



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE ECONOMÍA Y EMPRESA
CARRERA DE CONTABILIDAD Y AUDITORÍA**

TÍTULO:

“Propuesta metodológica para la reducción de riesgos de los sistemas de información contable de empresas del sector acuícola de la provincia del Guayas”.

AUTORES:

**Carrasco Viteri, Conny Sheeys
Torres Chávez, Deisy Alexandra**

**Trabajo de titulación previo a la obtención del título de
LICENCIADA EN CONTABILIDAD Y AUDITORÍA**

TUTOR:

Ing. Delgado Loor, Fabian Andrés

Guayaquil, Ecuador

16 de septiembre del 2022



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE ECONOMÍA Y EMPRESA
CARRERA DE CONTABILIDAD Y AUDITORÍA

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por:
Carrasco Viteri, Conny Sheeys y Torres Chávez, Deisy Alexandra como
requerimiento parcial para la obtención del Título de: Licenciada en
Contabilidad y Auditoría.

TUTOR (A)

f. _____
Ing. Fabian Andrés, Delgado Loor

DIRECTOR DE LA CARRERA

f. _____

Ph. D. Said Diez

Guayaquil, a los 16 días del mes de septiembre del año 2022



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE ECONOMÍA Y EMPRESA
CARRERA DE CONTABILIDAD Y AUDITORÍA

DECLARACIÓN DE RESPONSABILIDAD

**Nosotras Carrasco Viteri, Conny Sheeys
Torres Chávez, Deisy Alexandra.**


DECLARAMOS QUE:


El Trabajo de Titulación “**Propuesta Metodológica para la Reducción de Riesgos de los Sistemas de Información Contable de Empresas del Sector Acuícola de la Provincia del Guayas**” previa a la obtención del Título de: Licenciada en Contabilidad y Auditoría, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de nuestra total autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance científico del Trabajo de Titulación referido.

Guayaquil, a los 16 días del mes de septiembre del año 2022

LOS AUTORES

f. 
Carrasco Viteri, Conny Sheeys

f. 
Torres Chávez, Deisy Alexandra



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE ECONOMÍA Y EMPRESA
CARRERA DE CONTABILIDAD Y AUDITORÍA


AUTORIZACIÓN


Nosotras Carrasco Viteri, Conny Sheeys
Torres Chávez, Deisy Alexandra.

Autorizamos a la Universidad Católica de Santiago de Guayaquil, la publicación en la biblioteca de la institución del Trabajo de Titulación **“Propuesta Metodológica para la Reducción de Riesgos de los Sistemas de Información Contable de Empresas del Sector Acuícola de la Provincia del Guayas”**, cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y total autoría.

Guayaquil, a los 16 días del mes de septiembre del año 2022

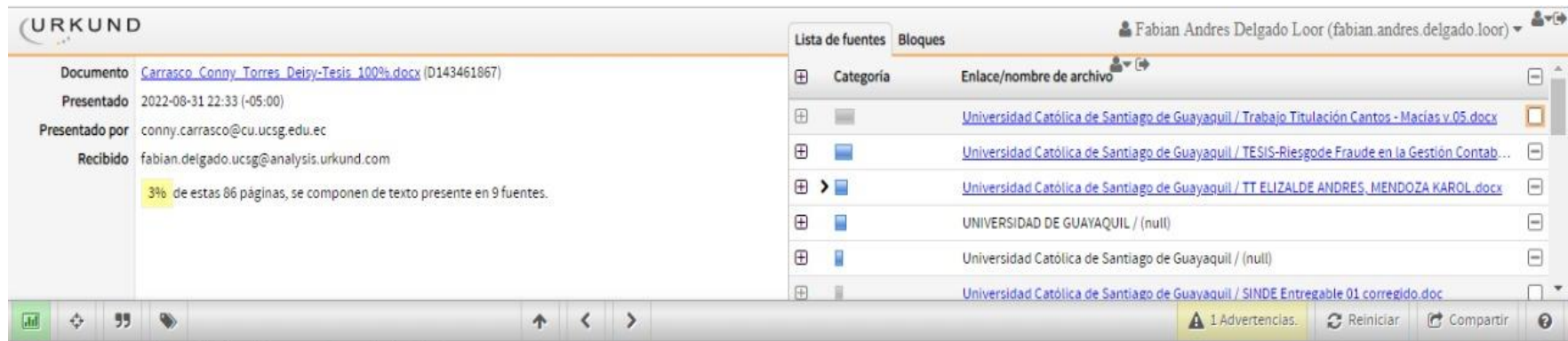
LOS AUTORES

f. 
Carrasco Viteri, Conny Sheeys

f. 
Torres Chávez, Deisy Alexandra

REPORTE URKUND

<https://secure.orkund.com/old/view/136838841-628087-803013#FcqxCGJBDATQf9l6kGSTzSb3K2lhh8oWXnOl+O+OkAczZD7tfbbtKlCeQvuEGqN1MnlaFPT/JRXUBQZTcMeZg90V3uHMAZ8YGIbARCI7ciADyZYoiKD8hnau17Gea78f+6NtcpFe6mNqL58yQiK+Pw==>



The screenshot displays the URKUND interface. On the left, document details are shown: 'Documento: Carrasco_Conny_Torres_Deisy-Tesis_100%.docx (D143461867)', 'Presentado: 2022-08-31 22:33 (-05:00)', 'Presentado por: conny.carrasco@cu.ucsg.edu.ec', and 'Recibido: fabian.delgado.ucsg@analysis.orkund.com'. A yellow highlight indicates '3% de estas 86 páginas, se componen de texto presente en 9 fuentes.' On the right, a table titled 'Lista de fuentes' lists sources with columns for 'Categoría' and 'Enlace/nombre de archivo'. The sources include 'Universidad Católica de Santiago de Guayaquil / Trabajo Titulación Cantos - Macías v.05.docx', 'Universidad Católica de Santiago de Guayaquil / TESIS-Riesgode Fraude en la Gestión Contab...', 'Universidad Católica de Santiago de Guayaquil / TT ELIZALDE ANDRES, MENDOZA KAROL.docx', 'UNIVERSIDAD DE GUAYAQUIL / (null)', 'Universidad Católica de Santiago de Guayaquil / (null)', and 'Universidad Católica de Santiago de Guayaquil / SINDE Entregable 01 corregido.doc'. The bottom of the interface shows navigation icons and a status bar with '1 Advertencias.', 'Reiniciar', and 'Compartir' buttons.

TUTOR



f. _____
Ing. Fabián Delgado MSc

AGRADECIMIENTO

Quiero expresar mi agradecimiento primeramente a Dios, por darme la fortaleza y perseverancia durante este tiempo para culminar mi etapa académica, recordándome su palabra en aquel versículo bíblico “Yo soy quien te manda que tengas valor y firmeza. No tengas miedo ni te desanimes porque yo, tu Señor y Dios, estaré contigo dondequiera que vaya “Josué 1:9 DHH
Agradezco a mis padres y hermanos por ser mi fuente de inspiración para luchar por mis sueños.

Agradezco a mi compañera de tesis, que más que compañera ha sido una amiga, ha sido pilar fundamental para realizar esta tesis.

También agradezco a mis profesores durante toda mi carrera profesional porque todos han aportado con un granito de arena a mi formación y en especial mi tutor de tesis por su apoyo y paciencia para que este trabajo sea de calidad.

Así mismo aquellas personas que han sido de gran ayuda e inspiración para continuar esta etapa universitaria.

Deisy Alexandra Torres Chávez

AGRADECIMIENTO

Agradezco en primer lugar a Dios por ser mi fortaleza en todo tiempo, ya que a pesar de los obstáculos que se presentaron siempre pude ver su respaldo y su pronta ayuda. Durante todo este tiempo de estudio, me aferré a un versículo bíblico que se encuentra en Josué 1:9 “Esfuézate y sé valiente. No temas ni desmayes, que yo soy el Señor tu Dios, y estaré contigo por donde quiera que vayas”. El cual, me alentaba a seguir luchando y no desmayar, a poner mi mirada en él y confiar en su poder.

Agradezco a mi esposo en especial ya que, sin su ayuda, motivación en todo momento no hubiera podido avanzar y culminar mi carrera.

Agradezco a mis hijos porque ellos son mi motivación e inspiración, el que se sientan orgulloso de tener una mamá que a pesar de los obstáculos pudo lograr ser una profesional y demostrarles que ellos también pueden lograr sus metas con esfuerzo y dedicación.

Agradezco a mi madre por su apoyo incondicional, sus oraciones, por cada uno de sus esfuerzos y sacrificios que realizó para ayudarme en los momentos que más necesitaba.

Agradezco a mi familia por cada palabra de motivación y ánimo que me daban para que continúe mi carrera universitaria.

Agradezco de forma especial al Dr. Edwy Gándara Quintong por brindarme su apoyo en todo tiempo y a cada uno de mis compañeros de trabajo por su acompañamiento.

Agradezco a todos mis amigos que fueron de ayuda en esta etapa de mi vida, en especial a Katty y Alexandra, ya que por medio de ellas pude experimentar un verdadero compañerismo y amistad en cada momento.

Me agradezco por ser una persona responsable, dedicada en cada área que se me delega en mis manos y por cada esfuerzo realizado.

Conny Sheeys Carrasco Viteri

DEDICATORIA

El presente trabajo se lo dedico principalmente a Dios por darme la salud, la sabiduría y la fortaleza para culminar mi etapa universitaria, a mis padres por su amor y apoyo, a mis hermanos por estar siempre conmigo, a mis pastores que estuvieron siempre orando por mí, a mis amigos por sus palabras de ánimo, a mis compañeros de trabajo por compartirme sus conocimientos y experiencias laborales y de vida, y a todas aquellas personas especiales que me han estado brindándome su apoyo.

Deisy Alexandra Torres Chávez

Este trabajo lo dedico en primer lugar a Dios porque sin su ayuda no lo hubiera logrado. A mi familia por su amor y apoyo incondicional en todo momento.

Conny Sheeys Carrasco Viteri



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE ECONOMÍA Y EMPRESA
CARRERA DE CONTABILIDAD Y AUDITORÍA**

TRIBUNAL DE SUSTENTACIÓN

f. _____

Ph. D. Said Vicente Diez Farhat
DIRECTOR DE CARRERA

f. _____

Patricia Salazar Torres MSc, CPA
COORDINADOR DEL ÁREA

f. _____

Cpa. Jimmy Marín Delgado
OPONENTE



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE ECONOMÍA Y EMPRESA
CARRERA DE CONTADURÍA PÚBLICA E INGENIERÍA EN
CONTABILIDAD Y AUDITORÍA

CALIFICACIÓN

f. _____

Ing. Fabian Delgado Loor
TUTOR

Índice General

Introducción	2
Antecedente de la Investigación.....	2
Contextualización del Problema	5
Antecedentes del Problema.....	5
Definición del Problema.....	7
Justificación de la Investigación.....	11
Objetivos	11
Objetivo General.....	11
Objetivos Específicos	12
Preguntas de Investigación	12
General.....	12
Específicas	12
Delimitación.....	12
Limitación	13
Capítulo 1: Fundamentación Teórica	14
Marco Teórico	14
Riesgos de Sistemas	14
Teorías de Riesgos.....	15
Teoría Control Interno.....	16
Modelo del COSO.....	21

Modelo de COSO 2017: Gestión de Riesgos Empresariales Integrado con Estrategia y Desempeño.....	23
Acceso Físico y Lógico de los Sistemas de Información Contable	25
Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT)	27
Prevención de Errores y Fraudes	38
El Triángulo del Fraude	38
Marco Conceptual	40
Sistema de Información	40
Características de Sistemas	40
Tipos de Sistemas	41
Elementos de Sistemas	42
Componentes de Sistemas.....	42
Actividades de los Sistemas de Información.....	43
Riesgos.....	44
Características del Riesgo	45
Tipos de Riesgos	45
Fraudes.....	46
Tipos de Fraudes.....	47
Clasificación de Fraudes.....	48
Características de un Defraudador	49
Control	49

Tipos de Control	49
Seguridad Informática.....	50
Tipos de Seguridad.....	51
Políticas de Seguridad.....	51
Errores en Sistemas	52
Marco Referencial	52
Estudios Previos	52
Sector Acuícola.....	54
Las Empresas Medianas y Pequeñas (PYMES).....	56
Clasificación de las PYMES.....	57
Aporte de las PYMES en el Ecuador	58
Las PYMES y la Facturación Electrónica.....	59
Marco Legal.....	60
Sistemas de Gestión de Seguridad de Información: ISO 27001	60
ISO 27002: Mejoras Prácticas Para Gestión de la Seguridad de la Información	62
ITIL	63
La versión Actual: ITIL 4	64
Código Orgánico Integral Penal, Artículo 234, Acceso no Consentido a un Sistema Informático	65
Normas de Auditoría NIA 315, Identificación y Valoración de los Riesgos de Incorrección Material Mediante el Conocimiento de la Entidad y de su Entorno	65

El Sistema de Información, Incluidos los Procesos de Negocio Relacionados, Relevante para la Información Financiera, y la Comunicación.....	66
Norma de Auditoria 240, Responsabilidades del Auditor en la Auditoría de Estados Financieros con Respecto al Fraude	68
Capítulo 2: Metodología de la Investigación.	69
Diseño de investigación	69
Según su propósito: Observacional	69
Según la Cronología: Prospectivo	70
Según su Medición: Transversal.....	70
Enfoque de Investigación	70
Tipo de Investigación	71
Fuente de Información	72
Población.....	73
Técnicas de Recolección de Datos / Herramientas Cualitativas	81
Diseño de Instrumentos de Investigación.....	82
Resultados	83
Primera Entrevista a Experto de Jefe de Sistema	84
Segunda Entrevista a Experto Analista de Sistemas.....	89
Tercera Entrevista a Experto como Contador.....	94
Cuarta Entrevista a Experto como Asistente Contable	97
Quinta Entrevista a Experto como Asistente Contable	100

Sexta Entrevista a Experto a Gerente de una Empresa	104
Matriz de Hallazgos	107
Análisis de Resultados	115
Capítulo 3: Propuesta Metodológica para Evaluación de Riesgos.....	119
Planificación	120
Ejecución.....	121
Supervisar	121
Acciones Correctivas.....	122
Riesgo I – Acceso Físico y Lógico a los Sistemas de Información Contable	123
Riesgo II – Manuales de Procedimientos y Políticas del Departamento Contable	126
Riesgo III – Estructura del Departamento Contable.....	129
Riesgo IV – Riesgos de Fraudes y Errores.....	132
Matriz de Riesgos Identificados	135
Plan de Acción para Reducción de Riesgos.....	137
Conclusiones	140
Recomendaciones	142
Referencia	143

Lista de Tablas

Tabla 1	Producción mundial estimada de camarón de cultivo.....	3
Tabla 2	Principales países del mundo donde el Ecuador exporta camarón .	4
Tabla 3	Número de empresas y empleados según el tamaño de la organización.....	5
Tabla 4	Tipos de fraudes experimentados por tamaño de las organizaciones (en ingresos globales).....	10
Tabla 5	Tipos de datos	44
Tabla 6	Especies cultivadas de camarón mundial.....	56
Tabla 7	Clasificación PYMES de acuerdo normativa interandina y la Superintendencia de compañías.....	58
Tabla 8	Delimitación del diseño de investigación	69
Tabla 9	Explotación de criaderos de camarones.....	74
Tabla 10	Preparación, conservación y elaboración de productos de camarón y langostinos.	75
Tabla 11	Venta al por mayor de camarón y langostinos.....	76
Tabla 12	Características que debe cumplir el perfil del experto	80
Tabla 13	Expertos que cumplieron las características	83
Tabla 14	Perfil de expertos.....	83
Tabla 15	Matriz de hallazgos (parte I)	108
Tabla 16	Matriz de hallazgos (parte II)	109
Tabla 17	Matriz de hallazgos (parte III)	110

Tabla 18	Matriz de hallazgos (parte IV).....	111
Tabla 19	Matriz de hallazgos (parte V).....	112
Tabla 20	Matriz de hallazgos (parte VI).....	113
Tabla 21	Matriz de hallazgos (parte VII).....	114

Lista de Figuras

Figura 1 Ventajas al aplicar las NIIF en las empresas	6
Figura 2 Errores y Fraudes ocasionados en los Sistemas de información....	8
Figura 3 Serie de delitos y fraudes.....	9
Figura 4 Tipos de fraudes que se analizan en el control interno	17
Figura 5 Evolución del control interno	18
Figura 6 Componente del control interno	19
Figura 7 Componentes de los tres modelos del informe COSO.....	22
Figura 8 Componentes del modelo de COSO 2017.....	23
Figura 9 Los principios del control COSO	24
Figura 10 Marco de Gestión del riesgo empresarial.....	25
Figura 11 Procesos de TI definidos dentro de los cuatro dominios de COBIT	28
Figura 12 Objetivos de control de alto nivel	29
Figura 13 PO9 - Evaluación de riesgos.....	30
Figura 14 AI2 - Software de aplicación.	31
Figura 15 Administración de cambios-AI 6.....	32
Figura 16 DS5 - Garantizar la seguridad de los sistemas	33
Figura 17 DS7 - Educación y entrenamiento de usuarios.	34
Figura 18 Administración de la configuración-DS 9	35
Figura 19 DS10 Administración de problemas e incidentes.....	36
Figura 20 DS11 Entrega de servicios y soporte: administración de datos. .	37

Figura 21 El triángulo del fraude	39
Figura 22 Formas de cometer un fraude	47
Figura 23 Esquema de fraude por corrupción	48
Figura 24 Mayores productoras de camarón acuícola 2021	55
Figura 25 Proporción del empleo por tamaño de las empresas y trabajadores autónomos	57
Figura 26 Modelo del SGSI de la norma	61
Figura 27 Estructura de los controles de la norma ISO 27002.....	63
Figura 28 Identificación de riesgos significativos	67
Figura 29 Participación (%) del # empresas dedicadas a la explotación de criaderos de camarones.	74
Figura 30 Participación (%) del # empresas dedicadas a la preparación y conservación de camarón y langostinos.	75
Figura 31 Venta al por mayor de camarón y langostinos.	76
Figura 32 Tipos de muestra	78
Figura 33 Esquema para la aplicación de la propuesta metodológica	120
Figura 34 Rúbrica de calificación de preguntas	121
Figura 35 Matriz de riesgos y su escala de calificación	122
Figura 36 Programa evaluación de riesgo I	123
Figura 37 Cuestionario evaluación de riesgo I	124
Figura 38 Programa evaluación de riesgos II.....	126
Figura 39 Cuestionario evaluación de riesgo II	127

Figura 40	Programa evaluación de riesgo III	129
Figura 41	Cuestionario evaluación de riesgo III	130
Figura 42	Programa evaluación de riesgo IV	132
Figura 43	Cuestionario evaluación de riesgo IV.....	133
Figura 44	Calificación de matriz de riesgo	135
Figura 45	Resultados automatizados.....	136
Figura 46	Mapa de calor	136
Figura 47	Plan acción- reducción de riesgo I	137
Figura 48	Plan acción- reducción de riesgo II y III	138
Figura 49	Plan acción- reducción de riesgo IV.....	139

Resumen

La metodología propuesta se basa en la Reducción de Riesgos en los accesos físico y lógico de los Sistemas de Información Contables, para prevenir errores y fraudes que se pueden presentar en las empresas PYMES del sector Acuícolas.

El trabajo investigado se fundamenta en las teorías de riesgos y controles interno para la mitigar los riesgos identificados o existentes.

Se realizó el enfoque de la investigación mediante datos cualitativas, aplicando herramienta para recolección de datos a través de entrevistas a profundidad, efectuada a seis expertos. Desarrollando en resumen los principales hallazgos, planteando las repuestas encontradas e identificando las similitudes y diferencias en una matriz.

Concluimos con la propuesta metodológica desarrollando un proceso de reducción de riesgo, mediante un esquema que consiste de cuatro etapas que son: (a) planificar el programa para evaluación de riesgo, (b) ejecutar cuestionarios, (c) supervisar los riesgos identificados mediante una matriz con mapa de calor, y (d) dar respuesta a los riesgos con acciones correctivas.

Palabras Claves: Riesgos, Sistemas de información, Errores, Fraudes, Control, Acceso físico, Acceso lógico.

Abstract

The proposed methodology is based on the Reduction of Risks in the physical and logical access of the Accounting Information Systems, to prevent errors and frauds that may occur in SMEs in the Aquaculture sector.

The researched work is based on risk theories and internal controls to mitigate identified or existing risks.

The research approach was carried out using qualitative data, applying a tool for data collection through in-depth interviews, carried out with six experts. Developing in summary the main findings, raising the answers found and identifying the similarities and differences in a matrix.

We conclude with the methodological proposal by developing a risk reduction process, through a scheme that consists of four stages that are: (a) plan the program for risk assessment, (b) execute questionnaires, (c) monitor the risks identified through a matrix with a heat map, and (d) respond to the risks with corrective actions.

Keywords: Risks, Information Systems, Errors, Fraud, Control, Physical Access, Logical Access

Introducción

Antecedente de la Investigación

La acuicultura es una actividad milenaria que ha evolucionado lentamente, sobre la base de conocimientos tradicionales, cuyos adelantos se han logrado gracias a la curiosidad, las necesidades, las experiencias positivas y los errores de los piscicultores. En consecuencia, se ha ido expandiendo durante épocas, integrada con su ambiente natural, social, económico y cultural. El resultado fue un crecimiento sin precedentes, que proporciona más de la mitad de los camarones y peces al mundo. (Organización de las Naciones Unidas para la alimentación y agricultura, 2021a, p. 1)

A nivel mundial, el camarón se ha cultivado durante varios años y actualmente ha logrado una producción aproximadamente en 50 países alrededor del mundo, aunque la industria camaronera se concentra en dos regiones principales como: las Américas y Asia. A continuación, se detalla la producción a nivel mundial del camarón cultivado (ver Tabla 1), de acuerdo con las encuestas *Global Aquaculture Alliance*¹ (GOAL) 2016 y 2017 y su respectivo desglose porcentual de las principales regiones productoras. (Darryl, 2018a)

La acuicultura está relacionado a los cultivos de los organismos acuáticos (vegetales y animales) entre los que se encuentran los peces, anfibios (rana toro), crustáceos, moluscos, algas y plantas acuáticas. Esta continúa convirtiéndose, a nivel mundial, en una actividad de la agroindustria incrementando su valor agregado, provenientes de mayores, medianas y pequeñas producciones. (Vila, 2013, p. 4)

¹ GOAL: Alianza Global Acuicultura, es una asociación comercial Internacional, sin fines de lucro, dedicada a promover la acuicultura responsable.

Tabla 1*Producción mundial estimada de camarón de cultivo*

Región	Producción 2016 (MT)	Mundial 2016	Producción 2017 (MT)	Mundial 2017
Sureste Asiático	1.483.935	36,6%	1.574.077	36,9%
China	1.352.762	33,4%	1.350.622	31,6%
India	438.579	10,8%	494.959	11,6%
Américas	701.200	17,3%	756.430	17,7%
MENA	53.796	1,3%	63.990	1,5%
Otros	25.419	0,6%	27.422	0,6%
Total	4.055.691	100%	4.267.500	100%

Nota: Tomado de “*La producción actual, desafíos y el futuro del cultivo del camarón*”, por Darryl, 2018.

Como resultado de la encuesta GOAL 2016 y 2017, la producción global en el 2016 fue de 4.055.690 toneladas métricas (MT), en el 2017 aumentó aproximadamente 5 por ciento a 4.267.500 toneladas métricas. Los países asiáticos (China, Tailandia, Vietnam, Indonesia, Malasia, Filipinas, India y Bangladesh, principalmente) representaron aproximadamente 3,42 millones de toneladas métricas (MT) o alrededor del 80,1 por ciento de la producción mundial en 2017. Las Américas (Ecuador México, Brasil, Venezuela, Honduras Nicaragua, Guatemala, Belice, Panamá, Perú y otros) producen alrededor de 756.430 TM o 17,7 por ciento; y el resto del mundo representó alrededor de 85.000 TM o aproximadamente el 2 por ciento del total. (Darryl, 2018a, p. 1)

La producción camaronera ecuatoriana da su comienzo en el año 1968, logrando su expansión industrial en 1970. Sin embargo, se conoce históricamente que la actividad camaronera ecuatoriana tiene aproximadamente 50 años de respaldo, alcanzando un trascendental desarrollo técnico productivo en lo referente al área de cultivo, comercialización y exportación de camarón. (Varela et al., 2017, pp. 1-6)

A continuación, se detalla en la siguiente Tabla 2, los principales países en el mundo que el Ecuador exporta camarón:

Tabla 2

Principales países del mundo donde el Ecuador exporta camarón

Países	2017	2018	2019	2020	2021
China	104.456.563	611.186.335	1.986.273.374	1.876.600.318	2.296.094.721
EE. UU.	467.269.640	453.119.972	446.920.954	634.497.130	1.187.959.191
España	218.158.139	214.361.159	206.446.398	243.371.437	320.952.650
Francia	181.377.614	189.001.875	186.094.589	189.664.194	273.347.957
Italia	141.562.058	154.429.256	141.335.769	120.960.768	159.795.004
Total	1.112.824.014	1.622.098.598	2.967.071.084	3.065.093.847	4.238.149.523

Nota: Adaptado de “*Revista de estadística de reporte de exportaciones Ecuador*”, por Cámara Nacional de Acuicultura, 2022.

Según Rivera (2018) en su estudio de análisis de oferta y demanda de camarón concluyó que “el camarón ecuatoriano es considerado como un destacado producto de consumo, con ciertas particularidades desde su proceso de siembra, desarrollo y cosecha, contando con una alta calidad de trazabilidad que lo ubica en el segundo productor y exportador de camarón” (p. 15).

El sector acuícola ha permitido crear numerosas plazas de empleos, ayudando a la economía de los ecuatorianos. Durante el año 2020, existieron 1.057 empresas dedicadas a la explotación de criaderos de larvas de camarón, donde el 55 por ciento se encuentran ubicada en la provincia del Guayas dando paso así a generar 40.257 empleos (ver Tabla 3). (Corporación Financiera Nacional, 2021)

Tabla 3

Número de empresas y empleados según el tamaño de la organización

Tamaño de Empresa	# Empresa 2020	# Empleados
Grande	75	28.833
Mediana	214	5.767
Pequeña	356	3.718
Microempresa	405	1.939
No definido	7	0
Total	1057	40.257

Nota: Tomado de “*Ficha Sectorial del Camarón*” por Corporación Financiera Nacional (CFN), 2021.

Contextualización del Problema

Antecedentes del Problema

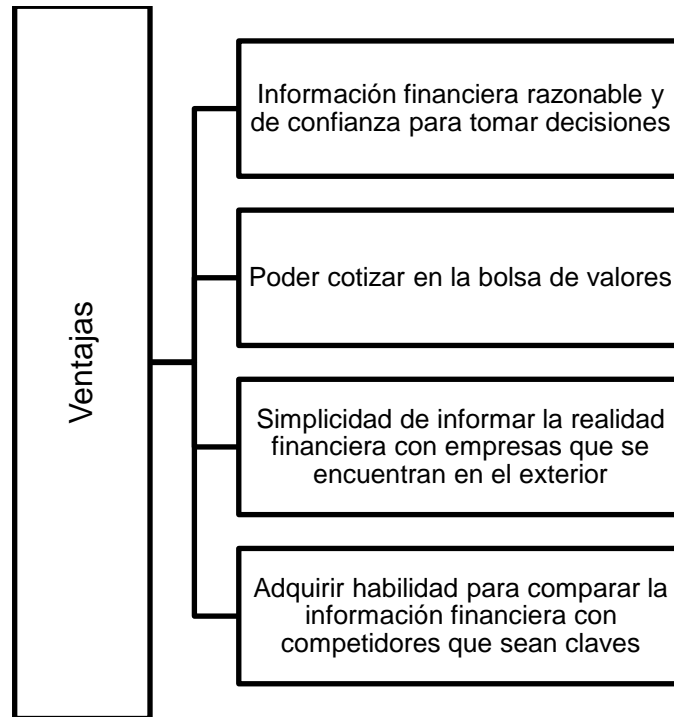
En Ecuador el Superintendente de Compañía durante el año 2006, en la Resolución No. 06.Q.ICI.004, publicada en el Registro Oficial N°348; indicó adoptar las Normas Internacionales de Información Financiera (NIIF) y que estas sean aplicadas con carácter obligatorio en todas las empresas que están siendo reguladas por la Superintendencia de Compañías (SUPERCIAS) desde el primero de enero del 2009, derogando de tal forma las Normas Ecuatorianas de Contabilidad (NEC). (Superintendencia de Compañías, 2008)

Barberán (2017) determinó que el objetivo de poder adoptar las NIIF es presentar los estados financieros en un respectivo lenguaje mundial, de tal forma que los usuarios puedan entender, interpretar y analizar la información financiera de una organización empresarial para que puedan tomar decisiones, considerando una misma base y así armonizar cada uno de los principios que rige la contabilidad a nivel mundial.

Por lo tanto, al aplicar las NIIF en las empresas de Ecuador se evidencio diferentes ventajas, de las cuales detallamos en la Figura 1. (IAASB, 2022)

Figura 1

Ventajas al aplicar las NIIF en las empresas



Nota: Adaptado de “*Normas Internacionales de Información Financiera*” por Deloitte, 2022.

La aplicación de las NIIF en Ecuador sirvió de gran apoyo a los entes reguladores, para que estos puedan tener control sobre la información que presentan las empresas de forma anual. Para su adopción llevó a las empresas a que apliquen diferentes estrategias y a diseñar un programa donde incluye lo siguiente: (a) modificación de manuales y políticas contables, (b) determinar debilidades y deficiencias de los sistemas de información que presentan las organizaciones empresariales, (c) proceder a actualizar y cambiar procesos del sistema de información existentes, ajustando a las necesidades de la información, y (d) diseñar e implementar estrategias para conformar nuevos procesos en los sistemas de información. (Barberán, 2017)

Toda la información que actualmente se maneja en la contabilidad es originada mediante una aplicación de tecnología de información (TI), la cual es un conjunto de programas de cómputo que son utilizados en una empresa para poder ingresar información y generar transacciones. Además, existe

información que es procesada en hojas de Excel y dicha información debe ser evaluada; es aquí cuando se origina la importancia de validar la información producida por las entidades (IPE). (Barberán, 2017)

Los principales riesgos que se pueden presentar en la IPE son los siguientes: (a) los datos que son procesados por las aplicaciones de TI en donde la IPE los desarrolla y produce dichos datos no son íntegros ni tampoco exactos. (b) los datos que se extraen de la aplicación TI y que se convierten a IPE no suelen ser los datos correctos o no se encuentran completos. (c) los datos que proceden los usuarios a ingresar son inapropiados. (d) los cálculos que son realizados en la creación de la IPE no suelen ser exactos o íntegros. (e) los datos que son entregados por la aplicación a la herramienta de cómputo de los respectivos usuarios finales suelen modificarse o se pierden cuando estos son transferidos. (Barberán, 2017)

Definición del Problema

En Centro América, el Consejo Superior de la Empresa Privada (COSEP) y la Organización Internacional del Trabajo (OIT), realizaron una encuesta en Nicaragua en el 2015 sobre las empresas sostenibles que llevan una contabilidad formal, como resultado de dicha encuesta se obtiene lo siguiente: el 58,6% de las empresas emplean alguna formalidad contable, ya sea que hayan anotado en un cuaderno o realizando cuentas sin tener un correcto registro. El 36,8% de las empresas encuestadas no realizan ningún control contable. Y el 4,6% se detallan a las empresas que tienen contabilidad formal en Nicaragua. (Bejarano, 2017)

Bejarano (2017) indicó que normalmente las pequeñas y medianas empresas no poseen registros contables, porque no conocen mucho del tema de la contabilidad. Algunos empresarios aplazan la implementación de un sistema contable y evitan el gasto de la contratación de un contador, lo cual al no buscar estos métodos les podría generar muchas pérdidas económicas.

Algunas organizaciones siguen utilizando los sistemas clásicos de costeo, desarrollados a partir de la revolución industrial, negándose a tener la oportunidad de participar en la nueva dinámica empresarial

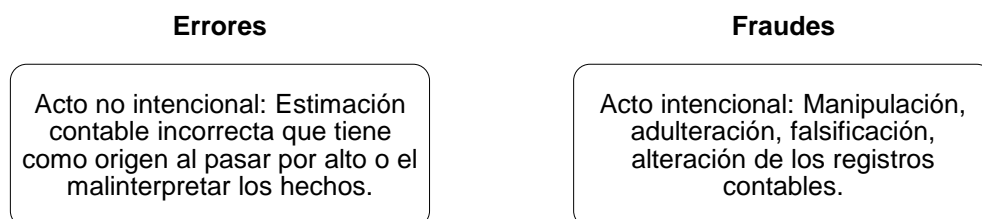
contemporánea, quedando rezagadas a un panorama de participación en mercados locales, poca competitividad, sin innovación, destinados a salir de la competencia. (Buelvas & Mejía, 2014, p. 2)

Los entes reguladores como el Servicio de Rentas Internas y la Superintendencia de Compañía recomiendan que la contabilidad sea manejada bajo herramientas eficaz y fácil de operar para su correcta interpretación y desarrollo. Las empresas que cuentan con sistemas de información contables y son manejados directamente o por terceras personas, desarrollan y mejoran su entorno comercial, alcanzando una mayor posibilidad de financiamiento y a su vez cumplir con la respectiva legislación fiscal y laboral. (Bejarano, 2017)

Los problemas que se suscitan en el proceso del acceso físico y lógico en los sistemas de información contable pueden ocasionar riesgo como errores y fraudes, siendo este el acto no intencional o intencional (ver Figura 2), que realizan los usuarios internos: empleados, personal administrativo y directivos de la empresa a base de engaño y manipulación de la información registrada para obtener ventajas injusta o ilegal. A veces creemos que las amenazas de fraudes y seguridad en una empresa está relacionada con personas externas, sin darnos cuenta de que también son los trabajadores internos que representan un peligro en la seguridad, ya que ellos tienen el acceso a la información privilegiada, y al haber procedimientos de seguridad interna descuidados, pueden manejar la información para su propio beneficio personal sin dejar rastro. (Crespo, 2009)

Figura 2

Errores y Fraudes ocasionados en los Sistemas de información

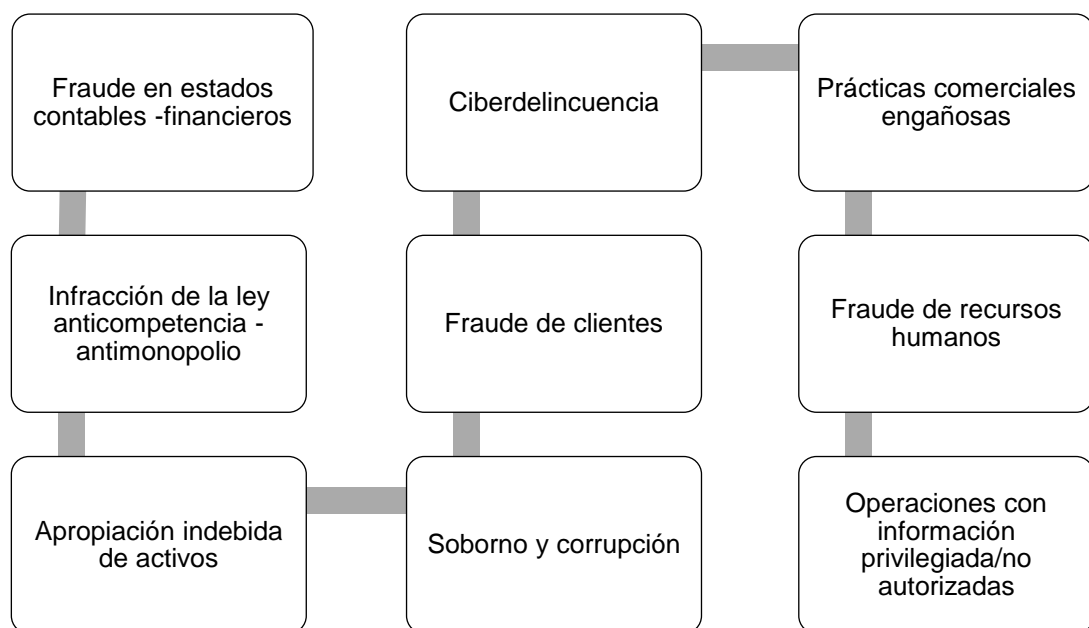


Nota: Adaptado de “*Ranking Empresarial 2022*” por Superintendencia De Compañías, Valores y Seguros, 2022.

Mediante la encuesta *Global Economic* que realizó *PriceWaterHouseCoopers (PwC's)* sobre los fraudes y delitos económicos en el año 2022, investigó las actitudes de las organizaciones hacia los delitos: financieros, económicos y el fraude en el entorno actual; recopilando respuestas de 1.296 encuestados en 53 países y regiones. Esta encuesta se centró en las tendencias de fraude y el riesgo de conducta. Durante más de 20 años *Global Economic* ha recopilado por medio de encuestas unas series de delitos y fraudes, concluyendo en la Figura 3 los delitos que se han cometido con mayor frecuencia. (*PricewaterhouseCoopers, 2022*)

Figura 3

Serie de delitos y fraudes



Nota: Adaptado de “*Encuesta mundial sobre fraude y delitos económicos*”, por *PriceWaterHouseCoopers (PwC's)*, 2022.

En la encuesta mundial sobre fraude y delitos económicos de PwC's concluyó que los mayores riesgos en las organizaciones de todos los tamaños son: el delito cibernético que ocupa el primer lugar ya que este representa la mayor amenaza, seguido por el fraude del cliente y en el tercer lugar la apropiación indebida de activos. (PwC's, 2022)

A continuación, según la Tabla 4 se detalla los tipos de fraudes experimentados por tamaño de las organizaciones en ingresos globales:

Tabla 4

Tipos de fraudes experimentados por tamaño de las organizaciones (en ingresos globales)

Por tamaño de organización (en ingresos globales)	Tipos de Fraudes Experimentados		
	Ciberdelincuencia	Fraudes al cliente	Apropiación indebida de los activos
Menos de 100 millones	32%	27%	23%
US \$100 -\$1 mil millones	41%	32%	23%
US \$1 mil millones - \$ 10 mil millones	42%	34%	24%
Más de US \$10 mil millones	35%	32%	31%

Nota: Adaptado de “Encuesta mundial sobre fraude y delitos económicos”, por PriceWaterHouseCoopers (PwC’s), 2022

Los fraudes en tiempo de recesión, como la pandemia, han creado una vulnerabilidad preocupante a medida que las organizaciones aceleraron el cambio a las operaciones digitales. Un punto positivo es que la apropiación indebida de activos es una de las principales categorías de fraude, la misma que disminuyó en los 24 meses; en parte esto se debe, porque ahora hay más empleados que trabajan de forma remota y con un acceso limitado a los activos de la empresa. (PwC’s, 2022)

Las recesiones pasadas, como la de los años 2007 al 2009, ofrecen lecciones valiosas para las organizaciones empresariales que navegan por la volatilidad a medida que comienzan a salir de la pandemia. La historia muestra que las tendencias de fraude en tiempos de turbulencia no surgen de inmediato. A menudo, se necesitan de 18 a 24 meses para que estos eventos se conviertan en conocido. Sin embargo, los puntos de inflexión, como el cambio de una economía en contracción a una en expansión, pueden ser faros para la identificación del fraude interno. Gran parte del fraude interno puede volverse visible en tiempos de transición porque el comportamiento del defraudador retrasa el cambio hacia nuevas metas y objetivos. (PwC’s, 2022, p. 7)

Los cambios en los sistemas de información han ayudado a las organizaciones a fortalecerse contra el fraude y otros delitos económicos. Particularmente, implementando políticas, procedimientos y capacitación ayudando a los empleados que desean hacer lo correcto. La encuesta afirma que las organizaciones están trabajando arduamente en mejorar las capacidades técnicas e implementar controles internos más sólidos. (PwC's, 2022)

Justificación de la Investigación

Este trabajo de titulación en el ámbito social será usado como material de consulta para auditores. A tener conocimiento sobre la metodología que se llevará a cabo, mediante la investigación sobre la reducción de riesgos en el acceso físico y lógico de los sistemas de información contables.

En la aplicación práctica, la propuesta metodológica será de gran beneficio para los gerentes, directivos y empresarios de empresas del sector acuícola. La cual, servirá como un manual de procedimiento para la reducción de riesgos en el acceso físico y lógico de los sistemas contables, logrando en los Estados Financieros una imagen fiel y de confianza.

En el ámbito académico esta propuesta metodológica serviría como un caso de estudio aplicado a los estudiantes de la carrera de contabilidad y auditoría, donde podrán visualizar procedimientos para la reducción de riesgos en el acceso físico y lógico de los sistemas de información contable, con la finalidad de prevenir fraudes y errores.

Objetivos

Objetivo General

Proponer una metodología para la reducción de riesgos en el acceso físico y lógico de los sistemas de información contable, para prevenir los errores y fraudes de empresas del sector acuícola de la provincia del Guayas.

Objetivos Específicos

1. Conocer los aspectos positivos, negativos de la parte interna y externa de los sistemas de información contable, apoyándonos por medio de un análisis de FODA.
2. Analizar los errores y fraudes en el acceso físico y lógico de los sistemas de información contable.
3. Diagnosticar los controles para la implementación de la metodología en la reducción de riesgos.
4. Establecer recomendaciones para la reducción de riesgos y recomendarlo como modelo de mejoramiento.

Preguntas de Investigación

General

¿Qué eventos incrementan el riesgo de acceso físico y lógico en los sistemas de información contable en el sector acuícola del Guayas, Guayaquil en 2022?

Específicas

¿Qué tipo de errores y de situaciones de fraudes se pueden presentar en el acceso físico y lógico de los sistemas de información contable en el sector acuícola del Guayas, Guayaquil en 2022?

¿Qué opinan los usuarios sobre las medidas de control para reducir el riesgo de acceso físico y lógico a los sistemas de información contable en el sector acuícola del Guayas, Guayaquil en 2022?

¿Qué opinan los expertos sobre las medidas de control para reducir el riesgo de acceso físico y lógico a los sistemas de información contable en el sector acuícola del Guayas, Guayaquil en 2022?

Delimitación

Tema: Reducción de riesgos en el acceso físico y lógico de los sistemas de información contable.

Problemática: Casos de errores y fraudes que se presentan en el acceso físico y lógico de los sistemas de información contable.

Población de estudio: Sector acuícola – camaronero.

Tamaño de Empresas: PYMES

Lugar (ciudad) de estudio: Provincia del Guayas – Cantón Guayaquil – Ciudad Guayaquil - Parroquia Tenguel.

Año de estudio: 2022.

Duración de la investigación: 16 semanas.

Limitación

Carencia de estudio de información comparativa, sobre los errores y fraudes que se comenten en los sistemas de información contable en compañías y sectores del Ecuador.

Falta de datos estadísticos disponibles y confiables.

Acceso denegado y limitado al investigar los errores y fraudes en el acceso físico y lógico de los sistemas de información contable que tiene el sector acuícola del Guayas, Guayaquil.

La movilización y la ejecución con el trabajo de campo para recolectar datos de fuentes primarias.

Capítulo 1: Fundamentación Teórica

Marco Teórico

Riesgos de Sistemas

Domínguez (2015) definió al riesgo como “la probabilidad que una eventualidad se aproveche de las vulnerabilidades de un sistema e imposibilite el cumplimiento de su objetivo o ponga en peligro los activos de la organización, ocasionándole daños o pérdidas” (p. 20).

En los Sistemas de Información según Montero (2016) indicó que los riesgos son: Oportunidades económicas originadas por errores o usos inadecuados de los sistemas informáticos y la tecnologías afines. Estos problemas afectan al desempeño, actividades y los servicios que brinda una institución financiera al poner en peligro la disponibilidad, integridad y confiabilidad de la información. Los riesgos sistemáticos incluyen software, equipos, infraestructura, sistema de respaldo, sistemas de seguridad, medios de comunicación, usuarios, capacitación, complejidad, profesionales de TI, gestión gerencial, capacidad económica de la institución financiera y la ocurrencia de eventos adversos externos. La gestión sistemática de riesgo tiene por objetivo reducir el riesgo, disminuir la probabilidad de ocurrencia y minimizar sus consecuencias. Algunos de los riesgos pueden mitigarse mediante planes de contingencia rigurosos y estricto de sistemas de seguridad.(p.24) En conclusión, los riesgos en los sistemas informáticos son cualquier tipo de debilidad o vulnerabilidad que podría potencialmente conducir a la pérdida de datos, accesos no autorizados, violación de la integridad y fallas del sistema.

El sistema de información (SI) es el estudio y uso del sistema para procesar datos de entrada para generar información que es esencial y útil para la gestión de operaciones. La tecnología de la información (TI) es básicamente el estudio y uso del sistema para establecer una comunicación más rápida, mantener el almacenamiento electrónico y brindar protección a los registros comerciales o de la empresa.

Según Hacknoid (2019) mencionó que existen muchas razones por las cuales los riesgos en la tecnología de información (TI) que pueden causar problemas en una empresa, los más comunes son:

- Error Humano, Personal TI sin experiencia. Estos errores pueden ser caudado por una mala programación o gestión de los recursos.
- Incidentes, Desastres y Robos a Nivel de Hardware. Desde destrucción accidental de pendrive con información importante hasta hurtos y desastres naturales y,
- Intrusiones y Amenazas a Nivel de Software. Los ataques cibernéticos, las intrusiones de terceros no autorizados en los sistemas de información de la empresa o los actos de malware pueden ocasionar daños irreparables. (p. 1)

Todos estos casos generan problemas a nivel de producción y optimización, afectando la eficiencia de las organizaciones empresariales.

Teorías de Riesgos

De acuerdo a Brito (2018) el riesgo estuvo ligado a la “incertidumbre sobre eventos difícil de eliminarlo. La única forma de enfrentarlo es administrándolo, distinguiendo las fuentes de donde proviene, midiendo el grado de exposición y eligiendo las mejores estrategias disponibles para controlarlo y conocer los grados de vulnerabilidad que se posee” (p. 271).

Teoría de riesgo según Luhmann (2006) indicó que el riesgo depende de reconocer el daño (posibles o efectivamente decididos), se entiende como la posibilidad de daño digno de atención, mientras que peligro se entiende como resultado de una decisión tomada en el sistema. Solo se procede indicar el riesgo en el caso de que el daño se hace posible como consecuencia de una decisión tomada y que este no puede acontecer sin que si hubiera tomado tal decisión. (p. 106)

La teoría del Riesgo SP/A (Seguridad-Potencial/Aspiración) de Lopes (1987) se trató de una teoría psicológica de tipo descriptiva de cómo los individuos valúan el riesgo, que se posiciona en dos criterios. Un primer criterio es (SA), donde S representa la seguridad y P el potencial; la preocupación se centra en S vs P. Es decir, cómo las personas se enfocan en resultados muy buenos y resultados muy malos, dependiendo de su motivación por la seguridad, donde las emociones pesan más que el miedo. El segundo criterio, sobre la base de A, se relaciona con el grado de aspiración para lograr la meta. López argumenta que los individuos buscan maximizar el criterio SP en su enfoque para calcular el riesgo, pero también buscan maximizar la probabilidad de lograr su nivel de ambición. Por ejemplo, una persona con aversión al riesgo que tiene que elegir entre un retorno seguro y un retorno aleatorio y que busca "ganar algo" estaría en el lado seguro, prefiriendo S sobre P, porque esta decisión corresponde al nivel de ambición A, aunque podría haber ganado más dinero con la otra opción. (Pascale, 2013, p. 14)

En conclusión, todo riesgo tiene una cantidad y calidad, este tipo de clasificación es el resultado de la identificación de la cualidad del riesgo, los valores que se transforman en pérdida. Por lo tanto, el riesgo tiene un carácter natural y otro concreto, el primero se da cuando se reconoce que todo está sujeto a cierto riesgo y el segundo el riesgo ya está identificado.

Teoría Control Interno

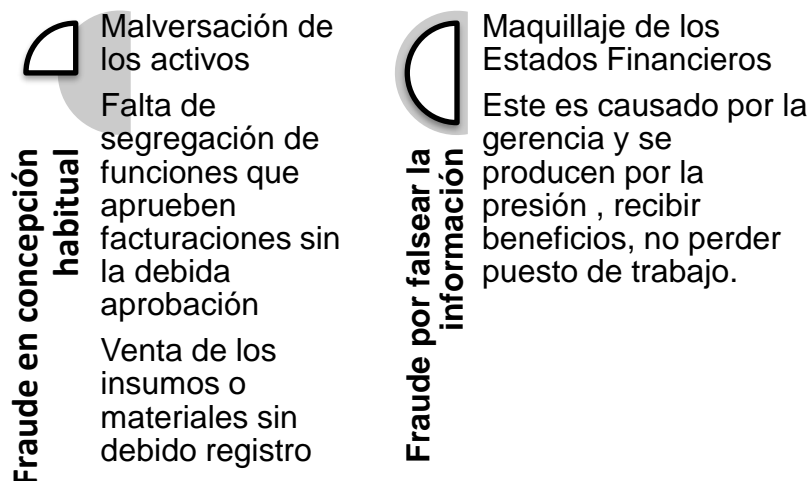
Debido a la corrupción y fraudes que se han detectados en las entidades en los últimos años se ha hecho fundamental la implementación de controles interno en las empresas. El control interno se lo puede relacionar a una serie de reglas y procedimientos que se implementan en una organización buscando la operatividad y transparencia del negocio. Vilorio (2005) definió al sistema de control interno como "plan de organización, métodos coordinados y medidas adoptadas en el negocio, para proteger activos. Verificar la precisión y confiabilidad de sus datos contables, mejorar la eficiencia en las

operaciones y estimular la adhesión a la práctica ordenada por la gerencia” (p. 88).

Para el autor Royo (2013) indicó que “la probabilidad de que exista fraude en la organización es alta, por tal motivo se debe aplicar sistemas de control interno para prevención y detección de lo mismo” (p. 25). A continuación, en la siguiente Figura 4 se muestra los fraudes que se deben controlar:

Figura 4

Tipos de fraudes que se analizan en el control interno



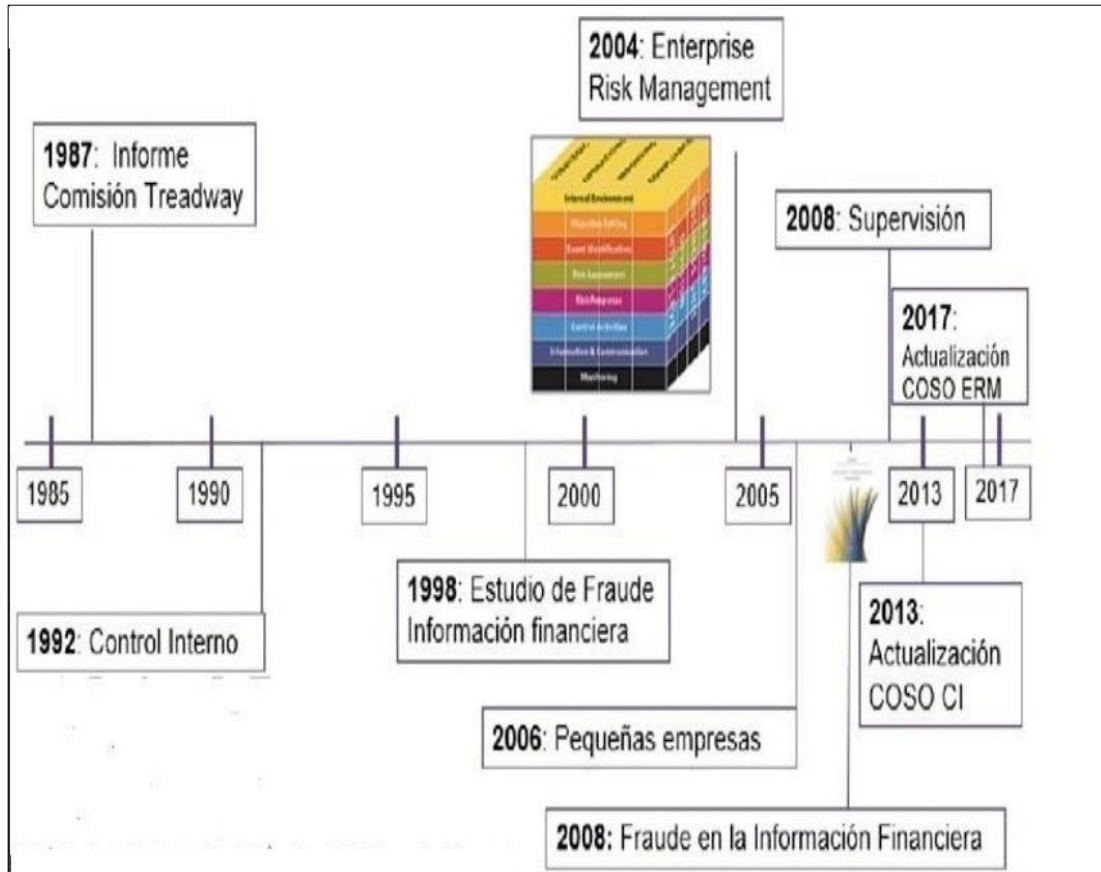
Nota: Adaptado de “Manual práctico de control interno”, por Royo, 2013.

El control interno comenzó a formarse como concepto a mitad del siglo XX, convirtiéndose en un elemento esencial en la marcha de la empresa en Estados Unidos debido a las crisis que atravesaban en los sistemas financieros. En los años 80 la comisión *Treadway*² realizó una investigación sobre las causas de presentación de informes financieros fraudulentos elaborando un reporte de guía destinado a todas las empresas y en especial a las compañías reguladas por la Comisión de Mercados y valores de Estados Unidos (SEC). Un tiempo después en la década de los 90 donde el control interno se posicionó como modelos de estudios que se podrán ver en la Figura 5. (Luna, 2013)

² El Comité de Organizaciones Patrocinadoras de la Comisión Treadway es una iniciativa conjunta para combatir el fraude corporativo

Figura 5

Evolución del control interno



Nota: Tomado de “Implementación y Evaluación de Control Interno los 17 principios de COSO”, por Badillo, 2017.

Podemos concluir que el control interno es de gran utilidad para la empresa, gerentes, personal, socios y en especial para la junta directiva, diseñando un proceso que garantizará la seguridad razonable, la efectividad y eficiencia en la operación, confiabilidad en la presentación de la información financiera y el cumplimiento de las leyes, alcanzado los objetivos planteados por la empresa. Además, nos ayudará a prevenir riesgos, evaluarlos e identificarlos, proponiendo controles para mitigarlos.

Desde el inicio de la aplicación de controles, se llevó la ardua tarea de revisiones minuciosa en los procesos administrativos de la compañía, y para esto se desarrolló cinco componentes que trabajan de forma multidireccional y permanente, influyendo el uno del otro (ver Figura 6), que conforman un sistema integrado que son los siguientes: (a) ambiente de control, (b) evaluación de riesgos, (c) actividades de control, (d) información y comunicación, y (e) supervisión. (Estupiñán, 2006)

Figura 6

Componente del control interno



Nota: Adaptado de “Control Interno y Fraudes con bases en los ciclos transaccionales”, por Estupiñán, 2006.

Entorno de Control. Estupiñán (1997) indicó que el entorno de control o ambiente de control “tiene una incidencia en la estructuración en el establecimiento de objetivos y en la evaluación de riesgos, así mismo influye en las actividades control y los sistemas de información, extendiendo su diseño del sistema en el funcionamiento diario” (p. 28). Por lo tanto, las empresas someten a sus empleados, colaboradores o directivos a un control eficaz, aumentando la integridad, desarrollando competencia y efectividad en el trabajo, logrando un alto estándar de la organización. “La eficacia del control interno no puede pesar más que la integridad de la dirección y el compromiso con los valores éticos, que son componentes esenciales de un entorno de control” (*Los Nuevos Conceptos del Control Interno*, 1997, p. 31).

Evaluación de Riesgo. Estupiñán (2006) mencionó que la evaluación de riesgos “es la identificación y análisis de los riesgos relacionado con el logro de los objetivos y es la base para determinar cómo mejorar esos riesgos” (p. 29). La evaluación de riesgo ayudó desde su inicio en la toma de decisiones, encontrando los riesgos y la debida implementación del tratamiento. Por otra parte, se sugiere la comparación de los niveles de riesgos que se hayan detectado.

Actividades de Control. Rivas (2011) definió que los controles son “políticas y procedimientos que aseguran que se estén llevando a cabo las directrices administrativas, con el propósito de garantizar que las metas de la empresa se alcancen, y las revisiones del procesamiento de la información, verificación y autorización de las transacciones” (p. 124). En la actividad de control el proceso de la información se realizan controles en los datos introducidos en el ordenador comprobando de forma manual lo mismo. En esta actividad se revisa los controles de aplicaciones que evita que se introduzcan manualmente errores en el sistema, corrigiendo y detectándolo.

Información y Comunicación. “En el estudio de Modelos contemporáneo de control interno, este componente de control interno, se refiere a métodos utilizados para identificar, agregar, categorizar, registrar e informar sobre las actividades de una entidad y mantener las cuentas de activos asociadas” (Tóala et al., 2018, p. 295). Es necesario saber qué “los

sistemas de información en la compañía pequeña y medianas empresa identifican e informan las incidencias, actividades y condiciones externas relevantes, pero su eficacia depende de la capacidad de la dirección” (*Los Nuevos Conceptos del Control Interno: Informe COSO, 1997, p. 91*).

Monitoreo. Blas (2014) definió al monitoreo como un “proceso que evalúa la calidad del control en el tiempo y permite al sistema reaccionar en forma dinámica, cambiando cuando las circunstancias así lo requieran” (p. 1). Un monitoreo de control sirve como evaluaciones permanentes para determinar el cumplimiento de los objetivos fijados por la gerencia.

Modelo del COSO

Para Gonzáles (2021) el COSO se dedicó a “desarrollar marcos y orientaciones generales sobre el control interno, la gestión del riesgo empresarial, la prevención del fraude diseñados para mejorar el desempeño organizacional, la supervisión, y reducción de riesgo de fraude en las organizaciones” (p. 3). Es decir, este control fue diseñado para facilitar los procesos de evaluación y control mejorando el sistema.

En 1992 se unieron profesionales de firmas de auditoría, ex funcionario de bolsa de Nueva York, exdirectores ejecutivos de compañía, realizando un estudio más profundo sobre el control interno, desarrollaron un modelo teórico conocido como COSO, fundamentando tres objetivos: (a) operación, (b) cumplimiento y, (c) información; y cinco componentes de control (ver Figura 7): (a) ambiente de control, (b) evaluación del riesgo, (c) actividades de control, (d) información y, (e) monitoreo. (Habana, 2018, p. 273)

Figura 7

Componentes de los tres modelos del informe COSO

COSO 1	COSO 2	COSO 3
1. Ambiente de control 2. Evaluación de riesgos 3. Actividades de control 4. Información y comunicación 5. Supervisión	1. Ambiente de control: se refiere a los valores y la filosofía de la organización. Influye en la visión de los trabajadores ante los riesgos y sus actividades de control. 2. Establecimiento de objetivos: estratégicos, operativos, de información y de cumplimientos. 3. Identificación de eventos que pueden tener impacto en el cumplimiento de objetivos. 4. Evaluación de riesgos: identificación y análisis de los riesgos relevantes para la consecución de los objetivos. 5. Respuesta a los riesgos: determinación de acciones frente a los riesgos. 6. Actividades de control: políticas y procedimientos que aseguran que se llevan a cabo acciones contra los riesgos. 7. Información y comunicación: eficaz en contenido y tiempo para permitir a los trabajadores cumplir con sus responsabilidades. 8. Supervisión: para realizar el seguimiento de las actividades.	Entorno de control: Principio 1: demuestra compromiso con la integridad y los valores éticos. Principio 2: ejerce responsabilidad de supervisión. Principio 3: establece estructura, autoridad y responsabilidad. Principio 4: demuestra compromiso para la competencia. Principio 5: hace cumplir con la responsabilidad. Evaluación de riesgos: Principio 6: especifica objetivos relevantes. Principio 7: identifica y analiza los riesgos. Principio 8: evalúa el riesgo de fraude. Principio 9: identifica y analiza cambios importantes. Actividades de control: Principio 10: selecciona y desarrolla actividades de control. Principio 11: selecciona y desarrolla controles generales sobre tecnología. Principio 12: se implementa a través de políticas y procedimientos. Principio 13: usa información relevante. Sistemas de información: Principio 14: comunica internamente. Principio 15: comunica externamente. Supervisión del sistema de control-monitoreo: Principio 16: conduce evaluaciones continuas y/o independientes. Principio 17: evalúa y comunica deficiencias.

Nota: Tomado de “El control interno y sus herramientas de aplicación entre COSO y COCO”, por Habana, 2018.






Modelo de COSO 2017: Gestión de Riesgos Empresariales Integrado con Estrategia y Desempeño

Como hemos visto en el tema anterior el COSO es un modelo de control interno que ha venido desarrollándose desde 1992, siendo un modelo muy usado a nivel mundial debido a los fraudes que se han presentado en la empresa. El COSO ha venido actualizándose desde la primera vez que se publicó COSO I DE 1992, COSO II, actualizado en 2004, el COSO III en el 2013 y el COSO IV en 2017. Este modelo busca alcanzar los objetivos aplicando herramientas para prevenir el fraude en las empresas.

El COSO ERM 2017, proporciona un marco para consejos de administración y equipos de gestión de entidades de todos los tamaños. Este marco analiza el nivel actual de riesgo que existe en el curso normal de los negocios. Estuvo estructurado por cinco componentes (ver Figura 8) y 20 principios (ver Figura 9) que ayudan a la identificación, administración, documentación y mitigación de riesgos en el gobierno corporativo, además de ser considerado un medidor de desempeño. (Hirth et al., 2017)

Figura 8






Componentes del modelo de COSO 2017

 Gobierno y Cultura	El gobierno establece el tono de la organización, reforzando la importancia de, y estableciendo responsabilidades de supervisión, para la gestión de riesgos empresariales. La cultura se refiere a valores éticos, comportamientos deseados y comprensión del riesgo en la entidad.
 Estrategia y objetivos	Gestión de riesgos empresariales, estrategia y objetivos trabajan juntos en el proceso de planeación estratégica. El apetito al riesgo es definido y alineado con la estrategia; los objetivos de negocio ponen la estrategia en práctica mientras sirve para identificar, evaluar y responder a los riesgos.
 Desempeño	Riesgos que pueden afectar el logro de la estrategia y los objetivos de negocio pueden ser identificados y evaluados. Riesgos son priorizados por severidad y en el contexto del apetito al riesgo. La organización selecciona las respuestas al riesgo y toma el riesgo que ha asumido.
 Revisión	Para revisar el desempeño de la entidad, una organización puede considerar qué tan bien funcionan los componentes de gestión de riesgos empresariales a lo largo del tiempo a la luz de cambios sustanciales y qué revisiones se necesitan.
 Información, comunicación y reporte	La gestión de riesgos empresariales requiere un proceso continuo para obtener y compartir información necesaria, de fuentes internas y externas, que fluya en todas las direcciones y a través de toda la organización.

Nota: Tomado de “Gestión del riesgo empresarial”, por Hirth et al., 2017, p. 24.

Figura 9

Los principios del control COSO

 Gobierno y Cultura	 Estrategia y objetivos	 Desempeño	 Revisión	 Información, comunicación y reporte
<ol style="list-style-type: none"> 1. La Junta Directiva ejerce supervisión sobre los riesgos 2. Establece estructuras operativas 3. Define la cultura deseada 4. Demuestra compromiso con los valores éticos 5. Atrae, desarrolla y retiene individuos competentes. 	<ol style="list-style-type: none"> 6. Analiza el contexto empresarial 7. Define el apetito al riesgo 8. Evalúa estrategias alternativas 9. Formula los objetivos empresariales 	<ol style="list-style-type: none"> 10. Identifica riesgos 11. Evalúa la severidad de los riesgos 12. Prioriza los riesgos 13. Implementa las respuestas al riesgo 14. Desarrollar un portafolio de riesgos 	<ol style="list-style-type: none"> 15. Evalúa los cambios sustanciales 16. Revisa los riesgos y el desempeño 17. Propone mejoras en la gestión de riesgos empresariales 	<ol style="list-style-type: none"> 18. Aprovecha la información y la tecnología 19. Comunica los riesgos de información 20. Informes sobre riesgos, cultura y desempeño

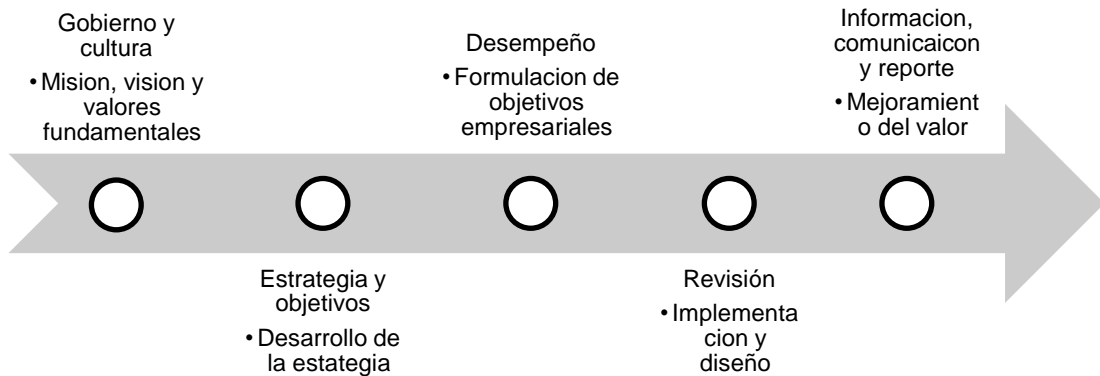
Nota: Tomado de “*COSO ERM 2017 y la Generación de Valor*”, por Hirth et al., 2017, p. 22.

Este modelo tiene gran importancia en la identificación de la metodología que se usará para controlar los riesgos, ayudando a documentar los riesgos desde la estrategia para que puedan ser medidos y establecer un medidor de desempeño para saber hasta dónde van los riesgos y cuál es el impacto que genera en el negocio. (*Isotools Excellence*, 2018, p. 1)

La gestión del riesgo empresarial, tal y como se ha venido practicando ha ayudado a muchas organizaciones a identificar, evaluar y gestionar los riesgos de la estrategia (ver Figura 10). Desde su publicación este marco se ha convertido a nivel mundial uno de los más utilizados en todos los sectores, organización, tamaño y tipo para identificar riesgos. La gestión del riesgo empresarial tiene que ver tanto con comprender las consecuencias resultantes de la estrategia y la posibilidad de que la estrategia esté desalineada como con gestionar los riesgos para establecer los objetivos. (Hirth et al., 2017, p. 9)

Figura 10

Marco de Gestión del riesgo empresarial



Nota: Adaptado de “*Gestión del riesgo empresarial*”, por Hirth et al., 2017, p. 22.

Se debe tener conocimiento de: (a) las clases de transacciones que son significantes, (b) forma en la cual las transacciones son iniciadas, registradas, procesadas, y reportadas, (c) los récords de contabilidad y los documentos soporte de cada transacción y, (d) los procesos de contabilidad involucrados, específicamente, aquellos procesos relacionados a la preparación de estados financieros incluidos estimados significantes.

En conclusión, en los errores y fraudes para su detección se aplicará una prevención a través de un riguroso sistema de control, donde los encargados será el auditor externo que para determinará los errores y fraude debe tener conocimientos del sistema de información de la organización.

Acceso Físico y Lógico de los Sistemas de Información Contable

Organization for Standardization (ISO) y Comisión Electrotécnica Internacional (IEC) (1999), forman el sistema especializado para la normalización mundial. Las mismas que fueron citadas por Crizón (2017) quien hizo la siguiente definición: La seguridad es la capacidad que tiene un producto de software para proteger los datos e información de manera que no pueda ser leído o modificado por personas no autorizadas, y el acceso no sea denegado a personal autorizado.

De acuerdo con Paz (2017) determinó que la seguridad se puede dividir en dos bloques principales que son:

Seguridad física y seguridad lógica. Para salvaguardar los activos de la empresa, uno no puede prescindir del otro, los dos son complementarios. De nada sirve controlar el acceso físico a las instalaciones para prevenir accidentes y proteger los activos, si se puede acceder cómodamente a la información confidencial de la empresa desde una computadora personal.

La seguridad física se encarga de la protección de los sistemas de una organización empresarial, frente a accesos no autorizados y ataques físicos sobre ordenadores, instalaciones, personal, documentación, etc. Consiste adicionalmente, en aplicar barreras físicas y procedimientos de control, tales como medidas preventivas y contramedidas, ante amenazas a recursos e información confidencial.

La seguridad lógica garantiza la seguridad a nivel de datos, permitiendo que solo las personas autorizadas accedan a la información. Esta lógica aplica mecanismos y barreras que mantengan a salvo la información de la organización desde su propio medio. A continuación, veremos algunos controles que pueden ser utilizados en la seguridad lógica:

- El acceso a ciertas aplicaciones, programas o archivos está restringido con claves o códigos de acceso.
- Menos privilegios otorgados a los usuarios del sistema informático. Es decir, sólo se otorga privilegios al personal que necesita para desempeñar sus actividades.
- Asegurarse de que los archivos, las aplicaciones y software utilizados dentro de la compañía se adapten a sus necesidades y se usan de manera adecuada por los empleados.
- Controlar que la información que entra o sale de la empresa es íntegra y sólo está disponible para los usuarios autorizados.(p. 71)

Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT)

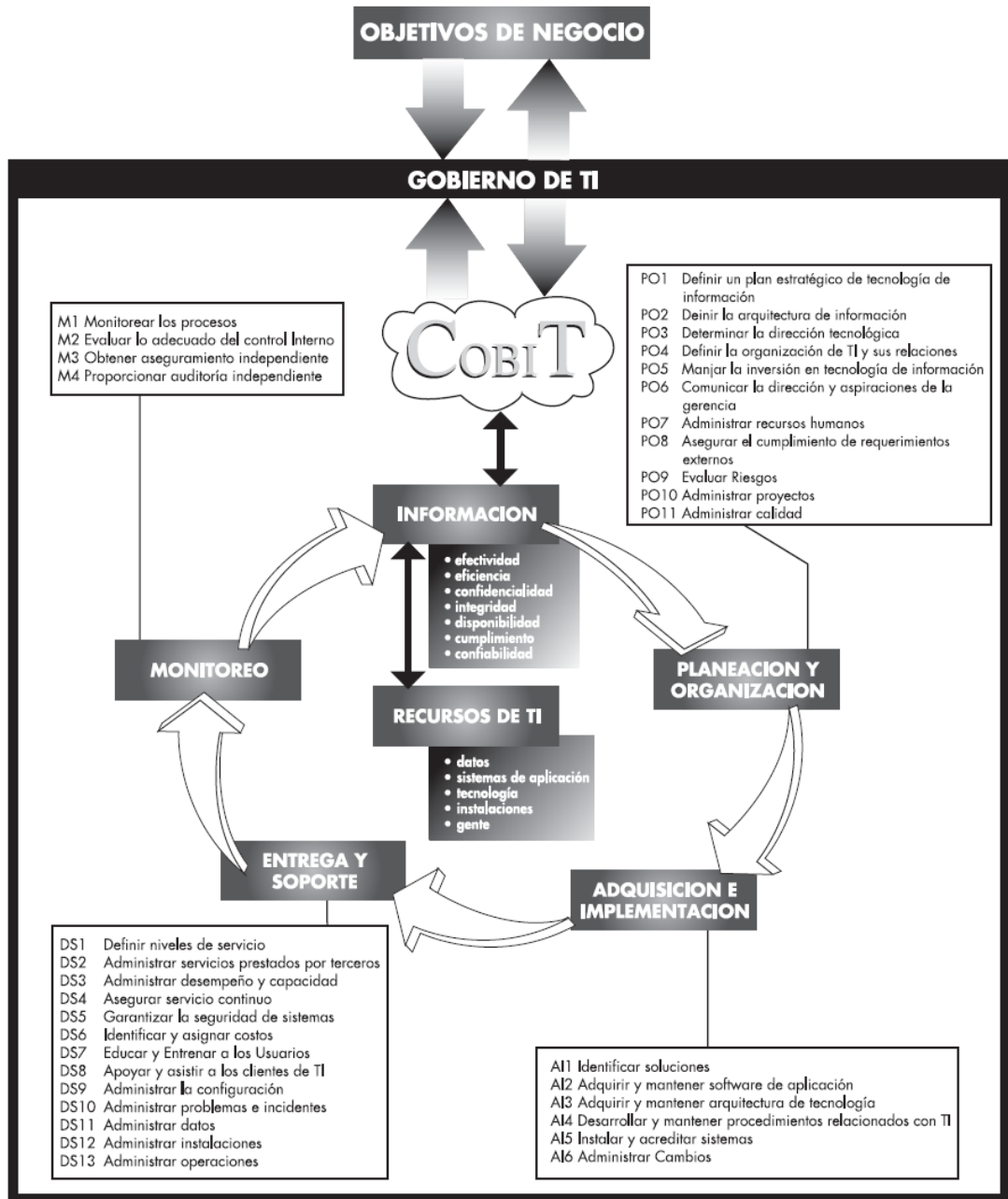
El COBIT conocido como objetivos de control para la información y tecnologías relacionadas, es una guía de auditoría que se ejecuta como control en los sistemas de información, creado en 1996 por un consorcio mundial de gobierno de Europa, Estados Unidos y Australia, concebido como un lenguaje inclusivo para otros marcos de trabajo en tecnología de la información, este incluye componentes de seguridad, calidad, eficacia y efectividad para identificar los riesgos, gestionar recursos y medir desempeño. Además, ha venido evolucionando de la siguiente manera: (a) COBIT 1 año 1996 Auditoría, (b) COBIT 2 año 1998 Control, (c) COBIT 3 año 2000 administración de gobierno (d) COBIT 2005/2007 Tecnología de la información, y (e) COBIT 2012 Gobierno TI de la empresa. (Aguilar, 2015)

Graterol y Hernández (2010) en su estudio de *Aplicación de la norma COBIT* en el monitoreo de transferencias electrónicas de datos contable-financiero indicaron lo siguiente:

La norma COBIT aparece como una posible alternativa factible y guía de acción para garantizar la calidad de los procesos de seguimiento, control, calidad y seguridad de los datos correspondientes a las operaciones contables. COBIT es la fusión entre prácticas de informática (ITIL, ISO/IEC17799) y prácticas de control (COSO), las cuales plantean tres tipos de requerimientos de negocio para la información: requerimientos de calidad (calidad, costo y entrega de servicio), requerimientos fiduciarios (efectividad y eficiencia de operaciones, confiabilidad de la información y cumplimiento de las leyes y regulaciones) y, por último, requerimientos de Seguridad (confidencialidad, integridad y disponibilidad). (p. 2)

Figura 11

Procesos de TI definidos dentro de los cuatro dominios de COBIT



Nota: Tomado de "COBIT Marco Referencial", por Comité Directivo de COBIT, 2002.

Figura 12

Objetivos de control de alto nivel

DOMINIO	PROCESO	Criterios de Información						Recursos de TI					
		efectividad	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad	recursos	sistemas de aplicación	tecnologías	instalaciones	datos
Planeación y Organización	PO1 Definir un plan estratégico de sistemas	P	S					✓	✓	✓	✓	✓	
	PO2 Definir la arquitectura de información	P	S	S	S				✓			✓	
	PO3 Determinar la dirección tecnológica	P	S							✓	✓		
	PO4 Definir la organización de TI y sus relaciones	P	S						✓				
	PO5 Administrar las inversiones (en TI)	P	P				S		✓	✓	✓	✓	
	PO6 Comunicar los objetivos y aspiraciones de la gerencia	P				S			✓				
	PO7 Administrar los recursos humanos	P	P						✓				
	PO8 Asegurar el cumplimiento de requerimientos externos	P				P	S		✓	✓		✓	
	PO9 Evaluar riesgos	P	S	P	P	P	S	S	✓	✓	✓	✓	✓
	PO10 Administrar proyectos	P	P						✓	✓	✓	✓	
	PO11 Administrar calidad	P	P	P			S		✓	✓	✓	✓	
Adquisición e Implementación	AI1 Identificar soluciones de automatización	P	S						✓	✓	✓		
	AI2 Adquirir y mantener software de aplicación	P	P		S	S	S		✓				
	AI3 Adquirir y mantener la arquitectura tecnológica	P	P		S					✓			
	AI4 Desarrollar y mantener procedimientos	P	P		S	S	S		✓	✓	✓	✓	
	AI5 Instalar y acreditar sistemas de información	P			S	S			✓	✓	✓	✓	✓
	AI6 Administrar cambios	P	P	P	P		S		✓	✓	✓	✓	✓
Entrega de Servicios y Soporte	DS1 Definir niveles de servicio	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
	DS2 Administrar servicios de terceros	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
	DS3 Administrar desempeño y capacidad	P	P		S					✓	✓	✓	
	DS4 Asegurar continuidad de servicio	P	S			P			✓	✓	✓	✓	✓
	DS5 Garantizar la seguridad de sistemas			P	P	S	S	S	✓	✓	✓	✓	✓
	DS6 Identificar y asignar costos		P					P	✓	✓	✓	✓	✓
	DS7 Educar y capacitar a usuarios	P	S						✓				
	DS8 Apoyar y orientar a clientes	P	P						✓	✓			
	DS9 Administrar la configuración	P				S	S			✓	✓	✓	
	DS10 Administrar problemas e incidentes	P	P			S			✓	✓	✓	✓	✓
	DS11 Administrar la información				P			P					✓
	DS12 Administrar las instalaciones				P	P					✓		
	DS13 Administrar la operación	P	P	S	S				✓	✓	✓	✓	✓
Monitoreo	M1 Monitorear el proceso	P	S	S	S	S	S	S	✓	✓	✓	✓	✓
	M2 Evaluar lo adecuado del control interno	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
	M3 Obtener aseguramiento independiente	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
	M4 Proporcionar auditoría independiente	P	P	S	S	S	S	S	✓	✓	✓	✓	✓

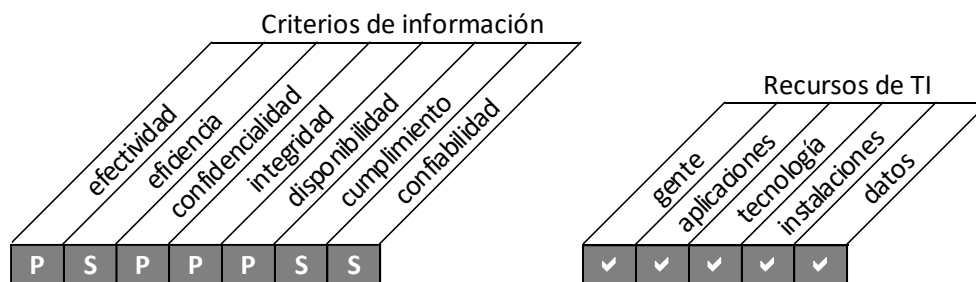
Nota: Tomado de “*COBIT Marco Referencial*”, por Comité Directivo de COBIT, 2002.

PO9 Planeación y Organización: Evaluación de Riesgos. El control sobre el proceso de TI, en la Evaluación de Riesgos tiene requerimientos que satisface a las empresas, como dar soporte a las decisiones de la gerencia a través del logro de los objetivos y responder a las amenazas reduciendo su complejidad. Esto se hace posible a través de la participación de la propia organización en la identificación de riesgos y en el análisis de impacto, involucrando funciones multidisciplinarias y tomando medidas costo-efectivas para mitigar riesgos.

Toman en consideración: (a) administración de riesgos de la propiedad y del registro de las operaciones, (b) diferentes tipos de riesgos de TI (por ejemplo: tecnológicos, de seguridad, de continuidad, regulatorios, etc.), (c) definir y comunicar un perfil tolerable de riesgos, (d) análisis de las causas sesiones de tormenta de ideas sobre riesgos, (e) medición cuantitativa de los riesgos, (f) metodología de análisis de riesgos, (g) plan de acción contra los riesgos y, (h) volver a realizar análisis oportunos. (Comité Directivo de COBIT, 2002, p. 34)

Figura 13

PO9 - Evaluación de riesgos.



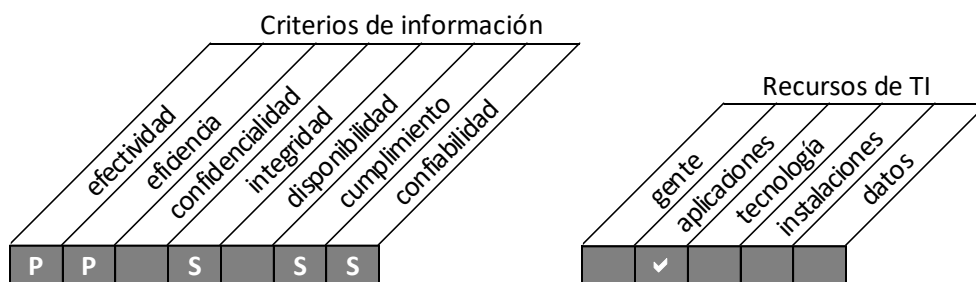
Nota: Tomado de “COBIT Marco Referencial”, por Comité Directivo de COBIT, 2002.

A12 Adquisición e Implementación: Software de Aplicación. El control sobre el proceso de TI, de la Adquisición y Mantenimiento del Software de Aplicación, tiene los siguientes requerimientos que satisface a las empresas como el de proporcionar funciones automatizadas que resistan efectivamente los procesos del negocio. Esto se hace posible a través de la definición de declaraciones específicas sobre requerimientos funcionales y operacionales y una implementación estructurada con entregables claros.

Toman en consideración: (a) pruebas funcionales y de aceptación, (b) controles de aplicación y requerimientos de seguridad, (c) requerimientos de documentación, (d) ciclo de vida del software de aplicación, (e) arquitectura en la información empresarial, (f) metodología para el ciclo de vida de desarrollo del sistema (g) interfase usuario-maquina, (h) personalización de paquetes. (Comité Directivo de COBIT, 2002, p. 38)

Figura 14

A12 - Software de aplicación.



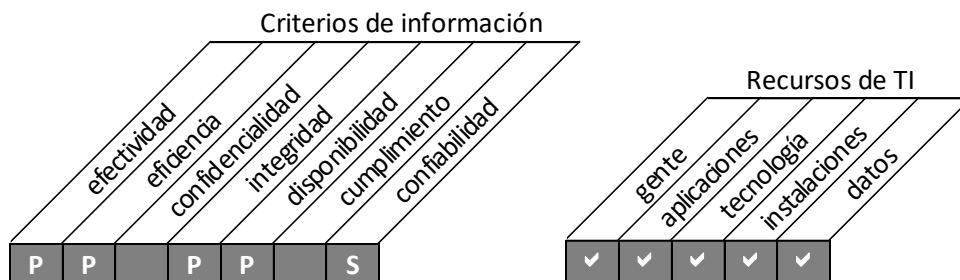
Nota: Tomado de "COBIT Marco Referencial", por Comité Directivo de COBIT, 2002.

AI6 Adquisición e Implementación: Administración de Cambios. El control sobre el proceso de TI, de la Administración de Cambios, tiene los siguientes requerimientos que satisface a las empresas como el minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores. Esto es posible gracias al sistema de gestión que permite el análisis, implementación y seguimiento de todos los cambios necesarios e implementados en la infraestructura de TI existente.

Toman en consideración: (a) identificación de cambios, (b) procedimientos de categorización, priorización y emergencia, (c) análisis de impacto, (d) autorización de cambios, (e) administración de la liberación del cambio, (f) distribución del software, (g) uso de herramientas automatizadas, (h) administración de la configuración, (i) rediseño del proceso del negocio. (Comité Directivo de COBIT, 2002, p. 42)

Figura 15

Administración de cambios-AI 6



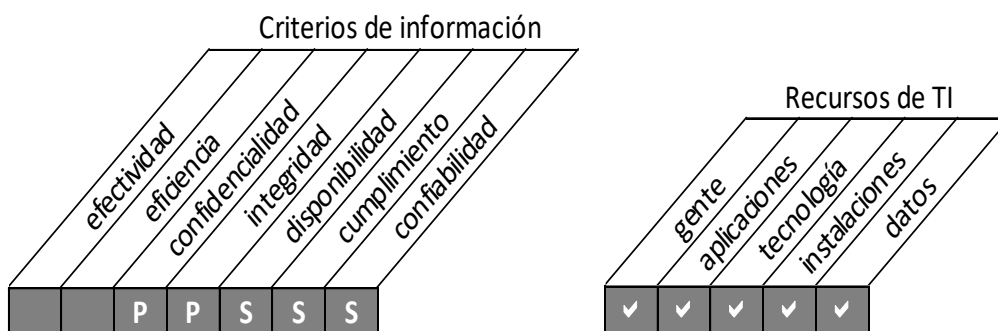
Nota: Tomado de "COBIT Marco Referencial", por Comité Directivo de COBIT, 2002.

DS5 Entrega de Servicios y Soporte: Garantizar la Seguridad de los Sistemas. El control sobre el proceso de TI, en el que consiste Garantizar la Seguridad de los Sistemas. Tiene los siguientes requerimientos que satisface a las empresas como el de salvaguardar la información contra uso no autorizado, divulgación o revelación, modificación, daño o pérdida. Esto es posible mediante controles de acceso lógico que dan seguridad a los sistemas de información.

Toman en consideración: (a) requerimiento de privacidad y confidencialidad, (b) autorización, autenticación y control de acceso, (c) identificación de usuarios y perfiles de autorización, (d) necesidad de saber y necesidad de tener, (e) administración de llaves criptográficas, (f) manejo, reporte y seguimiento de incidentes, (g) prevención y detección de virus, (h) firewalls, (i) administración centralizada de seguridad, (j) entrenamiento a los usuarios, y (k) herramientas para monitoreo del cumplimiento, pruebas de intrusión y reportes. (Comité Directivo de COBIT, 2002, p. 47)

Figura 16

DS5 - Garantizar la seguridad de los sistemas



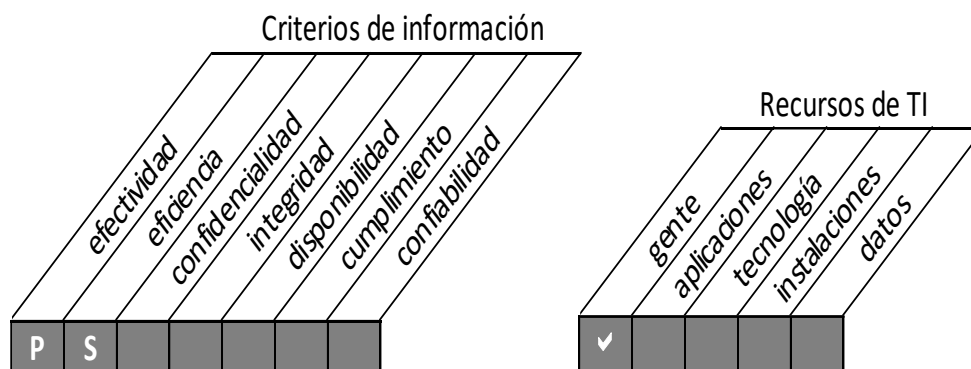
Nota: Tomado de "COBIT Marco Referencial", por Comité Directivo de COBIT, 2002.

DS7 Entrega de Servicios y Soportes: Educación y Entrenamiento de Usuarios. El control sobre el proceso de TI, que trata sobre la Educación y Entrenamiento de Usuarios, tiene los siguientes requerimientos que satisface a las empresas como el de asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y sean conscientes de los riesgos y responsabilidades involucrados. Esto se hace posible a través de un plan completo de entrenamiento y desarrollo.

Toman en consideración: (a) plan de entrenamiento, (b) inventario de habilidades, (c) campañas de concientización, (d) técnicas de concientización, (e) uso de nuevas tecnologías y métodos de entrenamiento, (f) productividad del personal, y (g) desarrollo de una base de conocimientos. (Comité Directivo de COBIT, 2002, p. 49)

Figura 17

DS7 - Educación y entrenamiento de usuarios.



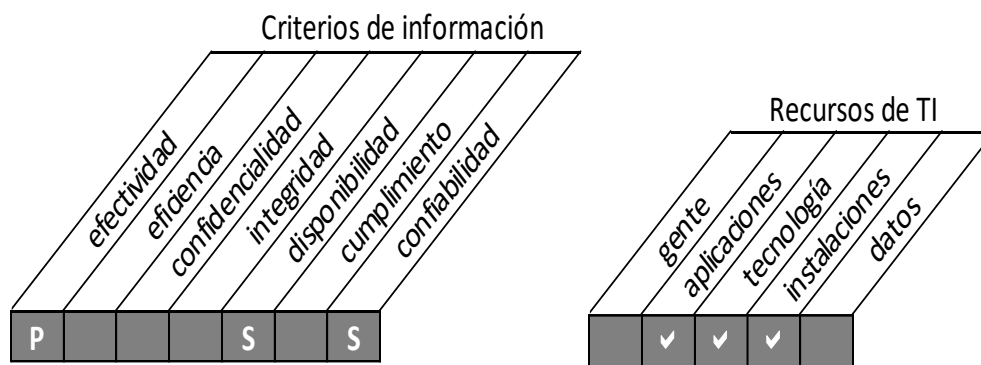
Nota: Tomado de "COBIT Marco Referencial", por Comité Directivo de COBIT, 2002.

DS9 Entrega de Servicios y Soportes: Administración de la Configuración. El control sobre el proceso de TI, que consiste en la Administración de la Configuración, tiene los siguientes requerimientos que satisface al negocio de dar cuenta de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para la sana administración del cambio. Esto se hace posible a través de controles que identifiquen y registren todos los activos de TI, así como su localización física y un programa regular de verificación que confirme su existencia.

Toman en consideración: (a) registro de activos, (b) administración de cambios en la configuración, (c) chequeo de software no autorizado, (d) controles de almacenamiento de software, (e) integración e interrelación de hardware y software, y (f) uso de herramientas automatizadas. (Comité Directivo de COBIT, 2002, p. 51)

Figura 18

Administración de la configuración-DS 9



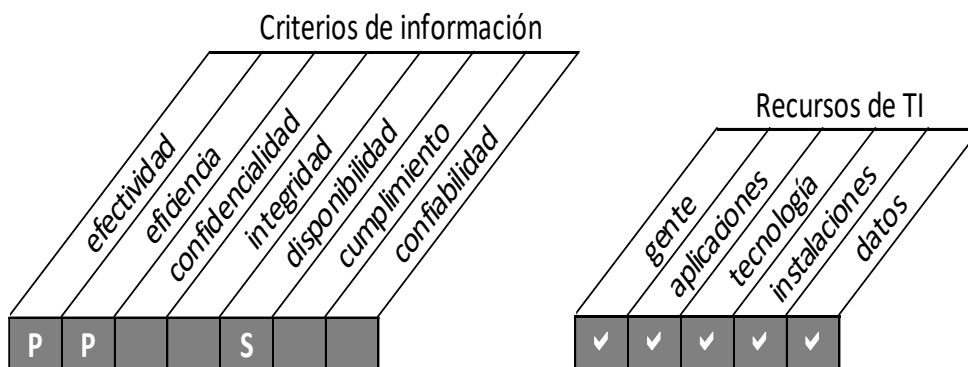
Nota: Tomado de "COBIT Marco Referencial", por Comité Directivo de COBIT, 2002.

DS10 Entrega de Servicios y Soportes: Administración de Problemas e Incidentes. El control sobre el proceso de TI, que trata sobre Administración de Problemas e Incidentes, tiene los siguientes requerimientos que satisface a las empresas como el de asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir cualquier recurrencia. Esto se hace posible a través de un sistema de administración de problemas que registre y dé seguimiento a todos los incidentes.

Toman en consideración: (a) pistas de auditoría de problemas y soluciones, (b) resolución oportuna de problemas reportados, (c) procedimientos de escalamiento (d) reportes de incidentes, (e) accesibilidad a la información de la configuración, (f) responsabilidades del proveedor, y (g) coordinación con la administración de cambios. (Comité Directivo de COBIT, 2002, p. 52)

Figura 19

DS10 Administración de problemas e incidentes.



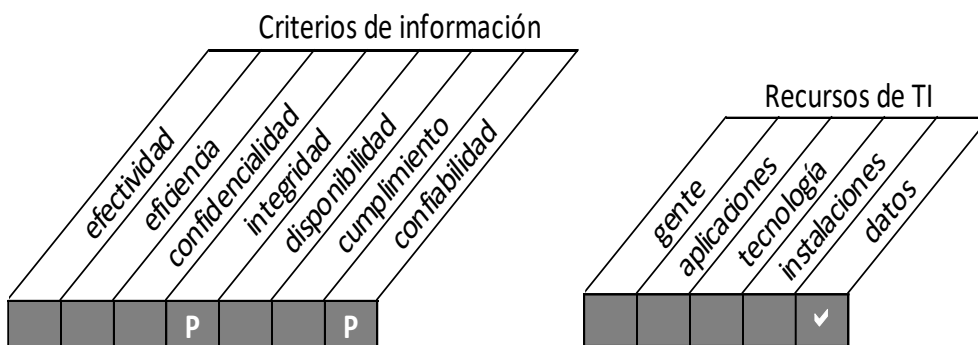
Nota: Tomado de "COBIT Marco Referencial", por Comité Directivo de COBIT, 2002.

DS11 Entrega de Servicios y Soporte: Administración de Datos. El control sobre el proceso de TI, que consiste en la Administración de datos, tiene los siguientes requerimientos que satisface a las empresas como el de asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización y almacenamiento. Esto se hace posible a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI.

Toman en consideración: (a) diseño de formatos, (b) controles sobre documentos fuente, (c) controles de entrada, procesamiento y salida, (d) identificación, movimiento y administración de la librería de medios, (e) recuperación y almacenamiento de datos, (f) autenticación e integridad, (g) propiedad de datos, (h) políticas de administración de datos, (i) modelos de datos y estándares de representación de datos, (j) integración y consistencia en todas las plataformas, y (k) requisitos legales y regulatorios. (Comité Directivo de COBIT, 2002, p. 53)

Figura 20

DS11 Entrega de servicios y soporte: administración de datos.



Nota: Tomado de "COBIT Marco Referencial", por Comité Directivo de COBIT, 2002.

Prevención de Errores y Fraudes

En el marco teórico de la metodología para la reducción de riesgos en los sistemas de información, se procede a identificar los conceptos generales de errores y fraude que son parte de los componentes del tema. Debemos saber que el fraude es un delito creativo que se comete en las empresas, donde los principales defraudadores son aquellas personas con mente agudas, inteligente y tiene cierta viveza para realizar los fraudes en los medios más vulnerable de la empresa. También son aquellas manipulaciones, falsificaciones y alteraciones de los registros y documentos, omitiendo en las transacciones los registros, estos se pueden detectar (a) observando y revisando los riesgos específicos de control, (b) vigilando el manejo de la administración, (c) revisando conciliaciones bancarias y de la información contable, y (d) efectuando pruebas de cumplimiento de controles. (*Hluppiciencias Gerenciales*, 2010)

En cambio, los errores son aquellos que se realizan sin intención y considerados como fallos matemáticos o administrativos en los registros contables y aplicación errónea de los Principios de Contabilidad Generalmente Aceptados (PCGA). Dentro de los errores existen dos tipos que son: errores de omisión no son intencionales, son errores humanos y los más numerosos y costosos en la industria y los errores intencionales que son los desfalcos y falsificaciones de registros. (*Hluppiciencias Gerenciales*, 2010)

El Triángulo del Fraude

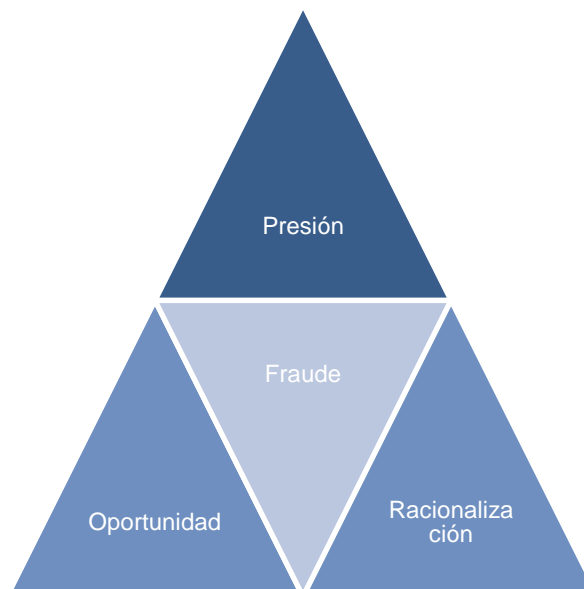
Las causas principales que motivaron a las personas a cometer un fraude son tan diversas como la falta de empleo por la situación económica que atraviesa el país donde se vive, o porque los ingresos alcanzados no son los suficientes para poder tener una vida cómoda, sin dejar de lado los aspectos de avaricia o dependencias del alcohol o las drogas. (Delgado, 2017)

Según Cressey (1973) las personas cometen fraude cuando combinan presión, oportunidad y racionalización para aceptar y no tomar conciencia de que el acto que se está realizando se encuentra en un mal camino. En el estudio realizado, la mayoría de los defraudadores o estafadores que él

examinó “habían vivido más allá de sus posibilidades durante un cierto tiempo antes de decidir los actos ilícitos”. Esta teoría se conoce con el nombre “El Triángulo del fraude” y se basa en que una persona bajo presión o que tiene un interés motivador busca lograr algo y si existen oportunidades debido a la debilidad del control en la empresa o la organización empresarial, como falta de multas, sanciones, etc., el defraudador podría cometer el acto ilícito si no siente que el asunto está mal o contraria a la moral y a las buenas costumbres.

Figura 21

El triángulo del fraude



Nota: Tomado de “Auditoría Forense”, por Rozas, 2009.

El Triángulo del fraude tienen vértices o componentes: presiones, incentivos percibido y Racionalización del comportamiento fraudulento. Así pues, los psicólogos expertos en fraude explican las causas para cometerlo en términos de lo que denominan el triángulo del fraude: oportunidad, presión y racionalización. Las oportunidades surgen cuando los controles son débiles y/o cuando las personas se encuentran en una posición de confianza. Las presiones sobre quienes cometen fraude suelen ser de naturaleza financiero, ya que es más

probable que los objetivos poco realistas de la empresa motiven a los empleados a cometer fraudes. Racionalización a menudo incluye creencias tales como: la actividad no es criminal, sus acciones son justificadas, se trata de un simple préstamo de dinero, estamos asegurando que se cumplan las metas de la empresa y, de manera especial, todo el mundo lo está haciendo. (Rozas, 2009, pp. 9-10)

Marco Conceptual

Sistema de Información

Un sistema de información (SI) es un conjunto de elementos o componentes interconectados que recopilan(entrada), manipulan proceso, almacenan y entregan (salida) datos e información y brinda una respuesta correctiva (mecanismo de retroalimentación) si no se ha logrado cumplir un objetivo. Los mecanismos de retroalimentación son los componentes que ayudan a una empresa a alcanzar sus objetivos: como aumentar las ganancias y mejorar el servicio al cliente. (*Stair & Reynolds*, 2010, p. 59).

O'Brien (2006) indicó que un sistema de información es: una combinación organizada de personas, hardware, software, redes de comunicación y recursos de información que almacena, recupera, transforma información en una organización. Las personas han confiado en los sistemas de información para comunicarse entre sí a través de varios dispositivos físicos (hardware), instrucciones y procedimientos de procesamiento de información (software), canales de comunicación (redes) y datos almacenados (recursos de información) desde los inicios de la civilización. (p. 39)

Características de Sistemas

Uriarte (2021) determinó que las principales características de los sistema de información son los siguientes:

- Puede ser un sistema formal, cuando utiliza medios computacionales o estructuras sólidas para lograr una meta u objetivo, o un sistema

informal, cuando utiliza estructuras básicas o artesanales, como papel y lápiz.

- Almacena información cualitativa (información no numérica) e información cuantitativa (variables numéricas).
- Incluye datos ingresados manual o automáticamente para crear una base de datos.
- Utiliza encuesta, cuestionarios, notas, censos o estudios para la recogida de datos.
- Debe ser evaluado y medido para actualizar o corregir cualquier error.
- Debe ser seguro para evitar la pérdida o robo de la información recopilada.
- Requiere de algún tipo de retroalimentación, esto quiere decir que la información sale del sistema y vuelve a ingresar con más detalle o más información. (p. 1)

Tipos de Sistemas

La revista Etecé (2022) mencionó que desde un punto de vista empresarial y organizacional, los tipos de sistemas se clasifican de la siguiente manera:

Sistemas de Procesamiento de Transacciones (TPS). Son sistemas de gestión operativa que recopilan la información pertinente a las transacciones de la organización, enfocándose en su funcionamiento.

Sistemas de Información Ejecutiva (EIS). Permiten monitorear las variables gerenciales respecto a un área específica de la organización, a partir de la información interna y externa de la misma.

Sistemas de Información Gerencial (MIS). Contemplan la información general de la organización y la comprenden como un todo.

Sistemas de Soporte de Decisiones (DSS). Orientados al procesamiento de información extra organizacional, para el apoyo en la dirección de la empresa.

Elementos de Sistemas

Normalmente existen elementos indispensables que ayudan a llevar adelante un sistema de información.

Recursos Humanos. Son aquellas personas que se encargan de recopilar y organizar la información. En muchos casos también se encargan de cargar los datos tanto en soportes materiales como en software o plataformas virtuales.

Datos. Son variables cualitativas o cuantitativas que se hacen referencia acerca de hechos o fenómenos. Una vez que los datos son procesados, se convierten en información que la organización empresarial utiliza.

Tecnología. Son las plataformas o software que se utilizan para almacenar y procesar los datos. Un sistema de información puede no ser digital y estar archivado en carpetas u otros tipos de archivos físicos. (Uriarte, 2021, p. 1)

Componentes de Sistemas

De acuerdo *BBC Bitesize* (2022) mencionó que los sistemas de información normalmente contienen los siguientes componentes:

Hardware. Los sistemas de información utilizan hardware de computadora, como procesadores, monitores, teclados e impresoras.

Software. Son los programas que se utilizan para organizar procesos y analizar datos, por ejemplo, bases de datos.

Usuario. Los diferentes elementos de una organización deben estar conectados entre sí, especialmente si muchas personas diferentes en la organización utilizan el mismo sistema de información.

Procedimientos. Describen cómo se procesan y analizan datos específicos para obtener las respuestas para las que está diseñado el sistema de información. (p. 1)

Actividades de los Sistemas de Información

Para López (2012) refirió el siguiente criterio sobre las actividades que se realizan en los sistemas de información , a continuación se detalla las más representativa.

Entrada de Datos. El sistema de información necesita tomar los datos que requiere para procesar la información. Las entradas pueden ser de forma manual o automática. Las unidades típicas de entrada de datos a las computadoras son las estaciones de trabajo, los dispositivos de almacenamiento, lector de código de barras, escáner, la voz, los monitores sensibles al tacto, teclado y mouse entre otras. (ver Tabla 5)

Almacenamiento de Datos. Mediante esta propiedad el sistema puede recordar la información guardada en la sesión o el proceso anterior. Esta información puede ser almacenada en estructuras de información denominadas archivos. Discos magnéticos o discos duros, discos flexibles, discos compactos, dispositivos de alta capacidad.

Procesamiento de Datos. Tiene la capacidad de efectuar cálculos de acuerdo con una secuencia de operaciones preestablecidas. Estas características de los sistemas permiten la transformación de datos fuentes en información que puede ser utilizada para la toma de decisiones.

Salida de la Información. Es la capacidad de un SI para sacar la información procesada o bien datos de entrada al exterior. Las unidades típicas de salida son las impresoras, estaciones de trabajo, dispositivos de almacenamiento, la voz, los graficadores, los plotters, entre otros. Puede constituir la entrada a otro SI o módulo a través de una interfaz automática. (pp. 8-12).

Tabla 5*Tipos de datos*

Datos	Representados Mediante
Datos alfanuméricos	Número, letras y otros caracteres
Datos de imágenes	Imágenes gráficas y fotos
Datos de audio	Sonidos, ruidos y tonos
Datos de video	Imágenes en movimiento o fotografías

Nota: Tomado de “*Principios de un Sistema de Información*”, por Stair & Reynolds, 2010.

Riesgos

El termino riesgo según el diccionario de la Real Academia Española (1992) refirió a contingencia o proximidad de un daño, es decir son aquellas eventualidad de un suceso que se presenta como problema de manera no prevista. Además, el riesgo se lo definió como la combinación de la probabilidad de un evento y sus consecuencias negativas. Sus elementos constitutivos son la amenaza y la vulnerabilidad. Donde la amenaza es aquel fenómeno, actividad o condición humana peligrosa que puede causar la muerte, lesiones, daños a la propiedad, pérdida de medios de subsistencia y servicios, trastorno económico y social, y la vulnerabilidad son las condiciones de una sociedad, sistema o activo que lo hacen venerables a efectos negativos de una amenaza o peligro. (Ciifen, 2022)

Briones (2005) indicó que el riesgo es “el concepto de riesgo comienza a desarrollarse, en el siglo XVII, con la idea de prudencia y seguridad, y con la posibilidad que tiene el hombre de elegir su destino”(p. 3).

Debemos saber que este término riesgo no siempre formó parte del vocabulario de la sociedad, ya que, en la antigüedad, lo que se marca es el peligro, mientras que, hasta hace poco, la sociedad moderna lo que integra como parte del vocabulario es el término riesgo. El mismo autor refiere que la utilización de un nuevo vocablo responde a la necesidad de conceptualizar una situación puntual, que no puede ser expresada con la precisión requerida por las palabras de que se dispone en el momento. (Chávez, 2018, p. 2)

Características del Riesgo

Según el Centro de Estudios superiores Maranathá (2022) determinó las siguientes características del riesgo:

- La pérdida potencial expresada en dinero.
- La probabilidad de que se produzca el riesgo.
- El nivel de riesgo, es decir, la relación entre el coste necesario para preparar y aplicar el riesgo y la pérdida potencial: si el resultado es superior a uno, el riesgo se considera poco razonable.
- La legitimidad del riesgo: este valor se determina por la probabilidad de que el riesgo esté dentro de los límites establecidos por la ley y las normas.
- También hay siempre un riesgo asociado a la vida humana. Puede ser causada por el entorno externo o por el propio individuo.(p. 1)

Tipos de Riesgos

Riesgos de Información. Para Rodríguez (2020) los riesgos de la información tiene que ver con las vulnerabilidades que se presentan en activos informáticos y presentan un riesgo para la información. Dos ejemplos de vulnerabilidades comúnmente encontradas en el análisis de riesgos informáticos son: (a) falta de actualizaciones de los sistemas operativos, por lo tanto, no incluyen los últimos parches de seguridad y, (b) el uso de contraseñas de acceso débiles, contraseñas cortas que usan combinación de letras, números, símbolos y letras mayúsculas y minúsculas, y que son fáciles de descifrar mediante procesos automatizados.

La alta dependencia de los sistemas de información trae cada vez más, preocupación en las organizaciones debido a los riesgos que generan la complejidad de los sistemas, posibles accidentes, errores o ataques, y la constante evolución en un entorno cambiante; por lo que la ejecución de estos riesgos puede afectar la continuidad de los servicios (internos y externos), la protección de la información en general, así como la validez y eficacia de los procesos que se basan en transacciones electrónicas; por lo tanto, es necesario aplicar un análisis

de riesgo para crear las políticas de seguridad basadas en una metodología para controlar los elementos que permiten reducir la exposición a los riesgos protegiendo los activos de una organización.(Mujica & Álvarez, 2009, p. 4)

Riesgos en Sistemas de Seguridad. Los riesgos en los Sistemas de Seguridad de la Información, se puede expresar en términos del efecto de la Vulnerabilidad sobre los objetivos de seguridad de la información. La vulnerabilidad se asocia con amenazas de un activo de información o grupo de activos de información, por lo tanto, puede causar daño a la organización. (ISO 27001, 2020)

Fraudes

En un sentido amplio Garner (2004) dio a entender que “el fraude puede abarcar cualquier delito para ganancia que utiliza el engaño como su principal *modus operandi*”(p.1). El *Black’s Law Dictionary* define al como el distorsionamiento u ocultamiento deliberadamente de un hecho importante para inducir a otros en hacerle daño. Por lo tanto, el fraude incluye cualquier acto intencional para privar a otra persona de bienes o dinero mediante engaño u otras prácticas desleales.

La NIA 240 definió el fraude como “acto intencionado realizado por una o más personas de la dirección, los responsables del gobierno de la entidad, los empleados o terceros, que conlleve la utilización del engaño con el fin de conseguir una ventaja ilegal” (IAASB, 2009a, p. 3).

Albizuri (2002) indicó que el fraude informático es el uso indebido o la manipulación fraudulenta de los elementos informáticos de cualquier tipo, que produce un beneficio ilícito (ver Figura 22). En cambio Lux y Calderón (2020) relacionó el fraude informático con “el phishing, que implica una obtención fraudulenta de datos de identidad personales de clientes de bancos y de sus cuentas bancarias o tarjetas de crédito orientada a ejecutar transacciones electrónicas a favor del agente o de terceros” (p. 13).

Figura 22

Formas de cometer un fraude

Manipulación de los datos de entrada

Este tipo de fraude informático es conocido como robo de datos, es el más común porque es fácil de cometer y difícil de detectar. Puede ser cometido por cualquier persona con acceso a los datos.

Manipulación de programas.

Consiste en modificar programas en el sistema computacionales o insertar nuevas rutinas, además es muy difícil de descubrir y a menudo pasa inadvertido, debido a que el delincuente debe tener conocimientos técnicos concretos de informática.

Manipulación de los datos de salida

Se realiza fijando un objetivo al funcionamiento del sistema informático. Se usa equipos y programas para codificar la información y cometer los fraudes.

Nota: Tomado de "Fraude Informático, Derecho Ecuador", por Vallejo, 2005, p. 1.

Tipos de Fraudes

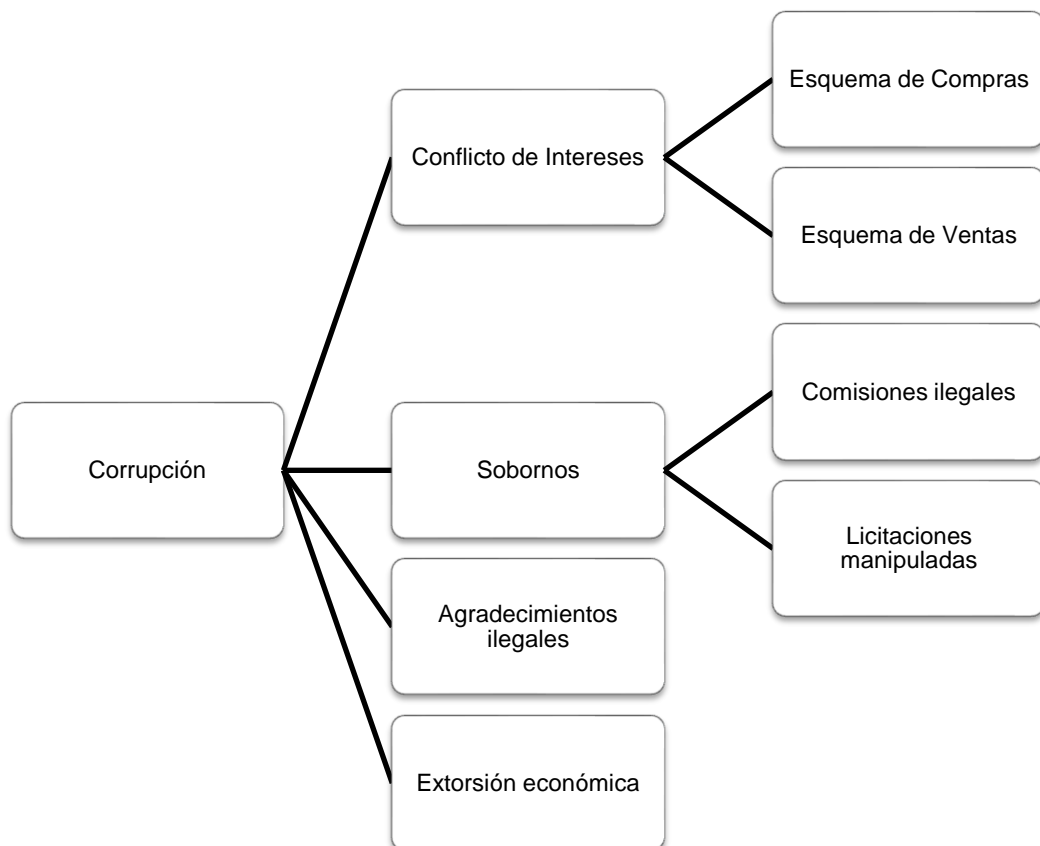
Rozas (2009) concluyó dos tipos de fraudes que son: (a) los informes financieros fraudulentos que son un error u omisión intencional en las cantidades o revelaciones con la intención de engañar a los usuarios, (b) la malversación de activos siendo este el fraude que involucra el robo de los activos de una entidad. Adicionalmente, mencionó otra forma similar de categorizar los fraudes como: (a) el fraude corporativo que es la distorsión de la información financiera realizada por parte o toda la alta gerencia con ánimo de causar perjuicio a los usuarios (prestamistas, inversionistas, accionistas, estado y sociedad) de los estados financieros, (b) el fraude laboral (ocupacional) este es la distorsión de la información financiera (malversación de activos) con ánimo de causar perjuicio a la empresa. (pp. 8-9)

Clasificación de Fraudes

De acuerdo con la Asociación de Examinadores de Fraudes Certificados (ACFE), el fraude se lo puede clasificar en tres grandes grupos: (a) corrupción, (b) apropiación indebida de activos, y (c) fraude financiero. Esta clasificación se conoce como el nombre del Árbol del Fraude y se incluyó en el primer Reporte a las Naciones sobre el Abuso y el Fraude Ocupacional en 1996. (ACFE, 2016). Al analizar los casos de fraude en este estudio, se observaron patrones en la forma en que se cometieron las irregularidades y casi todos los esquemas de fraude ocupacional caían en categorías específicas (ver Figura 23). Sobre la base de estas categorías, se generaron un sistema de clasificación integral de patrones de fraude ocupacional. (Delgado, 2017)

Figura 23

Esquema de fraude por corrupción



Nota: Tomado de “Reporte a las Naciones sobre el Abuso y el Fraude Ocupacional”, por Asociación de Examinadores de Fraudes Certificados ACFE, 2016, p. 11.

Si bien es cierto que las entidades son susceptibles al fraude, la corrupción es uno de los diversos patrones de fraude que consiste en: conflictos de intereses, sobornos, agradecimientos ilegales y extorsión económica. Según los estudios realizados por la ACFE “El fraude ocupacional es el uso de la posición organizacional para el enriquecimiento personal mediante la utilización ilícita o mala aplicación de los recursos o activos del empleado” (ACFE, 2016).

Características de un Defraudador

Entre las principales características del defraudador tenemos a las siguientes: (a) nunca toman vacaciones: con el fin de que no descubran las actividades ilícitas que está ejecutando, (b) son empleados de confianza: se aprovechan de esa confianza para realizar los fraudes, (c) mantienen un perfil bajo en la empresa: con el fin de encubrir sus actividades, y (d) logran despistar por completo: tienden a tener una educación por encima de la media nacional, son de trato agradable. Los defraudadores tratan de seguir con su “vida normal” al interior de las empresas, de tal manera que su conducta no despierte sospechas. (Delgado, 2017, p. 22)

Control

“Son todos los métodos, políticas y procedimientos que aseguran la protección de los activos de la organización, la precisión y confiabilidad de sus registros, y la adherencia operacional a los estándares de la administración” (Laudon & Laudon, 2016, p. 608).

Tipos de Control

Control de Seguridad. Los controles de acceso se pueden implementar a nivel de Sistema Operativo, sistemas de información, en bases de datos, en un paquete de seguridad específico y en cualquier otro utilitario. Estos controles constituyen una ayuda importante para proteger al sistema operativo de la red, a los sistemas de información y software adicional, de que puedan ser utilizados, modificados sin

autorización. También para mantener la integridad de la información, mediante la limitación usuarios y procesos con acceso autorizado y para resguardar la información confidencial de accesos no autorizados. (Cervantes, 2020, p.6)

Control de Acceso Lógico. Conceden permisos a usuarios o grupos de acceder a objetos, tales como ficheros o impresoras en la red. El control de acceso está basado en tres conceptos fundamentales: identificación, autenticación y autorización. Incluye autenticar la identidad de los usuarios o grupos y autorizar el acceso a datos o recursos. Son esenciales para proteger la confidencialidad, integridad y disponibilidad de la información, el activo más importante de una organización, pues impide que los usuarios no autorizados accedan a los recursos o datos que existen.(Red Hat, Inc., 2005, p. 1)

Control de Acceso Físico. Esta solución permite el control de los puntos estratégicos de una compañía mediante equipos que verifican la identidad de las personas en el momento de ingresar a las instalaciones. Este tipo de control maneja políticas totales o parciales de acceso, mantiene control de tiempo de las personas que realizan transacciones mediante un manejo avanzado de credenciales que permite controlar, limitar, monitorear y auditar el acceso físico. Este tipo de sistema es ideal para organizaciones que desean controlar una única área restringida o múltiples puertas de acceso. (Red Hat, Inc., 2005, p. 1)

Seguridad Informática

La seguridad informática según Aguilera (2010) indicó que "la disciplina que se ocupa de diseñar las normas, procedimiento, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable" (p. 9).

Villalón (2002) en su libro sobre la seguridad en Unix y Redes hace mención de los siguiente; Un sistema es seguro o confiable cuando asegura que la información está protegida y libre de peligro, daño o riesgo, por lo que debe ser infalible. En este sistema los siguientes aspectos están

comprometidos: (a) la privacidad donde la información es conocida solo por personas autorizadas, (b) la integridad significa que la información permanece a menos que esté autorizada para ser modificada por personal autorizado, y esta sea registrada para posteriores auditorías o evaluaciones, y (c) disponibilidad de la información para ser procesada por parte del personal autorizado. Esto requiere que dicha información se almacene correctamente con el hardware y el software funcionando perfectamente y que se respeten los formatos para poder recuperarlos satisfactoria.

“Políticas, procedimientos y medidas técnicas que se utilizan para evitar el acceso no autorizado, la alteración, el robo o el daño físico a los sistemas de información” (Laudon & Laudon, 2016, p. 615).

Tipos de Seguridad

Según Aguilera (2010) mencionó los siguientes tipos de seguridad:

La Seguridad Lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo permitan acceder a ellos a las personas autorizadas para hacerlo, y la Seguridad Física trata de la protección de los sistemas ante amenazas físicas. Se basa en la aplicación de barreras físicas y control, tales como medidas preventivas y contramedidas, ante amenazas a recursos e información confidencial. (p. 17)

Políticas de Seguridad

La implementación de un sistema de seguridad debe estar complementado con las políticas de seguridad, estas requieren no solamente conocer las amenazas a las que están expuestas la información y los recursos de una organización, sino también establecer el origen de estas, que pueden ser internas o externas a la organización. Las políticas de seguridad se desarrollan con el fin de preservar la información y los sistemas de una Empresa, y garantizando la integridad, confidencialidad y disponibilidad de la información. Los documentos relativos a las políticas de seguridad

deben contemplar los procedimientos para hacer cumplir las reglas, las responsabilidades en todos los niveles. Todos ellos deben tener el apoyo gerencial de la organización. (Velasco, 2008, pp. 67-68)

Errores en Sistemas

En un Sistema de Información pueden aparecer errores en distintas fases de su desarrollo como: toma de requerimientos, análisis, diseño, programación, pruebas o implementación; así pues, entre más tarde se detecte la falla, más costoso será corregirla. De acuerdo con una encuesta realizada en 2015 por *Statista*, en el Reino Unido se reportaron problemas con los sistemas de información debido a tres causas fundamentales: fallas de software (23%), errores humanos (28%) y ataques informáticos (49%). Asimismo, una encuesta realizada en Estados Unidos durante ese año, mostró que el 43% de las causas que originan la baja calidad en los datos de un sistema de información son por errores en el software, cifras muy elevadas si hablamos del costo que representa desarrollar un sistema más la infraestructura que gira a su alrededor. (Vélez, 2022, p. 1)

Marco Referencial

Estudios Previos

En la propuesta realizada por Arroyave y Ledesma, (2016) denominada *Sistema de información contable para mejorar la productividad y competitividad de las PYMES es de bordados del municipio de Cartago Valle*, empleó distintas bases teóricas, conceptuales y legales el mismo tuvo objetivo la implementación de los sistemas de información contables (SIC) para mejorar la productividad y competitivas en su actividad económica. Además, al aplicar técnicas y herramientas de información se pudo denotar que las empresas no cuentan con un SIC y mucho menos con un aplicativo contable propias de acuerdo con sus necesidades, prefiriendo para este proceso la contratación externa que conlleva un riesgo y desventaja informática que no permite mantener el control contable y administrativo de toda la empresa. Para

esto se elaboró una estructura que podría ayudar a las PYMES a tener una mayor productividad y, por ende, una mayor competitividad en el mercado.

Como resultado contribuye al desarrollo y a la sistematización de la contabilidad según las necesidades del negocio, con el cual será posible evaluar la situación económica en cuanto a solvencia y estabilidad con datos actualizados y veraces, para no caer en el rutinario y repetitivo registro de cuentas y poder avanzar y liberar al contador de esta fase del proceso, permitiéndole dedicar más tiempo a labores de mayor importancia, como el análisis e interpretación de la información dada por el sistema contable.

En otro proyecto de investigación *sobre Seguridad lógica y de accesos y auditoría*, se planteó el objetivo de concienciar a las empresas a la importancia de invertir tiempo, esfuerzo y recursos en los controles de seguridad de la información. Para ello se realiza una auditoria de tres etapas; (a) toma de contacto, es decir se perpetúa la auditoria recopilando la información necesaria, (b) desarrollo, uso de herramientas y técnicas para obtener evidencias e identificar mejoras, y, (c) presentación del informe final con las conclusiones y posibles correcciones evaluación. Además, como resultado se creó una aplicación que ayuda al contador a recopilar información durante la realización de la evaluación y recomendaciones para incluir en el informe final.(Monte, 2010a)

Por ultimo en el trabajo de titulación de Rambay (2020) con el tema de *factores que influyen en la sistematización de los procesos contables en PYMES del sector de cargas de la ciudad de Guayaquil*, tuvo como objetivo la sistematización de los procesos contables que protege la información financiera de la empresa, permitiendo garantizar el registro adecuado de las transacciones, la cual ayudara a determinar los riesgos potenciales y sus posibles acciones correctiva. Para esto se realiza entrevistas a expertos que, con su trayectoria y experiencia responderán las preguntas abiertas, para la determinación de factores y otros aspectos que inciden en la sistematización de los procesos contables en PYMES Consolidadas. Como resultados se determinó que sistematización de los procesos contables es esencial para la protección de la información financiera y no financiera de las Compañías,

además de facilitar los procesos, procedimientos internos y externos y el mejoramiento del flujo de información para la toma de decisiones. Finalmente hace recomendaciones relevantes, entre las que destacan: (a) sistematizar las operaciones comerciales arraigadas en las operaciones diarias del negocio, (b) la adopción de nuevas tecnologías (productos, procesos, información, etc.), (c) desarrollo de la seguridad de información bajo lineamientos tales como la evaluación de riesgos tecnológicos, y (d) establecer principios de seguridad de información.

Sector Acuícola

El sector acuícola tomo gran fuerza en el posicionamiento del mercado internacional, la Organización de las Naciones Unidas para la alimentación y agricultura en su reporte de exportaciones del Ecuador, indicó lo siguiente:

Las exportaciones de camarón en el año 2021, pese a la disminución del 38% de la demanda a su principal destino China, debido a la suspensión temporal de las importaciones en dicho país hacia ciertas camaroneras ecuatorianas, siguió siendo el principal proveedor de China estando a la par con las exportaciones del 2019 con 10.530 toneladas y productor de camarón cultivado a nivel internacional. El segundo mercado más importante del Ecuador es Estados Unidos que tuvo un aumento de las exportaciones del 7,6% comparado con el año 2020. (FAO, 2021a, p. 1)

Salen y Ontaneda (2019) en una entrevista comento que:

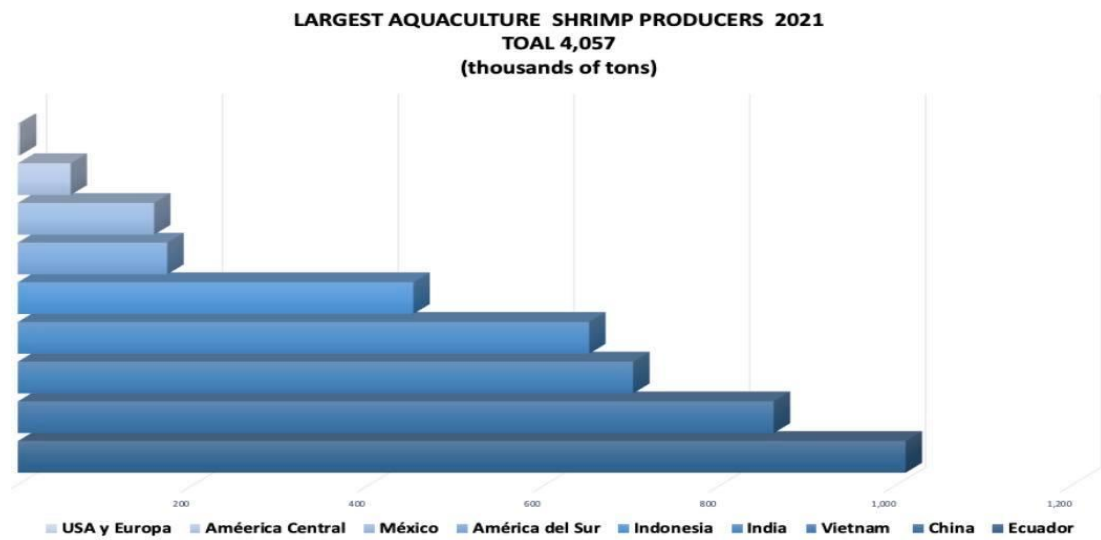
En 1986 se inició la primera industria acuícola fue la compañía Santa Priscila ubicada en km 5.5 vía Daule especializada en el área de desarrollo de piscinas camaronera a lo largo del país, actualmente se encuentra en el puesto 15 de las empresas más grandes por sus ventas, en el 2017. En ese año los ingresos fueron de 480,2 millones, de acuerdo con datos de la superintendencia de compañías, valores y seguros. En relación con el año 2016, presentó un incremento del 12,6%. Además, dichas compañías trabajan de forma ligada a las

inversiones en productividad y tecnología es decir siempre buscan nuevos mercados y nuevas oportunidades. (p. 1)

Según la revista *Aquaculture Magazine* (2021) Ecuador es el primer país en producir un millón de toneladas camarón, convirtiéndolo en el mayor productor de camarones del mundo. En el ranking que publica esta revista, se detalla que Ecuador encabeza la lista de mayores países productores de camarón en 2021, seguido de China, Vietnam, India, Indonesia, Sudamérica, México, Centroamérica, Estados Unidos y Europa. (ver Figura 24)

Figura 24

Mayores productoras de camarón acuícola 2021



Nota: Tomado de *“Ranking de los países productoras de camarón 2021”*, por *Aquaculture Magazine*.

El sector camaronero en el Ecuador corresponde 95 % de la acuicultura (ver Tabla 6) correspondiente al cultivo del camarón marino (*Litopenaeus* spp), en segundo lugar, el cultivo de la Tilapia, y por último otras especies (peces y crustáceos de agua dulce). Esta actividad camaronera se desarrolló en la región de la Costa desde la época de los años 70, empezando con pequeños estanques de cría de camarón y luego aumentaron creando empacadoras, laboratorios de larvas y fábricas de alimento balanceado y una serie de industrias que producen insumos para la actividad acuícola. (Schwartz, 2022)

Tabla 6*Especies cultivadas de camarón mundial*

Tipos de Camarón	Nombre Científico	Nombre de Mercado
Camarón Tigre Negro	Penaeus Monodon	Tigre negro, gigante o jumbo
Blanco del Pacífico	Penaeus Vannamei	Camarón Blanco occidental
Camarón Blanco Chino	Penaeus Chinensis	Camarón Blanco Chino
Camarón Rosado	Pandalus Borealis	Camarón Rosado

Nota: Adaptado de “Análisis del Sector Camaronero”, por Marriot, 2003.

Espinoza et al. (2017) en su investigación comentó lo siguiente:

El sector sector acuícola cuenta además con el Centro de Servicios para la Acuicultura (CSA) que es una fundación sin fines de lucro creada el 13 de noviembre de 1998 por la Cámara Nacional de Acuicultura, la Fundación CENAIM-ESPOL y la Escuela Superior Politécnica del Litoral (ESPOL). El objetivo del CSA es mejorar la producción camaronera buscando soluciones a las enfermedades del camarón. (p. 28)

Las Empresas Medianas y Pequeñas (PYMES)

En América Latina, estas empresas representan alrededor del 35% del empleo formal y el 20% del valor de la producción (pocas productivas en comparaciones con PYMES de regiones desarrolladas). No obstante, tiene una economía heterogénea y débil, es decir tiene problemas en el acceso a la financiación, crecimiento y supervivencia, sobre todo en tiempos difíciles de crisis económica. (Álvarez et al. 2021)

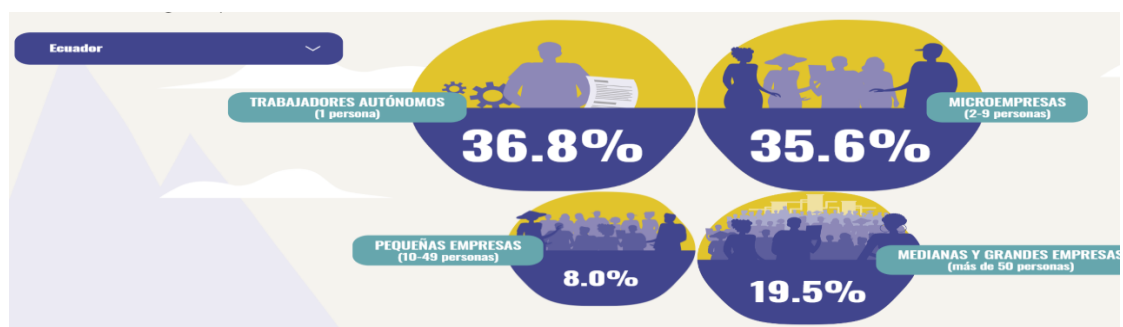
Según la organización Internacional del Trabajo indicó que:

Las PYMES por lo general cuenta con menos de 250 empleados. En otros países, más del 90% de la totalidad de las empresas pueden considerarse como PYMES, y gran parte de éstas se sitúan en la categoría de microempresas, al operar con menos de diez empleados. Los nuevos datos por la OIT (ver Figura 25) detallan que, al ser

consideradas conjunta, las actividades de las microempresas y las pequeñas empresas, sumada a los trabajadores por cuenta propia, alcanzan una tasa de 70% del empleo mundial. Por lo tanto, las empresas con menos de 100 empleados generan más del 50% de puestos nuevos de trabajo en todo el mundo. (OIT, 2019, p. 1)

Figura 25

Proporción del empleo por tamaño de las empresas y trabajadores autónomos



Nota: Tomado de “*Datos mundiales sobre las contribuciones al empleo de los trabajadores independientes, las microempresas y las PYMES*”, por Organización Internacional del Trabajo OIT, 2019.

Clasificación de las PYMES

Para organizar a los negocios por dimensión el Ecuador se refugia en la definición de la Comunidad Andina de Naciones (CAN). Este sistema estadístico regional establece que las PYMES comprenden a todas las empresas formales legalmente constituidas y/o registradas ante las autoridades competentes, que lleven registros contables y/o aporten a la seguridad social, comprendidas dentro de los umbrales establecidos en el artículo 3 de la Decisión 702. Según Tabla 7, muestra cómo se dividen las empresas en nuestro país. (*Comunidad Andina*, 2009, p. 1).

Tabla 7

Clasificación PYMES de acuerdo normativa interandina y la Superintendencia de compañías

Tipos de Empresas	Personal ocupado	Valor Bruto de Ventas Anuales	Monto de activos
Microempresa	De 1-9	Menor o Igual 100.000	Hasta \$100.000
Pequeña Empresa	De 10-49	100.001 a 1.000.000	De \$100.00 - \$750.000
Mediana Empresa	De 50-199	1.000.001 - 5.000.000	De \$750.0001 - \$3.999.999
Empresas Grandes	Mayor a 200	Mayor a 5.000.000	Mayor o Igual a \$4.000.000

Nota: Adaptado de “*Clasificación Nacional*”, por Comunidad Andina, 2009.

La Comunidad Andina. Es una comunidad de países en la que se reúnen voluntariamente con el objetivo de poder alcanzar un desarrollo integral, equilibrado y autónomo, mediante la integración andina, latinoamericana y suramericana. Los siguientes países la conforman: Bolivia, Colombia, Ecuador y Perú estando unidos por el mismo pasado, una variada geografía, una gran diversidad cultural y natural, así como por objetivos y metas comunes. (Servicio Nacional de Aduana Del Ecuador 2022, p. 1)

Aporte de las PYMES en el Ecuador

Las pequeñas y medianas empresas (PYMES) han aportado en la economía del país, generando ingresos y fuentes de empleos. Según, Andrade et al. (2016) estas empresas están relaciona de acuerdo al volumen de ventas, capital social, cantidad de empleados y nivel de producción. Por su parte Correa Luna (2005) indicó que estas empresas aporta a la reducción y distribución de bienes y servicios y su capacidad de adaptarse a los cambios tecnológico para el desarrollo de la industria.

Por su parte Yance et al. (2017) refirió que estas empresas PYMES han sido esenciales para el crecimiento social, económico de todos los países, lo que se suma a la necesidad de aumentar la eficiencia y la necesidad de implementar estrategias que beneficien la operación con el objetivo de reducir

los costos operativos, y mejorar la eficiencia de ellos procesos, los niveles de inventario, calidad de productos y aumentar la productividad.

La pequeña y mediana empresa se ha constituido en objeto central de estudio de la teoría administrativa debido a que tienen una representación significativa en las economías de un país. Las investigaciones se han centrado fundamentalmente en el análisis de la perspectiva económica y en el ámbito de la gestión empresarial. (Zapata, 2004, p. 4)

Las PYMES y la Facturación Electrónica

Para Millet (2008) la facturación electrónica es “documento tributario generado por medios informáticos en formato electrónico, que reemplaza al documento físico, conservando el mismo valor legal y condiciones de seguridad no observada en la factura de papel” (p. 89). Para Barreix y Zambrano (2018) el sistema de facturación electrónica trae beneficios a las pequeñas y medianas empresas, disminuyendo el costo operativo y automatización, ahorro de papel y espacio físico y en especial el tiempo del envío de las facturas al cliente.

Vásquez (2019) indicó en su entrevista “las PYMES operan en Excel, a través de talonarios en papel, o incluso en el software de un contador externo. Pero relativamente muy pocas han dado el importante paso de comenzar a manejar su información financiera y operativa en un software propio, de fácil acceso por el gerente o el personal interno de la empresa” (p. 1).

Según el Servicio de Renta Interna (SRI) en la resolución NAC-DGERCGC18-00000191 reformada por la resolución No.NAC-DGERCGC18-00000431 en el 2022, los contribuyentes obligados a emitir facturas electrónicas son:

Las personas naturales y las sociedades, a excepción de las sociedades acogidas al Régimen Simplificado establecido en el Reglamento para la Aplicación de la Ley de Régimen Tributario Interno y de los sujetos domiciliados en la provincia de Galápagos que no mantengan establecimiento en el Ecuador continental, que tengan

ingresos anuales entre USD. 200.000,01 (doscientos mil dólares y un centavo de los Estados Unidos de América) y USD. 300.000,00. (trescientos mil dólares de los Estados Unidos de América) en el ejercicio fiscal anterior. (*Constitución de la República del Ecuador*, 2018, p. 1)

Marco Legal

Sistemas de Gestión de Seguridad de Información: ISO 27001

Es una norma que se creó por la organización internacional de la normalización (ISO), con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información. Esta medida aporta un Sistema de Gestión de Seguridad de la Información (SGSI) orientada a proteger la información, indistintamente del formato que se presenta, contra cualquier amenaza, de forma que garanticemos en todo momento la continuidad de las actividades de la empresa. (*Organización Internacional de Estandarización*, 2022)

Brenner (2008) en su artículo sobre la ISO 27001, afirmó que las ISO son usadas como requisitos para desarrollar un sistema de gestión de seguridad de la información. En cambio Kosutic (2022) determinó que esta norma puede ser implementada en cualquier tipo de empresa con o sin fines de lucro, privadas o pública, pequeña o grande, ya que su métodos está redactada por profesionales experto en el mundo.

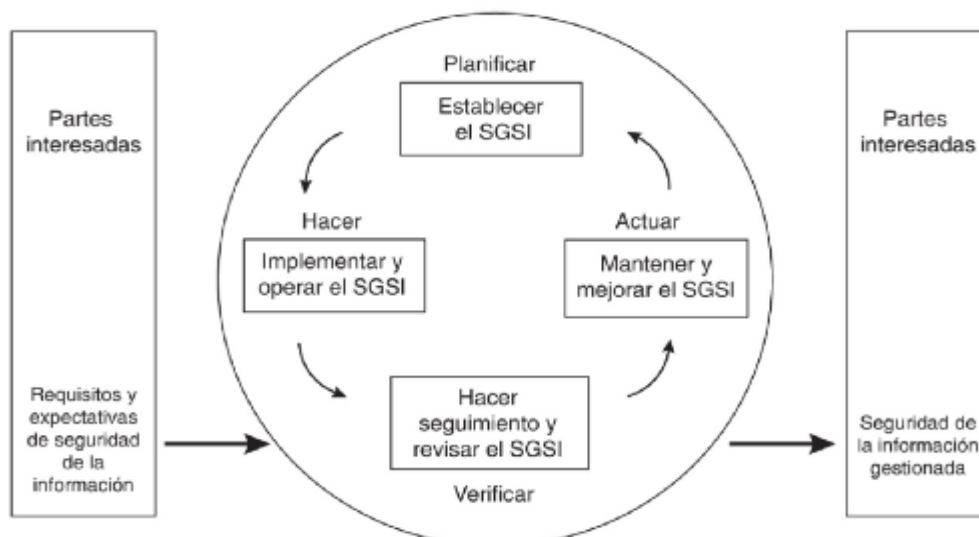
El SGSI es el conjunto de políticas, procedimientos y lineamientos que los recursos y actividades asociados que son administrados por una organización con el objetivo de proteger su información esencial. Adicionalmente, el SGSI desde la visión estándar internacional ISO 27001 es un enfoque sistemático para establecer, implementar, monitorear, revisar, mantener y mejorar la seguridad informativa de una organización y lograr sus objetivos comerciales y de servicio. (*Organización Internacional de Estandarización*, 2005, p. 1)

Fase de Implementación de ISO 27001. Las fases para la implementación de una norma ISO 27001 son la siguientes: (a) obtener la aprobación de la Dirección para iniciar el proyecto, (b) definir el alcance, los límites y la política del SGSI, (c) realizar el análisis de los requisitos de seguridad de la información, (d) realizar la valoración de riesgos y planificar el tratamiento de riesgos, (e) realizar la valoración de riesgos y planificar el tratamiento de riesgos. (Valencia & Orozco, 2017, p. 78)

Modelo del SGSI de la Norma ISO 27001. Este modelo inicia conociendo bien conceptos del alcance, determinando las áreas más críticas y procesos de la organización que se va aplicar el sistema, luego con la formulación de la política de gestión de la seguridad de la información considerando los riesgos que conlleva la información, este debe identificarse buscando las amenazas y puntos vulnerables, luego de identificar se plantea el control y tratamiento de los riesgos, a continuación se puede visualizar en la Figura 26 el modelo de gestión según la norma. (Atehortúa et al., 2008)

Figura 26

Modelo del SGSI de la norma



Nota: Tomado de “Sistema de gestión integral. Una sola gestión, un solo equipo”, por Atehortúa et al., 2008.

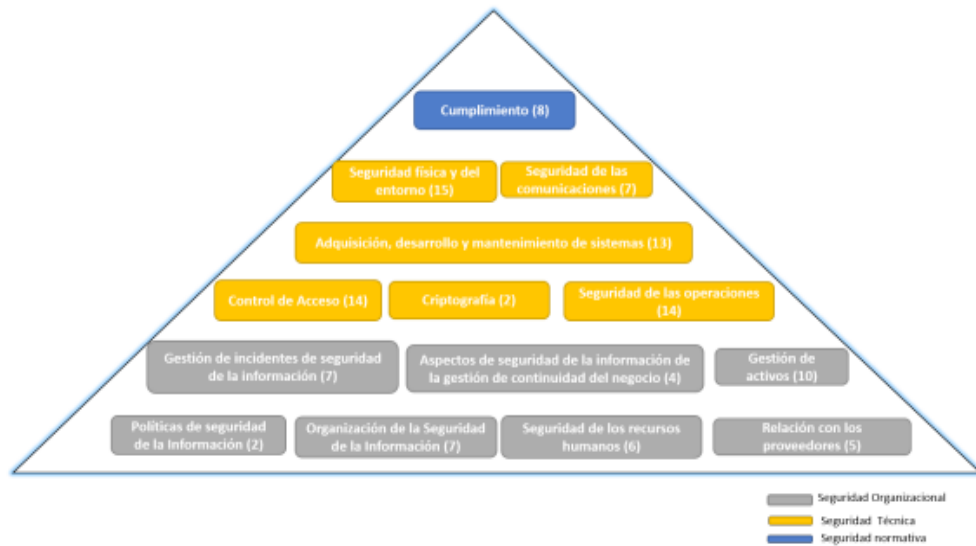
Norma oficialmente denominada Tecnología de Seguridad, Técnicas de la Información, Sistemas de Gestión de Requerimientos de Seguridad de la Información; la misma que especifica los requisitos para el establecimiento, implementación, operación, revisión, monitoreo, mantenimiento y un SGSI formalizado. El cumplimiento de los requerimientos de esta norma permite que una organización pueda obtener la certificación internacional en ISO/IEC 27001. (Valencia & Orozco, 2017, p. 76)

ISO 27002: Mejoras Prácticas Para Gestión de la Seguridad de la Información

Esta norma denominada formalmente como Tecnología de información - Técnica de seguridad -Código de prácticas para controles de seguridad de la información ha sido diseñada de acuerdo con ISO (2015) para ser usada en organizaciones que intentan: (a) seleccionar controles dentro de un proceso de implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001; (b) implementar controles de seguridad de la información comúnmente aceptados; (c) desarrollar sus propias guías de gestión de seguridad de la información. La estructura de los controles de seguridad de la información se encuentra conformada por 14 dominios, 35 objetivos de control y 114 controles, los cuales se encuentran divididos entre controles organizacionales, controles técnicos y controles normativos, como se puede apreciar en la Figura 27. (Valencia & Orozco, 2017, p. 76)

Figura 27

Estructura de los controles de la norma ISO 27002



Nota: Tomado de “*Revista Ibérica de Sistemas e Tecnología de Información*”, por Altamirano & Bayona, 2017

La norma ISO 27002 denominada anteriormente como ISO 17799, es un estándar para la seguridad de la información, la misma que ha publicado una organización internacional de normalización y una comisión electrotécnica internacional. La versión más reciente de la norma es la ISO 27002:2013. La norma ISO 27002 proporciona mejores prácticas en la gestión de la seguridad de la información a los interesados y responsables para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como la preservación de la confidencialidad, integridad y disponibilidad. (ISO Tools Excellence, 2017, p. 1)

ITIL

Las siglas ITIL significan *Information Technology Infrastructure Library*, que traduciríamos literalmente como Biblioteca de Infraestructura de Tecnologías de Información. ITIL es una guía de buenas prácticas para la gestión de servicios de tecnologías de la información (TI). La guía

ITIL ha sido elaborada para abarcar toda la infraestructura, desarrollo y operaciones de TI y gestionarla hacia la mejora de la calidad del servicio. Los pilares de ITIL son los siguientes principios, procesos, necesarios para la gestión de TI de acuerdo con la alineación de estos, dentro de la organización. Calidad, entendida como la entrega a cliente del producto o servicio óptimos, es decir, incluyendo las características acordadas. Cliente, su satisfacción es el objetivo de la mejora de los servicios, siendo, por lo tanto, el beneficiario directo de la implantación de las buenas prácticas de ITIL. Independencia, siempre deben mantenerse buenas prácticas a pesar de los métodos establecidos para cada proceso y de los proveedores existentes. (Alonso, 2020, p. 1)

La oficina del Gabinete del Reino Unido siendo una empresa pública/privada desarrolló como iniciativa un manual eficaz para la gestión de los servicios de tecnología de información. Este marco de guías se desarrolló en 1980 y en el 2019 se actualizó Itil 4. (Mann, 2021)

La versión Actual: ITIL 4

Dado que la industria de servicios moderna está siendo impulsada por la transformación digital, esta última versión actuará como una guía integral para que las organizaciones puedan gestionar mejor sus tecnologías de la información, y se enfoca en la creación de valor para los clientes. ITIL 4 también abarca las cuatro dimensiones de la gestión de servicios: organizaciones y personas, información y tecnología, asociados y proveedores, y procesos y fuentes de valor. Adicionalmente, introduce el sistema de valor de servicios de ITIL (SVS), que trata acerca de cómo los diversos componentes de la entrega de servicios se complementan en la creación de valor para los clientes. En otras palabras, ilustrará la importancia de la colaboración, las diversas prácticas y el trabajar al unísono para entregar valor, en lugar de trabajar en silos y optimizar internamente. En general, ITIL 4 continúa con el proceso de transición del ciclo de vida, y la creación de valor es su principal enfoque. (Mann, 2021, p. 1)

Código Orgánico Integral Penal, Artículo 234, Acceso no Consentido a un Sistema Informático

Art.234.- Acceso no Consentido aun Sistema Informático Telemático o de Telecomunicaciones. (a) La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho sobre dicho sistema, será sancionada con la pena privativa de la libertad de tres a cinco años. (b) Si la persona que accede al sistema lo hace para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar el tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a las o los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años. (Código Orgánico Integral Penal, 2021, p. 10)

Art. 234.1.- Falsificación Informática. (a) La persona que, con intención de provocar un engaño en las relaciones jurídicas, introducir, modificar, eliminar o suprimir contenido digital, o interferir de cualquier otra forma en el tratamiento informático de datos, produzca datos o documentos no genuinos, será sancionada con pena privativa de libertad de tres a cinco años, y (b) Quien, actuando con intención de causar un perjuicio a otro o de obtener un beneficio ilegítimo para sí o para un tercero, use un documento producido a partir de contenido digital que sea objeto de los actos referidos en el número uno, será sancionado con la misma pena.(Código Orgánico Integral Penal, 2021, p. 10b)

Normas de Auditoria NIA 315, Identificación y Valoración de los Riesgos de Incorrección Material Mediante el Conocimiento de la Entidad y de su Entorno

Esta NIA sobre la identificación y valoración de riesgo de incorrección material se estableció bajo reconocimiento del conocimiento del negocio, entorno y control interno. Esta norma servirá para el auditor como evidencia en el procedimiento de detección de riesgos y fraude. (Delgado, 2016)

Objetivos de la NIA. El objetivo del auditor es identificar y evaluar los riesgos de incorrección material, derivados de fraudes o errores, tanto en los estados financieros como en las afirmaciones, a través del conocimiento de la organización empresarial y de su entorno, incluido su control interno, para proporcionar una base para diseñar e implementar respuestas a los riesgos evaluados de incorrección material. (IAASB, 2009b, p. 3)

Valoración de Riesgo por la Entidad. El auditor obtendrá conocimiento de si la entidad tiene un proceso para: (a) la identificación de los riesgos de negocio relevantes para los objetivos de la información financiera, (b) la estimación de la significatividad de los riesgos, (c) la valoración de su probabilidad de ocurrencia, y (d) la toma de decisiones con respecto a las actuaciones para responder a dichos riesgos. (IAASB, 2009b, pp. 25-31)

El Sistema de Información, Incluidos los Procesos de Negocio Relacionados, Relevante para la Información Financiera, y la Comunicación.

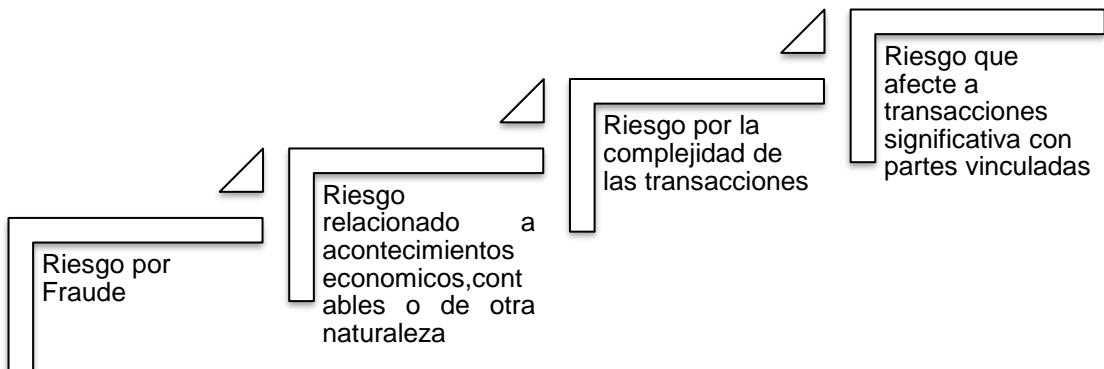
El auditor obtendrá conocimiento del sistema de información, incluidos los procesos de negocio relacionados, relevante para la información financiera, incluidas las siguientes áreas: (a) los tipos de transacciones en las operaciones de la entidad que son significativos para los estados financieros, (b) los procedimientos, relativos tanto a las tecnologías de la información (TI) como a los sistemas manuales, mediante los que dichas transacciones se inician, se registran, se procesan, se corrigen en caso necesario, se trasladan al libro mayor y se incluyen en los estados financieros, (c) los registros contables relacionados, la información que sirve de soporte y las cuentas específicas de los estados financieros que son utilizados para iniciar, registrar y procesar transacciones e informar sobre ellas; esto incluye la corrección de información incorrecta y el modo en que la información se traslada al libro mayor; los registros pueden ser tanto manuales como electrónicos, (d) el modo en que el sistema de información captura los hechos y condiciones, distintos de las transacciones, significativos para los

estados financieros, (e) el proceso de información financiera utilizado para la preparación de los estados financieros de la entidad, incluidas las estimaciones contables y la información a revelar significativas, y (f) los controles sobre los asientos en el libro diario, incluidos aquellos asientos que no son estándar y que se utilizan para registrar transacciones o ajustes no recurrentes o inusuales. (IAASB, 2009b, p. 5)

Riesgos que son Significativos. Para determinar si el riesgo identificado es significativo se considerará los siguientes apartados que se visualizan en la Figura 28.

Figura 28

Identificación de riesgos significativos



Nota: Adaptado de “Normas Internacionales de Auditoría Nía 315”, por IAASB, 2009

Norma de Auditoría 240, Responsabilidades del Auditor en la Auditoría de Estados Financieros con Respecto al Fraude

Según la firma de auditores SMS esta Norma 240 se relaciona al Fraude que se comente en la presentación de los Estados Financieros, donde se procede a identificar dos puntos: (a) el fraude intencional de los estados financieros y (b) errores no intencionales. De acuerdo con las responsabilidades es importante que se consideren las recomendaciones en implantar un sistema que les ayude a disminuir tales fraudes o errores. (Delgado, 2016a)

Evaluación de Factores de Riesgo de Fraude. El auditor evaluará si la información obtenida mediante otros procedimientos de valoración del riesgo y actividades relacionadas indica la presencia de uno o varios factores de riesgo de fraude. Si bien los factores de riesgo de fraude no indican necesariamente su existencia, a menudo han estado presentes en circunstancias en las que se han producido fraudes y, por tanto, pueden ser indicativos de riesgos de incorrección material debida a fraude. Apartados A23-27. (IAASB, 2009a, p. 141)

Responsabilidades en la Detección del Fraude. En la prevención y detección del fraude la dirección y gobierno de la empresa serán los encargados de la prevención y disuasión del fraude persuadiendo a los trabajadores a no cometer fraude, presentando una serie de control, midiendo la cultura de honestidad y comportamiento ético del personal. Esta responsabilidad también cae sobre los auditores que serán los encargados de detectar los errores y fraudes de la información presentada, mantenido una postura de escepticismo profesional durante el proceso de auditoría. (IAASB, 2009a)

Capítulo 2: Metodología de la Investigación.

Diseño de investigación

Coelho (2021) definió que la investigación es “un proceso intelectual y experimental que incluye un conjunto de métodos aplicados de manera sistemática, con el objetivo de investigar un asunto o tema, así como de ampliar o desarrollar el propio conocimiento, ya sea este de interés científico, humanístico, tecnológico social” (p. 1). Por su parte Baena (2017) indicó que la investigación es “un proceso que mediante la aplicación del método científico, procura obtener información relevante y fidedigna para entender, unificar, corregir o aplicar el conocimiento”(p. 7).

En cambio los diseños en una investigación son “conjunto de procedimientos que manipulan una o más variables independiente y se compara su efecto sobre una o más variable dependiente” (Bernal, 2010, p. 145). Un diseño de investigación se trabaja bajo la siguiente clasificación: (a) según el propósito, (b) según la cronología, y (c) según el número de mediciones. (ver Tabla 8).

Tabla 8

Delimitación del diseño de investigación

Clasificación	Aspectos
Según su Propósito	Observacional
Según la Cronología	Prospectivo
Según su Medición	Transversal

Nota: Adaptado de “El diseño de investigación: una breve revisión metodológica”, por Vallejo, 2002.

Según su propósito: Observacional

De acuerdo con Müggenburg y Pérez (2018) mencionó que el estudio observacional son aquellas técnicas que permite obtener información por medio de observación directa y registro de fenómeno sin ninguna intervención.

A partir de esto se analiza que esta investigación es de tipo observacional porque, por medio de la investigación directa del entorno y de donde se presenta la problemática existente, se registrará las características de los objetos estudiados. Por lo tanto, este no se limita al sentido de la vista, sino que se procederá a tomar en cuenta todo sin manipular el entorno natural del estudio.

Según la Cronología: Prospectivo

De acuerdo con Müggenburg y Pérez (2018) definió que los estudios prospectivos son aquellos que empiezan indagando sobre hechos ocurridos en el pasado y continúan en el tiempo a fin de observar sus consecuencias.

A partir de esto, se analiza que esta investigación es de tipo prospectivo porque, se estudiará los hechos ocurridos en el tiempo y así proponer una metodología para prevenir errores y fraudes en los sistemas de información contable.

Según su Medición: Transversal

De acuerdo con Müggenburg y Pérez (2018) indicó que la medición transversal son “aquellos en los que se recolectan datos en un sólo momento, en un tiempo único. Su objetivo es poder describir variables y analizar su comportamiento en un momento dado”. (p. 37)

A partir de esto, se considera que esta investigación es de tipo transversal porque, permite recolectar datos, describir y analizar el comportamiento de las variables en un periodo de tiempo determinado. Con la finalidad de obtener información referente a las variables de la propuesta que tratan sobre: (a) los riesgos en sistemas, (b) el acceso físico y lógico de los sistemas de información contable, y (c) prevenir errores y fraudes.

Enfoque de Investigación

Este trabajo se diseñará bajo el enfoque de investigación cualitativo, ya que es el que mejor se adapta a las necesidades de la investigación.

Hernández et al, (2014) mencionó que en el enfoque cualitativo “se utiliza la recolección y análisis de los datos para desarrollar las preguntas de

investigación o revelar nuevas interrogantes en el proceso de interpretación” (p. 7). Adicionalmente, comentó “el propósito no es siempre contar con una idea y planteamiento de investigación completamente estructurados; pero sí con una idea y visión que nos conduzca a un punto de partida” (Hernández et al., 2014, p. 26).

Por otra parte, Bernal (2010) indicó que los investigadores que utilizan el método cualitativo buscan comprender la situación social en su conjunto, teniendo en cuenta sus características y dinámicas. La investigación cualitativa tiene como objetivo conceptualizar la realidad, a partir de la información obtenida de la población o las personas estudiadas.

A partir de esto se analiza que esta investigación se realizará por medio del enfoque cualitativo, donde se pretende realizar entrevistas a profundidad determinar las problemáticas existentes en el estudio, con la finalidad de completar la información y buscar alternativas de mejoramiento en el entorno de las PYMES y en el acceso físico y lógicos de los sistemas de información contable en el sector acuícola.

Tipo de Investigación

Bernal (2010) indicó que “una de las funciones principales de la investigación descriptiva es la capacidad para seleccionar las características fundamentales del objeto de estudio y su descripción detallada de las partes, categorías o clases de ese objeto” (p. 113). En la investigación descriptiva “muestran, identifican hechos, situaciones, rasgos o atributos de la población de un objeto de estudio” (Bernal, 2010, p. 120).

Según Hernández et al, (2014) indicó que los estudios descriptivos tiene como objetivo indagar a profundidad sobre la información de forma independiente o conjunta sobre los conceptos o las variables a los que se refieren. Por lo tanto, pueden integrar las medidas o información de cada una de dichas variables o conceptos para decir cuál es el fenómeno de interés y cómo se manifiesta. (p. 95)

A partir de esto se analiza que esta investigación es de tipo descriptiva, la misma que permite identificar los orígenes y las situaciones en que se

presenta la problemática de estudio y sus variables, considerando que la investigación se centra en el sector acuícola, con la finalidad de obtener información y generar una base fundamental para desarrollar la propuesta metodológica que trata sobre la reducción de riesgos en el acceso físico y lógico de los sistemas de información contable.

Fuente de Información

Una fuente de investigación es todo documento, persona, organización u objeto que sirven como base de datos para analizar, reconstruir hechos y base de conocimiento para lograr los objetivos del estudio originado del problema de la investigación, convirtiéndose en datos o fuentes confiables. (Maranto & González, 2015, p. 2)

Estas fuentes pueden ser primaria y secundaria para Bernal (2010) las fuentes primarias han sido “aquellas de las cuales se obtiene información directa, es decir, de donde se origina la información, ejemplo cuando se entrevista a las personas que tienen relación directa con la situación objeto del estudio” (p. 182). Y las fuentes secundarias son “aquellas que ofrecen información sobre el tema que se va a investigar, en referencia, por ejemplo: (a) libros, (b) revistas, (c) artículos académicos, y (d) medios electrónicos” (Bernal, 2010, p. 192). En otras palabras, la información primaria no existe en el momento que el investigador lo requiera, sino que debe desarrollarse, en cambio la información secundaria, son datos que alguien ya reunió para otras investigaciones y puede ser usada como manual de consulta en la propuesta metodológica.

Por medio de la investigación se procederá a utilizar la fuente primaria, la misma que se llevará a cabo por medio de entrevista para la obtención de información primaria dando como resultado las opiniones de los expertos en sistemas de información y encargados de las áreas contables, las cuales servirán como una guía para desarrollar la propuesta metodológica que trata sobre la reducción de riesgos en el acceso físico y lógico de los sistemas de información contable para prevenir errores y fraudes. Además, utilizaremos la información secundaria de diversas fuentes de información como sustento a

lo investigado y complementar a la investigación primaria en las Pymes del sector acuícola. Estas fuentes generarán la información necesaria para la propuesta metodológica.

Población

La población de estudio es un conjunto de casos, definidos y accesibles, los mismos que se constituyen como referencia para la selección de la muestra y que cumple una serie de criterios. Cabe precisar que, al hablar de población de estudio, el término no designa exclusivamente a humanos, sino que puede corresponder a animales, prototipos biológicos, archivos, hospitales, objetos, familias, organizaciones, etc.; para estos últimos quizás sería más apropiado utilizar un término análogo como universo de estudio. (Arias, 2016)

La Corporación Financiera Nacional CFN (2022) detalló los siguientes datos sobre las empresas del sector acuícola:

- En el año 2020 existieron 1.301 empresas pertenecientes al sector camaronero, de las cuales el 88% del total eran empresas dedicadas a la explotación de criaderos de camaroneros.
- Se concentraron en la actividad de explotación de criaderos de camarones, el 80% de los 52.399 empleos registradas en el sector camaronero.
- En las tres actividades se observó que más del 50% de las empresas se encontraron en la Provincia de Guayas. (p. 5)

A continuación, se muestra tablas y figuras correspondientes a los datos de la población del sector acuícola:

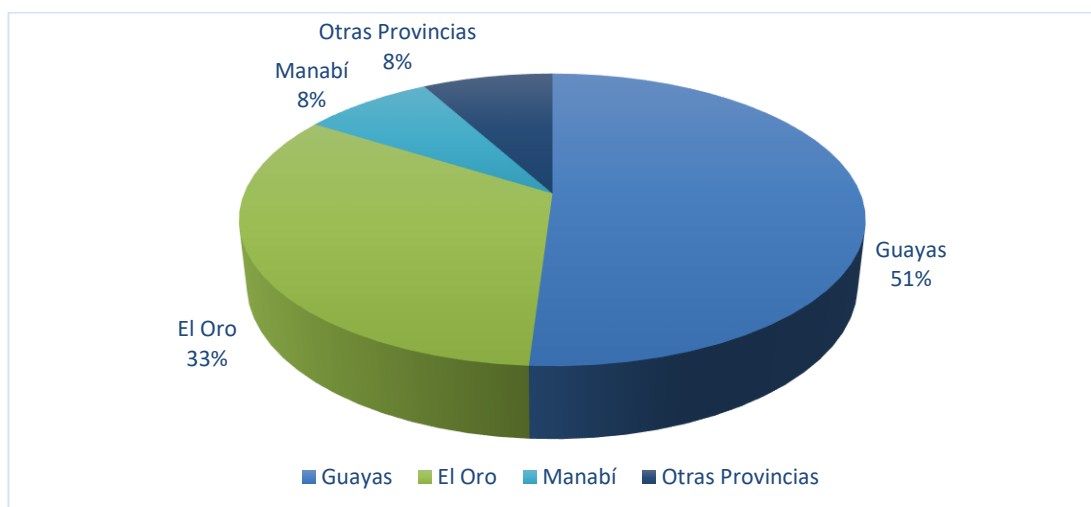
Tabla 9*Explotación de criaderos de camarones*

Tamaño Empresa	# Empresas 2020	# Empleados 2020
Grande	87	29.601
Mediana	229	6.252
Pequeña	353	3.840
Microempresa	466	2.332
No Definido	8	0
Total	1.143	42.025

Nota: Tomado de “Ficha Sectorial Camarón”, por Corporación Financiera Nacional, 2022

Figura 29

Participación (%) del # empresas dedicadas a la explotación de criaderos de camarones.



Nota: Tomado de “Ficha Sectorial Camarón”, por Corporación Financiera Nacional, 2022

De acuerdo a la Tabla 9 y Figura 29 se concluyó que, el sector acuícola es considerado como uno de los principales sectores económicos del país, debido a su contribución con la economía. En el año 2020 existieron tres actividades comerciales, de las cuales el 88% del total de las empresas corresponde a la explotación de criaderos de camarones, teniendo como resultado 1.143 empresas y 42.025 empleados. La participación porcentual de

los números de empresas dedicadas a la explotación de criaderos de camarones en el sector acuícola a nivel nacional es: Guayas posee una participación del 51%, seguido de El Oro con un 33%, Manabí 8% y Otras Provincias 8%. La distribución porcentual a nivel nacional denota que la Provincia del Guayas es la predominante en cuanto a su actividad en la explotación de criaderos de camarones.

Tabla 10

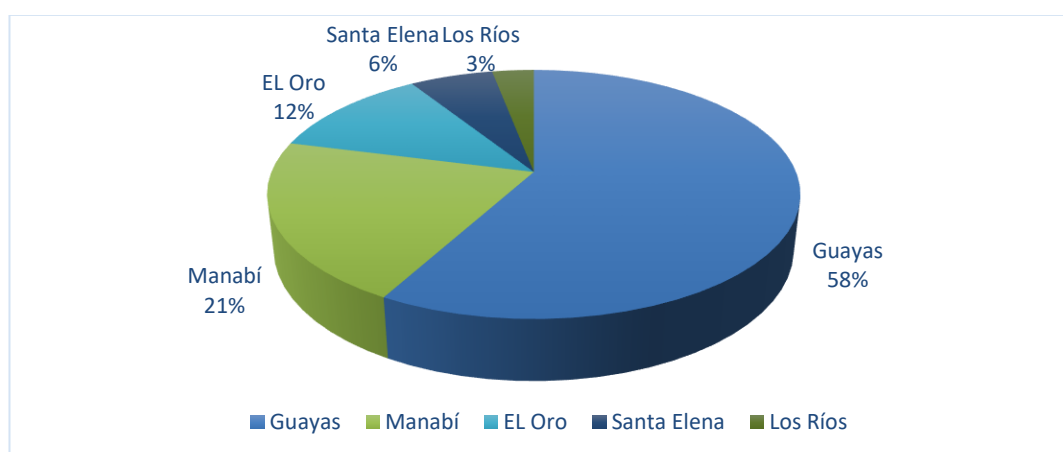
Preparación, conservación y elaboración de productos de camarón y langostinos.

Tamaño Empresa	# Empresas 2020	# Empleados 2020
Grande	12	7.814
Mediana	3	164
Pequeña	7	66
Microempresa	11	50
Total	33	8.094

Nota: Tomado de “Ficha Sectorial Camarón”, por Corporación Financiera Nacional, 2022

Figura 30

Participación (%) del # empresas dedicadas a la preparación y conservación de camarón y langostinos.



Nota: Tomado de “Ficha Sectorial Camarón”, por Corporación Financiera Nacional, 2022

En la Tabla 10 y Figura 30, se muestra a la actividad de preparación y conservación de camarón y langostinos durante el 2020, la misma que posee un total de 33 empresas y 8.094 empleados. La participación porcentual del

número de empresas dedicadas a la preparación y conservación de camarón y langostinos en el sector acuícola a nivel nacional es: Guayas con una participación del 58%, seguido de Manabí 21%, El Oro con un 12%, Santa Elena 6% y Los Ríos 3%. La distribución porcentual a nivel nacional denota que la Provincia del Guayas es la predominante en cuanto a su actividad en la preparación y conservación de camarón y langostinos.

Tabla 11

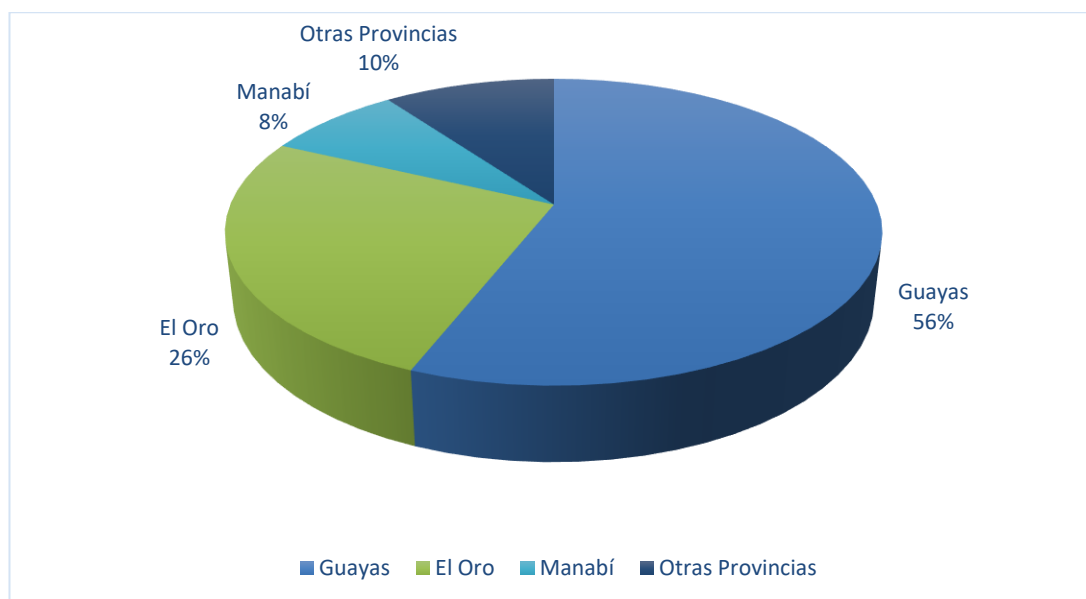
Venta al por mayor de camarón y langostinos.

Tamaño Empresa	# Empresas 2020	# Empleados 2020
Grande	10	1.697
Mediana	12	82
Pequeña	30	179
Microempresa	71	322
No Definido	2	0
Total	125	2.280

Nota: Tomado de “Ficha Sectorial Camarón”, por Corporación Financiera Nacional, 2022

Figura 31

Venta al por mayor de camarón y langostinos.



Nota: Tomado de “Ficha Sectorial Camarón”, por Corporación Financiera Nacional, 2022

Tabla 11 y Figura 31, detalla la actividad de venta al por mayor de camarón y langostinos durante el 2020, la misma que posee un total de 125 empresas y 2.280 empleados. La participación porcentual del número de empresas dedicadas a la venta al por mayor de camarón y langostinos en el sector acuícola a nivel nacional es: Guayas con una participación del 56%, seguido de El Oro 26%, Manabí 8% y Otras Provincias 10%. La distribución porcentual a nivel nacional denota que la Provincia del Guayas es la predominante en cuanto a su actividad en la venta al por mayor de camarón y langostinos.

Para el desarrollo en esta investigación se procederá con la obtención de información por medio de entrevistas a expertos, considerando nuestra población dentro del territorio de la Provincia del Guayas, por cuanto se observó que en las tres actividades que ejercen las empresas del sector acuícola, más del 50% de las empresas se encontraron radicadas en la provincia de Guayas, población en la que se espera conseguir información específica sobre los errores y fraudes que existen al momento de acceder a los sistemas de información contable a través de un enfoque cualitativo y por consiguiente revelar los orígenes de los casos.

Muestra

Según Hernández et al.,(2014) la muestra ha sido “una unidad de análisis o un grupo de personas, contextos, eventos, sucesos, comunidades etc., de análisis sobre la cual se habrán recolectar datos, sin que necesariamente sean representativo del universo o población que se estudia” (p. 242).

La muestra es un subgrupo de la población, y se pueden dividir en muestra probabilísticas y no probabilísticas, donde las probabilísticas requerirá precisar el tamaño de la muestra, es decir la población con la misma posibilidad de ser escogidos para la muestra y pueden ser: (a) aleatoria simple, (b) sistemático, (c) estratificado, entre otras (ver Figura 32). Mientras que la no probabilística no dependerán de la probabilidad sino de las causas asociadas por unos casos o varios propósitos, dependerá del juicio del

investigador, se usará en técnicas utilizadas en estudios cualitativos, además se usa cuando el tiempo es limitado de la investigación y se realiza para observar si un tema necesita un análisis más profundo. (Hernández et al., 2014)

Figura 32

Tipos de muestra



Nota: Adaptado de “El muestreo en la investigación cualitativa”, por Martínez, 2012.

La elección de una muestra no probabilística o de juicio, no parte de un número determinado de antemano. Como suele declararse insistentemente, en este campo no probabilístico, no hay reglas para decidir el tamaño de la muestra y, si tuviera que decir una, es: “todo depende”. Depende del objetivo del estudio, qué es útil para su realización, que hay en esto que lo hace probable y finalmente hasta qué es posible. Así, para poder juzgar si una muestra es adecuada, es necesario conocer el contexto del estudio. Otra característica de este tipo de procedimiento es que el tamaño de la muestra no se conoce al inicio, sino cuando se completa lo investigado. La forma del muestreo inicia en la búsqueda de los participantes, pero su incorporación se hace de acuerdo a la información que surge en el trabajo de campo. Como

señalan los expertos de este tipo de investigación, aquí lo decisivo no es el tamaño de la muestra sino la riqueza de los datos aportados por los participantes, la capacidad de observación y análisis del investigador. (Patton, 2002)

El presente trabajo se considera la muestra no probabilística, ya que los procedimientos de selección responden más a el juicio del investigador y conveniencia, donde se recogerá información de expertos en los sistemas de información y encargados de las áreas contables en el sector acuícola, para encontrar respuestas al problema de estudio.

En relación a la muestra no probabilística, ésta fue diseñada por medio del muestreo caso típico. Peña (2006) mencionó que el muestreo de caso típico tiene como propósito mostrar a quién no está familiarizado con la realidad objeto de análisis los rasgos más comunes de dicha realidad. La definición de “típico” está construida a partir del consenso de opiniones entre los informantes clave, que conocen la realidad que se estudia.

Esta técnica de muestreo se usa en trabajos de investigación para recolectar datos específicos y de alta calidad, no se enfocan en la cantidad, ni en los resultados de toda una población. Este tipo estudio se relaciona un poco con la fundamentación, en el sentido, de que intentan investigar todo lo relacionado con el problema examinado. Por ejemplo, estudios en profundidad de las experiencias creencias, actitudes, etc., de los entrevistados. (Martínez, 2012)

En el muestreo caso típico, los expertos deben cumplir con ciertas características (ver Tabla 12): (a) tener cinco años laborando en el sector acuícola, (b) tener cargos medios y altos en la entidad donde labora, (c) tener conocimiento sobre el acceso físico y lógico de los sistemas de información, (d) tener conocimientos contables, y (e) tener conocimientos en el control interno. Esta muestra está principalmente destinada para realizar la entrevista a expertos en el acceso físico y lógico de los sistemas de información y encargados del área contable del sector acuícola. Además, para el desarrollo de las entrevistas se definió un tamaño de 15 muestras, pero estas deben cumplir con todas las características, caso contrario no serán consideradas.

Tabla 12

Características que debe cumplir el perfil del experto

Características que debe cumplir el experto	Cumplimiento														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Tener cinco años laborando en el sector acuícola.	✓	×	✓	✓	✓	✓	✓	×	×	✓	×	✓	×	✓	×
Tener cargos medios y altos en la entidad donde labora.	×	×	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Tener conocimientos sobre el acceso físico y lógico de los SI.	✓	✓	✓	✓	✓	×	✓	✓	×	✓	×	✓	×	✓	×
Tener conocimientos contables.	✓	✓	✓	×	✓	×	✓	✓	✓	✓	✓	✓	×	✓	×
Tener conocimientos en el control interno.	×	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	✓
Cumplimiento del experto	NO	NO	SI	NO	SI	NO	SI	NO	NO	SI	NO	SI	NO	SI	NO

Nota: Adaptado de “*El muestreo en la investigación cualitativa*”, por Martínez, 2012.

Entre la muestra tenemos a seis expertos que cumplen con todas las características, los mismos que serán considerados para la recolección de datos.

Técnicas de Recolección de Datos / Herramientas Cualitativas

Hernández y Ávila (2020) indicaron que las técnicas en la recolección de datos son “aquellos procedimientos que recogen los datos primarios y secundarios según el propósito para obtener información necesaria para dar respuesta a las preguntas de investigación, entre las técnicas usadas está la entrevistas, usando instrumentos como (a) cuestionarios, y (b) guías de preguntas” (p. 2).

De acuerdo con el enfoque cualitativo, la técnica de recolección de datos es fundamental para obtener información de sujetos, comunidades, expertos que con sus experiencias de vidas aportan al tema de la propuesta metodológica, y el principal objetivo es profundizar en el tema. (Hernández et al., 2014). En nuestro trabajo de investigación se empleará la técnica de la entrevista, para la obtención de los datos primario que se aplicará a experto de manera individual.

Entrevistas a Profundidad

Hernández et al., (2014) definió a la entrevista como “una conversación entre una persona (el entrevistador) y otra (el entrevistado) u otros (entrevistados), aplicando cuestionarios como instrumentos cualitativos, siendo las preguntas bajo la división de (a) estructuradas, y (b) semiestructurada” (p. 371).

Se procederá a trabajar en la propuesta metodológica con las entrevistas semiestructuradas, que podrán ser flexibles a la hora de responder por el entrevistado y a la vez el entrevistador tendrá libertad de realizar preguntas adicionales para definir conceptos y obtener mayor información sobre el objetivo planteado.

Díaz et al., (2013) indicó que las entrevistas semiestructuradas son aquellas que ofrecen más flexibilidad que las entrevistas estructuradas, porque parten de preguntas planificadas, que se pueden ajustar a los entrevistados. Tiene como ventaja el poder adaptarse a temas de enormes posibilidades para motivar al interlocutor, aclarar términos, poder identificar ambigüedades y reducir el formalismo. (p. 163)

Análisis de Datos

En el análisis cualitativo, una vez obtenidos los resultados de la entrevista, se debe reducir los datos, teniendo cuidado de no perder información o descartar datos valiosos.

Hernández (2014) indicó que la recolección de datos y el análisis ocurren en paralelo, donde el propósito de su análisis cualitativos son: (a) explorar los datos, (b) imponer una estructura, (c) interpretar y explicar los conceptos obtenidos, (d) comprender en profundidad el contexto que rodea los datos, (e) reconstruir hechos e historias, y (f) vincular los resultados y generar teorías en los datos. (p. 451)

Los datos en la técnica de la entrevista fueron recolectados bajo el instrumento de entrevistas semiestructuradas, permitiendo que los entrevistados tenga libertad en responder y el entrevistador realice preguntas abiertas para profundizar en el tema y así obtener los resultados. Se procederá con la documentación de los resultados, de acuerdo a las opiniones de los expertos de sistemas de información y encargados del área contable, las mismas servirán como aporte a la propuesta metodológica para la reducción de riesgos de los sistemas de información contable de empresas del sector acuícola de la provincia del Guayas.

Diseño de Instrumentos de Investigación

Dicha entrevista tiene como objetivo profundizar en el tema propuesto para la reducción de los riesgos en los sistemas de información contable, con la finalidad de identificar los posibles errores y fraudes más comunes que existen en las áreas críticas que seleccione los expertos.

Las entrevistas serán aplicadas a dos expertos en los sistemas de información y cuatro expertos encargados en las áreas contables, de acuerdo a nuestra muestra caso típico se seleccionaron a los expertos que cumplieron con todas las características que se solicitaron. (ver Tablas 13 y 14)

Tabla 13*Expertos que cumplieron las características*

Características que debe cumplir el experto	Cumplimiento					
	3	5	7	10	12	14
Tener cinco años laborando en el sector acuícola.	✓	✓	✓	✓	✓	✓
Tener cargos medios y altos en la entidad donde labora.	✓	✓	✓	✓	✓	✓
Tener conocimientos sobre el acceso físico y lógico de los SI.	✓	✓	✓	✓	✓	✓
Tener conocimientos contables.	✓	✓	✓	✓	✓	✓
Tener conocimientos en el control interno.	✓	✓	✓	✓	✓	✓
Cumplimiento del experto	SI	SI	SI	SI	SI	SI

Nota: Adaptado de “*El muestreo en la investigación cualitativa*”, por Martínez, 2012.

Por lo tanto, se detalla en la siguiente tabla el perfil de los expertos seleccionados y aptos para las entrevistas semiestructuradas:

Tabla 14*Perfil de expertos*

Perfil de Expertos	Número
Asesor de Sistemas	1
Desarrollador de Sistemas	1
Administrador General	1
Contador	1
Asistente Contable	2
Total	6

Nota: Adaptado de “*La entrevista, recurso flexible y dinámico*”, por Díaz et al., 2013.

Resultados

Los resultados se han recolectado a través de la entrevista a profundidad, indagando sobre los datos cualitativos que permitió generar amplitud y profundidad en los resultados al proceder de diversos expertos que poseen conocimientos sobre los accesos a los sistemas de información contables.

Primera Entrevista a Experto de Jefe de Sistema

Nombre del Experto: Ing. Jorge Luis Viteri Ulloa.

Perfil del Experto: Desarrollador de Sistemas, Asesor en Auditoría de Sistemas y Contable.

1. Desde su punto de vista ¿Cuál es el motivo por el cual los empresarios adquieren un sistema de información?

Desde mi punto de vista existe dos motivos, la primera es por controlar la información ya que con esta les permite controlar el dinero y el segundo motivo para obtener información de ese control, todas las personas que trabajan en una empresa o en una organización necesitan ingresar información para obtener información, el sistema actúa como un puente, en el que ordena todo lo que se ha ingresado para obtener lo que se necesita y la mayor parte de los empresarios necesitan tener información y controlar lo que se ingresa.

2. De acuerdo con su criterio ¿Qué ventajas obtienen las empresas al adquirir un sistema de información?

Unas de las ventajas que se obtiene al manejar los sistemas de información es el control individual de los procesos. Es decir, tener información precisa de todas las actividades que se realiza en una camaronera.

3. De acuerdo con su criterio ¿Qué desventajas obtienen las empresas al adquirir un sistema de información?

Lo único que se puede considerar como desventaja es la capacitación de las personas, la competencia de las personas con las que se va a trabajar es el único detalle con lo que se puede enfrentar un empresario al implementar un sistema de información y la selección del sistema o usar un sistema que ya tenga experiencia en lo que se hace, porque el problema sería adquirir un sistema que recién está trabajando, recién se está desarrollando para aplicarlo en el giro del negocio.

4. Si tuviese que dibujar los flujos de la información en los sistemas de información contable del sector acuícola ¿Qué elementos resaltaría en dicho gráfico?

Unos de los procesos o subprocesos que resaltaría más, es el proceso de la crianza del camarón, ya que en este intervienen varios factores, entre esos está el costo del mantener una piscina y de ahí influye todos los costos para obtener al final un camarón, desde las larvas, el mantenimiento de las piscinas, el balanceado que se va a usar, durante qué tiempo, cual es el tiempo de crecimiento de ese camarón, todos esos temas influirían, específicamente la crianza del camarón todos los gastos que este incurre para al final lograr obtener un balance y saber cuánto se gastó en esa producción y en cuanto de vendió.

5. ¿Cuáles cree que son los problemas que se pueden presentar al momento de implementar un sistema de información? Liste los problemas de mayor a menor magnitud.

Existen varios problemas entre uno de ellos, el sistema que requisitos solicita a nivel de equipos de computación o solicita unos PC con tecnología de procesadores algo especiales, esto ya sería un gasto, si el sistema requiere de servidores especiales, una red, un sistema de comunicación especial, al referirse especial se habla de costos, una de las cosas principales es que un sistema debe ser adaptable a lo que tenemos, por ejemplo existe ciertas computadoras que puedan aplicarse a los requisitos del sistema, porque si existe computadoras con más de cinco años de antigüedad y no contamos con servidores ni con redes que faciliten el trabajo eso incurriría un gasto mayor, a veces el costo del sistema no es igual al costo del hardware, el software es mucho más caro que el hardware, ese sería uno de los problemas mayores, a esto se le llamaría la infraestructura. El otro problema que podría existir son las personas con las que se cuenta para ejecutar las actividades, que plan de capacitación se va a implementar, durante qué tiempo se va a capacitar en el software, cuáles son los requisitos o levantamiento de la información que el software debe cumplir, quien va a liderar esa implantación,

son puntos que las empresas no toman en cuenta al implementar un sistema. Hay otro problema que las empresas no están organizadas estructuralmente como una organización, no cuentan con manuales de procedimientos, manuales de funciones, organigramas, caracterización de los procesos, tener clara toda esa parte porque todo lo que se tiene como organización documental, tiene que estar y formar parte del software para poder implementar.

6. De acuerdo con su criterio ¿Cuáles son las áreas más críticas donde puede existir mayores riesgos de errores y fraudes en los sistemas de información de este tipo de compañía? Favor liste primero y ordene desde la mayor a la menor criticidad.

Existe fraude en cualquiera de los procesos o subprocesos de la organización, puede haber fraude en el inventario poder ingresar información de alguna manera para poder afectar el inventario, también existe fraude en la parte financiera, administrativa, en los costos de producción, en las importaciones, en todos los procesos puede existir fraude. El tema está en identificar como evitar ese fraude por eso que el contralor interno, debe ser una persona que conozca muy bien el software, que conozca el giro del negocio para poder intervenir y poder observar en donde se pueden ocasionar estas situaciones, el hecho de tener un sistema de información no implica que no vaya a existir fraudes, lo puede haber, pero siempre tiene que estar controlado.

7. ¿Qué eventos o situaciones considera usted que podrían generar situaciones de riesgo de acceso físico y lógico en los sistemas de información contable en el sector acuícola? (Analizar de forma general)

Las empresas invierten cantidades de dinero para evitar que accedan a la información externamente pero no se puede acceder a la información externamente si no tienen a alguien interno, por eso es bueno controlar al personal que se contrata que tenga toda su documentación al día, poderlos investigar, saber dónde viven, a que se dedican a que se dedicaron, porque

el acceso físico de la información se lo hace internamente no externamente, si instalan un virus lo instalan de forma interna para que de forma externa controlarlo y el costo de esta situación es demasiado alto para controlar, porque a veces las organizaciones piensan que al colocar firewall o sistemas de seguridad ante hackeo pueden ayudarlo pero no es así, el problema radica de manera interna.

8. ¿Qué tipo de errores y de situaciones de fraudes se pueden presentar en el acceso físico y lógico de los sistemas de información contable en el sector acuícola? (Analizar de forma específico)

Existen errores al ingresar mal la información, no parametrizar las opciones de acceso a los usuarios, no tener pruebas de validación de información y notificaciones automatizadas que genere el sistema a los encargados departamentales y contralor interno para que estos estén informados de las actividades que se realiza.

9. Desde el punto de vista de un usuario ¿Cuáles podrían ser las medidas de control que se deberían implementar para reducir el riesgo de acceso físico y lógico a los sistemas de información contable en el sector acuícola?

El análisis de riesgos se basa en una metodología o una norma en este caso, la norma ISO 33000, esta norma analiza el riesgo desde el punto de partida del usuario, que riesgos como usuario puede tener al facilitar una clave al compañero, que riesgo se puede obtener a que observen la clave, que riesgo se puede tener al que el computador no tenga un antivirus, que riesgo se puede obtener a que el usuario comparta información, que riesgo se puede tener a que usuario tome una foto de la computadora, todo esto se basa al riesgo de la seguridad de la información, quienes tienen acceso a las computadoras, quienes pueden acceder por medio de teléfonos tal vez los que tienen acceso puede lograr tener información genérica no general de toda la empresa como la información más delicada, es ahí como expertos en sistemas parametrizamos los sistemas conforme a los usuarios y si el usuario

tiene una clave con privilegios que puede acceder a la información importante de la empresa y esa clave es tomada por otro usuario talvez con la finalidad de poder espiar o acceder a los sistemas ahí puede surgir un problema, por eso las claves de acceso y los métodos de accesos deben ser muy analizados en cuanto al tema del giro del negocio, cuando el sistemas es mucho más seguro en ese tema es más costoso. Porque a veces algunos de los accesos son con la huella dactilar, otro es con la retina del ojo, con tarjetas otros funcionan con la voz; realmente estos son los problemas más grandes el acceso a las claves con privilegio.

10. Desde el punto de vista de un experto en sistemas ¿Cuáles cree que podrían ser las medidas de control que se deberían implementar para reducir el riesgo de acceso físico y lógico a los sistemas de información contable en el sector acuícola?

Realizar evaluaciones para medir conocimientos, iniciativas y aspiraciones que tienen en la empresa y establecer específicamente su experiencia con el sistema. Con la finalidad de conocer y analizar el método que están ejecutando en los accesos físicos y lógico de los sistemas y así buscar los controles indicados para mitigar los riesgos.

11. ¿Qué tipo de educación y entrenamiento se aplica para desarrollar una base de conocimientos a los usuarios para el manejo de la parte física y lógica de los sistemas de información del área que considera más crítico?

Las capacitaciones constantes de acuerdo al sistema que se adquiere, incluso capacitaciones sobre el mal uso de los sistemas que resultados se obtienen al manejar dichos sistemas y cuáles son los métodos correctivos que se aplicaría.

12. Si tuviese que armar un FODA para los sistemas de información para este tipo de empresa PYMES que elementos incluiría en cada parte.

ANÁLISIS FODA		
	ASPECTOS POSITIVOS	ASPECTOS NEGATIVOS
ANÁLISIS INTERNO	<p>FORTALEZAS</p> <p>Controlar la información.</p>	<p>DEBILIDADES</p> <p>El acceso a las claves con privilegios.</p>
ANÁLISIS EXTERNO	<p>OPORTUNIDADES</p> <p>Información ordenada.</p>	<p>AMENAZAS</p> <p>El hackeo a los sistemas de información.</p>

13. Desde su perspectiva, ¿Qué otra cosa considera usted podría ayudar en la reducción de riesgos en los sistemas de información contable?

Tener métodos de análisis para dar los accesos a los usuarios, investigar los antecedentes de los usuarios, donde trabajaron, a que se dedicaron, tener un contralor que conozca el software y todo el tema del giro del negocio y que este pueda identificar con mayor rapidez donde puede estar los riesgos y establecer controles internos.

Segunda Entrevista a Experto Analista de Sistemas

Perfil del Experto: Cargo Jefe de Ingeniería de Procesos.

Experiencia: Analista de Aplicaciones por 10 años, Jefe de Tecnologías de Información por cuatro años, Ingeniero de Procesos por cinco años, Jefe de Procesos por un año, Desarrollo y Administración de Aplicaciones.

1. Desde su punto de vista ¿Cuál es el motivo por el cual los empresarios adquieren un sistema de información?

Desde mi punto de vista los motivos por los que se adquieren un sistema de información son por: (a) optimización de procesos, (b) seguridad y control,

(c) mejoras operativas o funcionales, (d) ahorros económicos, y (e) mayor competitividad.

2. De acuerdo con su criterio ¿Qué ventajas obtienen las empresas al adquirir un sistema de información?

Las ventajas que se obtienen al adquirir un sistema de información son: (a) la seguridad de la información, (b) el control y seguimiento de procesos, (c) los reportes en tiempo real, (d) indicadores de desempeño, y (e) empresa apoyada en tecnología.

3. De acuerdo con su criterio ¿Qué desventajas obtienen las empresas al adquirir un sistema de información?

Según mi criterio entre las desventajas tenemos la dependencia de la tecnología, alta inversión inicial, brechas de seguridad informática, requerimiento de expertos, y gastos en capacitación a empleados.

4. Si tuviese que dibujar los flujos de la información en los sistemas de información contable del sector acuícola ¿Qué elementos resaltaría en dicho gráfico?

En los flujos de información en los sistemas de información contable del sector acuícola los elementos que resaltaría serían cinco: (a) gastos, (b) insumos, (c) ingresos, (d) laboratorio, y (e) producción.

5. ¿Cuáles cree que son los problemas que se pueden presentar al momento de implementar un sistema de información? Liste los problemas de mayor a menor magnitud.

Los problemas que se presentan al implementar un sistema de información son los siguientes considerando de mayor a menor magnitud: (a) falta de presupuesto, (b) obsolescencia tecnológica, (c) renuncias de personal, (d) problemas con proveedores, y (e) resistencia al cambio.

6. De acuerdo con su criterio ¿Cuáles son las áreas más críticas donde puede existir mayores riesgos de errores y fraudes en los sistemas de información de este tipo de compañía? Favor liste primero y ordene desde la mayor a la menor criticidad.

Las áreas más críticas de mayor a menor donde se presentan riesgos de errores en los sistemas de información son de: (a) finanzas, (b) seguridad de TI, (c) inventarios, (d) impuestos, y (e) otros.

7. ¿Qué eventos o situaciones considera usted que podrían generar situaciones de riesgo de acceso físico y lógico en los sistemas de información contable en el sector acuícola? (Analizar de forma general)

Entre las situaciones que generarían riesgos de acceso físico y lógico son: (a) la falta de seguridad o su ausencia, (b) falta de conocimiento, (c) cambios de personal, (d) insatisfacción de empleados, y (e) importancia de la empresa.

Análisis:

- A mayor tecnología mayor vulnerabilidad.
- Los sistemas de información pueden ser atacados local o remotamente lo cual aumenta esta probabilidad.
- Muchas empresas descuidan o no implementan seguridades a sus sistemas de información lo cual disminuye su fiabilidad.
- El personal siempre será la primera línea de defensa para un sistema de información por lo cual debe estar capacitado, satisfecho y empoderado con la empresa.

8. ¿Qué tipo de errores y de situaciones de fraudes se pueden presentar en el acceso físico y lógico de los sistemas de información contable en el sector acuícola? (Analizar de forma específico)

Bueno, entre los tipos de errores y situaciones de fraudes que se presentan en el acceso físico se puede mencionar que son los fraudes económicos, eliminación de información, robo de información, espionaje empresarial, y falsa contabilidad.

9. Desde el punto de vista de un usuario ¿Cuáles podrían ser las medidas de control que se deberían implementar para reducir el riesgo de acceso físico y lógico a los sistemas de información contable en el sector acuícola?

Desde mi punto de vista como usuario, las medidas de control como usuario diría que se deberían implementar para reducir riesgos de acceso físico y lógico en los sistemas de información son: el buen manejo de claves, validación de resultados, auditorías Informáticas, segmentación de perfiles, y actualización de seguridad.

10. Desde el punto de vista de un experto en sistemas ¿Cuáles cree que podrían ser las medidas de control que se deberían implementar para reducir el riesgo de acceso físico y lógico a los sistemas de información contable en el sector acuícola?

Desde el punto de vista de un experto en sistemas las medidas de control sería: Seguridad por hardware, seguridad por software, control de acceso por perfiles, logs de transacciones, y módulo de auditoría.

11. ¿Qué tipo de educación y entrenamiento se aplica para desarrollar una base de conocimientos a los usuarios para el manejo de la parte física y lógica de los sistemas de información del área que considera más crítico?

Los tipos de educación a los usuarios y entrenamiento se desarrollaría para el manejo de la parte física y lógica de los sistemas de información contables, están (a) uso del sistema con manuales, (b) administración del sistema, (c) manejo ofimático, (d) KB con videos/foros/imágenes, y (e) preguntas y respuesta.

12. Si tuviese que armar un FODA para los sistemas de información para este tipo de empresa PYMES que elementos incluiría en cada parte.

ANÁLISIS FODA		
	ASPECTOS POSITIVOS	ASPECTOS NEGATIVOS
ANÁLISIS INTERNO	<p>FORTALEZAS</p> <p>Optimización del Proceso.</p> <p>Control y Seguridad.</p> <p>Manejo de Datos.</p>	<p>DEBILIDADES</p> <p>Dependencia de la Tecnología.</p> <p>Dependencia de Usuarios Clave.</p> <p>Resistencia al Cambio.</p>
ANÁLISIS EXTERNO	<p>OPORTUNIDADES</p> <p>Mejoras Futuras.</p> <p>Detección de Fallas.</p> <p>Personal Capacitado.</p>	<p>AMENAZAS</p> <p>Ataques informáticos.</p> <p>Robo de Información.</p> <p>Espionaje Empresarial.</p>

13. Desde su perspectiva, ¿Qué otra cosa considera usted podría ayudar en la reducción de riesgos en los sistemas de información contable?

Otra cosa que consideraría para ayudar en la reducción de riesgo en los sistemas contables tenemos que deben, concientizar a los empleados, apoyarse en expertos, incentivar el uso del sistema, capacitación permanente y análisis de datos.

Tercera Entrevista a Experto como Contador

Nombre del Experto: CPA. Verónica Montesdeoca Villamar

Perfil del Experto: Sector camaronero, Asistente contable, Asistente Financiera, Asistente de Producción, Jefe Financiero y Contadora de Costo.

1. Desde su punto de vista ¿Cuál es el motivo por el cual los empresarios adquieren un sistema de información?

Para registrar cada una de las operaciones que se realizan dentro de la empresa.

2. De acuerdo con su criterio ¿Qué ventajas obtienen las empresas al adquirir un sistema de información?

Obtener información oportuna para toma de decisiones con respecto al negocio.

3. De acuerdo con su criterio ¿Qué desventajas obtienen las empresas al adquirir un sistema de información?

No considero que sea una desventaja adquirir un sistema contable, más bien desde mi punto de vista considero que es una organización y control de las operaciones del negocio.

4. Si tuviese que dibujar los flujos de la información en los sistemas de información contable del sector acuícola ¿Qué elementos resaltaría en dicho gráfico?

La parte de operación del área de producción, costos, ventas.

5. ¿Cuáles cree que son los problemas que se pueden presentar al momento de implementar un sistema de información? Liste los problemas de mayor a menor magnitud.

- Que la operación de campo se refleje en el sistema de información.
- Parametrizaciones de cuentas
- Integración de módulos
- Saldos iniciales al momento de realizar la migración de información.

6. De acuerdo con su criterio ¿Cuáles son las áreas más críticas donde puede existir mayores riesgos de errores y fraudes en los sistemas de información de este tipo de compañía? Favor liste primero y ordene desde la mayor a la menor criticidad.

El área más crítica que considero es el módulo de inventarios (compras / consumos).

7. ¿Qué eventos o situaciones considera usted que podrían generar situaciones de riesgo de acceso físico y lógico en los sistemas de información contable en el sector acuícola? (Analizar de forma general)

Una de las situaciones que generarían riesgos en el acceso es la manipulación de registros de las operaciones.

8. ¿Qué tipo de errores y de situaciones de fraudes se pueden presentar en el acceso físico y lógico de los sistemas de información contable en el sector acuícola? (Analizar de forma específico)

Se podrían presentar errores si el sistema no cuenta con cierres o avisos al momento de registrar la información.

9. Desde el punto de vista de un usuario ¿Cuáles podrían ser las medidas de control que se deberían implementar para reducir el riesgo de acceso físico y lógico a los sistemas de información contable en el sector acuícola?

- Claves personalizadas con determinado tiempo para su caducidad.
- Los módulos deberían notificar al momento que el usuario está registrando de manera incorrecta.

10. Desde el punto de vista de un experto en sistemas ¿Cuáles cree que podrían ser las medidas de control que se deberían implementar para reducir el riesgo de acceso físico y lógico a los sistemas de información contable en el sector acuícola?

Se deberían implementar medidas o metodologías de seguridad que permita que los sistemas de información estén protegidos ante amenazas de robo de información de la empresa.

11. ¿Qué tipo de educación y entrenamiento se aplica para desarrollar una base de conocimientos a los usuarios para el manejo de la parte física y lógica de los sistemas de información del área que considera más crítico?

La que recomendaría serían las capacitaciones según el área de trabajo.

12. Si tuviese que armar un FODA para los sistemas de información para este tipo de empresa PYMES que elementos incluiría en cada parte.

ANÁLISIS FODA		
	ASPECTOS POSITIVOS	ASPECTOS NEGATIVOS
ANÁLISIS INTERNO	<p>FORTALEZAS</p> <p>Registros de las operaciones, organización de información para análisis de movimientos según cada área de la empresa.</p>	<p>DEBILIDADES</p> <p>Libre acceso a todos los módulos sin restricción por usuarios. Error en registros, manipulación de la información.</p>
ANÁLISIS EXTERNO	<p>OPORTUNIDADES</p> <p>Integración con nuevas reformas gubernamentales, exportación de información para entregar de manera externa.</p>	<p>AMENAZAS</p> <p>Virus, robo de información.</p>

13. Desde su perspectiva, ¿Qué otra cosa considera usted podría ayudar en la reducción de riesgos en los sistemas de información contable?

Medidas de seguridad que nos permitan estar protegidos ante amenazas de robo de información de la empresa.

Cuarta Entrevista a Experto como Asistente Contable

Nombre del Experto: CPA. María José Chiriboga

Perfil del Experto: Asistente Contable durante cinco años, Tareas: Registro de compras, Ventas, Elaboración de retenciones, conciliaciones bancarias, y declaraciones de impuestos.

1. Desde su punto de vista ¿Cuál es el motivo por el cual los empresarios adquieren un sistema de información?

El principal motivo es para mantener controlada la información de la empresa y así poder tomar decisiones en tiempo real.

2. De acuerdo con su criterio ¿Qué ventajas obtienen las empresas al adquirir un sistema de información?

Las ventajas para mí son (a) Información al día y (b) base de datos completas.

3. De acuerdo con su criterio ¿Qué desventajas obtienen las empresas al adquirir un sistema de información?

- No cumple con todas las especificaciones que necesita la empresa.
- Tiempo para su implementación.
- Difícil manejo de los usuarios.

4. Si tuviese que dibujar los flujos de la información en los sistemas de información contable del sector acuícola ¿Qué elementos resaltaría en dicho gráfico?

Dentro del sector acuícola, lo que debe resaltar es la salida de los productos para el consumo en el proceso.

5. ¿Cuáles cree que son los problemas que se pueden presentar al momento de implementar un sistema de información? Liste los problemas de mayor a menor magnitud.

- Ordenador lento.
- Internet lento.

- No se puede actualizar sistema.
- No se ingresa la información completa.

6. De acuerdo con su criterio ¿Cuáles son las áreas más críticas donde puede existir mayores riesgos de errores y fraudes en los sistemas de información de este tipo de compañía? Favor liste primero y ordene desde la mayor a la menor criticidad.

Entre las áreas más crítica consideró este orden de menor a mayor criticidad: (a) área de compras, (b) área de producción, (C) área de ventas, y (d) área de pago.

7. ¿Qué eventos o situaciones considera usted que podrían generar situaciones de riesgo de acceso físico y lógico en los sistemas de información contable en el sector acuícola? (Analizar de forma general)

- Personal no autorizado.
- Virus informático.

8. ¿Qué tipo de errores y de situaciones de fraudes se pueden presentar en el acceso físico y lógico de los sistemas de información contable en el sector acuícola? (Analizar de forma específico)

Fallas en el ingreso biométrico en las áreas de trabajo, por lo cual personal no indicado entra a las áreas incorrectas. Al ingresar un virus informático, el problema que causaría es el no poder acceder al sistema y se puede perder información.

9. Desde el punto de vista de un usuario ¿Cuáles podrían ser las medidas de control que se deberían implementar para reducir el riesgo de acceso físico y lógico a los sistemas de información contable en el sector acuícola?

- Crear una lista de personal que tiene permitido el acceso.
- Ingreso mediante contraseña.

10. Desde el punto de vista de un experto en sistemas ¿Cuáles cree que podrían ser las medidas de control que se deberían implementar para reducir el riesgo de acceso físico y lógico a los sistemas de información contable en el sector acuícola?

Contraseñas personalizadas para ingresar al sistema.

11. ¿Qué tipo de educación y entrenamiento se aplica para desarrollar una base de conocimientos a los usuarios para el manejo de la parte física y lógica de los sistemas de información del área que considera más crítico?

Dar cursos de acuerdo al manejo del sistema y de la misma forma entregar manuales de instrucciones para que puedan tener apoyo y respuestas inmediatas ante cualquier duda o problema que se le presenten.

12. Si tuviese que armar un FODA para los sistemas de información para este tipo de empresa PYMES que elementos incluiría en cada parte.

ANÁLISIS FODA		
	ASPECTOS POSITIVOS	ASPECTOS NEGATIVOS
ANÁLISIS INTERNO	<p>FORTALEZAS</p> <p>Contar con tecnología avanzada. Logar el crecimiento de la compañía, mediante la expansión.</p>	<p>DEBILIDADES</p> <p>Incurrir en sobrecostos por la mala implementación del sistema. Personal no apto para el manejo del sistema.</p>
ANÁLISIS EXTERNO	<p>OPORTUNIDADES</p> <p>Integrar todas las áreas para automatizar los procesos. Incremento en la productividad y rentabilidad.</p>	<p>AMENAZAS</p> <p>Sistemas más avanzados que posea la competencia.</p>

13. Desde su perspectiva, ¿Qué otra cosa considera usted podría ayudar en la reducción de riesgos en los sistemas de información contable?

Rotar al personal, para evitar que una misma persona tenga pleno conocimiento del área y pueda ejecutar fraude sin ser descubierto.

Quinta Entrevista a Experto como Asistente Contable

Nombre del Experto: Ing. Angie Gonzabay.

Perfil del Experto: Asistente Contable.

1. Desde su punto de vista ¿Cuál es el motivo por el cual los empresarios adquieren un sistema de información?

Desde mi punto de vista. ¿porque los empresarios estos adquieren un sistema de información? pues muy fácil, para optimizar tiempos y lograr procesos muchos más eficaces. Con un sistema de información se pueden interconectar todos los departamentos, en especial el desde el departamento contable donde puedo observar los ingresos de compras, facturación, podía hacer llamados atención, correcciones, realizar arqueo de caja, etc. Entonces este sistema favorece muchísimo la empresa porque vamos a evitar cuellos de botella y los procesos van a hacer más transparentes, se podrá realizar una conexión total entre compras con bodega, logística. Entonces para mí la obtención de un sistema de información es de vital importancia con una empresa ya pues está bien estructurada.

2. De acuerdo con su criterio ¿Qué ventajas obtienen las empresas al adquirir un sistema de información?

Ayuda a poder incrementar la efectividad de las operaciones que ejecuta la empresa, mejora la disponibilidad de la información al obtenerla en tiempo real de acuerdo a las necesidades que tenga la organización empresarial.

3. De acuerdo con su criterio ¿Qué desventajas obtienen las empresas al adquirir un sistema de información?

Rara vez se puede caer el sistema y paralizarse el ingreso de información, al igual cuando haya actualizaciones, toca esperar mucho tiempo.

4. Si tuviese que dibujar los flujos de la información en los sistemas de información contable del sector acuícola ¿Qué elementos resaltaría en dicho gráfico?

Si tuviera que dibujarlo, lo explicaría así, en el sector acuícola como vital importancia, tenemos los siguientes pasos, primero es el requerimiento de producción, los productos, se envía una orden de compra a logística, luego este lleva al jefe de campo, se realiza las cotizaciones, aprobación de compra, se recibe la factura, luego se recibe la mercancía, e ingresa al sistema de inventario. Luego sigue el otro proceso donde el departamento contable, recibe la factura, guías e ingresa al sistema emitiendo los cheques para el pago en la fecha pactada.

5. ¿Cuáles cree que son los problemas que se pueden presentar al momento de implementar un sistema de información? Liste los problemas de mayor a menor magnitud

- Los ingresos se hagan de manera incorrectos que lo que conste en el papel por ejemplo de lo que va llegando no sea lo mismo que conste manera virtual.
- Que las personas sean reacias a querer manejar lo que es un computador no todos están aptos y dispuestos a manejar la tecnología.
- Que los ingresos no se hagan de manera continua e inmediata, sino que se acumulen, entonces si hay documentos sin registrarse no va a verse reflejado eso en el resto de departamentos.

6. De acuerdo con su criterio ¿Cuáles son las áreas más críticas donde puede existir mayores riesgos de errores y fraudes en los sistemas de información de este tipo de compañía? Favor liste primero y ordene desde la mayor a la menor criticidad.

Para mi criterio el área de mayor criticidad sería el área contable ya que en este se puede ingresar datos erróneos y maquillar facturas para la conveniencia del defraudador.

7. ¿Qué eventos o situaciones considera usted que podrían generar situaciones de riesgo de acceso físico y lógico en los sistemas de información contable en el sector acuícola? (Analizar de forma general)

Unos de los eventos que considero que podría generar riesgo son las claves de acceso ya que cualquier puede estar atento para espiar y obtener las claves y de esa forma de cometer sus objetivos para sus propios beneficios.

8. ¿Qué tipo de errores y de situaciones de fraudes se pueden presentar en el acceso físico y lógico de los sistemas de información contable en el sector acuícola? (Analizar de forma específico)

Al momento de conseguir las claves de los usuarios se pueden generar situaciones de ingresos de datos al sistema con el objetivo de realizar daños a la empresa o a los usuarios que le corresponde la clave.

9. Desde el punto de vista de un usuario ¿Cuáles podrían ser las medidas de control que se deberían implementar para reducir el riesgo de acceso físico y lógico a los sistemas de información contable en el sector acuícola?

Antes de contratar a una persona investigar totalmente de sus antecedentes con la finalidad de validar lo que entrega en su hoja de vida, probar a los trabajadores para medir su integridad y honestidad, trabajar en unión con los departamentos de sistemas para generar pruebas de errores y fraudes en los sistemas.

10. Desde el punto de vista de un experto en sistemas ¿Cuáles cree que podrían ser las medidas de control que se deberían implementar para reducir el riesgo de acceso físico y lógico a los sistemas de información contable en el sector acuícola?

Recomendaría, una medida de control para evitar pérdida de información se sabe que existe un servidor madre en las empresas, pero este servidor es físico si se llega a quemar, dañar o algo con el servidor madre se va a perder toda la información, porque esta información no está cargada directamente en

la nube, cómo ejemplo: si se llega a quemar el CPU central se perdería toda la información registrada de todos los años anteriores. Realmente, es importante que un sistema tenga respaldo en la nube para evitar este tipo de pérdida de información.

11. ¿Qué tipo de educación y entrenamiento se aplica para desarrollar una base de conocimientos a los usuarios para el manejo de la parte física y lógica de los sistemas de información del área que considera más crítico?

Realizar capacitaciones y evaluaciones para medir sus conocimientos y de acuerdo a los resultados fortalecer con cursos para que obtengan una base de conocimiento en los sistemas.

12. Si tuviese que armar un FODA para los sistemas de información para este tipo de empresa PYMES que elementos incluiría en cada parte.

ANÁLISIS FODA		
	ASPECTOS POSITIVOS	ASPECTOS NEGATIVOS
ANÁLISIS INTERNO	<p>FORTALEZAS</p> <p>El sistema de información permite analizar, revisar los archivos logs, el cual ayuda con la revisión del historial de las diferentes actividades que realizan los usuarios en cada departamento de la empresa.</p>	<p>DEBILIDADES</p> <p>Existen usuarios de varios departamentos que no ingresan correctamente los datos o lo ingresan de forma incompleta que ocasiona bajo rendimiento en los procesos de la empresa.</p>
ANÁLISIS EXTERNO	<p>OPORTUNIDADES</p> <p>Mediante actualizaciones de sistemas se puede adquirir licencias con costos más bajos y estas puedan ser usadas en computadoras nuevas que quisieran adaptar.</p>	<p>AMENAZAS</p> <p>Los servidores están conectados por una red y esta se maneja con internet, puede existir fallas del internet o que se vaya la energía ocasionando problemas con la información del sistema.</p>

13. Desde su perspectiva, ¿Qué otra cosa considera usted podría ayudar en la reducción de riesgos en los sistemas de información contable?

Considero, para la reducción riesgos, una sola persona debe ser la única que sepa manejar todo el sistema de información, puede haber más personal con acceso, pero partes restringidas (bloqueo de acceso) ya que si todo el resto de personal maneja la misma información cada uno de ellos modifica a su gusto y es allí donde se generan fraudes. Además, todo lo que se ingrese, modifique, debe aparecer el usuario que realizo, fecha, desde que maquina o servidor lo realizo. Recomiendo que cada usuario tenga activado solo las opciones que compete a su área, que las otras opciones no la tengan visible o sin acceso, para evitar los fraudes.

Sexta Entrevista a Experto a Gerente de una Empresa

Nombre del Experto: Ing. Carlos Montalván Suarez

Perfil del Experto: Gerente Financiero de Mason Industrias

1. Desde su punto de vista ¿Cuál es el motivo por el cual los empresarios adquieren un sistema de información?

Para tener un control total de las actividades de la empresa, que les permita tener un marco de resultados generales con variaciones estadísticas que identifiquen los logros, las desventajas y las falencias de la organización, con esto se puede determinar la eficiencia en cuanto al manejo organizacional de la empresa.

2. De acuerdo con su criterio ¿Qué ventajas obtienen las empresas al adquirir un sistema de información?

Las ventajas serias (a) control de sus actividades, (b) determinación de ideas, (c) factores externos para mitigar riesgos futuros, (d) orientación hacia sus objetivos principales, (e) fortalecimiento de los conceptos técnicos para el desarrollo general del trabajo, y (f) una visión optima de las necesidades de la empresa.

3. De acuerdo con su criterio ¿Qué desventajas obtienen las empresas al adquirir un sistema de información?

Considero que la única desventaja podría ser el margen de error que esta contenga, lo que involucraría un desabastecimiento y error de la información.

4. Si tuviese que dibujar los flujos de la información en los sistemas de información contable del sector acuícola ¿Qué elementos resaltaría en dicho gráfico?

En primera instancia los niveles de producción que se podrían reflejar en una base historial ya que con esta información podría cuantificar los objetivos financieros y contables para elevar la producción sin que esto afecte a los costos y sobre todo genera una utilidad mucho más amplia a futuro.

5. ¿Cuáles cree que son los problemas que se pueden presentar al momento de implementar un sistema de información? Liste los problemas de mayor a menor magnitud.

Los problemas mayores podrían ser la filtración de información falsa, con datos erróneos que ocasionen un problema grave en el desarrollo de las actividades contables y financieras de la empresa.

6. De acuerdo con su criterio ¿Cuáles son las áreas más críticas donde puede existir mayores riesgos de errores y fraudes en los sistemas de información de este tipo de compañía? Favor liste primero y ordene desde la mayor a la menor criticidad.

Áreas financieras, áreas de ventas, y de administración general. Dentro de este orden el grado de afectación sería en orden ascendente a descendente.

7. ¿Qué eventos o situaciones considera usted que podrían generar situaciones de riesgo de acceso físico y lógico en los sistemas de información contable en el sector acuícola? (Analizar de forma general)

La aplicación de distintos productos químicos que generan una afectación en la persona que se encargue del desarrollo de campo y parte operativa ya

que una mala orientación en la información puede generar pérdidas económicas graves para la empresa.

8. ¿Qué tipo de errores y de situaciones de fraudes se pueden presentar en el acceso físico y lógico de los sistemas de información contable en el sector acuícola? (Analizar de forma específico)

Un mal registro de las actividades que no prioricen el enfoque técnico y real que la empresa requiera, adicional a un mal detalle de descripción que ocasione el no entendimiento de la información.

9. Desde el punto de vista de un usuario ¿Cuáles podrían ser las medidas de control que se deberían implementar para reducir el riesgo de acceso físico y lógico a los sistemas de información contable en el sector acuícola?

Utilizar una base exclusiva y única de la empresa que tenga un marco de seguridad muy amplio tales como claves de accesos únicas para usuarios de la empresa y registros únicos personales.

10. Desde el punto de vista de un experto en sistemas ¿Cuáles cree que podrían ser las medidas de control que se deberían implementar para reducir el riesgo de acceso físico y lógico a los sistemas de información contable en el sector acuícola?

Utilizar una base exclusiva y única de la empresa que tenga un marco de seguridad muy amplio tales como claves de accesos únicas para usuarios de la empresa y registros únicos personales.

11. ¿Qué tipo de educación y entrenamiento se aplica para desarrollar una base de conocimientos a los usuarios para el manejo de la parte física y lógica de los sistemas de información del área que considera más crítico?

Información simple, clara y contrastada.

12. Si tuviese que armar un FODA para los sistemas de información para este tipo de empresa PYMES que elementos incluiría en cada parte.

ANÁLISIS FODA		
	ASPECTOS POSITIVOS	ASPECTOS NEGATIVOS
ANÁLISIS INTERNO	<p>FORTALEZAS</p> <p>Control total de las actividades de la empresa.</p>	<p>DEBILIDADES</p> <p>Margen de error que el sistema contenga, lo que involucraría un desabastecimiento y error de la información</p>
ANÁLISIS EXTERNO	<p>OPORTUNIDADES</p> <p>Complementación de datos lo más exacto posible.</p>	<p>AMENAZAS</p> <p>Filtración de información falsa, con datos erróneos que ocasionen un problema grave en el desarrollo de las actividades contables y financieras de la empresa.</p>

13. Desde su perspectiva, ¿Qué otra cosa considera usted podría ayudar en la reducción de riesgos en los sistemas de información contable?

Una revisión diaria de la base de datos general de información, más el detalle específico de cada actividad que se desarrolle en el sistema de información, con la complementación de datos lo más exacto posibles.

Matriz de Hallazgos

A continuación, se detalla la matriz de hallazgos con las respuestas generadas a cada uno de los entrevistados seleccionados como expertos en los sistemas de información y de las áreas contables.

Tabla 15

Matriz de hallazgos (parte I)

Preguntas	Experto 1	Experto 2	Experto 3	Experto 4	Experto 5	Experto 6
1.Motivo al adquirir un sistema de información	Controlar la información y obtener información de ese control.	Optimización de procesos, seguridad y control, mejoras operativas o funcionales, ahorros económicos, mayor competitividad.	Registrar cada una de las operaciones que se realizan dentro de la empresa.	Mantener controlada la información de la empresa y así poder tomar decisiones en tiempo real.	Optimización de tiempo, procesos eficaces y transparentes, interconexión entre todos los departamentos.	Control total de las actividades de la empresa, eficacia en cuanto al manejo organizacional de la empresa.
2.Ventajas de los sistemas de información	Control individual de los procesos, tener información precisa de todas las actividades.	Seguridad de la información, control y seguimiento de procesos, reportes en tiempo real, indicadores de desempeño, empresa apoyada en tecnología.	Obtener información oportuna para toma de decisiones con respecto al negocio.	Información al día. Base de datos completas.	Incrementa la efectividad de las operaciones, mejora la disponibilidad de la información en tiempo real.	Control de sus actividades, determinación de ideas, factores externos para mitigar riesgos futuros, orientación hacia sus objetivos principales, fortalecimiento de los conceptos técnicos para el desarrollo general del trabajo, visión óptima de las necesidades de la empresa.
3. Desventajas de los sistemas de información	Adquirir un sistema que recién se está desarrollando para aplicarlo en el giro del negocio, personal poco capacitado para ejecutar el manejo del sistema.	Dependencia de la tecnología, alta inversión inicial, brechas de seguridad informática, requerimiento de expertos, gastos en capacitación a empleados.	No considera el sistema de información como una desventaja, más bien considera como organización y control de las operaciones de un negocio.	No cumple con las todas las especificaciones que necesita la empresa, tiempo para su implementación, difícil manejo de los usuarios.	Paralizar el ingreso de información cuando se cae el sistema.	Podría ser el margen de error que esta contenga, lo que involucra un desabastecimiento y error de la información.

Tabla 16

Matriz de hallazgos (parte II)

Preguntas	Experto 1	Experto 2	Experto 3	Experto 4	Experto 5	Experto 6
4. Elementos importante que resaltan en los flujos de información de los sistemas de información contables	Se resaltaría más el proceso de producción, ya que por medio del sistema se ingresaría todos los datos que incurren en dicho proceso para identificar en un balance los costos y venta de esa producción.	En los sistemas de información contable del sector acuícola los elementos que resaltaría: gastos, insumos, ingresos, laboratorio y producción.	La parte de operación del área de producción, costos y ventas.	Dentro del sector acuícola, lo que debe resaltar es la salida de los productos para el consumo en el proceso.	Es de vital importancia el requerimiento de la producción ya que, en base a esa solicitud, se genera la orden de compra a logística, se procede con las cotizaciones y la aprobación con el proceso de compra y el pago correspondiente.	Los niveles de producción podrían reflejar una base historial, con esta base se puede cuantificar los objetivos financieros y contables para elevar la producción sin que afecte los costos y sobre todo generar una utilidad mucho más amplia a futuro.
5. Problemas que se presentan al implementar un sistema de información	Que los equipos de computación no cumplan con los requisitos que solicita el sistema, no contar con la organización documental: manuales de procedimientos, manuales de funciones y organigramas, ya que esta documentación forma parte del software para poder implementar.	Los problemas son: falta de presupuesto, obsolescencia tecnológica, renuncias de personal, problemas con proveedores, y resistencia al cambio.	Que la operación de campo se refleje en el sistema de información, parametrizaciones de cuentas, integración de módulos, saldos iniciales al momento de realizar la migración de información.	Los problemas son: ordenador lento, internet lento, no se puede actualizar sistemas, y no se ingresa la información completa.	Ingresos incorrectos. Personas reacias a querer manejar un computador. Ingresos que no se hagan de manera continua e inmediata.	Filtración de información falsa, con datos erróneos, ocasionando problemas graves en el desarrollo de las actividades contables y financieras de la empresa.

Tabla 17

Matriz de hallazgos (parte III)

Preguntas	Experto 1	Experto 2	Experto 3	Experto 4	Experto 5	Experto 6
6. Áreas críticas donde se presentan los mayores riesgos de errores y fraudes	Áreas críticas: Inventario, financiero, administrativa, y producción. En todos los procesos pueden existir fraudes.	Las áreas más críticas son de: finanzas, seguridad de TI, inventarios, impuestos, y otros.	El área más crítica es el módulo de inventarios (compras / consumos).	Las áreas más críticas son: área de compras, área de producción, área de ventas y área de pago.	El área con mayor criticidad es el área contable.	Las áreas más críticas: áreas financieras, áreas de ventas, áreas administrativas.
7. Situaciones que generarían riesgos de acceso físico y lógico en los sistemas de información contable.	No controlar el personal que se contrata, ya que el acceso físico de la información se lo hace internamente no externamente, el problema radica de manera interna.	Falta de seguridad o su ausencia, falta de conocimiento, cambios de personal, insatisfacción de empleados, importancia de la empresa.	Manipulación de registros de las operaciones.	Personal no autorizado, virus informático.	Claves de acceso sin seguridad.	Mala orientación en la información puede generar pérdidas económicas graves para la empresa.
8. Tipos de errores y situaciones de fraudes que se presentan en los sistemas de información contable.	Existe errores al ingresar mal la información, no parametrizar las opciones de acceso a los usuarios, no tener pruebas de validación de información y notificaciones automatizadas que genere el sistema a los encargados departamentales.	Se puede presentar los siguientes tipos de errores y fraudes: eliminación de información, robo de información, espionaje empresarial, y falsa contabilidad.	Se podrían presentar errores si el sistema no cuenta con cierres o avisos al momento de registrar la información.	Fallas en el ingreso biométrico en las áreas de trabajo, por lo cual personal no indicado entra a las áreas incorrectas.	Generar situaciones en el ingreso de datos al sistema con el objetivo de realizar daños a la empresa o a los usuarios que le corresponde la clave.	Mal registro de actividades que no prioricen el enfoque técnico y real, mal detalle de descripción de la información ocasionando confusiones.

Tabla 18

Matriz de hallazgos (parte IV)

Preguntas	Experto 1	Experto 2	Experto 3	Experto 4	Experto 5	Experto 6
9. Desde el punto de vista de un usuario: cuáles son las medidas de control que se implementan para reducir riesgos en los sistemas de información contable.	Parametrizar los sistemas conforme a los usuarios y estipular métodos de accesos para que estos puedan ser muy analizados en cuanto al tema del giro del negocio.	Las medidas de control como usuario se deberían implementar para reducir riesgos de acceso físico y lógico en los sistemas de información son: el buen manejo de claves, validación de resultados, auditorias informáticas, segmentación de perfiles, y actualización de seguridad.	Claves personalizadas con determinado tiempo para su caducidad, los módulos deberían notificar al momento que el usuario está registrando de manera incorrecta.	Crear una lista del personal que tiene permitido el acceso, ingreso mediante contraseña.	Investigar los antecedentes de los trabajadores para medir su integridad y honestidad, trabajar en unión con los departamentos de sistema para generar pruebas de errores y fraudes.	Utilizar base exclusiva y única de la empresa, marco de seguridad amplio como claves de accesos únicas de usuarios, registros únicos personales.
10. Desde el punto de vista de un experto: cuáles son las medidas de control que se implementan para reducir riesgos en los sistemas de información contable.	Realizar evaluaciones para medir conocimientos y establecer la experiencia del personal con el sistema.	Seguridad por hardware, seguridad por software, control de acceso por perfiles, archivos logs de transacciones, módulo de auditoría.	Implementar medidas de seguridad que permita que los sistemas de información estén protegidos ante amenazas de robo de información de la empresa.	Contraseñas personalizadas para ingresar al sistema.	Medida de control para evitar pérdida de información, crear sistemas con respaldo en la nube para evitar pérdida de información.	Utilizar una base exclusiva y única de la empresa que tenga un marco de seguridad amplio tales como: claves de acceso únicas para usuarios y registros únicos personales.
11. Tipo de capacitaciones a los usuarios	Capacitaciones constantes del sistema. Capacitaciones sobre el mal uso sistemas y métodos correctivo que se aplicaría.	Uso del sistema con manuales, administración del sistema, manejo ofimático, KB con videos/foros/imágenes, preguntas y respuesta.	Capacitaciones según el área de trabajo.	Dar cursos de acuerdo al manejo del sistema, entrega de manuales de instrucciones de apoyo a problemas que se presenten.	Capacitaciones y evaluaciones para medir sus conocimientos.	Información simple, clara y contrastada.

Pregunta 12 Análisis de FODA: Fortaleza y Oportunidad.

Tabla 19

Matriz de hallazgos (parte V)

		ASPECTOS POSITIVOS					
		FORTALEZAS					
		Experto 1	Experto 2	Experto 3	Experto 4	Experto 5	Experto 6
ANÁLISIS INTERNO		Controlar la Información.	Optimización del Proceso. Control y Seguridad. Manejo de Datos.	Registros de las operaciones, organización de información para análisis de movimientos según cada área de la empresa.	Contar con tecnología avanzada. Lograr el crecimiento de la compañía, mediante la expansión.	Permite analizar, revisar archivos logs con la finalidad de obtener el historial de las diferentes actividades que realizan los usuarios.	Control total de las actividades de la empresa.
		OPORTUNIDADES					
		Experto 1	Experto 2	Experto 3	Experto 4	Experto 5	Experto 6
ANÁLISIS EXTERNO		Disponer de información ordenada	Mejoras futuras. Detección de fallas. Personal capacitado.	Integración con nuevas reformas gubernamentales, exportación de información para entregar de manera externa.	Integrar todas las áreas para automatizar los procesos. Incremento en la productividad y rentabilidad.	Adquirir licencias con bajos costos mediante las actualizaciones de los sistemas.	Complementación de datos lo más exacto posible.

Pregunta 12 Análisis de FODA: Debilidad y Amenaza

Tabla 20

Matriz de hallazgos (parte VI)

ASPECTOS NEGATIVOS						
DEBILIDADES						
	Experto 1	Experto 2	Experto 3	Experto 4	Experto 5	Experto 6
ANÁLISIS INTERNO	Acceso a las claves con privilegios.	Dependencia de la Tecnología. Dependencia de usuario clave. Resistencia al cambio.	Libre acceso a todos los módulos sin restricción por usuarios. Error en registros, manipulación de la información.	Incurrir en sobrecostos por la mala implementación del sistema. Personal no apto para el manejo del sistema.	Existen usuarios que ingresan datos incorrectos o incompletos generando bajo rendimiento en los procesos de la empresa.	Margen de error que el sistema contenga, lo que involucraría un desabastecimiento y error de la información.
AMENAZAS						
	Experto 1	Experto 2	Experto 3	Experto 4	Experto 5	Experto 6
ANÁLISIS EXTERNO	Hackeo a los sistemas de información.	Ataques informáticos Robo de información. Espionaje empresarial.	Virus, robo de información.	Sistemas más avanzados que posea la competencia.	Los servidores están conectados por una red y esta es manejada con internet, puede existir falla de internet o se vaya la energía ocasionando problemas con la información.	Filtración de información falsa, con datos erróneos que ocasiona problemas graves en el desarrollo de las actividades contables y financieras de la empresa.

Tabla 21*Matriz de hallazgos (parte VII)*

Preguntas	Experto 1	Experto 2	Experto 3	Experto 4	Experto 5	Experto 6
13.Recomendaciones para reducir los riesgos en los SI	Tener métodos de análisis para dar los accesos a los usuarios, investigar los antecedentes de los usuarios, tener un contralor que conozca el software y giro del negocio, establecer controles internos.	Concientizar a los empleados, apoyarse en expertos, incentivar el uso del sistema, capacitación permanente, análisis de datos.	Medidas de seguridad que nos permitan estar protegidos ante amenazas de robo de información de la empresa.	Rotar al personal, para evitar que una misma persona tenga pleno conocimiento del área y pueda ejecutar fraude sin ser descubierto.	Una persona sepa manejar todo el sistema de información, personal con accesos restringidos, cada usuario tenga activado solo las opciones que compete en su área.	Revisión diaria de la base de datos general de información más el detalle específico de cada actividad que se desarrolle en el sistema de información.

Análisis de Resultados

Por medio de la entrevista se pudo obtener información acerca del tema propuesto para la reducción de los riesgos en los sistemas de información contable, con la finalidad de identificar los posibles errores y fraudes más comunes que existen en las áreas críticas, de las cuales mencionamos las siguientes:

Los sistemas de información ayudan a controlar la información y por medio de ese control se puede obtener información precisa de todas las actividades que realiza una organización empresarial y por consiguiente se puede tomar decisiones en tiempo real logrando de tal forma optimizar la búsqueda de datos.

Las ventajas al adquirir un sistema de información este permite tener un control individual de los procesos, obtener información oportuna para tomar decisiones respecto al negocio, tener una base de datos completas y seguridad de la información, lo cual ayuda a incrementar la efectividad en las operaciones.

Así como existe ventajas también se pudo constatar sus desventajas al momento de adquirir e implementar un sistemas de información, como el ejecutar un sistema que recién se esté desarrollando y este no cuente con pruebas de errores puede ocasionar pérdida de información y fallas al momento de manejar el sistema, además surgiría costos muy altos al momento de ejecutar el sistema y las empresas no cuente con equipos de computación modernos o que tengan una vida útil mayor a cinco años estos elementos pueden elevar el costo de la adquisición de un sistema ya que no solo sería la inversión del sistema si no también los costos de los equipos de computación que tocaría comprar para que el sistema pueda tener su rendimiento correcto.

De acuerdo a los elementos más importante al momento de resaltar los flujos de información en el sector acuícola se seleccionó el proceso de producción ya que por medio del sistema se ingresaría todos los datos que incurren en dicho proceso, el cual permite poder identificar en un balance los

costos y ventas de la producción que ejerce la organización empresarial y con esa base de datos obtener un historial en el que se pueda cuantificar los objetivos financieros y contables para elevar la producción sin que afecte los costos y sobre todo generar una utilidad mucho más amplia en el futuro.

Los problemas que se presentan al momento de implementar un sistema de información, es que la empresa no cuente con la organización documental como manuales de procedimientos, manuales de funciones y organigramas, que forma parte en la implementación de un sistema. Además, la falta de presupuesto, la obsolescencia tecnológica, renuncias del personal, problemas con proveedores, resistencia al cambio, filtración de información falsa con datos erróneos son causantes de problemas al momento de ingresar y procesar la información contable y financiera en los sistemas.

Respecto a las áreas críticas de la empresa donde se presenta mayores riesgos de errores y fraudes es el área de inventario, seguida el área de producción, luego el área de ventas y el área contable.

Las situaciones que generaría riesgos de acceso físico y lógico en los sistemas de información sería el no controlar el personal que se contrata e investigar sus antecedentes en otras organizaciones, esto puede ocasionar fuga de información por medio del acceso físico y lógico de los sistemas, mediante infiltrados internos que dan acceso a terceras personas para controlar el hardware y software de manera externa, con la intención de perjudicar a la empresa. En fin, el riesgo de acceso físico y lógico radica siempre de manera interna, no externamente.

En referencia a los tipos de errores y situaciones de fraude que se presentan en los sistemas de información contable serían: ingresar de forma incorrecta la información, no parametrizar las opciones de acceso a los usuarios, no contar de pruebas de validación de información, que el sistema no cuente con cierres o avisos al momento de registrar la información, mal detalle de descripción de la información ocasionando confusiones, eliminación de la información voluntaria e involuntaria, robo de información, espionaje empresarial y lograr una falsa contabilidad con el objetivo de perjudicar a la empresa y beneficiarse en el caso de los defraudadores.

Medidas de control desde el punto de vista de un usuario, se enfocan en parametrizar los sistemas conforme a los perfiles de los usuarios y actividades que realizan, validación de resultados, auditorías informáticas, actualización de seguridad, claves personalizadas con determinado tiempo para su caducidad.

Medidas de control desde el punto de vista de un experto, se enfocan en realizar evaluaciones para medir conocimientos y establecer la experiencia del personal con el sistema de información, constar con seguridad para hardware y software, tener control de acceso por perfiles, archivos logs o historial de todas las actividades realizadas detallando los responsables de dicha transacción, crear sistemas con respaldos en la nube para evitar pérdida de la información.

Se debería capacitar a los usuarios de forma constante y mantener conocimientos actualizados en cuanto al manejo del sistema de información, entregar manuales de instrucciones para que se puedan guiar con rapidez ante un problema que se presente, manteniendo información simple, clara y contrastada.

Según el análisis de FODA, podemos tener resultados en cuanto los aspectos positivos, su fortaleza es contar con una optimización del proceso, seguridad, manejo de datos, control total de las actividades de la empresa, tecnología avanzada, logrando el crecimiento de la compañía mediante su expansión. Sus oportunidades, podemos disponer de información ordenada y automatizada, incrementado la productividad del flujo de información en cada departamento, logrando ser eficaces y eficientes en la búsqueda y entrega de información. En referencia a los aspectos negativos, sus debilidades son el acceso a las claves con privilegios, dependencia de la tecnología, resistencia al cambio, tener libre acceso a todos los módulos sin restricción a los usuarios. Sus amenazas, sería hackeo a los sistemas de información, robo de información, espionaje empresarial, filtración de información falsa que ocasiona graves problemas en el desarrollo de las actividades contables y financieras de la empresa.

Entre las recomendaciones para reducir estos riesgos son la implementación de medidas de seguridad, investigar antecedentes históricos de los usuarios, controlar los accesos de claves con accesos restringidos, y la revisión diaria de la base de datos de las actividades en el sistema de información.

Capítulo 3: Propuesta Metodológica para Evaluación de Riesgos

En relación a la matriz de hallazgos y el análisis de resultados, en la que se conllevó los temas de ventajas, desventajas, áreas, situaciones y eventos críticos que se presentan en los sistemas de información. Se pudo concluir la necesidad de evaluar los riesgos por medio de un cuestionario y ponderar sus resultados mediante una rúbrica para medir el nivel de riesgo de la organización, ya que si existe deficiencias en los controles generarían riesgos en la operación y gestión de la empresa. Ante lo indicado, la propuesta metodológica consta de cuatro temas, de los cuales se definirán como riesgos:

- Riesgo I – Acceso Físico y Lógico a los Sistemas de Información Contable: el personal no autorizado pueda acceder de forma física y lógica a los sistemas de información.
- Riesgos II – Manuales de Procedimientos y Políticas del Departamento Contable: el departamento Contable no cuenta con manuales de procedimientos y políticas en cada uno de sus procesos.
- Riesgo III – Estructura del Departamento Contable: la estructura del departamento contable no cuenta con una segregación de funciones en el personal, que ocasiona deficiencia en los controles para reducir los riesgos.
- Riesgo IV – Riesgos de Fraudes y Errores: la empresa no cuenta con pruebas de cumplimiento de controles para prevenir los riesgos de fraudes que son los más críticos y los errores involuntarios que pueden afectar la continuidad de la organización empresarial.

Esta propuesta metodológica tiene como finalidad, tener un control individual de cada una de sus áreas y obtener información oportuna para tomar decisiones respecto a la organización empresarial, permitiendo tener una base de datos completas y seguridad de información, lo cual ayudaría a incrementar la efectividad en las operaciones.

Se aplicará la propuesta metodológica mediante el siguiente esquema de proceso para la reducción de riesgos en los sistemas de información contable, según Figura 33.

Figura 33

Esquema para la aplicación de la propuesta metodológica



Nota: Adaptado de “El muestreo en la investigación cualitativa”, por Martínez, 2012.

El proceso de reducción de riesgo consta de cuatro etapas, las mismas que se definirán de la siguiente manera:

Planificación

Se encarga de programar todas las actividades que incluye todo el proceso de la evaluación de los riesgos y así poder ejecutarlo de forma efectiva y oportuna. Se presentará los programas de evaluación de cada uno de los riesgos identificados en esta propuesta metodológica, que consta de la siguiente estructura: (a) introducción, en esta se da un pequeño resumen de los riesgos identificados, (b) objetivos, se planteará los objetivos claves de los riesgos identificados, y (c) procedimiento, son los pasos que seguiremos para evaluar los riesgos y proponer el plan de acción.

Ejecución

Mediante esta etapa se evalúa los riesgos por medio de un cuestionario para determinar el nivel de confianza y el riesgo de control. Además, se enfoca en analizar cada uno de los eventos y situaciones que se presentan en cada riesgo identificado, dicho cuestionario estará conformado por una serie de preguntas, las mismas que serán ponderadas sobre 10 puntos y calificadas mediante una rúbrica. (ver Figura 34)

Figura 34

Rúbrica de calificación de preguntas

Rúbrica para Calificación	Puntos
Excelente	10
Muy Bueno	8-9
Bueno	6-7
Regular	3-5
Insuficiente	0-2

Supervisar

La matriz de riesgos es una herramienta que analiza la probabilidad y severidad según el caso, permitiendo estudiar la frecuencia como: (a) aceptable, (b) tolerable, (c) alto, y (d) extremo. La matriz nos ayuda a identificar los niveles de riesgos existentes y generar reportes gráficos (mapa de calor) que sirven para representar la criticidad de estos, concientizando a la gerencia y administración a dar priorización y mitigación de los riesgos. (Albanese, 2012). Para continuar con el proceso en la reducción de riesgos de los sistemas de información contable, se elaboró la matriz de riesgo con sus respectivas escalas. (ver Figura 35).

Figura 35

Matriz de riesgos y su escala de calificación

		Matriz de Riesgo					Color	Nivel del Riesgo
		Probabilidad						
		Improbable	Posible	Ocasional	Moderado	Constante		
Severidad		2	4	6	8	10		
Insignificante	1	2	4	6	8	10	2 a 8	Riesgo Aceptable
Menor	2	4	8	12	16	20	10 a 18	Riesgo Tolerable
Moderado	3	6	12	18	24	30	20 a 24	Riesgo Alto
Crítico	4	8	16	24	32	40	30 a 50	Riesgo Extremo
Catastrófico	5	10	20	30	40	50		

Nota: Adaptado de “Análisis y evaluación de riesgos”, por (Albanese, 2012).

Acciones Correctivas

En este último punto del proceso para la reducción de riesgo, se llevará a cabo un plan de acción donde se presentará repuestas a los riesgos, las cuales serán aplicada a cada uno de los departamentos involucrados en el acceso físico y lógico de los sistemas de información. Se procedió a detallar los resultados de la siguiente manera: (a) riesgos identificados, (b) nivel de riesgo calificado, (c) personal y departamento responsable, y (d) medidas de control para reducir los riesgos

Los datos obtenidos en el proceso de reducción de riesgo fueron tomados mediante el levantamiento de la información, utilizando las entrevistas a profundidad que fueron realizadas a expertos del sector acuícola y complementado la información con el marco teórico.

A continuación, se presentará la metodología de la propuesta, aplicando cada una de las etapas para la reducción de riesgos en los sistemas de información contable, la misma que puede ser utilizada por diferentes departamentos de la PYMES del sector Acuícola y otros sectores como industriales, comerciales, bancarias o de servicios.

Riesgo I – Acceso Físico y Lógico a los Sistemas de Información Contable

Figura 36

Programa evaluación de riesgo I

Programa de Evaluación de Riesgos en los Sistemas de Información Contable				
Riesgo I - Acceso Físico y Lógico a los Sistemas de Información Contable				
No	Descripción	Tiempo		Elaborado por
		Estimado	Utilizado	
	Introducción			
1	Es importante conocer cuáles son los diferentes factores que conlleva a que se produzca el riesgo en el acceso físico y lógico a los sistemas de información contable.			
	Objetivos			
1	Identificar los riesgos en el acceso físico y lógico en los sistemas de información contable.	1 día	1 día	D.T
2	Verificar los riesgos existentes en las aplicaciones y sus controles en los sistemas de información contable.	1 día	1 día	D.T
3	Evaluar los niveles de riesgos por cada uno de los factores.	2 días	2 días	D.T
	Procedimientos			
1	Evaluar los riesgos mediante cuestionarios de preguntas.			
2	Responder el cuestionario de evaluación de riesgos.			
3	Calificar las preguntas mediante la rúbrica establecida.			
4	Elaborar cuadro de análisis de datos obtenido.			
5	Determinar el nivel de riesgo y análisis de resultados.			
6	Realizar matriz de riesgos identificados para determinar la probabilidad y severidad según el caso.			
7	Ubicar los riesgos en el mapa de calor para concientizar sus niveles.			
8	Establecer plan o medidas de acción.			
		Supervisado por: Conny Carrasco Fecha: 20/08/2022 Elaborado por: Deisy Torres		

Figura 37

Cuestionario evaluación de riesgo I

Cuestionario de Evaluación de Riesgos					
Preguntas	Respuestas		Ponderación	Calificación	
	Si	No			
Riesgo I - Acceso Físico y Lógico a los Sistemas de Información Contable					
1	¿Personas no autorizadas pueden tener acceso a las funciones de procesamiento de transacciones de los programas de aplicación, permitiéndoles leer, modificar, agregar o eliminar datos o ingresar transacciones no autorizadas para su procesamiento?		x	10	10
2	¿Los datos ingresados al sistema de información para el procesamiento pueden ser imprecisos, incompletos o ingresados más de una vez?	x		10	5
3	¿Las transacciones reales ingresadas para su procesamiento o generadas por el sistema pueden perderse, estar procesadas o registradas de forma incompleta, inexacta o en el periodo contable incorrecto?	x		10	4
4	¿Existen alarmas automatizadas, que nos informe inconsistencias en el proceso de la información?	x		10	10
5	¿El departamento de Recursos Humanos y el Administrador de Seguridad cuentan con información actualizada y sincronizada, referente al listado del personal y perfiles de los usuarios? ¿Para controlar el acceso al sistema de información, de acuerdo al personal activo con sus funciones asignadas y el personal inactivo?		x	10	0
6	¿Se efectúa revisión de los riesgos existentes en las aplicaciones y sus controles en los sistemas de información contable?		x	10	3
7	¿Existe plan de entrenamiento para el manejo de los sistemas de información contable?	x		10	8
8	¿Existe Campañas de concientización y técnicas para el uso de nuevas tecnologías?		x	10	0
9	¿El personal administrativo regularmente asiste a las capacitaciones que le ofrece la empresa para el desarrollo de una base de conocimientos en cuanto al sistema de información contable?		x	10	0
Total		4	5	90	40

Cuadro para Análisis de Datos Obtenidos
Cuestionario de Evaluación del Riesgo I

Total, de Preguntas Aplicadas en el Cuestionario	9
Respuestas Si	4
Respuestas No	5
Total de Respuestas	9

Determinación del Nivel de Riesgo I

CP = Confianza Ponderada

CT = Calificación Total

PT = Ponderación Total

$$CP = \frac{CT * 100}{PT}$$

$$CP = \frac{40 * 100}{90} = 44\%$$

Porcentaje	Nivel de Confianza	Riesgo de Control
10% - 50%	Bajo	Alto
51% - 75%	Moderado	Moderado
76% - 100%	Alto	Bajo

Análisis de los Resultados:

De acuerdo al resultado obtenido, la confianza ponderada está en 44% lo que representa un nivel de confianza – bajo y un riesgo de control – alto. Por tal motivo se debe ejecutar un plan de acción para fortalecer el nivel de confianza y sus controles.

Riesgo II – Manuales de Procedimientos y Políticas del Departamento Contable

Figura 38

Programa evaluación de riesgos II

Programa de Evaluación de Riesgos en los Sistemas de Información Contable				
Riesgos II – Manuales de Procedimientos y Políticas del Departamento Contable				
No	Descripción	Tiempo		Elaborado por
		Estimado	Utilizado	
	Introducción			
1	Los manuales de procedimientos son importantes para la empresa a la hora de controlar los accesos físico y lógico de los sistemas contables, estos controles se deben monitorear bajo políticas departamental.			
	Objetivos			
1	Identificar en los procesos de transacciones en el ingreso de datos y uso de los sistemas, si se aplica los manuales de procedimiento.	1 día	1 día	D.T
2	Verificar si existe fuga de información por falta de políticas de los accesos.	2 días	1 día	D.T
3	Solicitar de manera física o digital los manuales y políticas que se aplica en los procesos.	3 días	3 días	D.T
4	Evaluar los puntos débiles de los manuales y políticas existentes.	2 días	2 días	D.T
5	Proponer mejoras en los manuales y políticas de la empresa para evaluar los riesgos en los sistemas de información contable.	3 días	3 días	D.T
	Procedimientos			
1	Evaluar los riesgos mediante cuestionarios de preguntas.			
2	Responder el cuestionario de evaluación de riesgos.			
3	Calificar las preguntas mediante la rúbrica establecida.			
4	Elaborar cuadro de análisis de datos obtenido.			
5	Determinar el nivel de riesgo y análisis de resultados.			
6	Realizar matriz de riesgos identificados para determinar la probabilidad y severidad según el caso.			
7	Ubicar los riesgos en el mapa de calor para concientizar sus niveles.			
8	Establecer plan o medidas de acción.			
		Supervisado por: Conny Carrasco		
		Fecha: 20/08/2022		
		Elaborado por: Deisy Torres		

Figura 39

Cuestionario evaluación de riesgo II

Cuestionario para Evaluación de Riesgos					
Preguntas	Respuestas		Ponderación	Calificación	
	Si	No			
Riesgos II – Manuales de Procedimientos y Políticas del Departamento Contable					
1	¿La entidad dispone de reglamentos definidos y aprobados por escrito?	x		10	10
2	¿Los manuales de procedimientos y políticas están actualizados y comunicados a los involucrados?		x	10	0
3	¿Existen políticas en cuanto al mal manejo de los sistemas de información contable?		x	10	0
4	¿Existe métodos de buenas prácticas sobre los procesos críticos?		x	10	0
5	¿Los manuales de procedimientos y políticas del departamento tienen debilidades o mejoras que puedan ser aplicados?		x	10	0
Total		1	4	50	10

**Cuadro para Análisis de Datos Obtenidos
Cuestionario de Evaluación del Riesgo II**

Total de Preguntas Aplicadas en el Cuestionario	5
Respuestas Si	1
Respuestas No	4
Total de Respuestas	5

Determinación del Nivel de Riesgo II

CP = Confianza Ponderada

CT = Calificación Total

PT = Ponderación Total

$$CP = \frac{CT * 100}{PT}$$

$$CP = \frac{10 * 100}{50} = 20\%$$

Porcentaje	Nivel de Confianza	Riesgo de Control
10% - 50%	Bajo	Alto
51% - 75%	Moderado	Moderado
76% - 100%	Alto	Bajo

Análisis de los Resultados:

De acuerdo al resultado obtenido, la confianza ponderada está en 20% lo que representa un nivel de confianza – bajo y un riesgo de control – alto. Por tal motivo se debe ejecutar un plan de acción para fortalecer el nivel de confianza y sus controles.

Riesgo III – Estructura del Departamento Contable

Figura 40

Programa evaluación de riesgo III

Programa de Evaluación de Riesgos en los Sistemas de Información Contable				
Riesgo III – Estructura del Departamento Contable				
No	Descripción	Tiempo		Elaborado por
		Estimado	Utilizado	
	Introducción			
1	Los usuarios deberán tener el respectivo acceso a los sistemas de información contable de acuerdo a las funciones y tareas que se le delega al momento de su contratación.			
	Objetivos			
1	Pedir a cada usuario por escrito de las tareas y funciones que realiza en los sistemas.	1 día	1 día	D.T
2	Verificar las tareas escritas de cada usuario con los accesos y parametrización.	1 día	1 día	D.T
3	Evaluar el desempeño de cada empleado para reducir los riesgos al no contar con una estructura definidas.	2 días	2 días	D.T
	Procedimientos			
1	Evaluar los riesgos mediante cuestionarios de preguntas.			
2	Responder el cuestionario de evaluación de riesgos.			
3	Calificar las preguntas mediante la rúbrica establecida.			
4	Elaborar cuadro de análisis de datos obtenido.			
5	Determinar el nivel de riesgo y análisis de resultados.			
6	Realizar matriz de riesgos identificados para determinar la probabilidad y severidad según el caso.			
7	Ubicar los riesgos en el mapa de calor para concientizar sus niveles.			
8	Establecer plan o medidas de acción.			
		Supervisado por: Conny Carrasco Fecha: 20/08/2022 Elaborado por: Deisy Torres		

Figura 41

Cuestionario evaluación de riesgo III

Cuestionario para Evaluación de Riesgos					
Preguntas	Respuestas		Ponderación	Calificación	
	Si	No			
Riesgo III – Estructura del Departamento Contable					
1	¿Se encuentra claramente definido la descripción de funciones para cargo dentro de la organización?	x		10	9
2	¿Dispone de un manual de funciones de acuerdo a sus asignaciones en el departamento contable?		x	10	0
3	¿El personal que labora en la compañía, cumple con todos los requerimientos para desempeñar su trabajo de la manera adecuada?	x		10	8
4	¿El sistema de información está parametrizado de acuerdo al perfil de cada usuario?	x		10	10
5	¿Existe segregación de funciones en la estructura del departamento contable, los cuales permiten prevenir fraudes?	x		10	8
Total		4	1	50	35

**Cuadro para Análisis de Datos Obtenidos
Cuestionario de Evaluación del Riesgo III**

Total de Preguntas Aplicadas en el Cuestionario	5
Respuestas Si	4
Respuestas No	1
Total de Respuestas	5

Determinación del Nivel de Riesgo III

CP = Confianza Ponderada

CT = Calificación Total

PT = Ponderación Total

$$CP = \frac{CT * 100}{PT}$$

$$CP = \frac{35 * 100}{50} = 70\%$$

Porcentaje	Nivel de Confianza	Riesgo de Control
10% - 50%	Bajo	Alto
51% - 75%	Moderado	Moderado
76% - 100%	Alto	Bajo

Análisis de los Resultados:

De acuerdo al resultado obtenido, la confianza ponderada está en 70% lo que representa un nivel de confianza – moderado y un riesgo de control – moderado. Por tal motivo se debe ejecutar un plan de acción para fortalecer el nivel de confianza y sus controles.

Riesgo IV – Riesgos de Fraudes y Errores

Figura 42

Programa evaluación de riesgo IV

Programa de Evaluación de Riesgos en los Sistemas de Información Contable				
Riesgo IV – Riesgos de Fraudes y Errores				
No	Descripción	Tiempo		Elaborado por
		Estimado	Utilizado	
	<p>Introducción</p> <p>Una de las cosas importante en el negocio es la identificación de los fraudes y errores que se estén cometiendo en el acceso físico y lógico en los sistemas de información contable.</p>			
	<p>Objetivos</p>			
1	Determinar los niveles de riesgos que se produce debido a los fraudes y errores en los sistemas de información contable.	1 día	1 día	D.T
2	Verificar cuales han sido los controles frente a este riesgo de fraudes y errores.	2 días	1 día	D.T
3	Detectar los procesos contables, errores involuntarios y repetitivos efectuados por ingreso de información en los sistemas.	3 días	3 días	D.T
	<p>Procedimientos</p>			
1	Evaluar los riesgos mediante cuestionarios de preguntas.			
2	Responder el cuestionario de evaluación de riesgos.			
3	Calificar las preguntas mediante la rúbrica establecida.			
4	Elaborar cuadro de análisis de datos obtenido.			
5	Determinar el nivel de riesgo y análisis de resultados.			
6	Realizar matriz de riesgos identificados para determinar la probabilidad y severidad según el caso.			
7	Ubicar los riesgos en el mapa de calor para concientizar sus niveles.			
8	Establecer plan o medidas de acción.			
<p>Supervisado por: Conny Carrasco Fecha: 20/08/2022 Elaborado por: Deisy Torres</p>				

Figura 43

Cuestionario evaluación de riesgo IV

Cuestionario para Evaluación de Riesgos					
	Preguntas	Respuestas		Ponderación	Calificación
		Si	No		
Riesgo IV – Riesgos de Fraudes y Errores					
1	¿Ha existido intento de fraudes en el departamento contable?	x		10	3
2	¿Se han detectado en los procesos contable, fraudes/robos/errores efectuados por ingreso de información no autorizados en las aplicaciones de los sistemas de información?	x		10	9
3	¿Se han detectado en los procesos contable, errores involuntarios y repetitivos efectuados por ingreso de información en los sistemas?	x		10	10
4	¿Se han efectuado cambios del personal involucrado en el área contable después de descubrir fraudes?	x		10	9
5	¿Existen herramientas para el monitoreo de cumplimiento, pruebas de intrusión y reportes en los sistemas de información contable?		x	10	1
6	¿Existe periodicidad para validar la adecuada operación de los controles implementados?		x	10	0
7	¿El personal involucrado en los procesos críticos de la empresa cuentan con controles de un archivo logs?		x	10	1
8	¿Existe un comité de seguridad donde integren los responsables de las áreas críticas y personas que tengan el poder de tomar decisiones para realizar mejoras?		x	10	0
9	¿Conoce las funciones del comité de seguridad y la periodicidad de las reuniones?		x	10	0
Total		4	5	90	33

**Cuadro para Análisis de Datos Obtenidos
Cuestionario de Evaluación del Riesgo IV**

Total de Preguntas Aplicadas en el Cuestionario	9
Respuestas Si	4
Respuestas No	5
Total de Respuestas	9

Determinación del Nivel de Riesgo IV

CP = Confianza Ponderada

CT = Calificación Total

PT = Ponderación Total

$$CP = \frac{CT * 100}{PT}$$

$$CP = \frac{33 * 100}{90} = 37\%$$

Porcentaje	Nivel de Confianza	Riesgo de Control
10% - 50%	Bajo	Alto
51% - 75%	Moderado	Moderado
76% - 100%	Alto	Bajo

Análisis de los Resultados:

De acuerdo al resultado obtenido, la confianza ponderada está en 37% lo que representa un nivel de confianza – bajo y un riesgo de control – alto. Por tal motivo se debe ejecutar un plan de acción para fortalecer el nivel de confianza y sus controles.

Matriz de Riesgos Identificados

La evaluación de estos riesgos está diseñada bajo los siguientes elementos: (a) primero la identificación de los riesgos existentes, (b) luego determinar el personal y departamentos responsable, (c) calificar la probabilidad y severidad para obtener el resultado, y (d) establecer los niveles de riesgos. (ver Figura 44)

Figura 44

Calificación de matriz de riesgo

Matriz de Evaluación de Riesgos Identificados						
	Riesgos Identificados	Personal y/o Departamento	Evaluación del Riesgo			
			Severidad	Probabilidad	Calificación	Nivel de Riesgo
1	Acceso Físico y Lógico a los Sistemas de Información Contable.	Usuarios. Departamento Contable. Departamento de sistemas. Administrador de Seguridad. Otros departamentos	4	8	32	Riesgo Extremo
2	Manuales de Procedimientos y Políticas del Departamento.	Departamentos: Contable, Recursos Humanos y Sistemas.	3	8	24	Riesgo Alto
3	Estructura del Departamento.	Departamento Recursos Humanos.	3	6	18	Riesgo Tolerable
4	Riesgos de Fraudes y Errores.	Departamentos: Contable, Recursos Humanos y Sistemas. Comité de Seguridad.	5	10	50	Riesgo Extremo

Como validación de la información, se procedió a utilizar herramientas de fórmulas con Excel, realizando una tabla de resultados con datos automatizados. (ver Figura 45).

Figura 45

Resultados automatizados

Riesgo	Severidad	Probabilidad	Nivel de Riesgo
1	Crítico	Moderado	Riesgo Extremo
2	Moderado	Moderado	Riesgo Alto
3	Moderado	Ocasional	Riesgo Tolerable
4	Catastrófico	Constante	Riesgo Extremo

Una vez obtenido los resultados de los niveles de riesgos, se procede a ubicarlos en el mapa de calor, con la finalidad de concientizar acerca de los riesgos identificado y existentes, de tal forma que se pueda proceder con medidas de acción. (ver Figura 46)

Figura 46

Mapa de calor

		Matriz de Riesgo						
		Probabilidad						
		Improbable	Posible	Ocasional	Moderado	Constante		
Severidad							Color	Nivel del Riesgo
Insignificante							2 a 8	Riesgo Aceptable
Menor							10 a 18	Riesgo Tolerable
Moderado				Riesgo III	Riesgo II		20 a 24	Riesgo Alto
Crítico					Riesgo I		30 a 50	Riesgo Extremo
Catastrófico						Riesgo IV		

Plan de Acción para Reducción de Riesgos

Figura 47

Plan acción- reducción de riesgo I

No. de Identificación	Riesgo Identificados	Nivel de Riesgo Calificado	Personal y/o Departamento Responsables	Plan de Acción sobre cómo Reducir los Riesgos
Riesgo I	Acceso Físico y Lógico a los Sistemas de Información Contable	Riesgo Extremo	Usuarios	Entrenamientos a los usuarios y desarrollo de una base de conocimientos referente a al buen manejo de los sistemas de información.
			Departamento Contable	Controlar la información que entra o sale de la empresa, siendo esta íntegra y sólo esté disponible para los usuarios autorizados.
			Departamento de Sistemas	Validar accesos a los usuarios de acuerdo a la segregación de funciones que se encuentre desde el contrato del personal.
				Pruebas de intrusión y reportes de archivos logs. Chequeo de Software no autorizado.
				Prevención y detección de virus.
				Controles de entrada, procesamiento y salida.
			Administrador de Seguridad	El Administrador de Seguridad deberá, asegurarse de que los archivos, las aplicaciones y software utilizados dentro de la compañía se adapten a sus necesidades y se usen de manera adecuada por los empleados.
Todos los departamentos de la empresa	Deberán, ejecutar menos privilegios de accesos otorgados a los usuarios en el sistema de información.			

Figura 48

Plan acción- reducción de riesgo II y III

No. de Identificación	Riesgo Identificados	Nivel de Riesgo Calificado	Personal y/o Departamento Responsables	Plan de Acción sobre cómo Reducir los Riesgos
Riesgo II	Manuales de Procedimientos y Políticas del Departamento	Riesgo Alto	Departamento Contable	Desarrollar manual de procedimientos y políticas de control en el ingreso, procesamiento y salida de la información contable del sistema.
			Departamento de Sistemas	Generar políticas al momento de que se solicite accesos nuevos o con privilegios a los usuarios, soportando con evidencias y firmas de los responsables de cada departamento.
			Departamento de Recursos Humanos	Mantener informados a todos los departamentos con las políticas actualizadas que se hayan implementado en la empresa.
Riesgo III	Estructura del Departamento	Riesgo Tolerable	Departamento de Recursos Humanos	Establecer una organización documental donde se estipulen todos los manuales de procedimientos, manuales de funciones y organigramas de cada uno de los departamentos de la empresa.
				Deberá ejercer un inventario de habilidades de los empleados y segregar funciones desde su contrato.

Figura 49

Plan acción- reducción de riesgo IV

No. de Identificación	Riesgo Identificados	Nivel de Riesgo Calificado	Personal y/o Departamento Responsables	Plan de Acción sobre cómo Reducir los Riesgos
Riesgo IV	Riesgos de Fraudes y Errores	Riesgo Extremo	Departamento Contable	Revisión diaria de la base datos de actividades realizadas en el sistema de información.
			Departamento de Sistemas	Ejecutar herramientas para monitoreo de cumplimientos de controles.
				Pruebas de errores que ayuden a evitar pérdida de información y fallas al momento de manejar el sistema.
			Departamento de Recursos Humanos	Implementar en el sistema de información controles de edición, validación de campos faltantes, dígito verificador, doble ingreso, balanceo, límites. Los cuales, ayuden a cumplir con los formatos establecidos, caso contrario la aplicación deberá enviar un mensaje al usuario indicando el error y no permitirle continuar en el ingreso de la información hasta que la misma sea corregida.
				Entrenamiento a los usuarios y capacitaciones en el buen manejo de los sistemas de información.
			Campañas y Técnicas de concientización acerca de los fraudes y errores en los sistemas de información, implementando normativas de consecuencias al realizar dichos actos.	
			Para prevenir fraudes es importante controlar el personal que se contrata e investigar sus antecedentes en otras organizaciones.	
Comité de Seguridad	Para controlar todos estos riesgos se considera la necesidad de crear un comité de seguridad, donde se encuentren todos los encargados o responsables de los departamentos de la empresa para así poder tener una supervisión en cuantos los riesgos identificados. Efectuando sus reuniones con una periodicidad trimestral, para validar el cumplimiento de sus medidas de control y reducción de riesgos.			

Conclusiones

Los sistemas de información se encuentran en un constante desarrollo y evolución, lo que conlleva a que estos sean evaluados y supervisados mediante controles. En una empresa, el área contable es el encargado de ingresar información, procesarla mediante transacciones y dar resultados, que requieren ser validados con la finalidad de dar cumplimiento a los objetivos operativos y administrativos que contenga una organización empresarial.

De acuerdo los aspectos positivos y negativos del sistema de información contable, se ejecutó un análisis de FODA, por medio de las entrevistas a profundidad. En lo que se pudo concluir, aspectos positivos: (a) fortaleza, cuenta con una optimización del proceso, seguridad, manejo de datos, control de las actividades empresariales y tecnología avanzada, logrando el crecimiento de la organización empresarial, y (b) oportunidades, disponen de información ordenada y automatizada, incrementando la productividad del flujo de información de cada departamento logrando ser eficaces y eficientes en la búsqueda y entrega de información. En referencia a los aspectos negativos: (a) debilidades, son el acceso a las claves con privilegios, dependencia de la tecnología, resistencia al cambio, tener libre acceso a todos los módulos sin restricción a los usuarios, y (b) amenazas, hackeo a los sistemas de información, robo de información, espionaje empresarial, filtración de información falsa que ocasiona graves problemas en el desarrollo de las actividades contables y financieras de la empresa.

Mediante el marco teórico pudimos analizar que el fraude es un delito creativo que se comete en las empresas, donde los principales defraudadores son aquellas personas con mente agudas, inteligente y tienen cierta viveza para realizar los fraudes en los medios más vulnerable de la empresa. En cambio, los errores existen dos tipos: (a) errores de omisión no intencionales, esto son errores humanos y los más numerosos y costosos en la industria, como fallos matemáticos y aplicación errónea de los Principios de Contabilidad Generalmente Aceptado, y (b) errores intencionales que son desfalcos y falsificaciones de registros.

Referente al diagnóstico de control en la implementación de la metodología de la reducción de riesgos, se procedió a realizar una matriz de riesgo, la cual ayuda a identificar los niveles de riesgos existentes y generar reportes gráficos (mapa de calor) que sirven para representar la criticidad de estos, concientizando a la gerencia y administración a dar priorización y mitigación de los riesgos.

De acuerdo al objetivo general de la propuesta metodología, se desarrolló un proceso de control que se encarga reducir los riesgos en los sistemas de información contable. Ante lo indicado, la propuesta metodológica consta de cuatro temas, de los cuales se definirán como riesgos: (a) Riesgo I – Acceso Físico y Lógico a los Sistemas de Información Contable: el personal no autorizado pueda acceder de forma física y lógica a los sistemas de información, (b) Riesgos II – Manuales de Procedimientos y Políticas del Departamento Contable: el departamento Contable no cuenta con manuales de procedimientos y políticas en cada uno de sus procesos, (c) Riesgo III – Estructura del Departamento Contable: la estructura del departamento contable no cuenta con una segregación de funciones en el personal, que ocasiona deficiencia en los controles para reducir los riesgos, (d) Riesgo IV – Riesgos de Fraudes y Errores: la empresa no cuenta con pruebas de cumplimiento de controles para prevenir los riesgos de fraudes que son los más críticos y los errores involuntarios que pueden afectar la continuidad de la organización empresarial.

En la aplicación del proceso planteado de la metodología, se pudo detectar que los riesgos identificados obtuvieron una calificación de nivel de riesgo extremo y tolerable, lo que significa que estos riesgos existentes pueden generar fraudes y errores intencionales o no intenciones en los sistemas de información contable. Por medio de este proceso las empresas PYMES del sector acuícola podrán, (a) planificar el programa para evaluación de riesgo, (b) ejecutar cuestionarios, (c) supervisar los riesgos identificados mediante una matriz con mapa de calor, y (d) dar respuesta a los riesgos con acciones correctivas. Ante lo mencionado, este proceso permitirá obtener mayor efectividad en los controles y rendimiento de las operaciones.

Recomendaciones

Se recomienda el uso de la propuesta metodológica para la Reducción de Riesgos en los Sistemas de Información Contables en las empresas PYMES del sector acuícola, utilizando el siguiente esquema: (a) planificar el programa para evaluación de riesgo, (b) ejecutar cuestionarios, (c) supervisar los riesgos identificados mediante una matriz con mapa de calor, y (d) dar respuesta a los riesgos con acciones correctivas, que permitirá obtener mayor efectividad en los controles y rendimiento de las operaciones.

Se recomienda el uso de la propuesta metodológica para la Reducción de Riesgos en los Sistemas de Información Contables, para los gerentes, directivos y empresarios de empresas del sector acuícola. La cual, servirá como un manual de procedimiento para la reducción de riesgos en el acceso físico y lógico de los sistemas contables, logrando en los Estados Financieros una imagen fiel y de confianza.

Se recomienda el uso de la propuesta metodológica para nuevos estudios sobre Reducción de Riesgos en los Sistemas de Información Contables, con finalidad de prevenir fraudes y errores.

Referencia

- ACFE. (2016). *Reporte a las Naciones sobre el Abuso y el Fraude Ocupacional*. https://acfe-mexico.com.mx/archivos/Reporte_Naciones_2016_esp.pdf
- Aguilar, L. (2015). *Sistemas de Información en la empresa: El impacto de la nube, la movilidad y los medios sociales*. (Primera). Alfaomega. <https://n9.cl/g7ukq>
- Aguilera, P. (2010). *Seguridad Informática*. Editex.
- Albanese, D. (2012). Análisis y evaluación de riesgos: Aplicación de una matriz de riesgo en el marco de un plan de prevención contra el lavado de activos. *Universidad de Vale de Rio de Sinos*, 9(3), 215.: <http://www.redalyc.org/articulo.oa?id=337228651001>
- Albizuri, B. (2002). El Fraude y la delincuencia Informática: Un Problema Jurídico y Ético. *Instituto Tecnológico Autónomo de México*. <http://www.revista.unam.mx/vol.3/num2/art3/index.html>
- Alonso, C. (2020). ¿Qué es ITIL y para qué sirve? *Global Suite Solutions*. <https://www.globalsuitesolutions.com/es/que-es-til-y-para-que-sirve/>
- Altamirano, J., & Bayona, S. (2017). Políticas de Seguridad de la Información: Revisión sistemática de las teorías que explican su cumplimiento. *Revista Ibérica de Sistemas de Tecnologías de Información*, 25, 112-134. <https://doi.org/10.17013/risti.25.112-134>
- Álvarez, F., López, O., & Toledo, M. (2021). *Acceso al financiamiento de las PYMES*. <https://scioteca.caf.com/bitstream/handle/123456789/1752/Acceso%20al%20financiamiento%20de%20las%20pymes.pdf?sequence=1&isAllowed=y>
- Andrade, C., Iriarte, M., & Zambrano, J. (2016). Caracterización de las MIPYMES cantón Flavio Alfaro, Provincia Manabí, Ecuador. *Revista Científica Dominio de las Ciencias*, 2(4), 461-471.

- Aquaculture Magazine. (2021). *Ecuador is the first country to produce one million tons of shrimp from aquaculture*. [Tweet]. Twitter. <https://twitter.com/AquacultureMag/status/1475676238098440197>
- Arias, J. (2016). El protocolo de Investigación III: La población de estudio. *Revista Alergia México*, 63(2), 201-206. <https://doi.org/10.29262/ram.v63i2.181>
- Arroyave, D. B. A., & Ledesma, M. D. L. (2016). *Propuesta Metodológica de un Sistema de Información Contable para Mejorar la Productividad y Competitividad de las Pymes*. <https://bibliotecadigital.univalle.edu.co/bitstream/handle/10893/21017/CB-0581253.pdf?sequence=1>
- Atehortúa, F., Bustamante, R., & Valencia, J. (2008). *Sistema de gestión integral una sola gestión, un solo equipo* (Primera Edición). Editorial Universidad de Antioquía; Gestión y Conocimiento.
- Badillo, J. (2017). *Implementación y Evaluación de Control Interno Los 17 Principios COSO*. <https://1library.co/document/qmkkmw4z-implementacion-y-evaluacion-de-control-interno-los-17-principios-coso-jorge-badillo-ayala.html>
- Baena, G. (2017). *Metodología de la Investigación* (Tercera). Grupo Editorial Patria. <http://public.ebookcentral.proquest.com/choice/publicfullrecord.aspx?p=5213563>
- Barberán, P. (2017). *Auditoría de Sistemas Informáticos*. Dirección de Publicaciones de la UCSG.
- Barreix, D., Zambrano, R., Costa, M., Bahía, Á., & Almeida, J. (2018). *Factura electrónica en América Latina*. Inter-American Development Bank.
- BBC Bitesize. (2022). *Finalidad, funcionalidad y usuarios*. BBC Bitesize. <https://www.bbc.co.uk/bitesize/guides/z8xpsbk/revison/1>
- Bejarano, M. (2017). *Empresas fracasan por falta de contabilidad*. <https://www.elnuevodiario.com.ni/economia/432215-empresas-fracasan-falta-contabilidad-dice-experto/>

- Bernal, C. A. (2010). *Metodología de la Investigación* (Tercera). Pearson.
<https://abacoenred.com/wp-content/uploads/2019/02/El-proyecto-de-investigaci%C3%B3n-F.G.-Arias-2012-pdf.pdf>
- Blas, P. (2014). *Diccionario de Administración y Finanzas*. Palibrío.
<http://www.vlebooks.com/vleweb/product/openreader?id=none&isbn=9781463354954>
- Brenner, J. (2008). ISO 27001. *Risk Management*, 54, 24-29.
<https://go.gale.com/ps/i.do?p=AONE&sw=w&issn=00355593&v=2.1&it=r&id=GALE%7CA157587924&sid=googleScholar&linkaccess=abs>
- Briones, F. (2005). *La complejidad del riesgo: Breve análisis transversal*. 20, 3. file:///C:/Users/DETPC/Downloads/pdfslide.net_la-complejidad-del-riesgo-breve-analisis-transversal.pdf
- Brito, D. (2018). *El Riesgo Empresarial*. 269-277.
<http://scielo.sld.cu/pdf/rus/v10n1/2218-3620-rus-10-01-269.pdf>
- Buelvas, C., & Mejía, G. (2014). *El papel de la Contabilidad de gestión en el sistema de información contable y su incidencia en la rentabilidad de las empresas*.
<https://dialnet.unirioja.es/servlet/articulo?codigo=5671113>
- Cámara Nacional de Acuacultura. (2022). *Estadísticas—Cámara Nacional de Acuacultura*. <https://www.cna-ecuador.com/estadisticas/>
- Centro de Estudios Superiores Maranathá. (2022). *Características y tipos de Riesgo*. <https://www.cesuma.mx/blog/caracteristicas-y-tipos-de-riesgo-empresarial.html>
- Chávez, S. (2018). El concepto de Riesgo. *Centro de Investigaciones Biológicas del Noroeste, S.C., Instituto Politécnico Nacional* 195, 4(32-52).
https://www.cibnor.gob.mx/revista-rns/pdfs/vol4num1/03_CONCEPTO.pdf
- Ciifen. (2022). *Definición de Riesgo*. <https://ciifen.org/definicion-de-riesgo/>
- Coelho, F. (2021). *Significado de Investigación*. Significados.
<https://www.significados.com/investigacion/>

- Comité Directivo de COBIT. (2002). *COBIT Marco Referencial*. 72. http://files.uladech.edu.pe/docente/02659781/CAT/S07/02_03MarcoReferencial.pdf
- Comunidad Andina. (2009). *Resolución 1260 Disposición Técnica para la Transmisión de Datos de Estadísticas de PYME de los Países Miembros de la Comunidad Andina*. <https://www.comunidadandina.org/StaticFiles/DocOf/RESO1260.pdf>
- Comunidad Andina. (2022). *Servicio Nacional de Aduana del Ecuador*. <https://www.aduana.gob.ec/comunidad-andina-can/>
- Constitución de la Republica del Ecuador. (2018). *Contribuyentes obligados a emitir comprobantes electrónicos*. <https://www.sri.gob.ec/de/contribuyentes-obligados-a-emitter-comprobantes-electronicos>
- Corporación Financiera Nacional. (2021). *Ficha Sectorial del Camarón*. <https://www.cfn.fin.ec/wp-content/uploads/downloads/biblioteca/2021/fichas-sectoriales-3-trimestre/Ficha-Sectorial-Camaron.pdf>
- Corporación Financiera Nacional. (2022). *Ficha Sectorial Camarón 2022*. <https://www.cfn.fin.ec/wp-content/uploads/downloads/biblioteca/2022/fichas-sectoriales-1-trimestre/Ficha-Sectorial-Camaron.pdf>
- Código Orgánico Integral Penal, 234 Código Orgánico Integral Penal 13 (2021). file:///C:/Users/DETPC/Downloads/1164643__202206212311259241.pdf
- Crespo, J. (2009). *Detección del fraude en una auditoría de Estados Financieros*. 17. <https://www.redalyc.org/pdf/4259/425942160012.pdf>
- Cressey, D. (1973). *Other people's money; a study in the social psychology of embezzlement*. <https://www.worldcat.org/title/other-peoples-money-a-study-in-the-social-psychology-of-embezzlement/oclc/628437>
- Crizón, S. (2017). *Auditoría de Seguridad Física y Lógica de los Sistemas Informáticos*. 170.

<http://dspace.esPOCH.edu.ec/bitstream/123456789/5110/1/82T00275.pdf>

- Darryl, J. (2018a). *La producción actual, desafíos y el futuro del cultivo del camarón*. Responsible Seafood Advocate. <https://www.globalseafood.org/advocate/la-produccion-actual-desafios-y-el-futuro-del-cultivo-del-camaron/>
- Darryl, J. (2018b). *La producción actual, desafíos y el futuro del cultivo del camarón*. Responsible Seafood Advocate. <https://www.globalseafood.org/advocate/la-produccion-actual-desafios-y-el-futuro-del-cultivo-del-camaron/>
- Delgado, A. B. (2016). *¿De qué trata la NIA 240? SMS Auditores del Ecuador*. <https://smsecuador.ec/nia-240-fraude-en-una-auditoria/>
- Delgado, F. (2016). *¿Qué establece la NIA 315? - SMS Auditores del Ecuador*. <https://smsecuador.ec/que-establece-la-nia-315/>,
<https://smsecuador.ec/que-establece-la-nia-315/>
- Delgado, F. (2017). *¿Cómo optimizar el control Interno para evitar los Fraudes?*
- Díaz, L., Torruco, U., Martínez, M., & Varela, M. (2013). La entrevista, recurso flexible y dinámico. *Investigación en Educación Médica*, 2(7), 162-167. [https://doi.org/10.1016/S2007-5057\(13\)72706-6](https://doi.org/10.1016/S2007-5057(13)72706-6)
- Domínguez, J. (2015). *Seguridad Informática Personal y Corporativa*. IEASS.
- Espinoza, J., Figueroa, I., & Laínez, A. (2017). *Revista de Negocios & PYMES. Ecorfan*, 3(9), 27-34). https://www.ecorfan.org/spain/researchjournals/Negocios_y_PyMES/vol3num9/Revista_de_Negocios_&_PYMES_V3_N9_3.pdf
- Estupiñán, R. (2006). *Control Interno y Fraudes con Base en los Ciclos Transaccionales*. (segunda). <http://fullseguridad.net/wp-content/uploads/2016/10/Control-Interno-y-Fraudes-Con-Base-en-Los-Ciclos-Transaccionales.pdf>
- Etecé. (2022). Sistema de Información—Concepto, tipos, elementos y ejemplos. *Concepto*. <https://concepto.de/sistema-de-informacion/>

- Garner, B. (2004). *¿Qué es el fraude?* Association of Certified Fraud Examiners. <https://acfe-spain.com/recursos-contra-fraude/que-es-el-fraude>
- González, R. (2021). Marco Integrado de Control Interno. Modelo COSO III. *Qualpro Consulting* S.G. <https://www.ofstlaxcala.gob.mx/doc/material/27.pdf>
- Graterol, C., & Hernández, A. (2010). Aplicación de la norma de auditoría COBIT en el monitoreo de transferencias electrónicas de datos contable-financieros. *Publicaciones en Ciencias y Tecnología*, 5(1), 27-42. <https://revistas.uclave.org/index.php/pcyt/article/view/1068>
- Habana, C. (2018). *El control interno y sus herramientas de aplicación entre COSO y COCO*. 16. <http://scielo.sld.cu/pdf/cofin/v12n1/cofin18118.pdf>
- Hacknoid. (2019). *Importancia de la gestión de riesgos informáticos*. <https://www.hacknoid.com/hacknoid/importancia-de-la-gestion-de-riesgos-informaticos/>
- Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la Investigación* (Sexta). McGraw-Hill Inter Americana. <https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf>
- Hirth, R., Chambers, R. F., Danaher, M. A., & Landes, C. E. (2017). *Committee of Sponsoring Organizations of the Treadway Commission*. 16. https://audidoresinternos.es/uploads/media_items/coso-2018-esp.original.pdf
- Hluppiciencias Gerenciales. (2010). *Control Interno: El fraude y el error*. <http://controlinternohoy.blogspot.com/2010/10/el-fraude-y-el-error.html>
- IAASB. (2009a). *NIA 240 responsabilidades del auditor en la auditoría de estados financieros con respecto al fraude*. http://www.aplicaciones-mcit.gov.co/adjuntos/niif/15-%20A012%202013%20IAASB%20Handbook%20ISA%20240%20ES_wm.pdf

- IAASB. (2009b). *Norma Internacional de Auditoría 315*.
<http://www.aplicaciones-mcit.gov.co/adjuntos/niif/15%20-%20NIA%20315.pdf>
- IAASB. (2022). *Normas Internacionales de la Información Financiera NIIF - IFRS*. Deloitte Colombia.
https://www2.deloitte.com/co/es/pages/ifrs_niif/normas-internacionales-de-la-informacion-financiera-niif---ifrs-.html
- ISO 27001. (2020). *Riesgos en los Sistemas de Gestión de Seguridad de la Información*. PMG SSI - ISO 27001. <https://www.pmg-ssi.com/2020/01/la-gestion-de-riesgos-en-los-sistemas-de-gestion-de-seguridad-de-la-informacion/>
- ISO Tools Excellence. (2017). *Norma ISO 27002: El dominio político de seguridad*. <https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/>
- Isotools Excellence. (2018). *Gestión de Riesgos: ¿Cómo ha cambiado el nuevo COSO ERM 2017?* <https://www.isotools.org/2018/02/07/ha-cambiado-nuevo-coso-erm-2017/>
- Kosutic, D. (2022). *¿Qué es norma ISO 27001?* <https://advisera.com/27001academy/es/que-es-iso-27001/>
- Laudon, K. C., & Laudon, J. P. (2016). *Sistemas de Información Gerencial*. Pearson Educación.
- López, A. (2012). *Fundamentos de Sistemas de Información (SI)*. 22.
- Los Nuevos Conceptos del Control Interno: Informe COSO*. (1997). Díaz de Santos. <https://books.google.com.ec/books?id=335uGf3nusoC>
- Los Nuevos Conceptos del Control Interno: Informe COSO* (Díaz de Santos S.A). (1997). Ediciones Díaz de Santos. https://books.google.com.ec/books?id=335uGf3nusoC&pg=PA27&hl=es&source=gbs_toc_r&cad=4#v=onepage&q&f=false
- Luhmann, N. (2006). *Sociología del Riesgo* (3. ed). Univ. Iberoamericana. https://books.google.com.ec/books?id=74RRXy0EX4wC&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

- Luna, J. E. (2005). *Influencia del capital humano para la competitividad de las Pymes* [Disertación doctoral, Celaya]. <https://www.eumed.net/tesis-doctorales/2013/jelc/jelc.pdf>
- Luna, O. (2013). *Sistemas de Control Interno para Organizaciones* (Primera). IICO.
<https://books.google.com.ec/books?hl=es&lr=&id=plsiU8xoQ9EC&oi=fnd&pg=PP1&dq=control+interno+segun+autores&ots=INrBIHd4l2&sig=7AK0UTx3VCNDEMLWuBwvuFxmST0#v=onepage&q&f=false>
- Lux, L., & Calderón, O. (2020). El delito de fraude informático: Concepto y delimitación. *Revista Chilena de Derecho y Tecnología*, 9(1), 151. <https://doi.org/10.5354/0719-2584.2020.57149>
- Mann, S. (2021). *¿Qué es ITIL? Una visión integral de la historia de ITIL*. <https://freshservice.com/es/itil/freshservice.com/es/itil>
- Maranto, M., & González, M. (2015). *Fuente de Información*. Universidad Autónoma Del Estado de Hidalgo. <https://repository.uaeh.edu.mx/bitstream/bitstream/handle/123456789/16700/LECT132.pdf>
- Marriot, F. (2003). *Análisis del Sector Camaronero*. <https://contenido.bce.fin.ec/documentos/PublicacionesNotas/Catalogo/Apuntes/ae29.pdf>
- Martínez, C. (2012). El muestreo en investigación cualitativa: Principios básicos y algunas controversias. *Ciencia & Saúde Colectiva*, 17(3), 613-619. <https://doi.org/10.1590/S1413-81232012000300006>
- Mendoza, S., & Ávila, D. (2020). Técnicas e instrumentos de recolección de datos. *Boletín Científico de las Ciencias Económico Administrativas del ICEA*, 9(17), 51-53. <https://doi.org/10.29057/icea.v9i17.6019>
- Millet, D. (2008). *Facturación electrónica: La búsqueda de la eficiencia y productividad*. <http://jggomez.eu/z%20Privado/b%20usuarios/n-revista/caja/2pd/2008/197B.pdf>
- Monte, M. (2010a). *Seguridad Lógica y Accesos y su Auditoría*. <https://e-archivo.uc3m.es/bitstream/handle/10016/10653/PFC+Seguridad+Logica+y+de+Accesos+y+su+Auditoria.pdf?sequence=1>

- Monte, M. (2010b). *Seguridad Lógica y de Accesos y su Auditoría*. 259. <https://e-archivo.uc3m.es/bitstream/handle/10016/10653/PFC+Seguridad+Logica+y+de+Accesos+y+su+Auditoria.pdf?sequence=1>
- Montero, C. (2016). *Modelos Prácticos de Administración de Riesgos*. Ediciones ISEF Empresa Líder.
- Müggenburg, M. C., & Pérez, I. (2018). Tipos de estudio en el enfoque de investigación cuantitativa. *Enfermería Universitaria*, 4(1). <https://doi.org/10.22201/eneo.23958421e.2007.1.469>
- Mujica, M., & Álvarez, Y. (2009). *El Análisis de Riesgo en la seguridad de la información*. 4. <file:///C:/Users/DETPC/Downloads/Dialnet-ElAnalisisDeRiesgoEnLaSeguridadDeLaInformacionNota-6505355.pdf>
- O'Brien, J. A. (2006). *Sistemas de Información Gerencial*. McGraw-Hill Interamericana de España.
- OIT. (2019). *El poder de lo pequeño: Hay que activar el potencial de las pymes*. <https://www.ilo.org/infostories/es-ES/Stories/Employment/SMEs#power-of-small>
- Organización de las Naciones Unidas para la alimentación y agricultura. (2021a). *Pesca y acuicultura*. <https://www.fao.org/fishery/es/aquaculture>
- Organización de las Naciones Unidas para la alimentación y agricultura. (2021b). *Pesca y Acuicultura*. <https://www.fao.org/fishery/es/aquaculture>
- Organización Internacional de Estandarización. (1999). *ISO/IEC 1999*. ISO. <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/03/28/32893.html>
- Organización Internacional de Estandarización. (2005). *SGSI*. <https://www.iso27000.es/sgsi.html>
- Organización Internacional de Estandarización. (2022). *ISO 27001 - Seguridad de la información: Norma ISO IEC 27001/27002. Normas ISO*. <https://www.normas-iso.com/iso-27001/>

- Pascale, R. (2013). *Teoría del Riesgo*. <https://ricardopascale.com/wp-content/uploads/2013/09/2010-Teor%C3%ADa-del-Riesgo-oct.pdf>
- Patton, M. (2002). *Qualitative research and evaluation methods* (3 ed). Sage Publications.
- Peña, A. (2006). Metodología de Investigación Científica Cualitativa. *Investigación cualitativa*, 38. <http://www.ubiobio.cl/miweb/webfile/media/267/3634305-Metodologia-de-Investigacion-Cualitativa-A-Quintana.pdf>
- PricewaterhouseCoopers. (2022). *PwC's Global Economic Crime and Fraud Survey 2022*. <https://www.pwc.com/gx/en/forensics/gecsm-2022/pdf/PwC%E2%80%99s-Global-Economic-Crime-and-Fraud-Survey-2022.pdf>
- PriceWaterHouseCoopers (PwC's). (2022). *PwC's Global Economic Crime and Fraud Survey 2022*. <https://www.pwc.com/gx/en/forensics/gecsm-2022/pdf/PwC%E2%80%99s-Global-Economic-Crime-and-Fraud-Survey-2022.pdf>
- PwC's. (2022). *PwC's Global Economic Crime and Fraud Survey 2022*. <https://www.pwc.com/gx/en/forensics/gecsm-2022/pdf/PwC%E2%80%99s-Global-Economic-Crime-and-Fraud-Survey-2022.pdf>
- Rambay, C. (2020). *Factores que influyen en la sistematización de los procesos contables en PYMES del sector consolidador de cargas de la ciudad de Guayaquil*. <http://repositorio.ucsg.edu.ec/bitstream/3317/15227/1/T-UCSG-PRE-ECO-CICA-452.pdf>
- Real Academia Española, R.-. (1992). *Riesgo | Diccionario de la lengua española*. «Diccionario de la lengua española» - Edición del Tricentenario. <https://dle.rae.es/riesgo>
- Red Hat, Inc. (2005). *Controles de seguridad*. <http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-sgs-ov-controls.html>
- Rivas, G. (2011). *Modelos contemporáneos de control interno. Fundamentos teóricos*. 23. <https://www.redalyc.org/pdf/2190/219022148007.pdf>

- Rivera, H. (2018). *Análisis de oferta y demanda del camarón en la provincia de El Oro y Ecuador en los últimos ocho años*. http://repositorio.utmachala.edu.ec/bitstream/48000/12221/1/DE00006_EXAMENCOMPLEXIVO.pdf
- Rodríguez, P. (2020). *Análisis de riesgos informáticos y ciberseguridad*. <https://www.ambit-bst.com/blog/análisis-de-riesgos-informáticos-y-ciberseguridad>
- Royo, M. (2013). *Manual práctico de Control Interno: Teoría y aplicación práctica*. Profit Editorial.
- Rozas, A. (2009). *Auditoría Forense*. file:///C:/Users/USER/Downloads/0.pdf
- Salen, P., & Ontaneda, I. (2019). *Expertos en camarón y tilapia*. <http://www.revistalideres.ec/lideres/camaron-pescado-produccion-industria-guayaquil.html>
- Schwarz. (2022). *Fisheries and Aquaculture—National Aquaculture Sector Overview—Ecuador*. FAO. FAO. <https://www.fao.org/fishery/en/countrysector/ec/es>
- Stair, R. M., & Reynolds, G. W. (2010). *Principios de un Sistema de Información—Un enfoque administrativo* (9th ed). Course Technology Cengage Learning.
- Superintendencia de Compañías. (2008). *Resolución No. 06.Q.ICI.004*. https://www.supercias.gob.ec/bd_supercias/descargas/niif/Resolucion.pdf
- Superintendencia de Compañías, Valores y Seguros. (2022). *Ranking Empresarial 2022*. <https://appscvsconsultas.supercias.gob.ec/rankingCias/>
- Tóala, S., Arteaga, K., & Álava, J. (2018). Control interno en los costos de fabricación de los productos lácteos en la Cooperativa de Producción Agropecuaria “Chone Ltda.”. *Polo del Conocimiento*, 3(11), 282. <https://doi.org/10.23857/pc.v3i11.796>
- Uriarte, J. (2021). *Sistema de Información*. Características. <https://www.caracteristicas.co/sistema-de-informacion/>

- Valencia, F., & Orozco, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Revista Ibérica de Sistemas de Tecnologías de Información*, 22, 73-88. <https://doi.org/10.17013/risti.22.73-88>
- Vallejo, M. (2002). *El diseño de investigación: Una breve revisión metodológica*. 72, 6. <https://www.medigraphic.com/pdfs/archi/ac-2002/ac021b.pdf>
- Vallejo, M. (2005). *Fraude informático—Derecho Ecuador*. <https://derechoecuador.com/fraude-informaacutetico/>
- Varela, H., Ramos, B., Solórzano, S., & Varela, G. (2017). *Exportación de camarón de la provincia de El Oro en el contexto del Tratado Comercial con la Unión Europea*. 19.
- Vásquez, A. (2019). *Las ventajas de sistematizar su Pyme*. Diario la República. <https://www.larepublica.co/economia/las-ventajas-de-sistematizar-su-pyme-2876743>
- Velasco, W. (2008). *Políticas y Seguridad de la Información*. 7.
- Vélez, C. (2022). *Errores de Software*. <http://www.ii.unam.mx/es-mx/AlmacenDigital/CapsulasTI/Paginas/erroresdesoftware.aspx>
- Vila, M. (2013). *Ministerio de Agricultura, Ganadería y Pesca, Argentina*.
- Villalón, A. (2002). *Seguridad en UNIX y Redes*. <https://www.rediris.es/cert/doc/unixsec/unixsec.pdf>
- Viloria, N. (2005). *Factores que inciden en el sistema de control interno de una organización*. <https://www.redalyc.org/pdf/257/257011111.pdf>
- Yance, C., Solís, L., & Burgos, I. (2017). *La importancia de las PYMES en el Ecuador*. <https://www.eumed.net/coursecon/ecolat/ec/2017/pymes-ecuador.html>
- Zapata, E. (2004). *Las PYMES y su problemática empresarial. Análisis de casos*. 119-135. <https://www.redalyc.org/pdf/206/20605209.pdf>



DECLARACIÓN Y AUTORIZACIÓN

Yo, **Carrasco Viteri, Conny Sheeys** con **C.C: # 093028479-9** y **Torres Chávez, Deisy Alexandra** con **C.C # 092743748-3**, autoras del trabajo de titulación: **“Propuesta metodológica para la reducción de riesgos de los sistemas de información contable de empresas del sector acuícola de la provincia del Guayas”**, previo a la obtención del título de Licenciada en Contabilidad y Auditoría, en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 16 de septiembre del 2022.

f. 

Carrasco Viteri, Conny Sheeys
C.C 0930284799

f. 

Torres Chávez, Deisy Alexandra
C.C: 0927437483



REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	"Propuesta metodológica para la reducción de riesgos de los sistemas de información contable de empresas del sector acuícola de la provincia del Guayas"		
AUTOR(ES)	Carrasco Viteri, Conny Sheeys Torres Chávez, Deisy Alexandra		
REVISOR(ES)/TUTOR(ES)	Ing. Delgado Loor, Fabian Andrés		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Economía y Empresa		
CARRERA:	Contabilidad y Auditoría		
TITULO OBTENIDO:	Licenciada en Contabilidad y Auditoría		
FECHA DE PUBLICACIÓN:	16 de septiembre del 2022	No. DE PÁGINAS:	153
ÁREAS TEMÁTICAS:	Control de procesos, Auditoria de sistemas, validación de procesos		
PALABRAS CLAVES	Riesgos, Sistemas de información, Errores, Fraudes, Control, Acceso físico, Acceso lógico.		
RESUMEN: La metodología propuesta se basa en la Reducción de Riesgos en los accesos físico y lógico de los Sistemas de Información Contables, para prevenir errores y fraudes que se pueden presentar en las empresas PYMES del sector Acuícolas. El trabajo investigado se fundamenta en las teorías de riesgos y controles interno para la mitigar los riesgos identificados o existentes. Se realizó el enfoque de la investigación mediante datos cualitativas, aplicando herramienta para recolección de datos a través de entrevistas a profundidad, efectuada a seis expertos. Desarrollando en resumen los principales hallazgos, planteando las repuestas encontradas e identificando las similitudes y diferencias en una matriz. Concluimos con la propuesta metodológica desarrollando un proceso de reducción de riesgo, mediante un esquema que consiste de cuatro etapas que son: (a) planificar el programa para evaluación de riesgo, (b) ejecutar cuestionarios, (c) supervisar los riesgos identificados mediante una matriz con mapa de calor, y (d) dar respuesta a los riesgos con acciones correctivas.			
ADJUNTO PDF:	<input checked="" type="checkbox"/> SI	<input type="checkbox"/> NO	
CONTACTO AUTOR/ES:	CON	Teléfono: +593-990278466 +593-998482755	E-mail: deisy.torres@cu.ucsg.edu.ec conny.carrasco@cu.ucsg.edu.ec
CONTACTO INSTITUCIÓN (COORDINADOR PROCESO UTE):	CON LA DEL	Nombre: Bernabé Argandoña, Lorena Carolina	
		Teléfono: +593-4- 3804600 ext.1635	
		E-mail: lorena.bernabe@cu.ucsg.edu.ec	
SECCIÓN PARA USO DE BIBLIOTECA			
Nº. DE REGISTRO (en base a datos):			
Nº. DE CLASIFICACIÓN:			
DIRECCIÓN URL (tesis en la web):			