatica se implementan consistentemente las actividades de gestión de riesgos?		0	**0**
	55	¿En el área de informática existe coherencia entre el rendimiento y la gestion de riesgos?		0	**0**
Sistema de seguridad de información	56	¿Permiten las copias de seguridad resolver en un plazo satisfactorio las pérdidas de información o fallos a causa de la materialización de las amenazas?	1		**1**
	57	¿Se llevan las copias de seguridad a dispositivos externos o en la nube?	1		**1**
	58	¿Está protegido el acceso físico a las instalaciones informáticas ?	1		**1**
	59	¿Están protegidas las instalaciones informáticas contra fallos en el fluido eléctrico, incendios, desastres naturales, etc.?	1		**1**
	60	¿Los coloraboradores cuidan el uso de la información para evitar fraude o sobornos?	1		**1**
	61	¿Se ha detectado inconsistencia en la información reportada por las herramientas informáticas que utiliza la empresa?	1		**1**
	62	¿ La empresa se cuida de ataques ciberneticos?	1		**1**
		PONDERACIÓN TOTAL			**62**
		CALIFICACIÓN TOTAL			**46**

Elaborado por: Sánchez (2023)

Ilustración 14. *Resultados de los componentes del COSO ERM 2017*

VALORACIÓN		
Calificación Total	46	
Ponderación Total	62	
Nivel de Confianza	74,19%	
Nivel de Riesgo Inherente / De control	25,81%	ENFOQUE DE AUDITORIA
	MODERADO	*MIXTO-DOBLE PROPÓSITO*

Gobierno y cultura		
Calificación Total	10	
Ponderación Total	14	
Nivel de Confianza	71,43%	
Nivel de Riesgo Inherente / De control	28,57%	ENFOQUE DE AUDITORIA
	MODERADO	*MIXTO-DOBLE PROPÓSITO*

Estrategia yobjetivos		
Calificación Total	7	
Ponderación Total	10	
Nivel de Confianza	70,00%	
Nivel de Riesgo Inherente / De control	30,00%	ENFOQUE DE AUDITORIA
	MODERADO	*MIXTO-DOBLE PROPÓSITO*

Desempeño		
Calificación Total	8	
Ponderación Total	13	
Nivel de Confianza	61,54%	
Nivel de Riesgo Inherente / De control	38,46%	ENFOQUE DE AUDITORIA
	MODERADO	*MIXTO-DOBLE PROPÓSITO*

Revisión		
Calificación Total	6	
Ponderación Total	8	
Nivel de Confianza	75,00%	
Nivel de Riesgo Inherente / De control	25,00%	ENFOQUE DE AUDITORIA
	MODERADO	*MIXTO-DOBLE PROPÓSITO*

Información, comunicación y reporte		
Calificación Total	8	
Ponderación Total	10	
Nivel de Confianza	80,00%	
Nivel de Riesgo Inherente / De control	20,00%	ENFOQUE DE AUDITORIA
	BAJO	*CUMPLIMIENTO*

Sistema de seguridad de información		
Calificación Total	7	
Ponderación Total	7	
Nivel de Confianza	100,00%	
Nivel de Riesgo Inherente / De control	0,00%	ENFOQUE DE AUDITORIA
	BAJO	*CUMPLIMIENTO*

Elaborado por: Sánchez (2023)

3.1.2 Fase de ejecución

3.1.2.1 NORMAS ISO/IEC 27000 Evaluación a los activos de información

La aplicación de estas evaluaciones nos permite conocer de mejor manera los activos de la empresa, conocer los más críticos y determinar medidas que ayuden a minimizar riesgos.

Los tipos de activos de información y se valoraron mediante los criterios de confidencialidad, integridad y disponibilidad, luego se pasó a promediar y se obtuvo el valor total del activo o nivel de tasación.

Ilustración 15. *Evaluación de Activos de información*

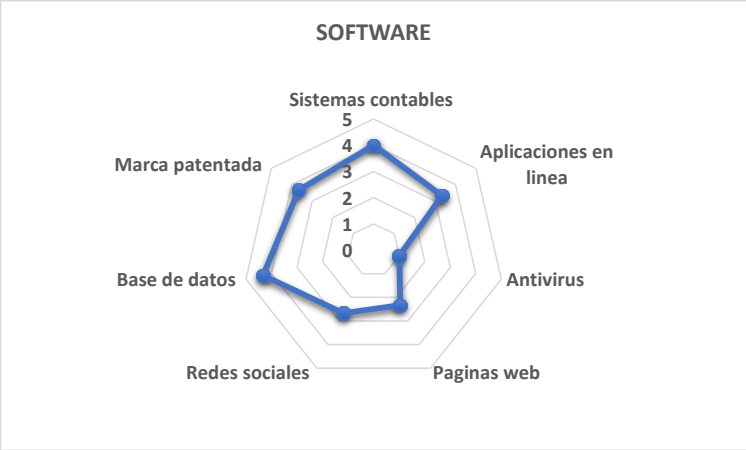
DEMACO CIA. LTDA.							
EVALUACIÓN DE ACTIVOS DE INFORMACIÓN ISO/IEC 27000							
Grupo Activos de Información	**Descripción Activos de Información**	**Detalle del Activo de Información**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Valor del Activo**	**Nivel de Tasación**
SOFTWARE	**Sistemas contables**	ORACLE EDWARDS 9.1 **Módulos:** Ventas, Compras, Cotización	*2*	*5*	*5*	**4**	**Alto**
	Aplicaciones en linea (Tributario y empresarial)	SRI	*5*	*2*	*3*	**3,333**	**Alto**
	Antivirus	No cuentan con antivirus actualmente	*1*	*1*	*1*	**1,000**	**Muy Bajo**
	Paginas web	**Cuentan con pagina web:** WWW.demaco.ec	*1*	*3*	*3*	**2,333**	**Medio**
	Redes sociales	**Utilizan redes sociales como:** Facebook, Whatsapp, Instagram,TIK TOK	*1*	*3*	*4*	**2,667**	**Medio**
	Base de datos	Cuentan con una Nube e información fisica	*3*	*5*	*5*	**4,333**	**Muy Alto**
	Marca patentada	El logo pertenece a la entidad	*1*	*5*	*5*	**3,667**	**Alto**
HARDWARE	**Equipos**	**3 computadoras HP** **Nombre del dispositivo:** Jenny **Procesador** Intel® Pentium® Gold G5600 CPU@ 3.90GHz 3.91GHz **RAM instalada:** 4,00 GB (3,87 GB Utilizable) **Id. del dispositivo:** 781D8D86-9B04-4CB4-97F2-C47C0195ACEE **Id. del producto:**0033-80000-00000-AA197 **Tipo de sistema**: Sistema operativo de 64 bits, procesador x64	*3*	*4*	*5*	**4**	**Alto**
	Impresoras	**2 Impresoras** **Sistemas de Operación:** Windows Vista® / 7 / 8 / 8.1 / 10 o más reciente (32bit, 64bit) Windows Server® 2003 (SP2) or later Mac OS X 10.5.8 o más reciente, macOS 11 o más reciente **Dimensiones:** Abierto: 37.5 cm x 57.8 cm x 25.3 cm Cerrado: 37.5 cm x 34.7 cm x 18.7 cm	*3*	*4*	*5*	**4**	**Alto**
	Scaners	**2 scaners HP** **Tipo de Escáner:** Alimentación vertical, Escáner a color dúplex de un paso **Dispositivo Fotoeléctrico:**CIS (Sensor de Contacto de Imagen) **Resolución Óptica:**600 dpi **Resolución Máxima:**1200 dpi **Profundidad del Bit de Color:** 30 bits interno / 24 bits externo **Profundidad de la Escala de Grises del Bit:**16 bits interno / 8 bits externo **Fuente de Luz:**LED RGB de 3 colores **Velocidad de Escaneo:**300 dpi : B/N & color (35 ppm/70 ipm)	*3*	*3*	*2*	**2,667**	**Medio**
	Discos duros	1 terabyte	*4*	*4*	*3*	**3,667**	**Alto**
	Pendrives	Cuentas con dos flash memorys	*3*	*1*	*1*	**1,667**	**Bajo**

REDES DE COMUNICACIÓN	**Cableado**	Cableado de energía, cables de alimentación y regletas y cables de internet	*2*	*5*	*5*	**4**	**Alto**
	Red	RED wifi y por cable	*3*	*4*	*5*	**4**	**Alto**
	Capacidad del servidor	223 megahercios con 256 de RAM	*5*	*3*	*4*	**4**	**Alto**
PERSONAL	**Gerente**	**Gerente:** Ing.	*5*	*5*	*5*	**5**	**Muy Alto**
	Contabilidad	**Auxiliar contble:** Lcda **Crédito y Cobranza:**Tec.	*4*	*4*	*4*	**4**	**Alto**
	Comercialización	**Jefe de ventas:** Tec. **Vendedor interno y externo**: Lic.	*4*	*4*	*4*	**4**	**Alto**
	Inventarios	**Jefe de bodega**: Lic.	*4*	*4*	*4*	**4**	**Alto**
	Recursos Humanos	**RRHH:** Ing.	*4*	*4*	*4*	**4**	**Alto**
	Área de informática	**Jefe área Informática:** Ing.	*4*	*4*	*4*	**4**	**Alto**

Elaborado por: Sánchez (2023)

A continuación, se representa gráficamente la valorización de los activos, obtenidos como resultados mediante la aplicación de las normas ISO/IEC 27000:

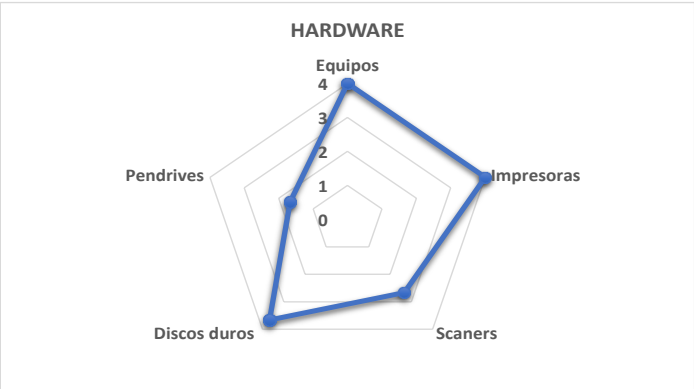
Ilustración 16. *Evaluación del Activo de Información Software*



Elaborado por: Sánchez (2023)

Como se observa en la ilustración 16, el grupo de activo Software cuenta con distintas valoraciones, se resalta que el componente antivirus el cual tiene un nivel de tasación Muy bajo con un valor de 1, se le considera un activo crítico ya que presenta problemas de seguridad que podría poner en peligro la información. Por otro lado, el componente Base de datos tiene un nivel de tasación Muy alto con un valor de 4, lo que significa que este activo de información cumple de manera óptima los criterios de confidencialidad, integridad y disponibilidad que resalta la norma ISO/IEC 27001.

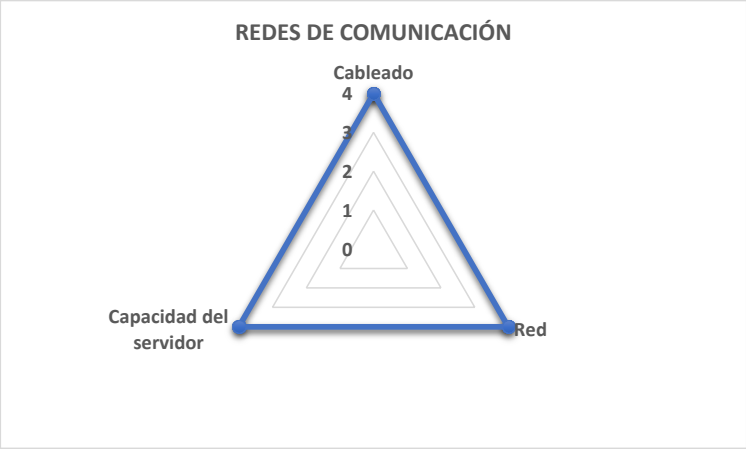
Ilustración 17. *Evaluación del Activo de Información Hardware*



Elaborado por: Sánchez (2023)

Como se observa en la ilustración 17, el grupo de activo Hardware la mayoría de sus componentes tienen niveles altos y medios, es decir, estos activos están controlados y requieren de autorizaciones para poder tener acceso a ellos y dar mantenimientos. Por otro lado, el componente pendrives con un nivel de tasación bajo valorado en 1,6 presenta graves falencias poniendo en riesgos los equipos e incluso dañando o alterando la información del ordenador.

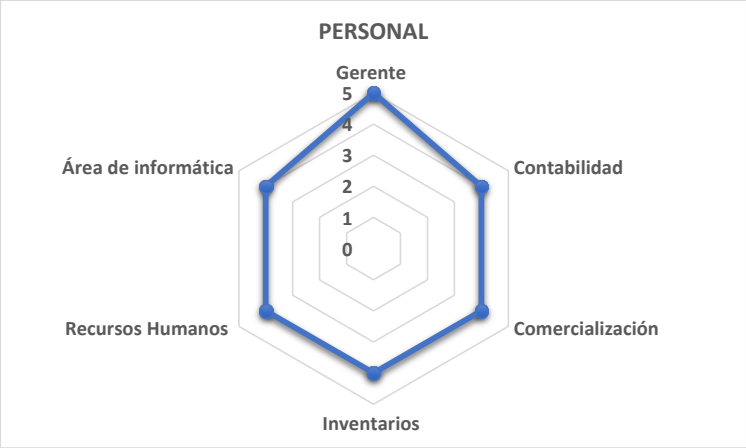
Ilustración 18. *Evaluación del Activo Redes de Comunicación*



Elaborado por: Sánchez (2023)

Como se observa en la ilustración 18, se realizó la valoración del activo Redes de Comunicación, interpretándolo como un componente que cuenta con elementos de un nivel de tasación Alto, es decir, estos activos se encuentran cumpliendo de manera eficiente los criterios de confidencialidad, integridad y disponibilidad según lo establecido la normas ISO/IEC 27001.

Ilustración 19. *Evaluación del Activo Personas (Trabajadores)*



Elaborado por: Sánchez (2023)

Como se observa en la ilustración 19, en el grupo de Activo Personas todos sus componentes cuentan con niveles de tasación Alto y Muy alto, es decir, el personal se encuentra apto y preparado para el desarrollo de sus actividades, cumpliendo y respetando los criterios de confidencialidad de la información, integridad y accesibilidad a la información previa autorización.

3.1.2.2 Flujogramas de procedimientos informatizados de transacciones.

Los flujogramas que son objeto de revisión y son realizados en la empresa DEMACO CIA. LTDA. Son:

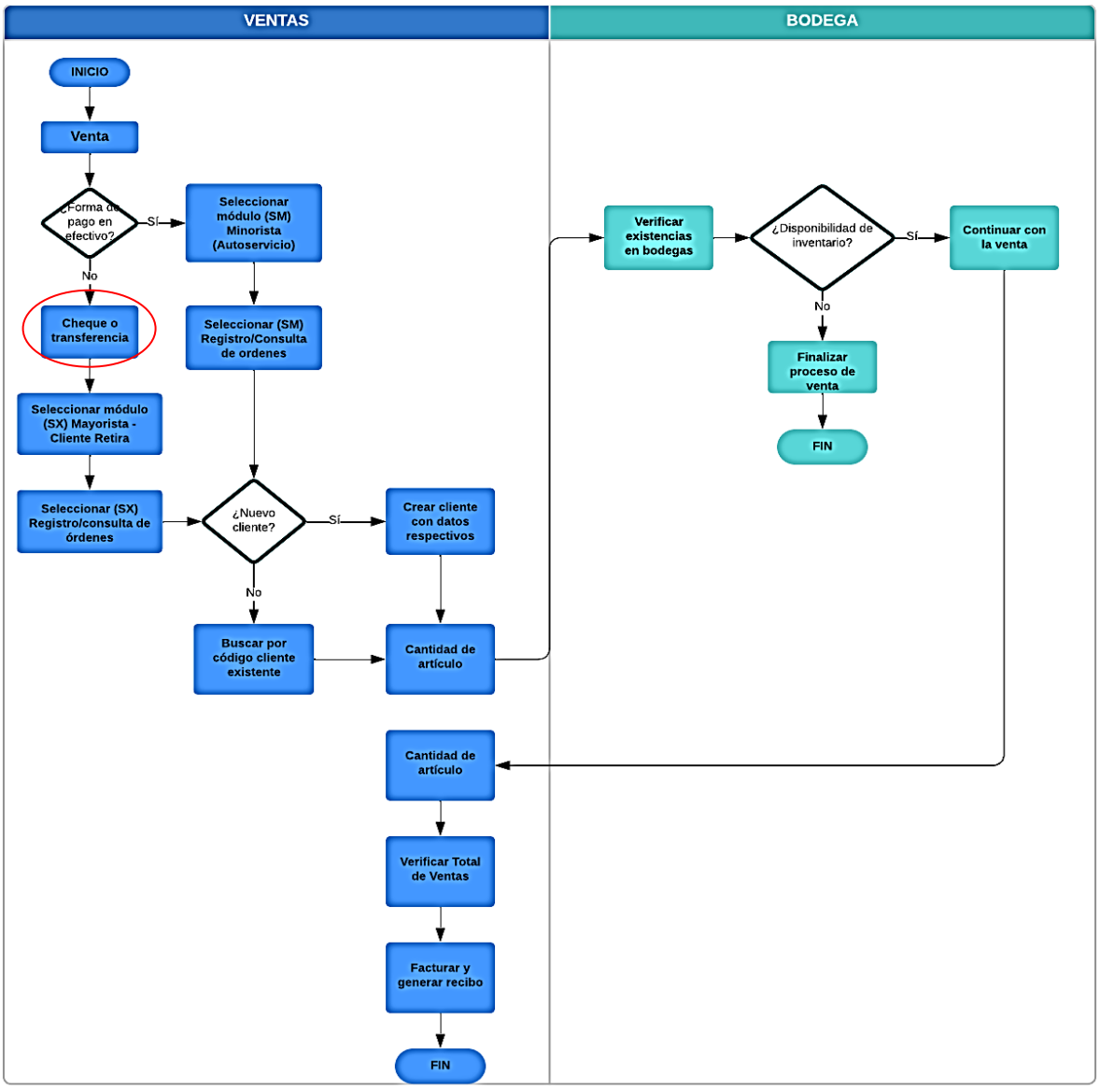
- ✓ Ventas de contado
- ✓ Ventas a crédito
- ✓ Cuentas por cobrar
- ✓ Pedidos para Adquisiciones
- ✓ Inventarios
- ✓ Cotización

Mientras que los demás procedimientos informatizados de transacciones lo controlan directamente la casa matriz en la ciudad de Guayaquil.

A continuación, se elaboraron flujogramas de los procesos informatizados que realiza la entidad, con la finalidad de identificar puntos débiles.

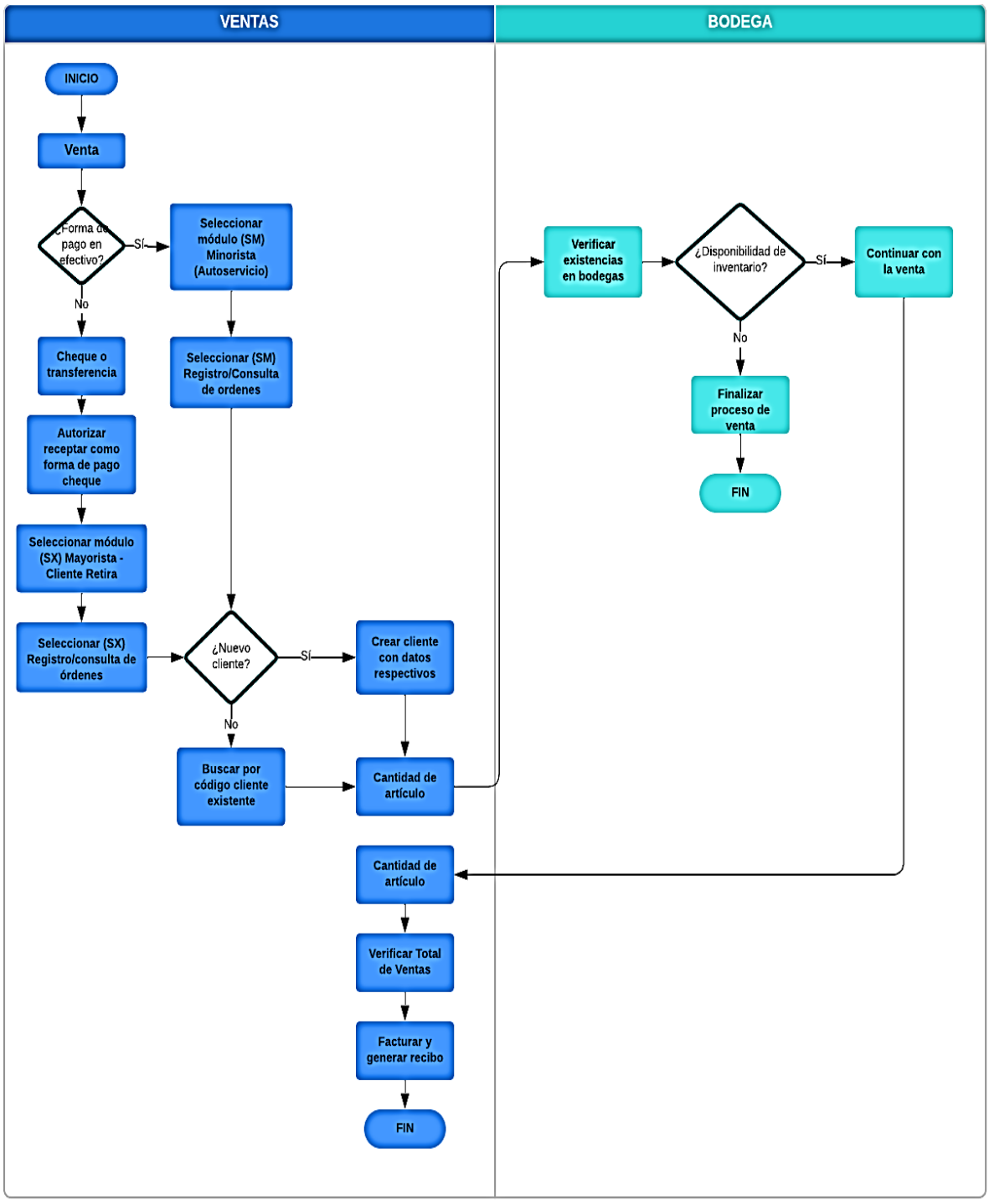
El siguiente flujograma muestra el proceso que se lleva a cabo para realizar una venta de contado, en el que interviene el departamento de comercialización y bodega. Además, se identificaron puntos débiles como: No existe una autorización para receptar como forma de pago un cheque.

Ilustración 20. *Flujograma de ventas de contado*



Elaborado por: Sánchez (2023)

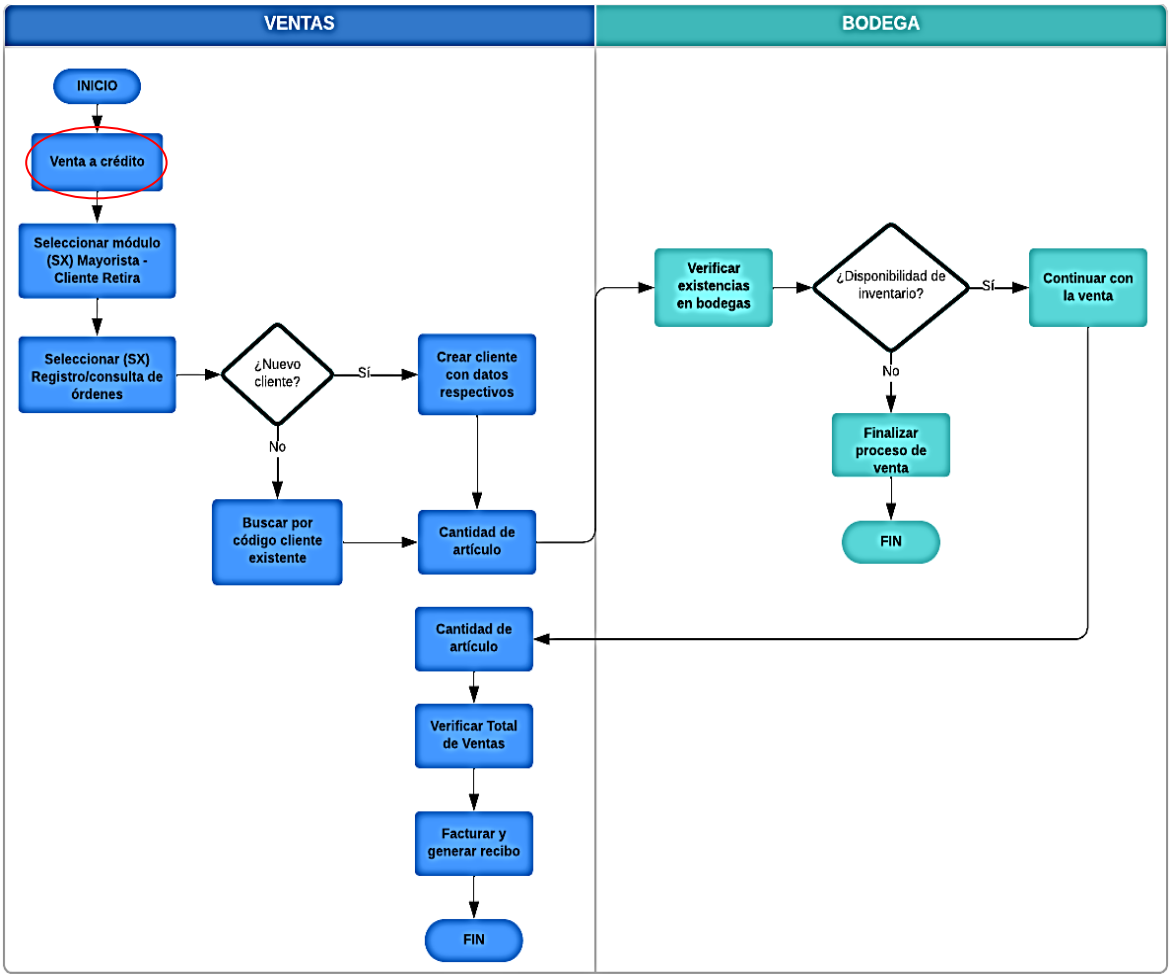
Ilustración 21. *Flujograma propuesto de ventas de contado*



Elaborado por: Sánchez (2023)

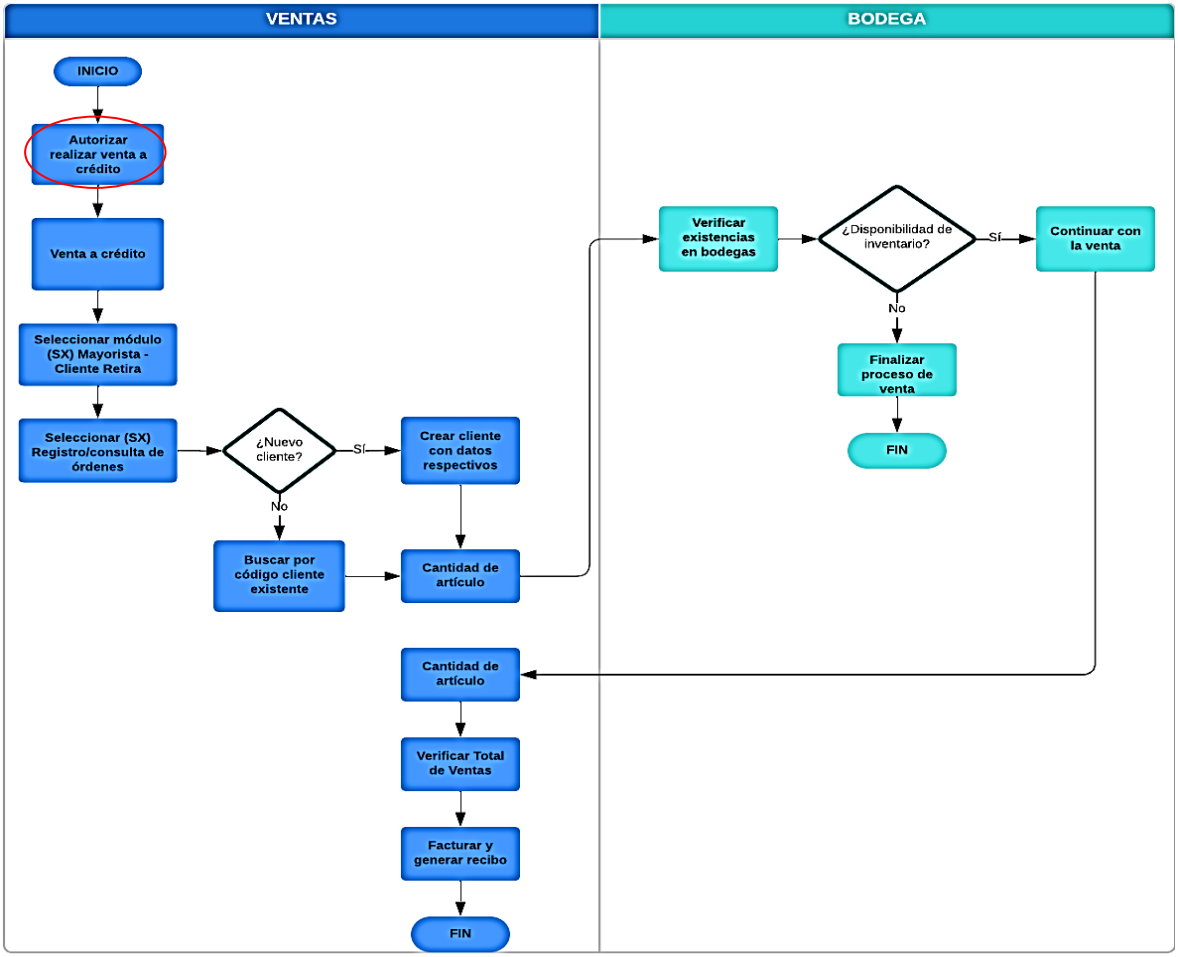
El siguiente flujograma muestra el proceso que se lleva a cabo para realizar una venta a crédito, en el que interviene el departamento de comercialización y bodega. Además, se identificó un punto débil, no hay una previa autorización para que se realice una venta a crédito.

Ilustración 22. *Flujograma de Ventas a crédito*



Elaborado por: Sánchez (2023)

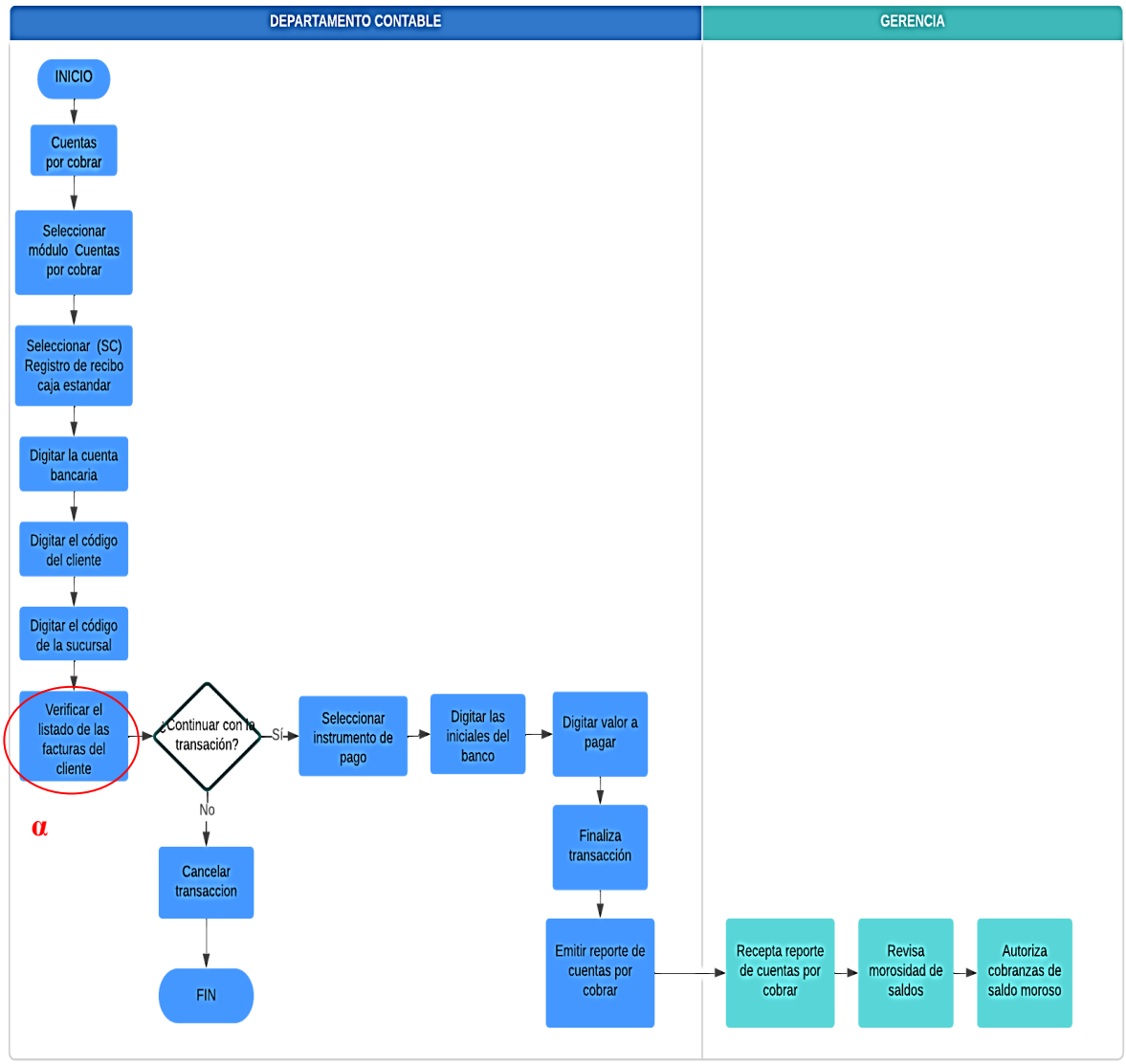
Ilustración 23. *Flujograma propuesto para ventas a crédito*



Elaborado por: Sánchez (2023)

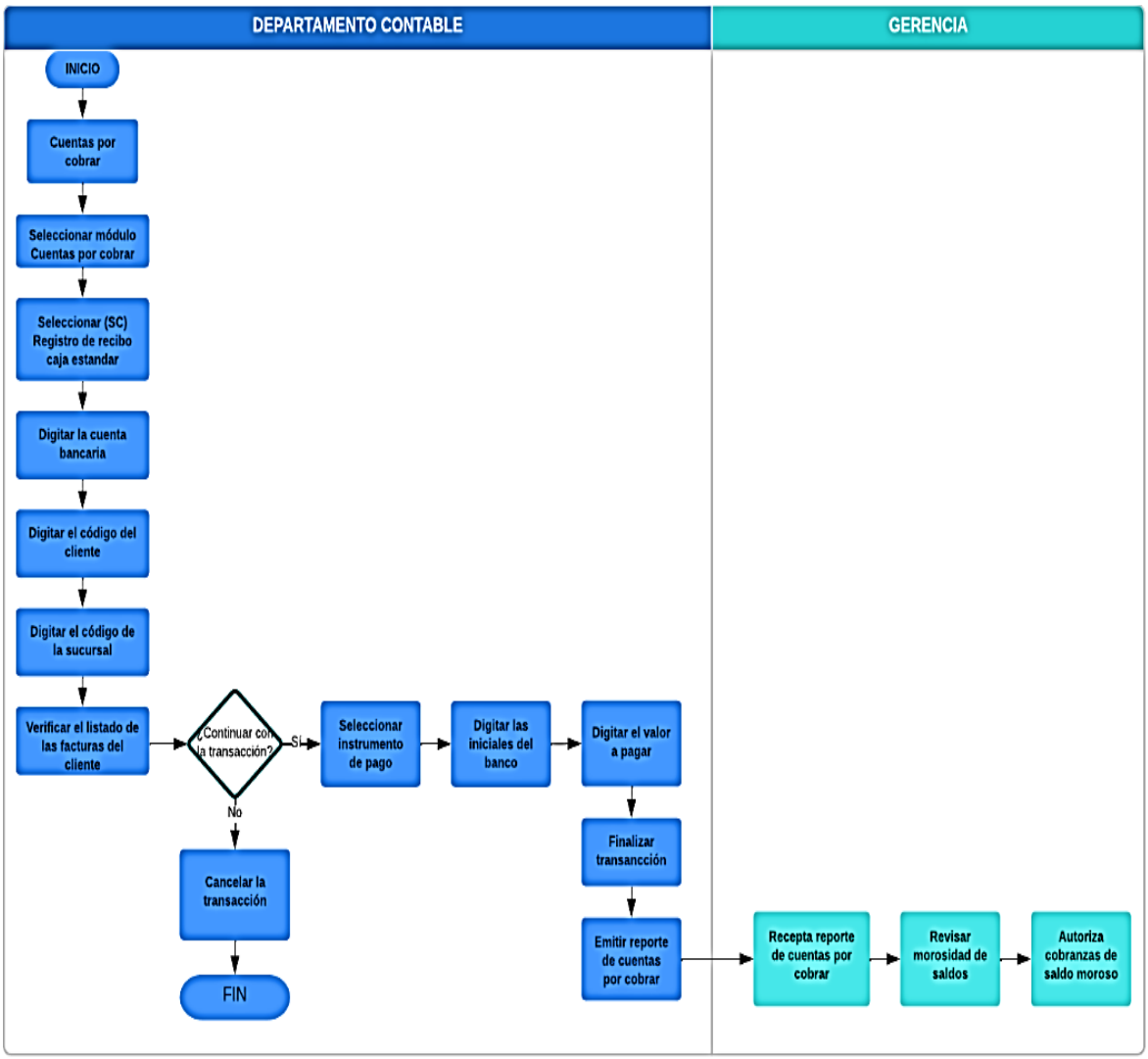
El siguiente flujograma muestra el proceso que se lleva a cabo para cuentas por cobrar, en el que interviene el departamento Contable y Gerencia. Además, se identificaron puntos débiles como: selección de facturas con saldos antiguos.

Ilustración 24. *Flujograma de cuentas por cobrar*



Elaborado por: Sánchez (2023)

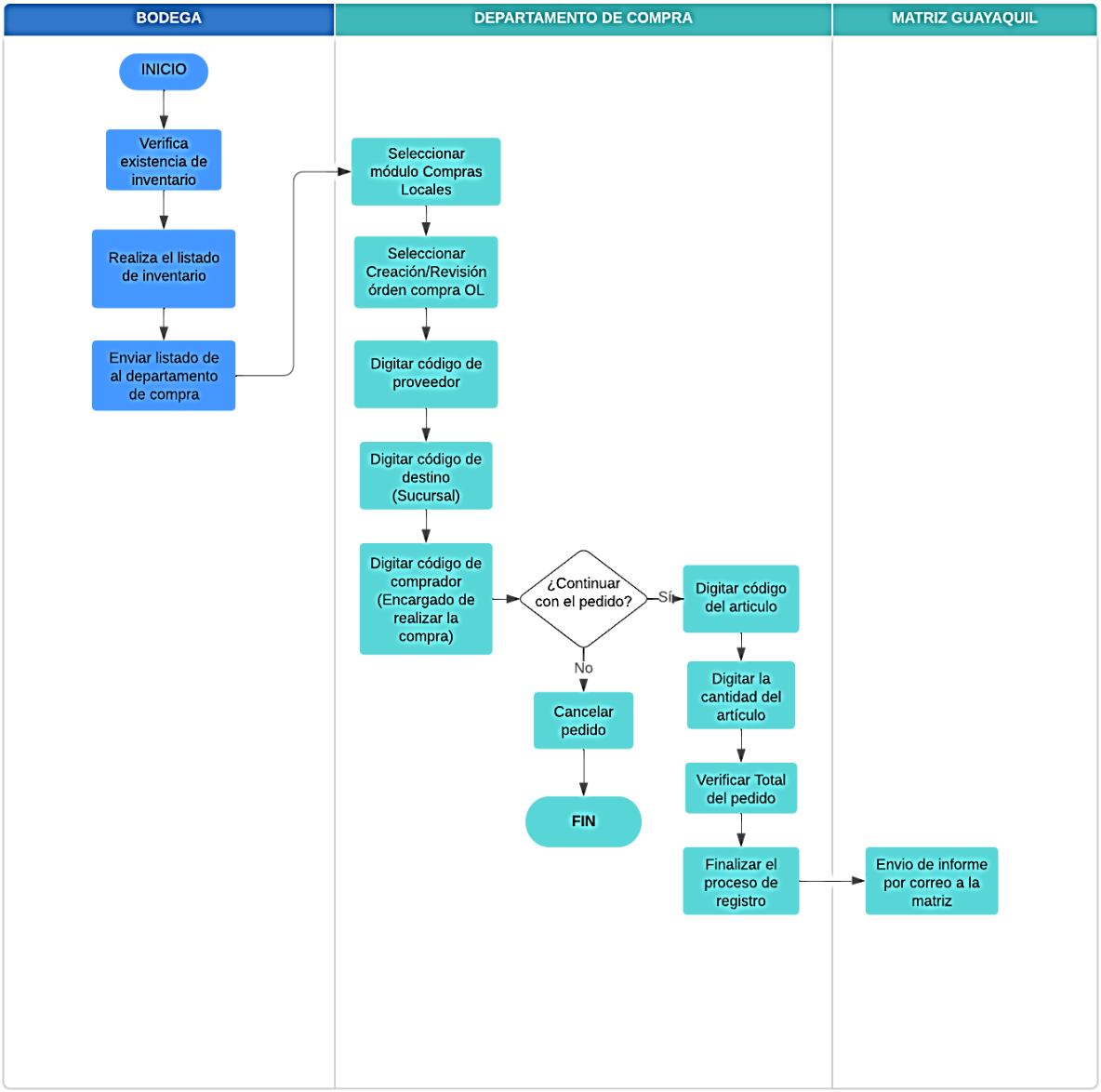
Ilustración 25. *Flujograma propuesto de Cuentas por cobrar*



Elaborado por: Sánchez (2023)

El siguiente flujograma muestra el proceso que se lleva a cabo para realizar pedidos, en el que intervienen departamentos de bodega, compra y la casa matriz de Guayaquil. Además, se identificaron puntos débiles como: No envían reporte de pedido a la sucursal, pero es un error del personal.

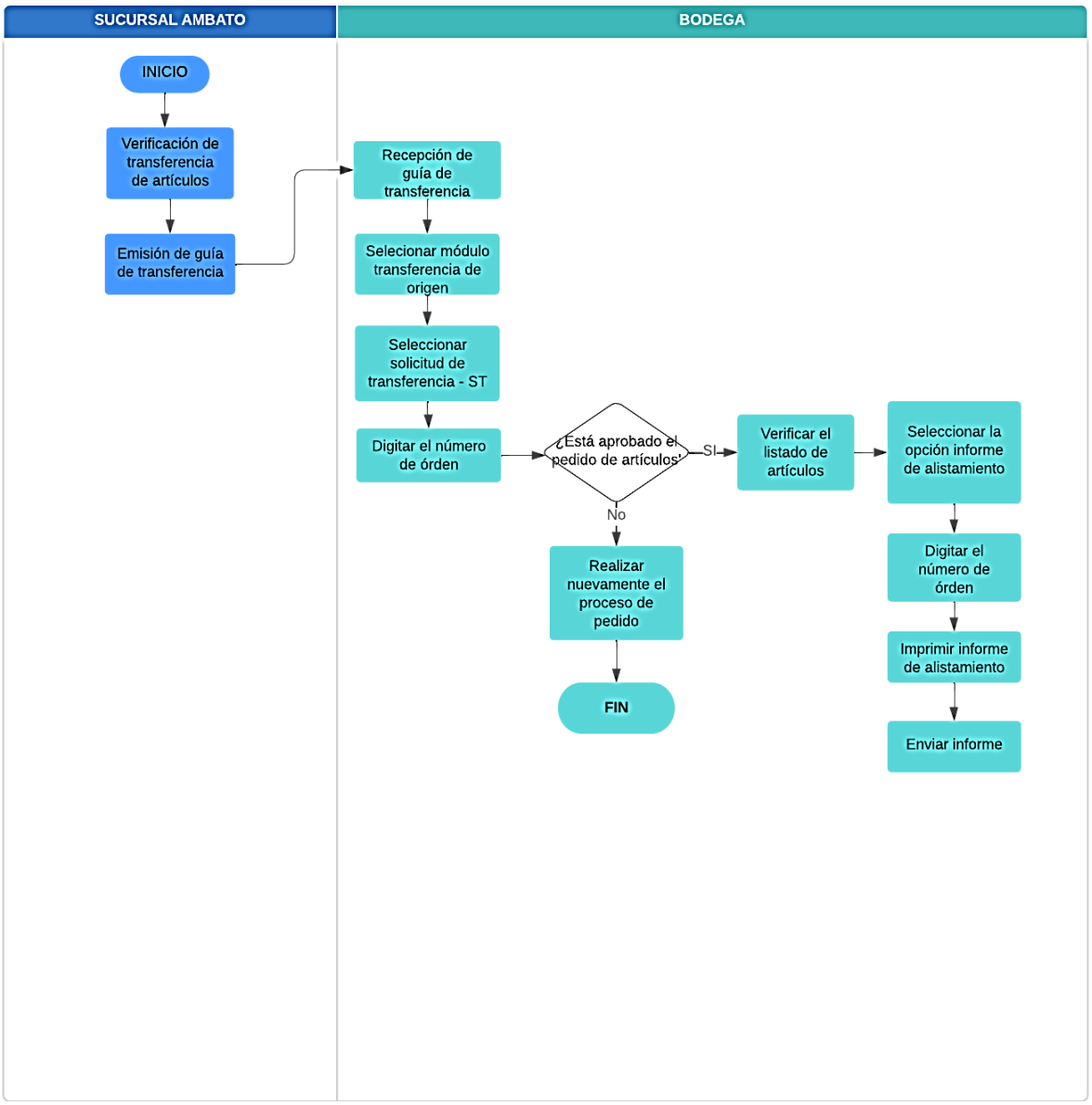
Ilustración 26. *Flujograma de pedidos para adquisiciones*



Elaborado por: Sánchez (2023)

El siguiente flujograma muestra el proceso que se lleva para inventarios, en el que intervienen Sucursal de Ambato y bodega.

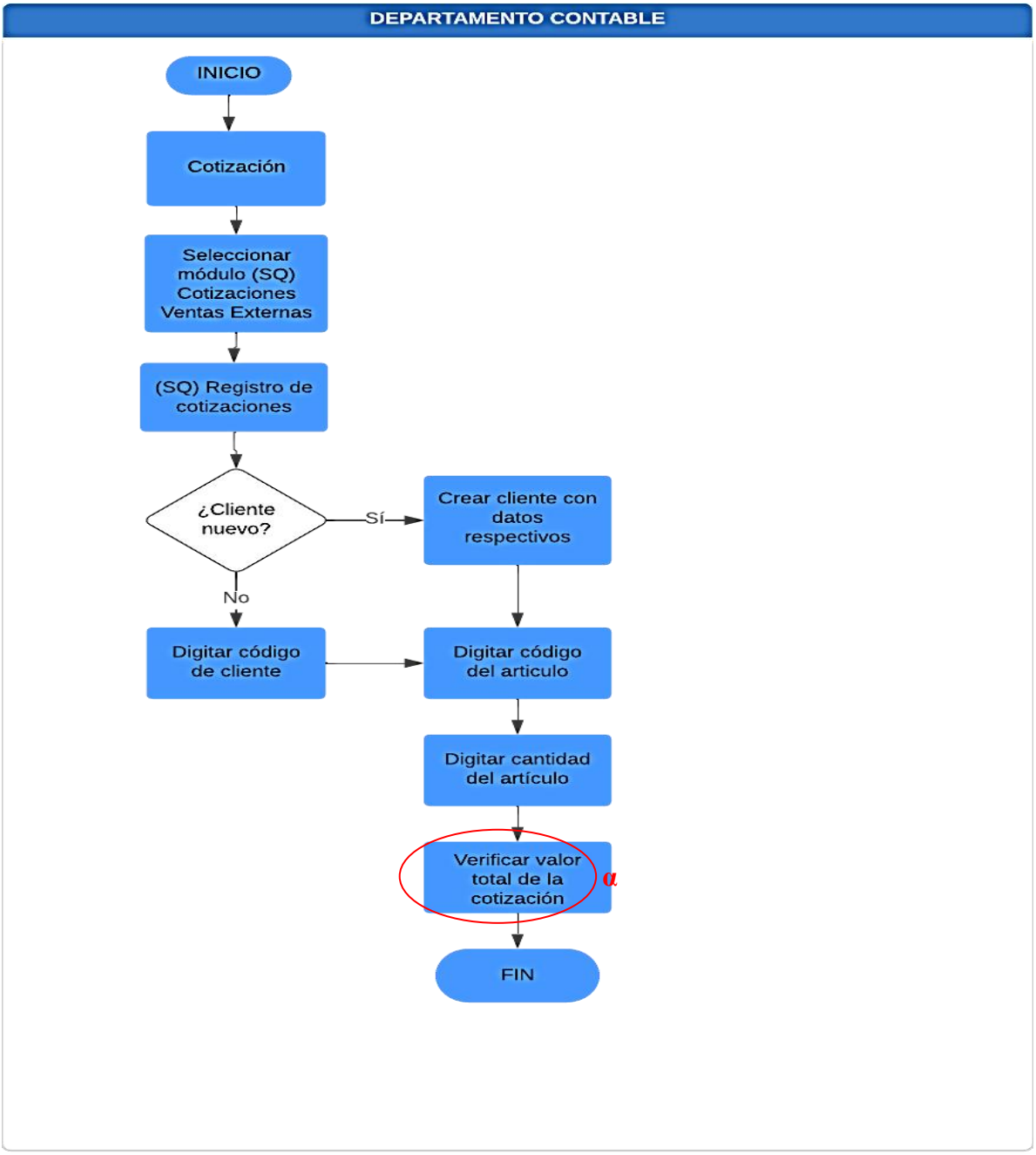
Ilustración 27. *Flujograma de Inventarios*



Elaborado por: Sánchez (2023)

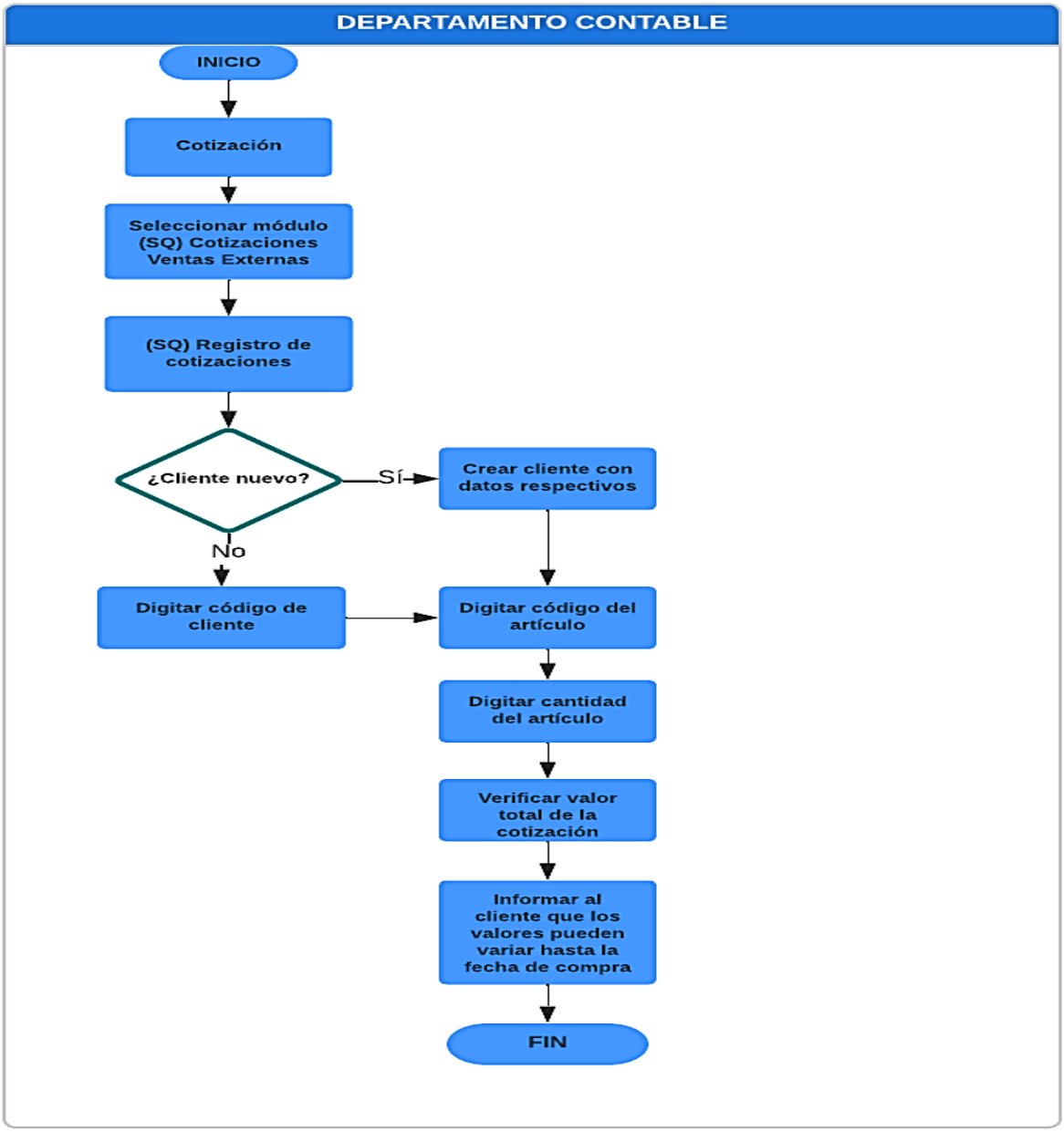
El siguiente flujograma muestra el proceso que se lleva a cabo para cotización, en el que interviene el departamento de comercialización. Además, se identificaron puntos débiles como: No verifican el listado de precios, esto sucede por la fluctuación de precios desde la fecha de cotización a la fecha de la compra.

Ilustración 28. *Flujograma de Cotización*



Elaborado por: Sánchez (2023)

Ilustración 29. *Flujograma propuesto de Cotización*



Elaborado por: Sánchez (2023)

3.1.2.3 Evaluación e identificación de controles de riesgos

Ilustración 30. *Evaluación de controles de riesgos de los Activos*

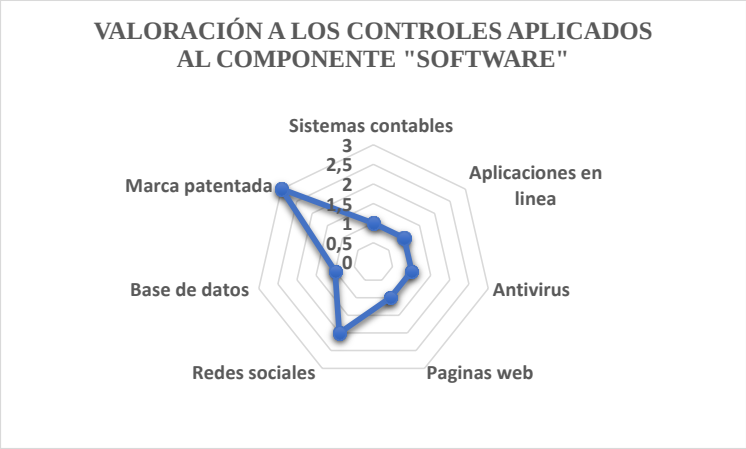
DEMACO										
EVALUACIÓN DE CONTROLES DE RIESGOS DE LOS ACTIVOS DE INFORMACIÓN										
Grupo Activos de Información	**Descripción Activos de Información**	**Vulnerabilidades**	**Amenazas**	**Riesgos**	**Controles actuales al Activo**	**Calificación Total del Control Actual**	**Preventivos**	**Detectivos**	**Correctivos**	**Controles sugeridos**
SOFTWARE	**Sistemas contables**	Modo en espera de forma ocasional, Interfaz de usuario, Contraseñas débiles o predeterminadas	Hackeo a la seguridad informatica del software.	No guarda la información registrada, se pierde información, Ralentización de registro de datos	Reinicio del sistema.	1			X	Solicitar al encargado del software verificar la situación, con soporte del proveedor matriz del programa para una solución pronta.
	Aplicaciones en linea (Tributario y empresarial)	Mantenimiento en paginas de internet utilizadas.	La aplicación no responde en ciertas ocaciones.	Incumplimiento de envio de reportes a entes de control, por lo tanto provocaría sanciones.	Esperar y ejecutar de nuevo.	1	X			Mantener la información requeridas por los entes de control con anticipación a la fecha de envio para evitar retraso y sanciones.
	Antivirus	Caducidad de la licencia, no cuenta con antivirus.	Infiltración de códigos dañinos y maliciosos en los equipos a traves de la red interna.	Pérdida de información en la base de datos, archivos infectados, daños del sistema operativo.	No existe ningún control	1		X		Comprar e instalar antivirus adecuados para la entidad y mantener una constante revisión de la caducidad de la licencia.
	Paginas web	Configuración de la página..	En ocaciones no funciona la pagian web.	Hackeo de información, bajo nivel en ventas en linea.	Revisión y mantenimiento de la página web periódico.	1	X			Realizar revisiones diarias de la pagina web y su funcionamiento.
	Redes sociales	Configuración de seguridad en redes sociales.	Suplantación de identidad	Pérdida de imagen y reputación empresarial.	Bloquear o reportar otras paginas que se hagan pasar por la entidad.	2	X			Revisón constante de las redes sociales para evitar robos de identidad, contraseñas, malware.
	Base de datos	Configuración del motor de base de datos.	Limitado almacenamiento de información.	Pérdida de información en el sistema.	Volver a llenar o pedir la información al encargado de la nube.	1			X	Otorgar acceso limitado al personal para la recuperación de la información, sacar backups semanales de la base de datos en la nube y discos externos.
	Marca patentada	Pago de un costo adicional al IEPI para realizar rasteros de marcas similares.	Creación de marcas similares.	Confunsión en escritura y pronunciacion de nuevas marcas.	La marca es propia de la entidad y se encuntra registrada en el IEPI, todo esta regulado.	3	X			Realizar un rastreo una vez al año sobre la aparición de marcas similares.
HARDWARE	**Equipos**	Configuración de los equipos Contraseñas predeterminadas en apertura de inicio en computadores	Los equipos tengan fallas de funcionamiento, Acceso a personal no autorizado al encendido y trabajo del equipo	Pérdida de información, Reemplazo del equipo.	Mantenimiento y cuidado de los equipos parcialmente.	2	X			Capacitar al personal para el correcto cuidado y capacidad de respuesta ante posibles fallas para no retrasar las actividades, los cuales deben ser informadas de forma inmediata al evento.
	Impresoras	Configuración de la impresora.	La impresora tenga fallas de funcionamiento.	No contar con el respaldo impreso como evidencia de la transacción.	Esperar a que funcionen nuevamente o dar aviso inmediato para revisión y mantenimiento.	1			X	Dar aviso inmediato para revisión y mantenimiento al encargado del área informática.
	Scaners	Configuración del equipo.	No responde en ciertas ocaciones.	No contar con el respaldo digital como evidencia de la transacción.	Esperar y ejecutar de nuevo.	2	X			Dar aviso inmediato para revisión y mantenimiento al encargado del área informática.
	Discos duros	Espacio de almacenamiento limitado en gigas.	Saturación de almacenamiento de información.	No poder recuperar la información guardada en e disco duro.	No existe control.	1	X			Revisar la capacidad de almacenamiento de los discos duros y adquirir nuevos de ser necesarios.
	Pendrives	Espacio de almacenamiento limitado en gigas.	Memorias con virus.	No poder recuperar la información guardada en el pendrive.	Formatear memorias.	1		X		Pedir al encargado formatear o adquirir nuevas memorias.

REDES DE COMUNICACIÓN	**Cableado**	Inestabilidad de conexión por puertos IP, o hosts Red wifi abierta	Fallas en conexión de equipos a la red e internet	Cortos circuitos por mal ubicación de los cables.	No existe ningún control	1		X		Verificar la correcta adecuación de los cables en la infraestructura.
	Red			Pérdida de información de archivos compartidos, Pérdida de tiempo en apertura del software, Tiempo de espera elevados	Llamar al distribuidor de internet	3	X			Realizar conexión con VPN o accesos remotos que permitan utilizar el software y abrir y grabar archivos compartidos
	Capacidad del servidor	Cierre de sesión inesperado, No se documenta las fallas	Interrupción en grabación de archivos, Cierre del sistema contable	Error en copias de seguridad, Daño de disco duro de almacenamiento, Saturación de capacidad de almacenamiento	No existe ningun control.	1	X			Ampliar las gigas o cambiar a un servidor Dedicado, o de alto rendimiento, que tengan velocidad y procesamiento para el almacenamiento de datos, fiable y seguro que permita obtener copias de seguridad permanentes
PERSONAL	**Gerente**	Sobrecarga de actividades, Falencias en registro y archivo de documentación de transacciones	Incumplimiento de actividades laborales en los puestos de trabajo y funciones,	Toma de decisiones inadecuadas	No existe ningun control,todo esta regulado.	3		X		Incluir en el plan operativo actividades que busquen asegurar las operaciones de seguridad de la información, que se ejecuten según lo planificado
	Contabilidad			Pérdida de productividad en el área debido a que las fallas en el sistema contable no permiten acceso al sistema instalado en el servidor.	Reiniciar el sistema y pedir sustento del ingeniero responsable	1			X	Solicitar al encargado de sistemas la revisión y mantenimiento de hardware y software o a su vez requerir ayuda de la matriz del programa para una solución pronta para evitar la ralentización de actividades y obtención de información contable.
	Comercialización			Pérdida de clientes, Aectación a nivel de ventas esperadas	No existe ningun control,todo esta regulado.	3	X			Crear un plan de fidelización de clientes. Planificar capacitaciones periódicas para el área
	Inventarios			Inconsistencia en toma física de inventarios, Descuadre de datos físicos con los reportados por el sistema contable, Gestión inadecuada de los inventarios	Se revisan las peticiones de nuevo y se corrigen las fallas.	1			X	Acceso limitado o no permitir modificaciones al sistema para evitar incovenientes.
	Recursos humanos			Contratación de personal no competente	Todo esta regulado.	3	X			Perfeccionar el proceso de selección de personal idóneo para los cargos laborales requeridos.
	Área de informática			Infraestructura tecnológica inestable, Inventario de activos desactualizada, Gestión y gobierno de TI dealineados a los objetivos corporativos	No existen acciones preventivas ante situcaciones que se presenten.	1			X	Elaborar planes adecuados para la prevención de amenzas y mitigación de riesgos Evaluar periódicamente la seguridad de la información tanto de hardware como de software y procesos informáticos con alineación a las actividades de la organización.

Elaborado por: Sánchez (2023)

A continuación, se presenta gráficamente la valoración de los controles aplicados por la empresa ante riesgos que se presentes en los activos:

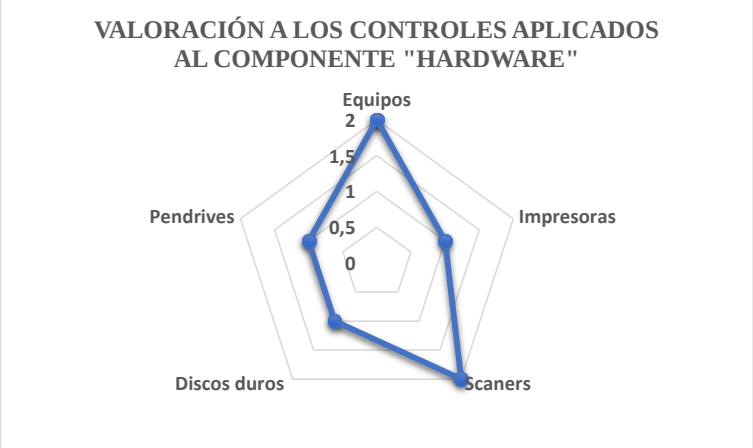
Ilustración 31. *Valoración de los controles del Activo Software*



Elaborado por: Sánchez (2023)

En la ilustración 31 se puede observar que la mayoría de los componentes tienen un nivel bajo en controles utilizados actualmente, es decir, son aplicados por la entidad, pero no garantizan la prevención o eliminación de riesgos, por lo tanto, los activos podrían sufrir daños o pérdidas.

Ilustración 32. *Valoración de los controles del Activo Hardware*

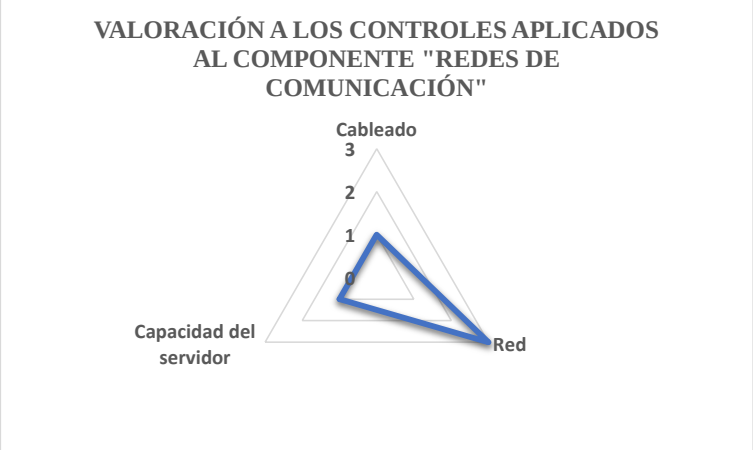


Elaborado por: Sánchez (2023)

Se puede evidenciar en la ilustración 32, que dos de los componentes tiene un nivel de control medio, es decir, los activos se encuentran controlados, pero no de forma muy

adecuada y posiblemente esto cause a corto o mediano tiempo algún daño o retraso en el desarrollo normal de sus actividades. Por otro lado, el resto de los componentes tienen un nivel de control bajo, lo que da a entender que existe un control mínimo y el riesgo podría materializarse afectando considerablemente a la información histórica de la entidad.

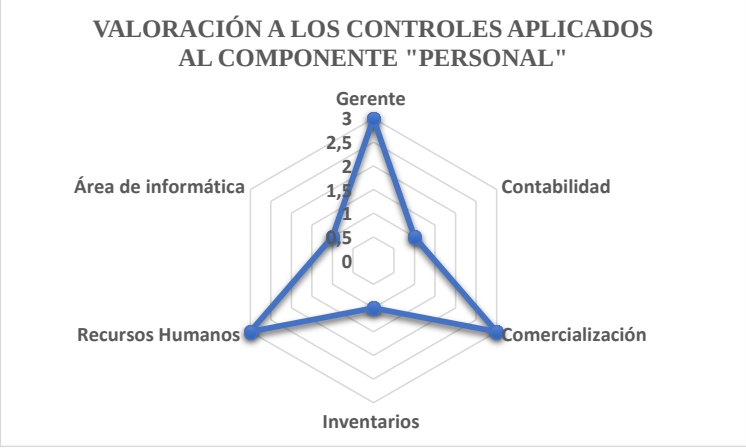
Ilustración 33. *Valoración de los controles del Activo Redes de Comunicación*



Elaborado por: Sánchez (2023)

Como se observa en la ilustración 33, el Activo Redes de comunicación no cuenta con ningún control para los componentes cableado y capacidad del servidor, es decir, no existe ningún plan o estrategia que ayude a mitigar riesgos y salvaguardar los activos.

Ilustración 34. *Valoración de los controles del Activo Personas (Trabajadores)*



Elaborado por: Sánchez (2023)

En la ilustración 34, se puede interpretar que, los componentes: área de informática, contabilidad e inventarios son valorados con un nivel bajo, es decir, no cuentan con controles efectivos y en otros casos no aplican los adecuados para evitar que los riesgos se materialicen. Por otro lado, hay componentes valorados con nivel alto, es decir, los activos se encuentran controlados y regulados.

3.1.2.4 Evaluación e identificación de riesgos

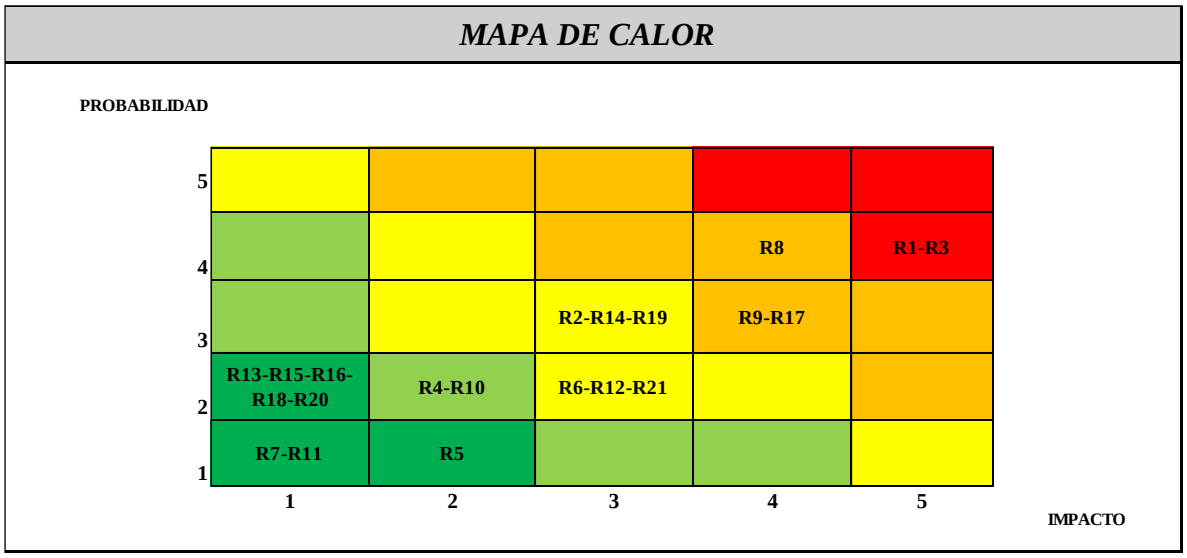
Ilustración 35. *Evaluación de riesgos de los Activos*

DEMACO							
EVALUACIÓN DE RIESGOS DE LOS ACTIVOS DE INFORMACIÓN							
Activos de información	**Nª**	**Descripción**	**Riesgos**	**Probabilidad**	**Impacto**	**Ocurrencia del Riesgo**	**RIESGO TOTAL**
SOFTWARE	R1	**Sistemas contables**	No guarda la información registrada, se pierde información, ralentización de registro de datos.	*4*	*5*	**Muy Alto**	**20**
	R2	**Aplicaciones en linea (Tributario y empresarial)**	Incumplimiento de envio de reportes a entes de control, por lo tanto provocaría sanciones.	*3*	*3*	**Medio**	**9**
	R3	**Antivirus**	Pérdida de información en la base de datos, archivos infectados, daños del sistema operativo.	*4*	*5*	**Muy Alto**	**20**
	R4	**Paginas web**	Hackeo de información, bajo nivel en ventas en linea.	*2*	*2*	**Moderado**	**4**
	R5	**Redes sociales**	Pérdida de imagen y reputación empresarial.	*1*	*2*	**Bajo**	**2**
	R6	**Base de datos**	Pérdida de información en el sistema.	*2*	*3*	**Moderado**	**6**
	R7	**Marca patentada**	Confunsión en escritura y pronunciacion de nuevas marcas.	*1*	*1*	**Bajo**	**1**
HARDWARE	R8	**Equipos**	Pérdida de información, Reemplazo del equipo.	*4*	*4*	**Alto**	**16**
	R9	**Impresoras**	No contar con el respaldo impreso como evidencia de la transacción.	*3*	*4*	**Medio**	**12**
	R10	**Scaners**	No contar con el respaldo digital como evidencia de la transacción.	*2*	*2*	**Moderado**	**4**
	R11	**Discos duros**	No poder recuperar la información guardada en el disco duro.	*1*	*1*	**Bajo**	**1**
	R12	**Pendrives**	No poder recuperar la información guardada en el pendrive.	*2*	*3*	**Moderado**	**6**

REDES DE COMUNICACIÓN	R13	**Cableado**	Cortos circuitos por mal ubicación de los cables.	***2***	***1***	**Bajo**	**2**
	R14	**Red**	Pérdida de información de archivos compartidos. Pérdida de tiempo en apertura del software. Tiempo de espera elevados.	***3***	***3***	**Medio**	**9**
	R15	**Capacidad del servidor**	Error en copias de seguridad, Daño de disco duro de almacenamiento, Saturación de capacidad de almacenamiento.	***2***	***1***	**Bajo**	**2**
PERSONAL	R16	**Gerente**	Toma de decisiones inadecuadas	***2***	***1***	**Bajo**	**2**
	R17	**Contabilidad**	Pérdida de productividad en el área debido a que las fallas en el sistema contable no permiten acceso al sistema instalado en el servidor.	***3***	***4***	**Medio**	**12**
	R18	**Comercialización**	Pérdida de clientes, Afectación a nivel de ventas esperadas.	***2***	***1***	**Bajo**	**2**
	R19	**Inventarios**	Inconsistencia en toma física de inventarios, Descuadre de datos físicos con los reportados por el sistema contable, Gestión inadecuada de los inventarios.	***3***	***3***	**Medio**	**9**
	R20	**Recursos Humanos**	Contratación de personal no competente.	***2***	***1***	**Bajo**	**2**
	R21	**Área de informática**	Infraestructura tecnológica inestable, Inventario de activos desactualizada, Gestión y gobierno de TI dealineados a los objetivos corporativos.	***2***	***3***	**Moderado**	**6**

Elaborado por: Sánchez (2023)

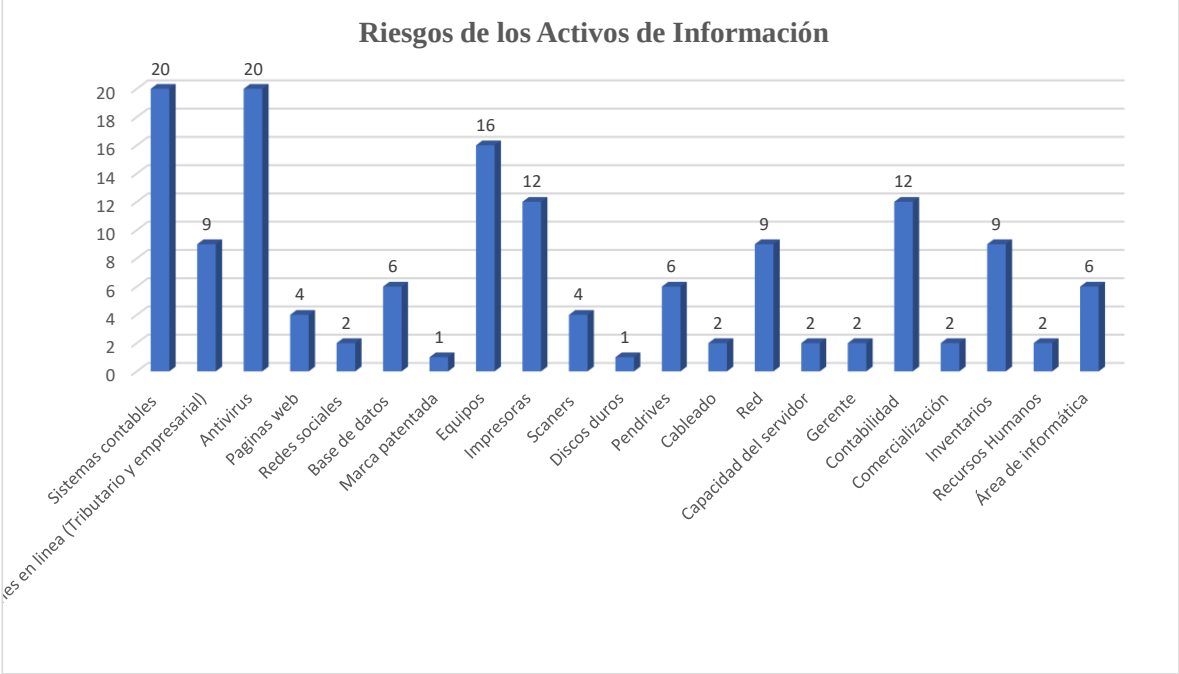
Ilustración 36. *Mapa de calor de los riesgos*



Elaborado por: Sánchez (2023)

A continuación, se presenta gráficamente la ocurrencia de los riesgos de los activos, valorados mediante criterios establecidos por niveles y valores:

Ilustración 37. *Valoración de los riesgos de los Activos*



Elaborado por: Sánchez (2023)

Mediante la ilustración 37, se puede observar que los controles aplicados por la entidad a los activos de información en su mayoría no son viables, los riesgos tienen valoraciones altas con un 20% y medio con un 15% valorados en una escala del 25% , lo que quiere decir, que sus activos frecuentemente tienen falencias y aún no se han podido controlar o eliminar los riesgos presentes, lo que conllevaría a que los activos de información sufran pérdida de datos, fraudes, robos de identidad a consecuencia del antivirus y sistemas contables. Por otro lado, se identificaron riesgos con niveles moderado y bajo, es decir, ocurren una vez al año o incluso raras veces, pero también es necesario tener en cuenta que si no se controla la amenaza esta podría materializarse y percudir el sistema de información de la empresa.

3.1.3 Informe general

A continuación, se presenta los resultados y hallazgos obtenidos durante las evaluaciones aplicadas:

Ilustración 38. *Informe general*

"CONSULTORA SÁNCHEZ & ASOCIADOS" *AUDITORES - CONSULTORES*
DEMACO CIA. LTDA. Sur Ambato ***INFORME GENERAL*** Auditoría al Sistema de Información de la empresa DEMACO CIA. LTDA. Sur Ambato. Abril - Julio 2023

SIGLAS/ABREVIATURAS	SIGNIFICADO
COSO	Committe of Sponsoring Organizations of the Tradeway Commission
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
SGSI	Sistema de gestión de seguridad de la información
TI	Tecnologías de la información

Elaborado por: Sánchez (2023)

Ambato, Julio de 2023

Ing. Tannia Ochoa
Gerente DEMACO CIA. LTDA. Sur Ambato

De mi consideración:
Se ha realizado la evaluación al sistema de información en el área de informática a la empresa DEMACO CIA. LTDA. Sur Ambato en el período comprendido del año 2023.

El examen se realizó de manera satisfactoria con la utilización del marco de referencia COSO ERM 2017 y aplicación de las normas ISO/IEC 27000 y 31000. Se ha identificado y considerado diversos factores informáticos que podrían estar interviniendo o afectando a la correcta ejecución de actividades empresariales. Por lo que, se brindará como apoyo recomendaciones y posibles soluciones que garanticen un óptimo resultado en cuanto al control interno, así como la prevención y el control de los riesgos en los activos de información.

La finalidad de la Auditoría al sistema de información es el correcto funcionamiento del área de informática, considerando como alcance el nivel de confianza en cuanto al control interno, evaluación de los activos de información, identificación de los controles aplicados a los activos, respuesta inmediata y adecuada a riesgos que podrían poner en peligro a la entidad.

Los resultados se encuentran manifestados en la condición, criterio, conclusión y recomendaciones que constan en el presente informe.

Atentamente,

Melanie Salomé Sánchez Ibarra

3.1.3.1. Resultado del examen

Resultado de la aplicación del Marco de referencia COSO ERM 2017

HALLAZGO 1 §

Comentario

En el área informática las políticas que cubren los controles de TI no son formales

NORMAS ISO/IEC

NORMA ISO/IEC 27001 Seguridad de la información: Proporciona a las organizaciones un modelo consistente que ayuda a establecer, implementar, monitorear, revisar y mantener un sistema de gestión de seguridad de la información.

NORMA ISO/IEC 27002 Buenas prácticas para los controles de seguridad de la información: Proporciona recomendaciones de las mejores prácticas para la gestión de seguridad de la información.

NORMA: ISO/IEC 27005 Gestión de riesgos de seguridad de la información: Proporciona directrices para establecer un enfoque sistemático de gestión de riesgos de seguridad de la información.

NORMA ISO/IEC 31000 Sistemas de gestión de riesgos: Proporciona directrices y principios para gestionar el riesgo de las organizaciones.

Incumplimiento de principio del COSO ERM 2017 - Gobierno y Cultura:

El gobierno establece el tono de la organización, reforzando la importancia y estableciendo responsabilidades de supervisión. La cultura se refiere a valores éticos, comportamientos deseados y comprensión del riesgo.

Conclusión

No hay políticas definidas ya que existen controles espontáneos ante riesgos detectados. Por lo que, no se podrá controlar de una manera adecuada lo que conllevará a a sufrir grandes perjuicios ante situaciones incontrolables.

Recomendaciones

Dirigido al área de Informática:

- Desarrollar planes de apoyo ante posibles sucesos.

- Examinar y evaluar posibles y presentes riesgos con las adecuadas herramientas y procedimientos para abordar soluciones viables.

HALLAZGO 2§

Comentario

En el área informática no existe conocimiento y aplicación acerca del marco de referencia COSO ERM 2017.

NORMAS ISO/IEC

NORMA: ISO/IEC 27005 Gestión de riesgos de seguridad de la información: Proporciona directrices para establecer un enfoque sistemático de gestión de riesgos de seguridad de la información.

NORMA ISO/IEC 31000 Sistemas de gestión de riesgos: Proporciona directrices y principios para gestionar el riesgo de las organizaciones.

Incumplimiento de principio del COSO ERM 2017 - Estrategia y Objetivos:

El riesgo es definido alineado con la estrategia, los objetivos de negocio ponen la estrategia en práctica mientras sirve para identificar, evaluar y responder a los riesgos.

Conclusión

El área informática desconoce acerca de la aplicación y estructura del marco de referencia COSO ERM 2017. Por lo que, no se puede verificar la efectividad de los sistemas de control y como mejorarlos, y tampoco prevenir la vulneración del sistema.

Recomendaciones

Dirigido al área de Informática:

- Emplear el marco de referencia COSO ERM para analizar meticulosamente su estructura y aplicarlo para un correcto apoyo en el área de informática y una correcta gestión de los riesgos.

HALLAZGO 3 §

Comentario

El área de informática no tiene estrategias adecuadas para prevenir posibles riesgos.

NORMAS ISO/IEC

NORMA ISO/IEC 27001 Seguridad de la información: Proporciona a las organizaciones un modelo consistente que ayuda a establecer, implementar, monitorear, revisar y mantener un sistema de gestión de seguridad de la información.

NORMA ISO/IEC 27002 Buenas prácticas para los controles de seguridad de la información: Proporciona recomendaciones de las mejores prácticas para la gestión de seguridad de la información.

NORMA: ISO/IEC 27005 Gestión de riesgos de seguridad de la información: Proporciona directrices para establecer un enfoque sistemático de gestión de riesgos de seguridad de la información.

NORMA ISO/IEC 31000 Sistemas de gestión de riesgos: Proporciona directrices y principios para gestionar el riesgo de las organizaciones.

Incumplimiento de principio del COSO ERM 2017 - Estrategia y Objetivos:

El riesgo es definido alineado con la estrategia, los objetivos de negocio ponen la estrategia en práctica mientras sirve para identificar, evaluar y responder a los riesgos.

Conclusión

Existen estrategias, pero no las adecuadas que ayuden a detectar y prevenir posibles riesgos. Por lo que, podría materializarse una amenaza y causar serios daños en la empresa

Recomendaciones

Dirigido al área de Informática:

- Identificar todas las actividades que se realizan en el área de informática con la finalidad de aplicar los marcos de referencia que ayuden a encontrar y prevenir riesgos.

- Emplear marcos reguladores de riesgo y cumplimientos de control interno como el COSO ERM, NORMAS ISO entre otros que puedan brindar apoyo para evitar posibles agravios en el área informática.

HALLAZGO 4 §

Comentario

No existen criterios claros para determinar los riesgos y probabilidad de que estos ocurran.

NORMAS ISO/IEC

NORMA ISO/IEC 27001 Seguridad de la información: Proporciona a las organizaciones un modelo consistente que ayuda a establecer, implementar, monitorear, revisar y mantener un sistema de gestión de seguridad de la información.

NORMA ISO/IEC 27002 Buenas prácticas para los controles de seguridad de la información: Proporciona recomendaciones de las mejores prácticas para la gestión de seguridad de la información.

NORMA: ISO/IEC 27005 Gestión de riesgos de seguridad de la información: Proporciona directrices para establecer un enfoque sistemático de gestión de riesgos de seguridad de la información.

NORMA ISO/IEC 31000 Sistemas de gestión de riesgos: Proporciona directrices y principios para gestionar el riesgo de las organizaciones.

Incumplimiento de principio del COSO ERM 2017 - Desempeño:

Riesgos que pueden afectar el logro de la estrategia y los objetivos de negocio pueden ser identificados y evaluados.

Conclusión

Se manejan procedimientos poco formales por lo que no se puede determinar con exactitud la probabilidad que ocurran. Por lo que, podría materializarse una amenaza y causar serios daños en la empresa.

Recomendaciones

Dirigido al área de Informática:

- Elaborar un manual de políticas que comprenda procesos de gestión de riesgos en el área de informática.
- Dar seguimiento al control interno y a la gestión de riesgos para prevenirlos, detectarlos y corregirlos.

HALLAZGO 5 §

Comentario

El área de informática no lleva a cabo medidas de mitigación ante riesgos observado.

NORMAS ISO/IEC

NORMA ISO/IEC 27001 Seguridad de la información: Proporciona a las organizaciones un modelo consistente que ayuda a establecer, implementar, monitorear, revisar y mantener un sistema de gestión de seguridad de la información.

NORMA ISO/IEC 27002 Buenas prácticas para los controles de seguridad de la información: Proporciona recomendaciones de las mejores prácticas para la gestión de seguridad de la información.

NORMA: ISO/IEC 27005 Gestión de riesgos de seguridad de la información: Proporciona directrices para establecer un enfoque sistemático de gestión de riesgos de seguridad de la información.

NORMA ISO/IEC 31000 Sistemas de gestión de riesgos: Proporciona directrices y principios para gestionar el riesgo de las organizaciones.

Incumplimiento de principio del COSO ERM 2017 - Desempeño:

Riesgos que pueden afectar el logro de la estrategia y los objetivos de negocio pueden ser identificados y evaluados.

Conclusión

En la empresa si existen medidas para mitigar riesgos, pero no las adecuadas y las suficientes. Por lo que, al no controlar estos riesgos es posible que la entidad corra peligro

Recomendaciones

Dirigido al área de Informática:

- Elaborar matrices que ayuden a identificar y controlar riesgos que puedan presentarse en los activos de información, software, hardware, redes de comunicación, personal a cargo dentro del área informática.

HALLAZGO 6

Comentario

El área informática no clasifica los riegos como aceptables o que requieren de acciones.

NORMAS ISO/IEC

NORMA ISO/IEC 27001 Seguridad de la información: Proporciona a las organizaciones un modelo consistente que ayuda a establecer, implementar, monitorear, revisar y mantener un sistema de gestión de seguridad de la información.

NORMA ISO/IEC 27002 Buenas prácticas para los controles de seguridad de la información: Proporciona recomendaciones de las mejores prácticas para la gestión de seguridad de la información.

NORMA: ISO/IEC 27005 Gestión de riesgos de seguridad de la información: Proporciona directrices para establecer un enfoque sistemático de gestión de riesgos de seguridad de la información.

NORMA ISO/IEC 31000 Sistemas de gestión de riesgos: Proporciona directrices y principios para gestionar el riesgo de las organizaciones.

Incumplimiento de principio del COSO ERM 2017 - Desempeño:

Riesgos que pueden afectar el logro de la estrategia y los objetivos de negocio pueden ser identificados y evaluados.

Conclusión

Se manejan procedimientos poco formales por lo que no existe una correcta clasificación de riesgos. Por lo que, al no existir una correcta clasificación de riesgos es posible que se materializarse una amenaza y ocurran daños irreversibles.

Recomendaciones

Dirigido al área de Informática:

- Elaborar matrices que ayuden a identificar y controlar riesgos que puedan presentarse en los activos de información, software, hardware, redes de comunicación, personal a cargo dentro del área informática.
- Dar seguimiento al control interno y a la gestión de riesgos para prevenirlos, detectarlos y corregirlos.

HALLAZGO 7 §

Comentario

No se controla con frecuencia el desempeño y el riesgo.

NORMAS ISO/IEC

NORMA ISO/IEC 27001 Seguridad de la información: Proporciona a las organizaciones un modelo consistente que ayuda a establecer, implementar, monitorear, revisar y mantener un sistema de gestión de seguridad de la información.

NORMA ISO/IEC 27002 Buenas prácticas para los controles de seguridad de la información: Proporciona recomendaciones de las mejores prácticas para la gestión de seguridad de la información.

NORMA: ISO/IEC 27005 Gestión de riesgos de seguridad de la información: Proporciona directrices para establecer un enfoque sistemático de gestión de riesgos de seguridad de la información.

NORMA ISO/IEC 31000 Sistemas de gestión de riesgos: Proporciona directrices y principios para gestionar el riesgo de las organizaciones.

Incumplimiento de principio del COSO ERM 2017 - Revisión:

Considerar qué tan bien funcionan los componentes de gestión de riesgos empresariales a lo largo del tiempo a la luz de cambios sustanciales y que revisiones se necesitan.

Conclusión

Poca supervisión y control por parte del encargado del área. Por lo que, Podrían ocasionar perjuicios y pérdidas en la entidad.

Recomendaciones

Dirigido al encargado del área de Informática:

- Supervisar de manera constante el desempeño y los riesgos detectados.
- Monitorear la evaluación del desempeño de las personas del área informática en cuanto al control interno y administración de riesgos.

HALLAZGO 8 §

Comentario

En el área informática no se toma en cuenta el dinamismo profesional.

NORMAS ISO/IEC

NORMA ISO/IEC 27001 Seguridad de la información: Proporciona a las organizaciones un modelo consistente que ayuda a establecer, implementar, monitorear, revisar y mantener un sistema de gestión de seguridad de la información.

NORMA ISO/IEC 27002 Buenas prácticas para los controles de seguridad de la información: Proporciona recomendaciones de las mejores prácticas para la gestión de seguridad de la información.

NORMA: ISO/IEC 27005 Gestión de riesgos de seguridad de la información: Proporciona directrices para establecer un enfoque sistemático de gestión de riesgos de seguridad de la información.

NORMA ISO/IEC 31000 Sistemas de gestión de riesgos: Proporciona directrices y principios para gestionar el riesgo de las organizaciones.

Incumplimiento de principio del COSO ERM 2017 - Revisión:

Considerar qué tan bien funcionan los componentes de gestión de riesgos empresariales a lo largo del tiempo a la luz de cambios sustanciales y que revisiones se necesitan.

Conclusión

No se valora el esfuerzo y dedicación de los empleados. Por lo que, hay poco rendimiento y compromiso en su desarrollo laboral.

Recomendaciones

Dirigido al encargado del área de Informática:

- Motivar al personal del área de informática que actúe con profesionalidad y dinamismo para un adecuado desarrollo de las actividades empresariales.
- Monitorear la evaluación del desempeño de las personas del área informática en cuanto al control interno y administración de riesgos.

HALLAZGO 9 §

Comentario

En el área informática no se implementan consistentemente las actividades de gestión de riesgos.

NORMAS ISO/IEC

NORMA ISO/IEC 27001 Seguridad de la información: Proporciona a las organizaciones un modelo consistente que ayuda a establecer, implementar, monitorear, revisar y mantener un sistema de gestión de seguridad de la información.

NORMA ISO/IEC 27002 Buenas prácticas para los controles de seguridad de la información: Proporciona recomendaciones de las mejores prácticas para la gestión de seguridad de la información.

NORMA: ISO/IEC 27005 Gestión de riesgos de seguridad de la información: Proporciona directrices para establecer un enfoque sistemático de gestión de riesgos de seguridad de la información.

NORMA ISO/IEC 31000 Sistemas de gestión de riesgos: Proporciona directrices y principios para gestionar el riesgo de las organizaciones.

Incumplimiento de principio del COSO ERM 2017 - Información, comunicación y reporte:

La gestión de riesgos empresariales requiere un proceso continuo para obtener y compartir información necesaria, de fuentes internas y externas.

Conclusión

Poca preocupación y desconocimiento de los procesos o actividades que se desarrollan. Por lo que, podrían ocasionar perjuicios y pérdidas en la entidad.

Recomendaciones

Dirigido al encargado del área de Informática:

- Realizar bitácoras como registros de la información sobre riesgos informáticos a las áreas de la empresa para su debida protección de modo preventivo a los sistemas de información.
- Dar mantenimiento y actualización de modo detectivo y correctivo a las bases de datos, redes, software, hardware que se encuentren expuestos a riesgos informáticos.

Resultado de la aplicación de la Normas ISO/IEC 27000 y 31000

HALLAZGO 10 ×

Comentario

El sistema contable no guarda la información registrada.

NORMAS ISO/IEC

NORMA ISO/IEC 27001 Seguridad de la información: Proporciona a las organizaciones un modelo consistente que ayuda a establecer, implementar, monitorear, revisar y mantener un sistema de gestión de seguridad de la información.

NORMA ISO/IEC 27002 Buenas prácticas para los controles de seguridad de la información: Proporciona recomendaciones de las mejores prácticas para la gestión de seguridad de la información.

NORMA: ISO/IEC 27005 Gestión de riesgos de seguridad de la información: Proporciona directrices para establecer un enfoque sistemático de gestión de riesgos de seguridad de la información.

NORMA ISO/IEC 31000 Sistemas de gestión de riesgos: Proporciona directrices y principios para gestionar el riesgo de las organizaciones.

Conclusión

Modo en espera de forma ocasional, Interfaz de usuario, Contraseñas débiles o predeterminadas. Por lo que, no guarda la información registrada, se pierde información, Ralentización de registro de datos.

Recomendaciones

Dirigido al encargado del área de Informática:

- Solicitar al encargado del software verificar la situación, con soporte del proveedor matriz del programa para una solución pronta.

HALLAZGO 11 ×

Comentario

Aplicaciones en línea en mantenimiento.

NORMAS ISO/IEC

NORMA ISO/IEC 27001 Seguridad de la información: Proporciona a las organizaciones un modelo consistente que ayuda a establecer, implementar, monitorear, revisar y mantener un sistema de gestión de seguridad de la información.

NORMA ISO/IEC 27002 Buenas prácticas para los controles de seguridad de la información: Proporciona recomendaciones de las mejores prácticas para la gestión de seguridad de la información.

NORMA: ISO/IEC 27005 Gestión de riesgos de seguridad de la información: Proporciona directrices para establecer un enfoque sistemático de gestión de riesgos de seguridad de la información.

NORMA ISO/IEC 31000 Sistemas de gestión de riesgos: Proporciona directrices y principios para gestionar el riesgo de las organizaciones.

Conclusión

Mantenimiento en páginas de internet utilizadas. Por lo que, sucede un incumplimiento de envío de reportes a entes de control, por lo tanto, provocaría sanciones.

Recomendaciones

Dirigido al encargado del área de Informática:

- Mantener la información requeridas por los entes de control con anticipación a la fecha de envío para evitar retraso y sanciones.

HALLAZGO 12 ×

Comentario

No cuenta con antivirus los equipos.

NORMAS ISO/IEC

NORMA ISO/IEC 27001 Seguridad de la información: Proporciona a las organizaciones un modelo consistente que ayuda a establecer, implementar, monitorear, revisar y mantener un sistema de gestión de seguridad de la información.

NORMA ISO/IEC 27002 Buenas prácticas para los controles de seguridad de la información: Proporciona recomendaciones de las mejores prácticas para la gestión de seguridad de la información.

NORMA: ISO/IEC 27005 Gestión de riesgos de seguridad de la información: Proporciona directrices para establecer un enfoque sistemático de gestión de riesgos de seguridad de la información.

NORMA ISO/IEC 31000 Sistemas de gestión de riesgos: Proporciona directrices y principios para gestionar el riesgo de las organizaciones.

Conclusión

Caducidad de la licencia de antivirus. Por lo que, ocurrirá una pérdida de información en la base de datos, archivos infectados, daños del sistema operativo.

Recomendaciones

Dirigido al encargado del área de Informática:

- Comprar e instalar antivirus adecuados para la entidad y mantener una constante revisión de la caducidad de la licencia.

HALLAZGO 13 ×

Comentario

La página web de la entidad en ocasiones no funciona.

NORMAS ISO/IEC

NORMA ISO/IEC 27001 Seguridad de la información: Proporciona a las organizaciones un modelo consistente que ayuda a establecer, implementar, monitorear, revisar y mantener un sistema de gestión de seguridad de la información.

NORMA ISO/IEC 27002 Buenas prácticas para los controles de seguridad de la información: Proporciona recomendaciones de las mejores prácticas para la gestión de seguridad de la información.

NORMA: ISO/IEC 27005 Gestión de riesgos de seguridad de la información: Proporciona directrices para establecer un enfoque sistemático de gestión de riesgos de seguridad de la información.

NORMA ISO/IEC 31000 Sistemas de gestión de riesgos: Proporciona directrices y principios para gestionar el riesgo de las organizaciones.

Conclusión

Baja supervisión y mantenimiento de la página web. Por lo que, podría sufrir un hackeo de información, y un bajo nivel en ventas en línea.

Recomendaciones

Dirigido al encargado del área de Informática:

- Realizar revisiones diarias de la página web y su funcionamiento.

HALLAZGO 14 ×

Comentario

Los equipos tienen fallas de funcionamiento.

NORMAS ISO/IEC

NORMA ISO/IEC 27001 Seguridad de la información: Proporciona a las organizaciones un modelo consistente que ayuda a establecer, implementar, monitorear, revisar y mantener un sistema de gestión de seguridad de la información.

NORMA ISO/IEC 27002 Buenas prácticas para los controles de seguridad de la información: Proporciona recomendaciones de las mejores prácticas para la gestión de seguridad de la información.

NORMA: ISO/IEC 27005 Gestión de riesgos de seguridad de la información: Proporciona directrices para establecer un enfoque sistemático de gestión de riesgos de seguridad de la información.

NORMA ISO/IEC 31000 Sistemas de gestión de riesgos: Proporciona directrices y principios para gestionar el riesgo de las organizaciones.

Conclusión

Baja supervisión y mantenimiento de la página web. Por lo que, podría sufrir pérdida de información, Reemplazo del equipo.

Recomendaciones

Dirigido al encargado del área de Informática:

- Capacitar al personal para el correcto cuidado y capacidad de respuesta ante posibles fallas para no retrasar las actividades, los cuales deben ser informadas de forma inmediata al evento.

HALLAZGO 15 ×

Comentario

Las impresoras tienen fallas de funcionamiento.

NORMAS ISO/IEC

NORMA ISO/IEC 27001 Seguridad de la información: Proporciona a las organizaciones un modelo consistente que ayuda a establecer, implementar, monitorear, revisar y mantener un sistema de gestión de seguridad de la información.

NORMA ISO/IEC 27002 Buenas prácticas para los controles de seguridad de la información: Proporciona recomendaciones de las mejores prácticas para la gestión de seguridad de la información.

NORMA: ISO/IEC 27005 Gestión de riesgos de seguridad de la información: Proporciona directrices para establecer un enfoque sistemático de gestión de riesgos de seguridad de la información.

NORMA ISO/IEC 31000 Sistemas de gestión de riesgos: Proporciona directrices y principios para gestionar el riesgo de las organizaciones.

Conclusión

Baja supervisión y mantenimiento de la página web. Por lo que, no contara con el respaldo impreso como evidencia de la transacción.

Recomendaciones

Dirigido al encargado del área de Informática:

- Dar aviso inmediato para revisión y mantenimiento al encargado del área informática.

HALLAZGO 16 ×

Comentario

Los Pendrives tienen virus.

NORMAS ISO/IEC

NORMA ISO/IEC 27001 Seguridad de la información: Proporciona a las organizaciones un modelo consistente que ayuda a establecer, implementar, monitorear, revisar y mantener un sistema de gestión de seguridad de la información.

NORMA ISO/IEC 27002 Buenas prácticas para los controles de seguridad de la información: Proporciona recomendaciones de las mejores prácticas para la gestión de seguridad de la información.

NORMA: ISO/IEC 27005 Gestión de riesgos de seguridad de la información: Proporciona directrices para establecer un enfoque sistemático de gestión de riesgos de seguridad de la información.

NORMA ISO/IEC 31000 Sistemas de gestión de riesgos: Proporciona directrices y principios para gestionar el riesgo de las organizaciones.

Conclusión

No hay una adecuada utilización de los pendrives. Por lo que, no se podrá recuperar la información guardada en el pendrive.

Recomendaciones

Dirigido al encargado del área de Informática:

- Pedir al encargado formatear o adquirir nuevas memorias.

HALLAZGO 17 ×

Comentario

Existen fallas en la red.

NORMAS ISO/IEC

NORMA ISO/IEC 27001 Seguridad de la información: Proporciona a las organizaciones un modelo consistente que ayuda a establecer, implementar, monitorear, revisar y mantener un sistema de gestión de seguridad de la información.

NORMA ISO/IEC 27002 Buenas prácticas para los controles de seguridad de la información: Proporciona recomendaciones de las mejores prácticas para la gestión de seguridad de la información.

NORMA: ISO/IEC 27005 Gestión de riesgos de seguridad de la información: Proporciona directrices para establecer un enfoque sistemático de gestión de riesgos de seguridad de la información.

NORMA ISO/IEC 31000 Sistemas de gestión de riesgos: Proporciona directrices y principios para gestionar el riesgo de las organizaciones.

Conclusión

Las fallas en conexión de equipos a la red e internet. Por lo que, ocurrirá una pérdida de información de archivos compartidos, Pérdida de tiempo en apertura del software, Tiempo de espera elevados.

Recomendaciones

Dirigido al encargado del área de Informática:

- Realizar conexión con VPN o accesos remotos que permitan utilizar el software y abrir y grabar archivos compartidos

HALLAZGO 18 ×

Comentario

Pérdida de productividad en el área contable.

NORMAS ISO/IEC

NORMA ISO/IEC 27001 Seguridad de la información: Proporciona a las organizaciones un modelo consistente que ayuda a establecer, implementar, monitorear, revisar y mantener un sistema de gestión de seguridad de la información.

NORMA ISO/IEC 27002 Buenas prácticas para los controles de seguridad de la información: Proporciona recomendaciones de las mejores prácticas para la gestión de seguridad de la información.

NORMA: ISO/IEC 27005 Gestión de riesgos de seguridad de la información: Proporciona directrices para establecer un enfoque sistemático de gestión de riesgos de seguridad de la información.

NORMA ISO/IEC 31000 Sistemas de gestión de riesgos: Proporciona directrices y principios para gestionar el riesgo de las organizaciones.

Conclusión

Incumplimiento de actividades laborales en los puestos de trabajo y funciones. Por lo que, ocurrirá una pérdida de productividad en el área debido a que las fallas en el sistema contable no permiten acceso al sistema instalado en el servidor

Recomendaciones

Dirigido al encargado del área de Informática:

- Solicitar al encargado de sistemas la revisión y mantenimiento de hardware y software o a su vez requerir ayuda de la matriz del programa para una solución pronta para evitar la ralentización de actividades y obtención de información contable.

HALLAZGO 19 ×

Comentario

Inconsistencias en toma física en el área de inventarios.

NORMAS ISO/IEC

NORMA ISO/IEC 27001 Seguridad de la información: Proporciona a las organizaciones un modelo consistente que ayuda a establecer, implementar, monitorear, revisar y mantener un sistema de gestión de seguridad de la información.

NORMA ISO/IEC 27002 Buenas prácticas para los controles de seguridad de la información: Proporciona recomendaciones de las mejores prácticas para la gestión de seguridad de la información.

NORMA: ISO/IEC 27005 Gestión de riesgos de seguridad de la información: Proporciona directrices para establecer un enfoque sistemático de gestión de riesgos de seguridad de la información.

NORMA ISO/IEC 31000 Sistemas de gestión de riesgos: Proporciona directrices y principios para gestionar el riesgo de las organizaciones.

Conclusión

Incumplimiento de actividades laborales en los puestos de trabajo y funciones. Por lo que, ocurrirá un descuadre de datos físicos con los reportados por el sistema contable, gestión inadecuada de los inventarios.

Recomendaciones

Dirigido al encargado del área de Informática:

- Acceso limitado o no permitir modificaciones al sistema para evitar inconvenientes.

HALLAZGO 20 ×

Comentario

Infraestructura tecnológica inestable, inventario de activo desactualizado en el área informática.

NORMAS ISO/IEC

NORMA ISO/IEC 27001 Seguridad de la información: Proporciona a las organizaciones un modelo consistente que ayuda a establecer, implementar, monitorear, revisar y mantener un sistema de gestión de seguridad de la información.

NORMA ISO/IEC 27002 Buenas prácticas para los controles de seguridad de la información: Proporciona recomendaciones de las mejores prácticas para la gestión de seguridad de la información.

NORMA: ISO/IEC 27005 Gestión de riesgos de seguridad de la información: Proporciona directrices para establecer un enfoque sistemático de gestión de riesgos de seguridad de la información.

NORMA ISO/IEC 31000 Sistemas de gestión de riesgos: Proporciona directrices y principios para gestionar el riesgo de las organizaciones.

Conclusión

Incumplimiento de actividades laborales en los puestos de trabajo y funciones. Lo que ocasiona infraestructura tecnológica inestable, inventario de activos desactualizada, gestión y gobierno de TI desalineados a los objetivos corporativos.

Recomendaciones

Dirigido al encargado del área de Informática:

- Elaborar planes adecuados para la prevención de amenazas y mitigación de riesgos. Evaluar periódicamente la seguridad de la información tanto de hardware como de software y procesos informáticos con alineación a las actividades de la organización.

Resultado de hallazgos en Flujogramas

HALLAZGO 21 α

Comentario

En los flujogramas de ventas se encontró que durante el proceso no existe una autorización para receptar como forma de pago un cheque.

NORMAS ISO/IEC

NORMA ISO/IEC 27001 Seguridad de la información: Proporciona a las organizaciones un modelo consistente que ayuda a establecer, implementar, monitorear, revisar y mantener un sistema de gestión de seguridad de la información.

NORMA ISO/IEC 27002 Buenas prácticas para los controles de seguridad de la información: Proporciona recomendaciones de las mejores prácticas para la gestión de seguridad de la información.

NORMA: ISO/IEC 27005 Gestión de riesgos de seguridad de la información: Proporciona directrices para establecer un enfoque sistemático de gestión de riesgos de seguridad de la información.

NORMA ISO/IEC 31000 Sistemas de gestión de riesgos: Proporciona directrices y principios para gestionar el riesgo de las organizaciones.

Conclusión

Se podrían adquirir cheques falsos de personas mal intencionadas. Lo que podría ocasionar al no ser clientes frecuentes podrían emitir cheques falsos lo que constituye una pérdida de mercadería y dinero para la entidad.

Recomendaciones

Dirigido al encargado del departamento de Comercialización y gerencia:

- Verificar la información del cliente y si su actividad es frecuente en la entidad para otorgar autorización de poder recibir el cheque.

HALLAZGO 22 α

Comentario

En el flujograma de cuentas por cobrar se encontró que no se realiza la selección de facturas con saldos antiguos.

NORMAS ISO/IEC

NORMA ISO/IEC 27001 Seguridad de la información: Proporciona a las organizaciones un modelo consistente que ayuda a establecer, implementar, monitorear, revisar y mantener un sistema de gestión de seguridad de la información.

NORMA ISO/IEC 27002 Buenas prácticas para los controles de seguridad de la información: Proporciona recomendaciones de las mejores prácticas para la gestión de seguridad de la información.

NORMA: ISO/IEC 27005 Gestión de riesgos de seguridad de la información: Proporciona directrices para establecer un enfoque sistemático de gestión de riesgos de seguridad de la información.

NORMA ISO/IEC 31000 Sistemas de gestión de riesgos: Proporciona directrices y principios para gestionar el riesgo de las organizaciones.

Conclusión

No se revisa adecuadamente el listado de compras del cliente. Lo que ocasiona un aumento de morosidad por parte de los clientes.

Recomendaciones

Dirigido al encargado del departamento contable y gerencia:

- Verificar y seleccionar en el software contable adecuadamente las facturas antiguas del cliente con la finalidad de disminuir la morosidad.

HALLAZGO 23 α

Comentario

En el flujograma de adquisición de pedidos se encontró que en ocasiones no se envían reporte de pedido a la sucursal.

NORMAS ISO/IEC

NORMA ISO/IEC 27001 Seguridad de la información: Proporciona a las organizaciones un modelo consistente que ayuda a establecer, implementar, monitorear, revisar y mantener un sistema de gestión de seguridad de la información.

NORMA ISO/IEC 27002 Buenas prácticas para los controles de seguridad de la información: Proporciona recomendaciones de las mejores prácticas para la gestión de seguridad de la información.

NORMA: ISO/IEC 27005 Gestión de riesgos de seguridad de la información: Proporciona directrices para establecer un enfoque sistemático de gestión de riesgos de seguridad de la información.

NORMA ISO/IEC 31000 Sistemas de gestión de riesgos: Proporciona directrices y principios para gestionar el riesgo de las organizaciones.

Conclusión

Por error del personal suelen olvidarse de enviar el reporte de pedidos de artículos a la casa matriz Guayaquil. Lo que ocasiona un desabastecimiento de artículos y materiales.

Recomendaciones

Dirigido al encargado del departamento de compra:

Realizar un previo listado de pedidos. generar enviar de manera inmediata el reporte de cada pedido a la matriz revisando que el reporte y el listado concuerden.

HALLAZGO 24 α

Comentario

En el flujograma de cotización se encontró que no verifican el listado de precios de los productos.

NORMAS ISO/IEC

NORMA ISO/IEC 27001 Seguridad de la información: Proporciona a las organizaciones un modelo consistente que ayuda a establecer, implementar, monitorear, revisar y mantener un sistema de gestión de seguridad de la información.

NORMA ISO/IEC 27002 Buenas prácticas para los controles de seguridad de la información: Proporciona recomendaciones de las mejores prácticas para la gestión de seguridad de la información.

NORMA: ISO/IEC 27005 Gestión de riesgos de seguridad de la información: Proporciona directrices para establecer un enfoque sistemático de gestión de riesgos de seguridad de la información.

NORMA ISO/IEC 31000 Sistemas de gestión de riesgos: Proporciona directrices y principios para gestionar el riesgo de las organizaciones.

Conclusión

Esto sucede por la fluctuación de precios desde la fecha de cotización hasta la fecha de compra. Lo que conlleva modificaciones en los precios de los productos.

Recomendaciones

Dirigido al encargado del departamento de comercialización:

Informar al cliente que los precios pueden variar durante la compra por la fluctuación de precios.

3.1.3.2. Matriz de Seguimiento y Monitoreo

Tiene por objetivo monitorear las actividades de los activos de información con el fin de controlar y eliminar de manera efectiva riesgos detectados.

La matriz de seguimiento y monitoreo está compuesta por:

Activos de información:

- ✓ Descripción de todos los activos que tiene la entidad.
- ✓ Columna que no será necesario modificarla o editarla.

Control sugerido:

- ✓ Controles que podrían eliminar o mitigar los riegos que se identificaron en la entidad.
- ✓ Columna que no será necesario modificarla o editarla.

Riesgo:

- ✓ Problemas que presentan los activos de información de la entidad.
- ✓ Columna que no será necesario modificarla o editarla.

Calificación del control sugerido:

- ✓ Calificación que se otorgará según la funcionalidad del control.
- ✓ Columna necesaria llenar según criterios definidos en la tabla.

Frecuencia:

- ✓ Regularidad con la que se llevan a cabo los controles.
- ✓ Columna necesaria llenar según criterios definidos en la tabla.

Meta:

- ✓ Se refiere a que tan funcionales llegaron a ser los controles.
- ✓ Columna que no será necesario modificarla o editarla ya que esta automatizada.

Porcentaje:

- ✓ Representación porcentual en cuanto a la funcionalidad de los controles aplicados.
- ✓ Columna que no será necesario modificarla o editarla ya que esta automatizada.

Observación:

- ✓ Se refiere a que tan efectivo fue el control para evitar o eliminar falencias que presentaron los activos.

- ✓ Columna que no será necesario modificarla o editarla ya que esta automatizada.

Acción a considerar:

- ✓ Situaciones que permitieron implementar los controles.
- ✓ Columna necesaria llenar según lo observado durante la aplicación de controles.

Responsable de monitoreo:

- ✓ Nombre del encargado de aplicar y llenar en los departamentos la matriz de seguimiento y monitoreo.
- ✓ Columna necesaria llenar para tener un adecuado registro.

Supervisor de monitoreo:

- ✓ Nombre del encargado de verificar que se haya utilizado de manera adecuada en los departamentos la matriz de seguimiento y monitoreo.
- ✓ Columna necesaria llenar para tener un adecuado registro.

Fecha de monitoreo:

- ✓ Registro de fechas según la frecuencia con la que se aplique el control.
- ✓ Columna necesaria llenar para tener un adecuado registro.

Es importante considerar los siguientes criterios para completar los campos:

Ilustración 39. *Criterios de controles*

CRITERIOS DE CONTROLES		
Calificación del control	**Porcentaje**	**Meta del control**
1	25%	CONTROL BAJO
2	75%	CONTROL MODERADO
3	90%	CONTROL ALTO

Elaborado por: Sánchez (2023)

Ilustración 40. *Matriz de seguimiento y monitoreo*

MATRIZ DE SEGUIMIENTO Y MONITOREO											
ACTIVOS DE INFORMACIÓN	CONTROL SUGERIDO	RIESGO	CALIFICACIÓN DE CONTROL SUGERIDO	FRECUENCIA	META	PORCENTAJE	OBSERVACIÓN	ACCIÓN A CONSIDERAR	RESPONSABLE DE MONITOREO	SUPERVISOR DE MONITOREO	FECHA DE MONITOREO
Sistemas contables	Solicitar al encargado del software verificar la situación, con soporte del proveedor matriz del programa para una solución pronta.	No guarda la información registrada, se pierde información, Ralentización de registro de datos.	1	DIARIO	CONTROL BAJO	25%	CONTROL NO EFECTIVO	Describir la situación que conllevo aplicar el control sugerido.	Nombre del responsable de aplicar el control	Nombre del supervisor de aplicar el control	Fecha según la frecuencia del control
Aplicaciones en linea (Tributario y empresarial)	Mantener la información requeridas por los entes de control con anticipación a la fecha de envio para evitar retraso y sanciones.	Incumplimiento de envio de reportes a entes de control, por lo tanto provocaría sanciones.	2	SEMANAL	CONTROL MODERADO	75%	CONTROL MEDIO	Describir la situación que conllevo aplicar el control sugerido.	Nombre del responsable de aplicar el control	Nombre del supervisor de aplicar el control	Fecha según la frecuencia del control
Antivirus	Comprar e instalar antivirus adecuados para la entidad y mantener una constante revisión de la caducidad de la licencia.	Pérdida de información en la base de datos, archivos infectados, daños del sistema operativo.	3	MENSUAL	CONTROL ALTO	100%	CONTROL EFECTIVO	Describir la situación que conllevo aplicar el control sugerido.	Nombre del responsable de aplicar el control	Nombre del supervisor de aplicar el control	Fecha según la frecuencia del control
Paginas web	Realizar revisiones diarias de la pagina web y su funcionamiento.	Hackeo de información, bajo nivel en ventas en linea.	1	TRIMESTRAL	CONTROL BAJO	25%	CONTROL NO EFECTIVO	Describir la situación que conllevo aplicar el control sugerido.	Nombre del responsable de aplicar el control	Nombre del supervisor de aplicar el control	Fecha según la frecuencia del control
Redes sociales	Revisón constante de las redes sociales para evitar robos de identidad, contraseñas, malware.	Pérdida de imagen y reputación empresarial.	2	SEMESTRAL	CONTROL MODERADO	75%	CONTROL MEDIO	Describir la situación que conllevo aplicar el control sugerido.	Nombre del responsable de aplicar el control	Nombre del supervisor de aplicar el control	Fecha según la frecuencia del control
Base de datos	Otorgar acceso limitado al personal para la recuperación de la información, sacar backups semanales de la base de datos en la nube y discos externos.	Pérdida de información en el sistema.	3	ANUAL	CONTROL ALTO	100%	CONTROL EFECTIVO	Describir la situación que conllevo aplicar el control sugerido.	Nombre del responsable de aplicar el control	Nombre del supervisor de aplicar el control	Fecha según la frecuencia del control
Marca patentada	Realizar un rastreo una vez al año sobre la aparición de marcas similares.	Confunsión en escritura y pronunciacion de nuevas marcas.	1	DIARIO	CONTROL BAJO	25%	CONTROL NO EFECTIVO	Describir la situación que conllevo aplicar el	Nombre del responsable de aplicar	Nombre del supervisor de aplicar el control	Fecha según la frecuencia del
Equipos	Capacitar al personal para el correcto cuidado y capacidad de respuesta ante posibles fallas para no retrasar las actividades, los cuales deben ser informadas de forma inmediata al evento.	Pérdida de información, Reemplazo del equipo.	2	SEMANAL	CONTROL MODERADO	75%	CONTROL MEDIO	Describir la situación que conllevo aplicar el control sugerido.	Nombre del responsable de aplicar el control	Nombre del supervisor de aplicar el control	Fecha según la frecuencia del control
Impresoras	Dar aviso inmediato para revisión y mantenimiento al encargado del área informática.	No contar con el respaldo impreso como evidencia de la transacción.	3	MENSUAL	CONTROL ALTO	100%	CONTROL EFECTIVO	Describir la situación que conllevo aplicar el control sugerido.	Nombre del responsable de aplicar el control	Nombre del supervisor de aplicar el control	Fecha según la frecuencia del control

Scaners	Dar aviso inmediato para revisión y mantenimiento al encargado del área informática.	No contar con el respaldo digital como evidencia de la transacción.	1	TRIMESTRAL	CONTROL BAJO	25%	CONTROL NO EFECTIVO	Describir la situación que conllevo aplicar el control sugerido.	Nombre del responsable de aplicar el control	Nombre del supervisor de aplicar el control	Fecha según la frecuencia del control
Discos duros	Revisar la capacidad de almacenamiento de los discos duros y adquirir nuevos de ser necesarios.	No poder recuperar la información guardada en e disco duro.	2	SEMESTRAL	CONTROL MODERADO	75%	CONTROL MEDIO	Describir la situación que conllevo aplicar el control sugerido.	Nombre del responsable de aplicar el control	Nombre del supervisor de aplicar el control	Fecha según la frecuencia del control
Pendrives	Pedir al encargado formatear o adquirir nuevas memorias.	No poder recuperar la información guardada en el pendrive.	3	DIARIO	CONTROL ALTO	100%	CONTROL EFECTIVO	Describir la situación que conllevo aplicar el control sugerido.	Nombre del responsable de aplicar el control	Nombre del supervisor de aplicar el control	Fecha según la frecuencia del control
Cableado	Verificar la correcta adecuación de los cables en la infraestructura.	Cortos circuitos por mal ubicación de los cables.	1	SEMANAL	CONTROL BAJO	25%	CONTROL NO EFECTIVO	Describir la situación que conllevo aplicar el control sugerido.	Nombre del responsable de aplicar el control	Nombre del supervisor de aplicar el control	Fecha según la frecuencia del control
Red	Realizar conexión con VPN o accesos remotos que permitan utilizar el software y abrir y grabar archivos compartidos.	Pérdida de información de archivos compartidos, Pérdida de tiempo en apertura del software, Tiempo de espera elevados	2	MENSUAL	CONTROL MODERADO	75%	CONTROL MEDIO	Describir la situación que conllevo aplicar el control sugerido.	Nombre del responsable de aplicar el control	Nombre del supervisor de aplicar el control	Fecha según la frecuencia del control
Capacidad del servidor	Ampliar las gigas o cambiar a un servidor Dedicado, o de alto rendimiento, que tengan velocidad y procesamiento para el almacenamiento de datos, fiable y seguro que permita obtener copias de seguridad permanentes.	Error en copias de seguridad, Daño de disco duro de almacenamiento, Saturación de capacidad de almacenamiento	3	TRIMESTRAL	CONTROL ALTO	100%	CONTROL EFECTIVO	Describir la situación que conllevo aplicar el control sugerido.	Nombre del responsable de aplicar el control	Nombre del supervisor de aplicar el control	Fecha según la frecuencia del control
Gerente	Incluir en el plan operativo actividades que busquen asegurar las operaciones de seguridad de la información, que se ejecuten según lo planificado.	Toma de decisiones inadecuadas	1	SEMESTRAL	CONTROL BAJO	25%	CONTROL NO EFECTIVO	Describir la situación que conllevo aplicar el control sugerido.	Nombre del responsable de aplicar el control	Nombre del supervisor de aplicar el control	Fecha según la frecuencia del control
Contabilidad	Solicitar al encargado de sistemas la revisión y mantenimiento de hardware y software o a su vez requerir ayuda de la matriz del programa para una solución pronta para evitar la ralentización de actividades y obtención de información contable.	Pérdida de productividad en el área debido a que las fallas en el sistema contable no permiten acceso al sistema instalado en el servidor.	2	ANUAL	CONTROL MODERADO	75%	CONTROL MEDIO	Describir la situación que conllevo aplicar el control sugerido.	Nombre del responsable de aplicar el control	Nombre del supervisor de aplicar el control	Fecha según la frecuencia del control
Comercialización	Crear un plan de fidelización de clientes. Planificar capacitaciones periódicas para el área.	Pérdida de clientes, Aectación a nivel de ventas esperadas	3	DIARIO	CONTROL ALTO	100%	CONTROL EFECTIVO	Describir la situación que conllevo aplicar el control sugerido.	Nombre del responsable de aplicar el control	Nombre del supervisor de aplicar el control	Fecha según la frecuencia del control

Inventarios	Acceso limitado o no permitir modificaciones al sistema para evitar incovenientes.	Inconsistencia en toma física de inventarios, Descuadre de datos físicos con los reportados por el sistema contable, Gestión inadecuada de los inventarios	1	SEMANAL	CONTROL BAJO	25%	CONTROL NO EFECTIVO	Describir la situación que conllevo aplicar el control sugerido.	Nombre del responsable de aplicar el control	Nombre del supervisor de aplicar el control	Fecha según la frecuencia del control
Recursos Humanos	Perfeccionar el proceso de selección de personal idóneo para los cargos laborales requeridos.	Contratación de personal no competente	2	MENSUAL	CONTROL MODERADO	75%	CONTROL MEDIO	Describir la situación que conllevo aplicar el control sugerido.	Nombre del responsable de aplicar el control	Nombre del supervisor de aplicar el control	Fecha según la frecuencia del control
Área de informática	Elaborar planes adecuados para la prevención de amenzas y mitigación de riesgos. Evaluar periódicamente la seguridad de la información tanto de hardware como de software y procesos informáticos con alineación a las actividades de la organización.	Infraestructura tecnológica inestable, Inventario de activos desactualizada, Gestión y gobierno de TI dealineados a los objetivos corporativos	3	TRIMESTRAL	CONTROL ALTO	100%	CONTROL EFECTIVO	Describir la situación que conllevo aplicar el control sugerido.	Nombre del responsable de aplicar el control	Nombre del supervisor de aplicar el control	Fecha según la frecuencia del control

Elaborado por: Sánchez (2023)

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- Mediante el presente proyecto se realizó una auditoria al sistema en la empresa DEMACO CIA. LTDA., evaluando el control interno se obtuvo como resultado que el área informática no cuenta con políticas y estrategias adecuadas para los controles de las TI y para prevenir y mitigar riesgos. Además, el personal se encuentra altamente capacitado para desempeñar sus actividades con normalidad, pero la falta de compromiso y el desconocimiento para gestionar riesgos ha dado lugar a la creación de puntos débiles en el sistema de información.

- Se identificaron y evaluaron los activos de información de la entidad, obteniendo como resultado que el área informática protege sus activos de amenazas externas, es decir la información que maneja el personal y la entidad respetan acuerdos de confidencialidad disponibilidad e integridad, pero a pesar del gran esfuerzo que realizan se observó que internamente sus activos han sufrido daños y alteraciones.

- Se observó que los activos de información no cuentan con controles formales y apropiados para prevenir o eliminar riegos. Lo que ocasiona retrasos en el desarrollo de las actividades y problemas significativos para la entidad, por lo que es importante tratarlos de manera inmediata para evitar que sucedan de manera frecuente y causen severos daños. Por otro lado, tomando en cuenta el tiempo que la entidad lleva utilizando el sistema contable se observaron falencias, pero dichas observaciones pertenecen al manejo incorrecto de los procedimientos, es decir suceden por errores del personal y falta de organización.

- Se establecieron controles para gestionar los riesgos de manera adecuada, con la finalidad de salvaguardar los activos de información, mediante procesos que

ayudarán a examinar y monitorear minuciosamente el comportamiento de los activos ante la implementación de nuevos controles.

4.2 Recomendaciones

- Es importante que la entidad supervise y evalúe constantemente la utilización de los activos de información en cada uno de los departamentos para eludir riesgos, por lo que también es importante capacitar al personal de la entidad sobre políticas y estrategias de la gestión de riesgos, con la finalidad de orientarse a la mejora continua y una responsable utilización de los activos de información.

- Se sugiere utilizar la matriz de seguimiento y monitoreo según la frecuencia con la que se presenten eventualidades en los activos de información para así poder llevar un correcto registro y verificar el cumplimiento óptimo de los controles. Lo cual ayudará a largo plazo a una mejor identificación y prevención de falencias y riesgos en la entidad.

REFERENCIAS BIBLIOGRÁFICAS

Albarracin, L., Marín, C., Lozada, J., & Martinez , J. (2021). Auditoría informática dentro de la empresa "Promaelec" de la ciudad de Quevedo, en tiempo de COVID-19. *Revista Universidad y Sociedad*. Obtenido de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202021000500345&lang=es

Alonso, C. (30 de Marzo de 2023). *Global Suite*. Obtenido de ISO 27000 y el conjunto de seguridades de la información: https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/

Alvarez, L. (2005). *Seguridad en informatica*. Mexico: Universidad Iberoamericana. Obtenido de http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

Andrade , J., & Chávez, C. (2018). *Generación de un plan para la gestión integral de seguridad de la información basado en el marco de la normas ISO 27001 y las mejores prácticas de seguridad de la norma ISO 27002 para la compañia international gym Ecuaintergym de la ciudad de Guayaquil.* Repositorio Institucional de la Universidad de Guayaquil, Guayaquil. Obtenido de http://repositorio.ug.edu.ec/bitstream/redug/32606/1/B-CINT-PTG-N.306%20Andrade%20Chila%20Juan%20Carlos%20.%20Ch%c3%a1vez%20Loor%20Carlos%20Erick.pdf

Andreu, R., Ricart, J., & Valor, J. (1991). *Estrategia y sistemas de información* . Madrid: McGraw-Hill.

Arcentales, D., & Caycedo, X. (2017). Auditoría informática: un enfoque efectivo. *Dominio de las Ciencias*, 157-173. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=6102836#:~:text=La%20importancia%20de%20las%20auditor%C3%ADas,mejores%20pr%C3%A1cticas%20en%20auditorias%20inform%C3%A1ticas.

Arévalo, F. (2020). Importancia de la seguridad de los sistemas de información frente el abuso, error y hurto de información. *Ciencias de la computación*, 835-846.

Avenía, C. (2017). Fundamentos de Seguridad Informática. *Fundación Universitaría del área Andina*, 12. Obtenido de https://core.ac.uk/download/pdf/326424171.pdf

Ávila, M., & Zambrano, E. (2022). Las auditorías de gestión en las empresas públicas del Ecuador. *RECUS*. Obtenido de https://oaji.net/articles/2023/6747-1673964413.pdf

Ayala, E., & Gonzales, S. (2015). *Tecnologías de la información y la comunicación.* Lima: Fondo Editorial de la UIGV. Obtenido de http://repositorio.uigv.edu.pe/bitstream/handle/20.500.11818/1189/Libro%20TIC%20%282%29-1-76%20%281%29.pdf?sequence=1

Bertalanffy, V. (1986). Teoría general de los sistemas. *Studocu*, 2-6.

Boccazzi , C., & Negrete, J. (2015). Evaluación de riesgos tecnológicos y percepción de la población residente y turista de las comunas de Quintero y Punchucaví. *Gestión Turística*, 70-97. Obtenido de https://www.redalyc.org/pdf/2233/223353236004.pdf

Brito, J., & Solis, G. (2004). Análisis y aprovechamiento de los sistemas de información para una eficiente auditoría y control de gestión. *Auditor de control de gestión*, 2-11. Obtenido de https://www.dspace.espol.edu.ec/bitstream/123456789/1901/1/3786.pdf

Carrión, D. (2005). Evaluación del sistema de mantenimiento asistido por computadora de una empresa del sector naviero. *Escuela Superior politecnica del Litoral*, 17-303.

Dávalos, Á. (2013). Auditoría de seguridad de Información. *Fides Et Ratio- Revista de Difusion cultural y cientifica de la Universdiad La Salle en Bolivia*, 19-30. Obtenido de http://www.scielo.org.bo/pdf/rfer/v6n6/v6n6_a04.pdf

DEMACO. (2023). *DEMACO*. Obtenido de HISTORIA: https://www.demaco.ec/

Díaz , G. A. (2020). La auditoría a los sistemas de información como aporte a la actividad gerencial. *Gestión de Organizaciones*, 239. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=7863432

Dominguez, J., & Solis, G. (2004). Analisis y aprovechamiento de los sistemas de inforación para uan eficiente auditoria y control de gestión. *Scielo*. Obtenido de https://www.dspace.espol.edu.ec/bitstream/123456789/1901/1/3786.pdf

Echenique, J. (2001). *Auditoría en Informática.* México: McGraw-Hill.

Espinosa, L., Mora, L., & Lopez , J. (2014). *Auditoría Informática de desarrollo de proyectos.* Caracas: Instituto Universitario de Tecnología del Oeste Mariscal Sucre. Obtenido de https://tiglobal2012.files.wordpress.com/2014/07/gerencia_de_proyecto2.pdf

Esucomex. (2017). Las organizaciones y auditoría de sistemas de información. *ESUCOMEX*. Obtenido de http://cursos.esucomex.cl/SP-Esucomex-2014/ASX7404/S1/MATERIAL%20DE%20ESTUDIO.pdf

Hernádez, A. (2003). Los sistemas de información: evolución y desarrollo. *Departamento de Economia y dirección de empresas Unviversidad de Zaragoza*, 149-150. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=793097

Kuna, H., García, R., & Villatoro, F. (2008). Procedimientos de la explotación de información para la identificación de datos faltantes, con ruido e inconsistentes. *CORE*, 1-3. Obtenido de https://core.ac.uk/download/pdf/301040258.pdf

Leiva, E. (2015). Estrategias nacionales de ciberseguridad: Estudio comparativo basado en enfoque Top-Down desde una visión global a una visión local . *Revista latinoamericana de ingenieria de software*, 161-176.

León, K., & Guerra, R. (2016). *Las Normas ISO 9000.* Cofin Habana. Obtenido de http://scielo.sld.cu/pdf/cofin/v10n2/cofin02216.pdf

Martínez, J., & Giraldo, C. (2019). Auditoría de seguridad Informática. *Password*, 2-5. Obtenido de https://www.academia.edu/32098381/AUDITORIA_DE_SEGURIDAD_INFORMATICA

Martinez, Y., Blanco, B., & Loy, L. (2012). Auditoría con Informática a Sistemas Contables. *Revista de Arquitectura e Ingeniería*, 1-14. Obtenido de https://www.redalyc.org/pdf/1939/193924743004.pdf

Negrín , E., López, L., Rodriguez, K., & Martínez, D. (2017). Propuesta de un programa de Auditoría a los sistemas de información. *Revista ECA*, 131-143. Obtenido de https://dialnet.unirioja.es/descarga/articulo/6230346.pdf

Normas Internacionales de Auditoría. (2016). *Auditoría en un Ambiente de Sistemas de Informacion por computadora (NIA 401).* Obtenido de http://www.grupomiranda.co.cr/despachos/nias_400_499_pdf/NIA_401.pdf

Organización internacional de Normalización . (2018). *ISO/IEC tecnología de la información, técnica de seguridad, sistemas de gestión de seguridad de la información, descripción general y vocabulario.* Obtenido de https://www.iso27000.es/sgsi.html

Piattini, M., & Del Peso, E. (2001). *Auditoría Informática.* Madrid: RA-MA. Obtenido de http://cotana.informatica.edu.bo/downloads/ld-Auditoria-informatica-un-enfoque-practico-Mario-Piattini-pdf.pdf

Prieto, A., & Martínez , M. (2004). *Sistemas de información en las organizaciones: Una alternativa para mejorar la productividad.* Maracaibo: Revista de Ciencias Social .

Ramirez, G., & Alvarez, E. (2003). Auditoría a la Gestión de las Tecnologías y Sistemas de Información. *Industrial Data*. Obtenido de https://www.redalyc.org/pdf/816/81606114.pdf

Ramos, M. (2015). La Auditoría Informatica. *Dialnet,* https://dialnet.unirioja.es/descarga/articulo/248905.pdf.

Rojas, O., & Martínez, C. (2011). Riesgos naturales: evolución y modelos conceptuales. *Revista Universitaria de Geografía*, 81-116. Obtenido de https://www.redalyc.org/pdf/3832/383239103004.pdf

Sabillón , R., & Cano, J. (2019). Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação,* 33-48. Obtenido de https://scielo.pt/scielo.php?script=sci_arttext&pid=S1646-98952019000200004&lng=pt&nrm=iso&tlng=es?script=sci_arttext&pid=S1646-98952019000200004&lng=pt&nrm=iso&tlng=es

Solano, O. J. (2011). *La Auditoría de sistemas de información como elemento de control.* Cuadernos de Administración. Obtenido de https://cuadernosdeadministracion.univalle.edu.co/index.php/cuadernos_de_administracion/article/view/198/270

Thomas, A. J. (1987). *Auditoría Informática.* Madrid: Paraninfo.

Vargas, F. (4 de noviembre de 2020). *Crowe.* Obtenido de Etapas de Auditoría: https://www.crowe.com/ve/insights/etapas-de-una-

auditoria#:~:text=El%20n%C3%BAmero%20de%20etapas%20es,Campo)%20y%20Emisi%C3%B3n%20de%20Informes.

Villazán, F. (2010). *Manual de informática I.* Mexico: Universidad Michoacana de San Nicolás de Hidalgo .

Westreicher, G. (1 de Mayo de 2021). *Normas Internacionales de Auditoría (NIA).* Obtenido de Economipedia: https://economipedia.com/definiciones/contabilidad/normas-internacionales-de-auditoria-nia.html#:~:text=Las%20Normas%20Internacionales%20de%20Auditor%C3%ADa%20(NIA)%20son%20una%20serie%20de,pr%C3%A1cticas%20realizadas%20por%20los%20auditores.