República del Ecuador

Universidad Tecnológica Empresarial de Guayaquil

Facultad de Postgrados e Investigación

Tesis en opción al título de Magister en:

Sistema de Información Gerencial

Tema de Tesis:

Modelos de seguridad de la información para el control de los riesgos informáticos en el área administrativa de una empresa de operadores logísticos de comercio exterior en la ciudad de Guayaquil

Autor:

Lcda. Elizabeth Loor Quimíz

Director de Tesis:

Ing. Diego Aguirre González MSc.

Noviembre 2021

Guayaquil - Ecuador

Declaración Expresa

En correspondencia con el Reglamento de postgrado cedemos el patrimonio, control y todo lo relacionado a las leyes de propiedad intelectual del presente trabajo de investigación a la Universidad Tecnológica Empresarial de Guayaquil.

Así mismo nos hacemos responsables del contenido vertido en la misma, pues corresponde al fruto de nuestra investigación para optar por el título de Master en Sistema de Información Gerencial.

Dedicatoria

A quienes siempre guardaron y transmitieron como testimonio de vida el lema, **“No te des por vencido ni aún vencido”** por eso dedico esta obra a mis dos siempre amadas madres Francisca Quimíz y Mariana Loor, quienes supieron inculcarme los mejores valores.

A mis dos hermanos Jenniffer y Kevin quienes están siempre a mi lado.

A las personas como: Mis tíos, que con esfuerzo y paciencia apoyaron mis ideales.

A quien me encamino por la senda progresiva infundiéndome siempre calma, amor y comprensión.

A todos los estudiantes que día a día se esfuerzan para obtener un futuro mejor, para ellos y sus familias que han pasado por diversos obstáculos y vicisitudes no se dan por vencido y siguen adelante camino al éxito.

Agradecimientos

A Dios todo poderoso ser supremo que me dio la vida.

A mi familia que de una u otra manera contribuyo para la realización de este proyecto.

A la Universidad Tecnológica Empresarial de Guayaquil, Facultad de Estudio de Postgrados por haberme abierto las puertas en su prestigiosa institución.

Al señor tutor MSC. Diego Aguirre González. porque en todo momento me brindo su valiosa colaboración en las asesorías de mi tesis.

Resumen

En algunas Pymes del Ecuador no cuentan con medidas de seguridad informática que permita proteger la información y los activos de las organizaciones lo cual repercute en que los procesos no sean ejecutados de manera eficiente afectando la gestión operativa. En esta investigación se realizó un estudio descriptivo de la empresa Torres y Torres para conocer la situación real de la empresa mediante una entrevista a 50 empleados, los cuales manifestaron lo siguiente: Al utilizar los modelos de seguridad informática utilizando la Ley SOX y SGSI se evita los riesgos, ataque de hackers, amenazas, el correcto funcionamiento de las máquinas y tener un control de quien tiene acceso a la información. Mediante las Normas ISO el personal los clientes tienen un acceso en tiempo real a sus productos mejora la calidad del servicio y abre más campos laborales, por ello se capacita al personal sobre los distintos riesgos a los cuales ha sido expuesta la empresa y protegiendo a los ordenadores de estas amenazas. Entre las vulnerabilidades se encontró que existen amenazas, vulnerabilidades y riesgos que han afectado a la empresa, con lo que se dedujo que el sistema puede ser atacado generando un riesgo del acceso cuando cualquier persona extraña infecta a la computadora, a la infraestructura y el desarrollo de la operación de estos. Para ello se recomienda proteger los ordenadores de las amenazas, riesgos y vulnerabilidades se recomienda instalar antimalware, tener un buen antivirus, evitar entrar sitios web sospechosos y en enlaces de correos electrónicos sospechosos.

Palabras claves: Seguridad informática, empresa, Ley SOX, SGSI, vulnerabilidades.

Abstract

In some SMEs in Ecuador, they do not have computer security measures to protect the information and assets of the organizations, which means that the processes are not executed efficiently, affecting the operational management. In this research, a descriptive study of the Torres y Torres company was carried out to know the real situation of the company through an interview with 50 employees, who stated the following: By using the computer security models using the SOX Law and SGSI, it is avoided risks, hacker attacks, threats, the correct functioning of the machines and having control of who has access to the information. Through ISO Standards, staff clients have real-time access to their products, improving the quality of service and opening up more labor fields, therefore, staff are trained on the different risks to which the company has been exposed and protecting the computers from these threats. Among the vulnerabilities, it was found that there are threats, vulnerabilities and risks that have affected the company, with which it was deduced that the system can be attacked, generating a risk of access when any stranger infects the computer, infrastructure and development of the operation of these. To do this, it is recommended to protect computers from threats, risks and vulnerabilities, it is recommended to install antimalware, have a good antivirus, avoid entering suspicious websites and in suspicious email links.

Keywords: Computer security, company, SOX Law, ISMS, vulnerabilities.

Índice General

Introducción 1

Capitulo I. Marco teórico conceptual 3

1.1. Antecedentes de la investigación 3

1.2. Planteamiento del problema de investigación 4

1.3. Formulación del problema 5

1.4. Sistematización del problema 5

1.5. Objetivos de la investigación 6

1.5.1. Objetivo general 6

1.5.2. Objetivos específicos 6

1.6. Justificación de la investigación 6

1.6.1. Conveniencia 6

1.7. Marco de referencia de la investigación 7

1.7.1. Sistema de gestión de la seguridad de la información 7

1.7.2. Seguridad de la información 8

1.7.3. Seguridad informática 9

1.7.4. Aspectos de la seguridad informática 10

1.7.5. Elementos de la seguridad informática 11

1.7.6. Amenazas de la seguridad informática 12

1.7.7. Tipos de amenazas 13

1.7.8. Estándares y normas para asegurar la información 14

1.8. Modelos de seguridad informática 16

1.8.1. Modelo COBIT 16

1.8.2. Modelo ITIL 20

1.8.3. Modelo COSO 21
1.8.5. Modelo LEY SOX 25
1.8.6. Modelo COCO 27
1.8.7. Modelo de seguridad CNSS 29
1.9. Riesgos de seguridad de la información 30
1.9.4. Valoración de riesgos de seguridad de la información 31
Capitulo II. Marco metodológico 32
2.1. Tipo de estudio, alcance y enfoque de la investigación 32
2.1.1. Tipo de estudio 32
2.1.2. Alcance de la investigación 32
2.1.3. Enfoque de la investigación 32
2.2. Métodos de investigación 35
2.3. Unidad de análisis, población y muestra 35
2.4. Variables de la investigación, operacionalización 36
2.4.1. Cuadro de operacionalización de variables 36
2.4.2. Tipos de Variables 36
2.5. Fuentes, técnicas e instrumentos para la recolección de información 37
2.5.1. Encuesta 38
2.5.2. Entrevistas 40
2.6. Tratamiento de la información 41
Capitulo III. Análisis, presentación de resultados y diagnostico 42
3.1. Seleccionar Modelo de Control de los riesgos informáticos. 42
3.2. Identificar las vulnerabilidades en la seguridad de la información. 45
3.3. Analizar de los riesgos de seguridad de la empresa. 56
IV. Conclusiones y recomendaciones 64

4.1. Conclusiones 64
4.2. Recomendaciones 65
Referencias bibliográficas 66
Anexos 74
Anexo 1. Modelo recolección de datos del modelo 74
Anexo 2. Modelo de encuesta 75
Anexo 3. Modelo de validación de Objetividad 81
Anexo 4. Modelo de validación de Contenido 82
Anexo 5. Tabulación de los resultados de la encuesta 83
Anexo 6. Alfa de Cronbach de dimensiones de la encuesta 84
Anexo 7. 86

Índice de tablas

Tabla 1. Baremo para el CVC 33

Tabla 2. Baremo de medición del Alfa de Cronbach 34

Tabla 3. Cuadro de Operacionalización de las variables 36

Tabla 4. Coeficiente de coincidencia del modelo COBIT 42

Tabla 5. Coeficiente de coincidencia del modelo ITIL 43

Tabla 6. Coeficiente de coincidencia del modelo COSO 43

Tabla 7. Coeficiente de coincidencia del modelo Ley SOX 43

Tabla 8. Coeficiente de coincidencia del modelo COCO 44

Tabla 9. Coeficiente de coincidencia del modelo CNSS 44

Tabla 10. Resumen del CVC de los modelos 45

Tabla 11. CVC de validez de Contenido de la encuesta 46

Tabla 12. CVC de validez de Objetividad de la encuesta 47

Tabla 13. Resultados de la Fiabilidad del instrumento de investigación 47

Tabla 14. Alfa de Cronbach Dimensión Garantía 84

Tabla 15. Alfa de Cronbach Dimensión Gobernanza 84

Tabla 16. Alfa de Cronbach Dimensión Identidad y Control de acceso 84

Tabla 17. Alfa de Cronbach Dimensión Gestión de riesgos 85

Tabla 18. Alfa de Cronbach Dimensión Servicio 85

Tabla 19. Alfa de Cronbach de la encuesta 85

Índice de gráficos

Gráfico 1. Área de desempeño de los encuestados..... 48

Gráfico 2. Pregunta 1 49

Gráfico 3. Pregunta 2 49

Gráfico 4. Pregunta 3 50

Gráfico 5. Pregunta 4 50

Gráfico 6. Pregunta 5 51

Gráfico 7. Pregunta 6 51

Gráfico 8. Pregunta 7 52

Gráfico 9. Pregunta 8 52

Gráfico 10. Pregunta 9 53

Gráfico 11. Pregunta 10 54

Gráfico 12. Pregunta 11 54

Gráfico 13. Pregunta 12 55

Gráfico 14. Pregunta 13 55

Gráfico 15. Pregunta 14 56

Índice de figuras

Figura 1. Pilares de la seguridad informática 11

Figura 2. Evolución del modelo COBIT 16

Figura 3. Principios del modelo COBIT 17

Figura 4. Modelo COBIT 18

Figura 5. Evolución del modelo ITIL 19

Figura 6. Modelo ITIL 20

Figura 7. Evolución del modelo COSO 22

Figura 8. Componentes y principios del modelo COSO 23

Figura 9. Modelo COSO 24

Figura 10. Evolución del modelo LEY SOX 25

Figura 11. Principios del modelo LEY SOX 26

Figura 12. Modelo LEY SOX 27

Figura 13. Modelo COCO 28

Figura 14. Modelo PHVA 30

Introducción

En el actual trabajo de investigación, el objeto de estudio es identificar un modelo de sistema de información para maximizar el control de los riesgos informáticos en el área administrativa, esencialmente en una empresa de operadores logísticos para el comercio exterior en la ciudad de Guayaquil, la cual es responsable del servicio integral de almacenamiento, importaciones, exportaciones y regímenes especiales.

La empresa logística ha ido desarrollando y mejorando día tras días sus actividades gracias a la tecnología, a tal punto que es parte fundamental en la misma, así mismo la dinámica online del mercado globalizado le ha exigido abrirse al mundo a través de las redes informáticas, lo que al momento es casi inimaginable concebir a la empresa sin toda esta tecnología.

Pero no todo es beneficio, los sistemas informáticos están sometidos a potenciales amenazas de diversas índoles, originadas tanto desde dentro de la propia empresa, como desde fuera, procedentes de una amplia variedad de fuentes de ahí la importancia de tener un sistema de seguridad, que permita la gestión de vulnerabilidades, riesgos y amenazas a las que normalmente se ve expuesta esta información, presente en cada uno de los procesos internos de las organizaciones.

Teniendo esto presente las instituciones aplican controles que incluyan políticas, procesos, procedimientos, órganos de control y activación de funciones tanto por hardware como por software, todos los cuales deben ser normados, implementados, supervisados y mejorados en un ciclo de cadena continua que lleven a mitigar estos delitos informáticos o amenazas a los que están expuestos los datos, comprometiendo la integridad, confidencialidad y disponibilidad de la información, basándonos en la seguridad de la información por los estándares actuales como la norma ISO 27000.

La implementación del modelo de sistema de información ayuda a controlar los sistemas informáticos y por tanto elevan la seguridad de la información de las organizaciones; garantizando el establecimiento de inspecciones positivos para lograr el nivel de seguridad necesario en alineación con los objetivos de las instituciones, de tal forma que se mantenga un nivel de riesgo mínimo por las entidades, entregando a la alta gerencia las herramientas adecuadas que les brinda una visión completa sobre el estado de sus sistemas informáticos, las revisiones de seguridad que se apliquen y los consecuencias que se obtenga de dicha aplicación, para la toma de decisiones de manera acertada sobre la estrategia aplicada.

Capitulo I. Marco teórico conceptual

1.1. Antecedentes de la investigación

La masiva utilización de las computadoras y redes como medios para transferir, procesar y almacenar información en los últimos años se ha incrementado, transformando la información en el activo de toda organización, el cual se debe proteger y asegurar, ya que está constantemente bajo amenaza de muchas fuentes, estas características pueden ser factores esenciales para mantener los niveles de competencia y lograr los objetivos propuestos por la organización (Romero M et al, 2018).

Los datos están en riesgo constantemente, las amenazas aumentan a medida rápidamente ya que puede implementar medidas contra ello, el uso intenso de la tecnología y el poco conocimiento de seguridad informático por parte de los usuarios, esto hace que la prevención de la seguridad de la información ya no sea una opción sino una obligación diaria (Alarcon J, 2016).

Los ciberataques son casi imposibles evitar, dada la apertura de las redes y la creciente sofisticación de las amenazas avanzadas, intentando recolectar, interrumpir, negar, degradar o destruir recursos del sistema de información o la información a sí mismo (Baca G, 2016).

En nuestro país la seguridad de la información está teniendo un empuje importante por los entes de control, motivado por constantes reportes de delitos informáticos en lo que se han vuelto inmersos entes públicos, privados, educativos, gubernamentales, financieros y las faltas de normas legales o inadecuación de las que existen (Zapata K, 2020); es importante en toda institución poseer modelos de seguridad de información ante cualquier eventualidad.

1.2. Planteamiento del problema de investigación

En algunas de las Pymes en Ecuador no cuentan con medidas de seguridad informática que permita proteger la información y los activos de las organizaciones, lo cual repercute en que los procesos no sean ejecutados de manera eficiente afectando la gestión operativa de estas empresas (Zapata K, 2020).

Las empresas manejan grandes volúmenes de datos, de ahí la importancia de tener un sistema de seguridad de la información que permita la gestión de vulnerabilidades, riesgos y amenazas a las que normalmente se ve expuesta esta información presente en cada uno de los procesos internos de estas compañías, en algunas de estas empresas no se tienen estandarizados controles que lleven a mitigar delitos informáticos o amenazas a los que están expuestos los datos, comprometiendo la integridad, confidencialidad y disponibilidad de la información (Bedoya M, 2020).

La empresa de operadores logísticos no realiza control de seguridad de la información, la falta de implementación de políticas de seguridad tales como: uso de claves de usuario, estándares de calidad en el manejo de los servicios y procesos, se maneja información de manera inapropiada siendo vulnerables a la fuga de datos y manipulación de la información por parte de personas no autorizadas así como el limitado personal especializado existente para implementar tales políticas y en pos de salvaguardar la información busca establecer modelos de seguridad de la información que permita controlar los riesgos informáticos existente en la organización (Departamento Juridico Torres and Torres, 2019).

La Empresa Torres y Torres comenzó a operar en 1986 como un operador logístico de comercio exterior el cual está formado por empresas que se encarga del transporte y distribución de mercaderías, la manipulación de cargas y la carga internacional.

La empresa Torres & Torres es un conjunto de empresas que ofrecen un servicio logístico integral de comercio exterior y transporte con presencia Internacional, se especializa en el Agenciamiento Aduanero, asesoría a Importadores y Exportadores con el objetivo de buscar alternativas logísticas.

Con el paso de los años ha mejorado las operaciones de importación y exportación gracias a los trabajadores, la infraestructura, uso de la tecnología y utilizando procesos en el sistema de gestión de calidad, pero los adelantos tecnológicos actuales han posibilitado escapes de información importante de sus instalaciones, elemento de alto riesgo para las actividades que desarrollan.

1.3. Formulación del problema

¿De qué manera incide el modelo de seguridad de la información para controlar los riesgos informáticos en el área administrativa en una empresa de operadores logísticos en la ciudad de Guayaquil?

1.4. Sistematización del problema

- ¿El modelo de seguridad de la información reducirá los riesgos informáticos en el área administrativa?

- ¿Existen auditorias para asegurar el cumplimiento con cualquier requerimiento legal o regulatorio?

- ¿Es viable la implementación de modelos de seguridad de la información para el control de los delitos informáticos?

- ¿Mediante que técnica se obtendrá información necesaria en el ámbito informático?

1.5. Objetivos de la investigación

1.5.1. Objetivo general

Proponer un modelo de sistema de información que se ajuste para el control de los riesgos informáticos en una empresa de operadores logísticos para el comercio exterior en la ciudad de Guayaquil.

1.5.2. Objetivos específicos

- Seleccionar un modelo que permita minimizar y realizar el control de los riesgos informáticos en la empresa.
- Identificar las vulnerabilidades en la seguridad de la información a través de un análisis situacional de una empresa de operadores logísticos.
- Analizar una valoración cualitativa y cuantitativa de los riesgos de seguridad a los que puede estar expuesta una empresa.

1.6. Justificación de la investigación

1.6.1. Conveniencia

La seguridad de la información permite proteger los datos que se encuentra en un sistema de computación, incluyendo el acceso a todos los recursos del sistema. Es de gran interés y de suma importancia que las empresas implemente modelos de seguridad de la información realizada en la presente investigación ya que invierten gran parte de su tiempo en el uso de la tecnología como herramienta de trabajo, y que servirá como aporte para controlar los riesgos informáticos permitiendo en el futuro mejorar la gestión de la seguridad, socializando la importancia y sensibilidad de la información y la seguridad.

1.6.2. Implicaciones practicas

Los modelos de seguridad de la información deben repasarse continuamente bajo un marco internacional para que se creen alternativas que puedan favorecer su mejor aplicabilidad y sean óptimas en el control de los delitos. Se debe propender porque estos modelos abarquen la mayor parte de manifestación de un hecho delictivo, y máxime si se tienen lineamientos establecidos por países más desarrollados en la lucha por frenar este fenómeno ofensivo.

1.6.3. Relevancia social

Como individuos, y desde cualquier campo de la ciencia, cada ciudadano está llamado a realizar aportes que contribuyan al fortalecimiento del sistema jurídico, y desde la Ingeniería de Sistemas, aún más, desde el punto de vista de los Especialistas en Seguridad Informática debe existir una preocupación más alta por formular alternativas de mejora a la normatividad.

Actualmente los riesgos informáticos han aumentado considerablemente al punto de ser necesario legislarlos para que tengan una justa penalización que pueda controlar su difusión y crecimiento. Se debe conocer el panorama de la legislación nacional e internacional en contra de los delitos informáticos para dimensionar la problemática que está afectando a las pymes en los diferentes países que se pueden encontrar en las mismas condiciones.

1.7. Marco de referencia de la investigación

1.7.1. Sistema de gestión de la seguridad de la información

Los Sistemas de Gestión de Seguridad de la información (SGSI) radica fundamentalmente en un grupo de normas, políticas y procedimientos que consienten en precisar, cimentar, desplegar y proteger la seguridad de los equipos y dispositivos electrónicos programables con cualquier sistema operativo, para garantizar la comprensión, la gestión y la disminución de

cualquier riesgos de seguridad de la información almacenada o gestionada por dicho dispositivo, que de forma documentada, metódica, organizada, verificada, repetible, eficaz y adaptada los controla y evita la contaminación de dicha información (Martelo et al, 2014).

SGSI establece mecanismo de gestión, para la confidencialidad integridad y disponibilidad de la información dentro de un conjunto de estándares seguros, teniendo como objetivo identificar cada una de las personas que apoyan los sistemas informáticos a través del proceso de gestión de riesgos asociados a la empresa. De esta manera se pueden establecer controles de seguridad de manera adecuada para cada componente y/o elemento que conforma los activos informáticos tangibles e intangibles (Guzmán A & Taborda C, 2015, pág. 49).

Un SGSI es un estándar para la seguridad de la información dentro de una organización específica el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la privacidad, entereza y disponibilidad de la información minimizando a la vez los riesgos de seguridad de la información (Domingo A, 2015, pág. 10).

1.7.2. Seguridad de la información

La seguridad de la información debe expresar el compromiso formal de la administración para la implementación y proteger y preservar la autenticidad y fiabilidad de la información y garantizar que las entidades puedan ser consideradas responsables (Altamirano J & Bayona S, 2017).

La seguridad de la información ha ido evolucionando con el paso del tiempo desde la seguridad física orientada a la protección de ordenadores y dispositivos de almacenamiento de información, pasando por la seguridad de sistemas y redes de tecnologías informáticas a concentrarse en la gestión de alto nivel mediante capacidades, instrucciones y inspecciones establecidos en las personas (Cárdenas et al, 2016).

Según (Solarte et al, 2015) afirma que la seguridad de la información no es sólo un tema particularmente técnico, si no que involucra procesos del negocio, actividades corporativo y gubernamentales que permitan asegurar una continua gestión de los riesgos y aseguramiento de los niveles de seguridad por la entidad.

1.7.3. Seguridad informática

La seguridad informática está relacionada con la información en sí misma, como activo estratégico de la organización, las TIC juega un rol importante al ser herramientas que permiten optimizar los procesos de gestión de la información y su función se desarrolla en todos los elementos técnicos que hacen parte de las TIC (Valencia F & Orozco M, 2017).

Los SGSI admite a las empresas preservar sus recursos financieros, informáticos, reputación, entorno legal y otros bienes tangibles e intangibles a través de la adopción de las medidas adecuadas gestionando eficazmente la seguridad de la información (Gil V & Gil J, 2017).

Según (Quiroz S & Macías D, 2017) expresa que la seguridad informática pretende identificar las amenazas y reducir los riesgos al detectar las vulnerabilidades nulificando o minimizando así el impacto nocivo sobre la organización.

El objetivo de la seguridad de la información es preservación de la confidencialidad, la integridad y la posibilidad de tener la disponibilidad de la información, al mismo tiempo también pueden estar comprometidos otras propiedades como la autenticidad, la responsabilidad, el no repudio y la fiabilidad (Sánchez J, 2017, pág. 6).

1.7.4. Aspectos de la seguridad informática

Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debe tener cuatro características (ver figura 1):

Integridad: Se refiere a la información no modificada o no afectada y protegida contra la alteración deliberada o accidental de un mensaje trasmitido y la integridad de los procesos de los datos intercambiados (Carpentier J, 2016, pág. 16).

Confidencialidad: Hace mención a todas las etapas del procesamiento de la información, está se encuentre protegida contra accesos no autorizados, las cuales pueden derivar en la alteración o robo de información privada (Baca G, 2016, pág. 12).

Disponibilidad: Debe estar utilizable cuando se exige. Se reseña a la continuación ejecutiva de la organización, la merma de disponibilidad puede involucrar, la pérdida de producción o de creencia de la entidad. El procedimiento contiene indagación o suministrar bienes que deben estar aprovechables a tiempo para compensar requisitos o evitar mermas significativas, como sistemas de seguridad y protección de la vida (Patiño et al, 2017).

No repudio: Consiste en realizar cualquier tipo de acciones informáticas es importante la contribución inmediata de ambas partes ya sea en sistemas o personas, ante una relación entre dos partes intentará evitar que cualquiera de ellas pueda negar que participara en esa relación (Chávez S, 2017, pág. 14).

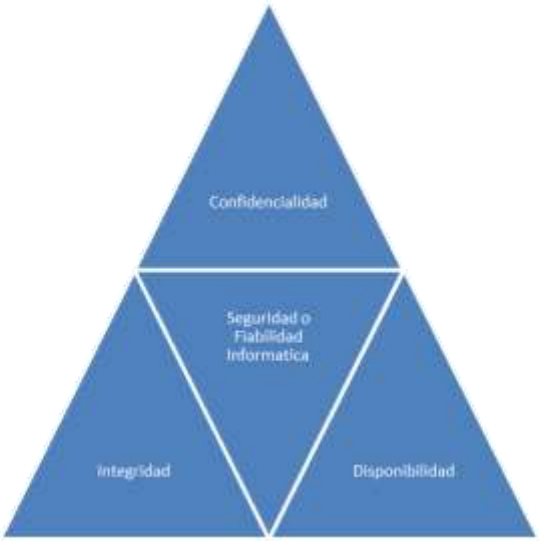

Figura 1. Pilares de la seguridad informática
Fuente: Elaboración propia

1.7.5. Elementos de la seguridad informática

Un activo informático es todo aquel dispositivo que prepara el proceso de la declaración, iniciando desde la indagación, su emisor y el medio por el cual se trasfiere, hasta su recibidor. Los activos son componentes que el sistema busca proteger, los cuales tienen valor para las organizaciones y por tanto como consecuencia de ello, requieren tomar un amparo conveniente para que sus servicios no sean perjudicados.

Son varios elementos que conforman lo que se denominan activos:

La información en la empresa es uno de los activos más importantes que posee y por ende se debería desarrollar mecanismos que les permitan asegurar la disponibilidad, integridad y confidencialidad en el manejo de los datos (Guaylupo J, 2017, pág. 14).

Los equipos que se implementan en la seguridad informática permiten almacenar, procesar la información sustancial en el desarrollo del negocio de una entidad, por tal motivo se deben aplicar controles que abarquen el mantenimiento preventivo y correctivo, para un rendimiento eficiente y que se pueda conservar la integridad del hardware y software (Torres C, 2020, pág. 41).

Otro elemento de la seguridad informática es el software y es un activo que contiene programas que se ejecutan dentro de un ordenador de cualquier tamaño para el procesamiento de datos de procesos, es decir, acceso, lectura, tránsito y acopio de la información, entre las que están las aplicaciones comerciales, programas institucionales, sistemas operativos y otros (Reyes D et al, 2016, pág. 15).

El hardware es un activo que representan toda la infraestructura tecnológica que ofrece soporte a la información durante su rutina, circulación y acumulación, los activos que conciernen a este grupo son aplicados a cualquier dispositivo en el cual se acumule, procese o comunique la información de la organización; computadoras, servidores, mainframes, medios de almacenamiento, equipos de conectividad (enrutadores, switches) y cualquier otro dispositivo de una red de ordenadores por donde circula la información (Cols C, 2015, pág. 4).

Dentro de los elementos de la seguridad informática la organización juega un rol importante en ella los gestores determinan detalladamente el procedimiento para alcanzar los objetivos, se componen la estructura física (ubicación física de los servidores y armarios donde están localizados los documentos) y organizativa (estructura departamental y funcional) de las empresas, es decir la estructura organizativa de la entidad (Silva M, 2019, pág. 39).

Los usuarios son un elemento débil de la seguridad informática por utilizar la estructura tecnológica y de comunicación de la compañía y que manipulan la información. El camino de la seguridad informática en los beneficiarios, está encaminado hacia la toma de conocimiento, de formación de la costumbre de la seguridad por parte de todos que pertenezcan a la empresa y en muchos casos el sistema y la información deben de protegerse del mismo usuario (Romero M et al, 2018, pág. 14).

1.7.6. Amenazas de la seguridad informática

Las amenazas a la seguridad informática resultan cualquier evento o situación que pueda afectar el desarrollo de las actividades dentro de la empresa

causando efectos negativos y no deseados de tipos económicos, financieros, sociales, activos, pérdida de la reputación, competitividad, pérdidas de oportunidades y/o confianza de sus clientes internos y externos (López R, 2017, pág. 6).

Las empresas hoy en día se enfrentan a numerosas amenazas contra la seguridad de la información, las misma que surgen al detectar la existencia de vulnerabilidades que pueden ser utilizadas para diversas situaciones sean perjudicar o robar información (Tigse J, 2020, pág. 10).

Los componentes más importantes a resguardar en cualquier SGSI son las plataformas de software, el equipamiento del hardware y los datos. Contra cualquiera de los elementos mencionados anteriormente (pero principalmente sobre los datos) se puede realizar una multitud de ataques o, dicho de otra forma, están expuestos a diferentes amenazas. Por lo general, la clasificación más básica de estas amenazas las fracciona en cuatro grandes grupos.

1.7.7. Tipos de amenazas

Las amenazas pueden catalogarse en dos tipos, el primero son deliberados que alcanza al hurto de información, el esparcimiento de códigos maliciosos y las tecnologías de ingeniería social, el segundo los no intencionales en donde se producen ejercicios o se dejan de hacer tareas que, si bien no buscan explotar una vulnerabilidad, en cambio sí ponen en riesgo los activos de la información y pueden producir daño (fenómenos naturales) (Rojas J, 2018, pág. 37).

La interrupción es una amenaza donde hace que un objeto del sistema se pierda, quede inutilizable o no disponible de los servicios informáticos y disminución de la productividad de la empresa (Pérez B, 2020, pág. 7).

La intercepción es una amenaza donde se lleva a cabo por personal no autorizado que consigue tener acceso a un determinado objeto del sistema, ya sea por un medio lógico o una red local permitiendo que el intruso genere copias

de la información de la empresa para ocupar dicha documentación con distintos fines (Cárdenas I, 2020, pág. 13).

Estudios realizados por (Estrada et al, 2019, pág. 123) indica que en el año 2017 los delitos informáticos más comunes realizados a empresa fueron por medio de malware, suplantación de identidad, phishing, vishing, amenazas a través de redes tales como smishing e ingeniería social.

Las amenazas de ciberataques que, en algunos casos por no tener medidas de prevención y control, las empresas se han visto abocadas mediante la modificación consiguiendo el acceso para modificar la información y así obtener un beneficio que pueda afectar seriamente los activos de información de la entidad (Caamaño E, 2020, pág. 64).

1.7.8. Estándares y normas para asegurar la información

Para la correcta administración de la seguridad de la información, se deben establecer y mantener acciones que busquen cumplir con los tres requerimientos de mayor importancia para la información, estos son [5]:

Confidencialidad: Busca prevenir el acceso no autorizado ya sea en forma intencional o no intencional a la información. La pérdida de la confidencialidad puede ocurrir de muchas maneras, como por ejemplo con la publicación intencional de información confidencial de la organización.

Integridad: Busca asegurar que no se ejecuten alteraciones por individuos no autorizadas a los datos o procesos, que no se ejecuten trasformaciones no autorizadas por personal acreditado a los datos o procesos y que los datos sean sólidos tanto interna como externamente.

Disponibilidad: Busca certificar acceso confiable y adecuado a la información de los datos o recursos para el personal adecuado.

Internacionalmente se han definido los estándares y las normas que apuntalan en igual medida el desempeño de las obligaciones oportunos expuestos anteriormente. Entre estas normas se destacan:

1.7.8.1. Norma ISO 2700

La Organización Internacional para la Normalización ISO/IEC 2700 permite proporcionar un marco de estandarización para la seguridad de la información para que sea aplicado en una organización o empresa y comprende un conjunto de normas sobre lo siguiente: Sistema de gestión de la seguridad de la información, valoración de riesgos y controles (Guevara R, 2017, pág. 8).

El estándar internacional de seguridad de la información de la norma ISO 2700 nos indica que ayuda a mantener la información resguardada de mejor manera utilizando buenas prácticas de seguridad mediante normas establecidas dentro de una organización (Chaso H, 2017, pág. 11).

1.7.8.2. Norma ISO 27001

Esta norma nos indica que especifica los requisitos de sistemas de gestión de la seguridad de la información utilizando técnicas que describen conceptos, modelos, y procesos para la perfecta ejecución de la gestión, además presenta la metodología de evaluación y tratamiento de los riesgos requeridos (Quevedo X & Vintimilla S, 2020, pág. 366).

1.7.8.3. Norma ISO 27002

La norma ISO 27002 permite implementar, mantener y mejorar la gestión de seguridad de la información dentro de una organización estándar, además sus controles reales atienden las necesidades específicas identificadas por medio de una evaluación de riesgos, proporcionando una guía para para el desarrollo de normas de seguridad y prácticas eficaces que ayuda a construir la confianza en las actividades interinstitucionales (Torres E, 2015, pág. 9).

1.7.8.4. Norma ISO 27003

Es una guía de implantación del sistema de administración y seguridad de la información que describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de ejecución, así como el proceso de obtención de aprobación por la dirección para efectuar un sistema de gestión de seguridad de la información (Garcés S, 2015, pág. 15).

1.8. Modelos de seguridad informática

1.8.1. Modelo COBIT

El modelo COBIT ha evolucionado a lo largo del tiempo y se ha extendido a muchas áreas (ver figura 2) nos permite tener un manejo adecuado a las buenas prácticas, ayuda a llevar un control adecuado de la información, se la aplica a los sistemas de información de toda la empresa, incluyendo computadoras y redes.

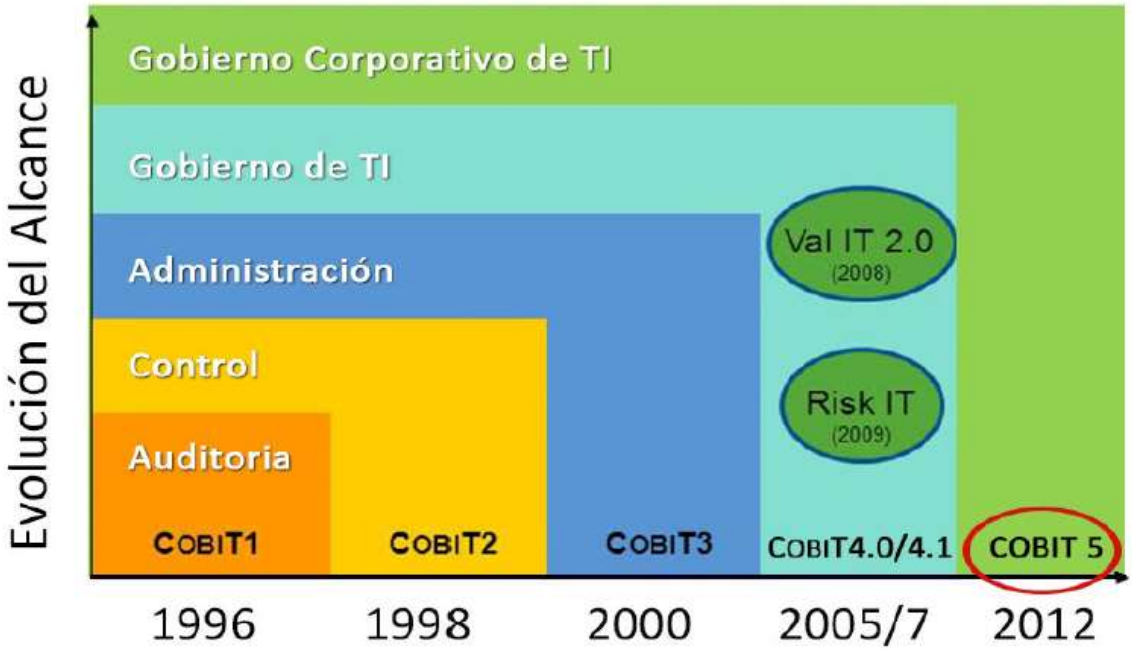

Figura 2. Evolución del modelo COBIT
Fuente: (Ruíz C, 2020)

Aplicar un marco de referencia único integrado en esta etapa se verifica si la empresa tienen estándares o normativas que ayuden a cumplir los objetivos de la seguridad informática, hacer posible un enfoque holístico con esto ayudara a que se consiga las metas de las empresas y por ultimo separa el gobierno de la gestión satisfaciendo a las partes interesadas basándose en las condiciones y necesidades mientras que la gestión trata de planificar y encargarse que se cumplan las actividades (Ruíz C, 2020, págs. 10 - 11).

Sus principios se basan en satisfacer las necesidades de las partes interesadas (ver figura 3), cubrir la empresa de extremo a extremo esto quiere decir cubre todas la funciones y procesos de toda la empresa para de cumplimiento de ellas.

Figura 3. Principios del modelo COBIT

Fuente: (Montaño V, 2011)

Según (Montaño V, 2011) indica que el modelo COBIT (Control Objectives for Information and related Technology u Objetivos de Control para la Información y Tecnologías Relacionadas), se utiliza para optimizar los controles de los datos mediante objetivos de control (ver figura 4), directrices de aseguramiento, mediciones de desempeño y resultados, factores críticos de éxito y modelos de madurez siendo un gran apoyo y generando satisfacción en las empresas al permitir cubrir las brecha entre los requisitos de control, los aspectos técnicos y riesgos de negocio.

Figura 4. Modelo COBIT

Fuente: (Molina E, 2016)

1.8.1.1. Características principales de COBIT

La evolución del modelo COBIT (ver figura 5) data del año 1988 y es orientado a las actividades comerciales cuyas particularidades son control en TI y se efectúa creando la información necesaria para dar sustento a los procesos del negocio hincado en una revisión crítica y analítica de las tareas y actividades en TI, están alineado con estándares de control y auditoria para el cumplimiento de las leyes, regulaciones y compromisos pactados con los cuales están

comprometida la empresa con sus responsabilidades alcanzando los objetivos de la entidad (Molina E, 2016, págs. 64 - 65).

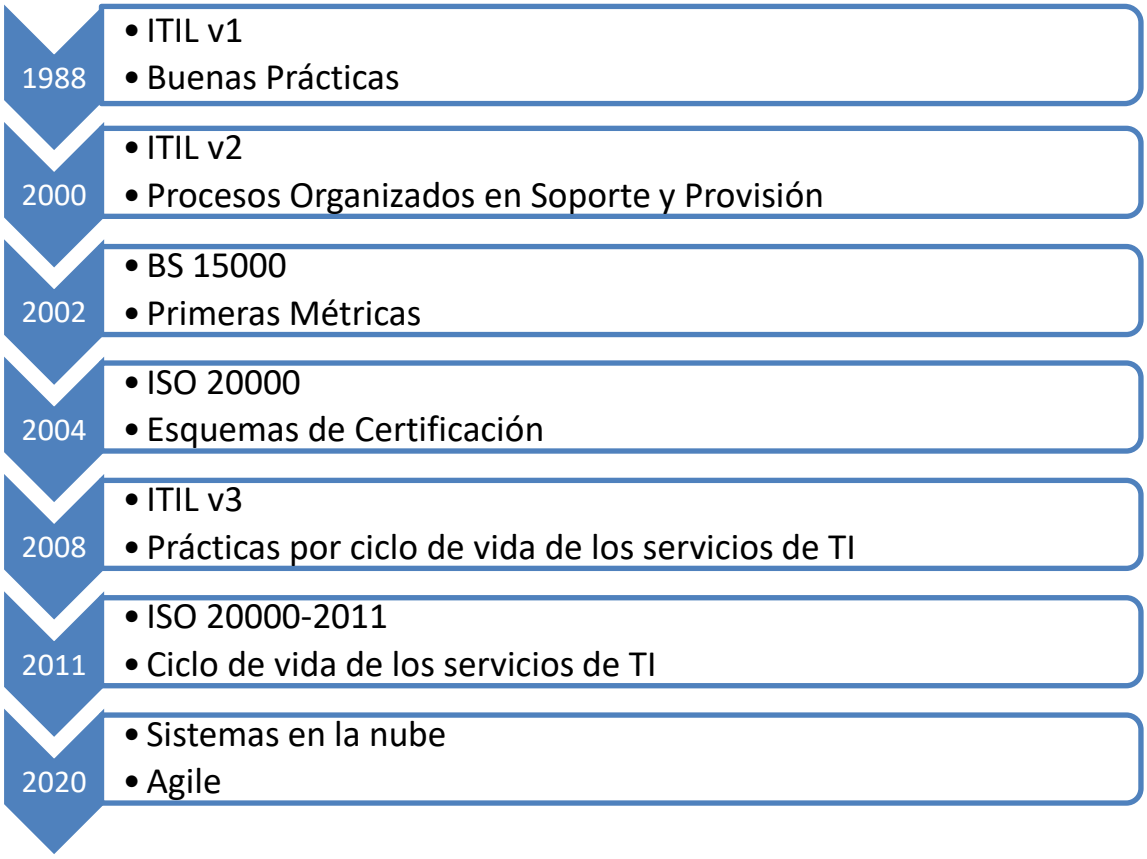

Figura 5. Evolución del modelo ITIL
Fuente: Elaboración propia según (Acosta C Malambo E & Segura D, 2019)

Según Acosta C Malambo E & Segura D (2019) COBIT fue creado para mejorar la seguridad, calidad, eficacia y la eficiencia en tecnología de la información cuyas características principales tales como el enfoque en los negocios, procesos de orientación, se basa en controles y es impulsado por métricas (pág. 16).

Las principales características de COBIT son: conceptualizar a TI como función inmersa en el negocio, estableciendo un vínculo entre TI y los requerimientos del negocios tales como organizar las actividades de TI, definir los objetivos de control gerenciales o de gestión, identificar los impulsores entre ellos tenemos: (Adecuada gestión de la Big Data, mejorar la relación con las

parte externas, orientar la innovación o adopción de tecnologías emergentes, tomar control sobre las soluciones generadas por los usuarios), establecer las necesidades del negocio: (Incrementar beneficios, mantener un riesgo aceptable, optimizar costos, cumplir con regulaciones y mantener información de alta calidad) (Suarez G, 2015, pág. 54).

1.8.2. Modelo ITIL

El modelo ITIL (Information Technology Infrastructure Library por sus siglas en idioma inglés) es una norma de mejores prácticas para la gerencia de productos de Tecnología de Información, desarrollada a finales del año 1980 por organizaciones públicas y privadas con la finalidad de reflexionar las mejores habilidades a nivel internacional (ver figura 6). Este método fue manejado primeramente como una guía para el gobierno de británico, pero es adaptable a cualquier tipo de organización (García J & Gavilanes M, 2015, pág. 18).

Figura 6. Modelo ITIL
Fuente: (Alarcon J, 2016)

El modelo ITIL responde a un enfoque empresarial para grandes corporaciones que utilizan ampliamente en sus operaciones, utilizando buenas prácticas para la gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en la seguridad de la información (Alarcon J, 2016, págs. 24 - 25).

Según estudios realizados por cita que el modelo ITIL disponen de estándares de calidad específicos para la gestión de servicios de tecnologías de información, logra beneficios con el transcurso del tiempo mediante la planeación y compromisos para resolver problemas y hace más eficaces el control de la seguridad (Ramos M & Solares P, 2015, págs. 69 - 70).

1.8.2.1. Características principales ITIL

Uno de las características principales de ITIL es el incidente donde se asegura la continuidad, disponibilidad y calidad del servicio al usuario, donde se ve afectado mediante interrupciones de las actividades de los usuarios en la organización en donde sus procesos son detenidos inesperados causando retraso en sus labores y las operaciones del negocio y amenazar la seguridad de la información (Baygorrea D, 2017, pág. 35).

Las características principales de ITIL son: ser desarrollado sin derechos de autor, de dominio público, compendio de mejores prácticas y regirse por estándares internacionales, permite que la empresa tenga ventaja competitiva, innovadora, perfeccionista y rediseñar procesos, facilita procesos administrativos, mejora la calidad y funcionalidad de sus productos (Catota X, 2015, pág. 7).

1.8.3. Modelo COSO

Este modelo COSO (The Committee of Sponsoring Organizations of the Treadway Commission's Internal Control-Integrated Framework, por sus siglas en idioma inglés) está dirigida a la vigilancia de la gestión financiera y contable de las empresas. Su evolución comienza en 1985 (ver figura 7).

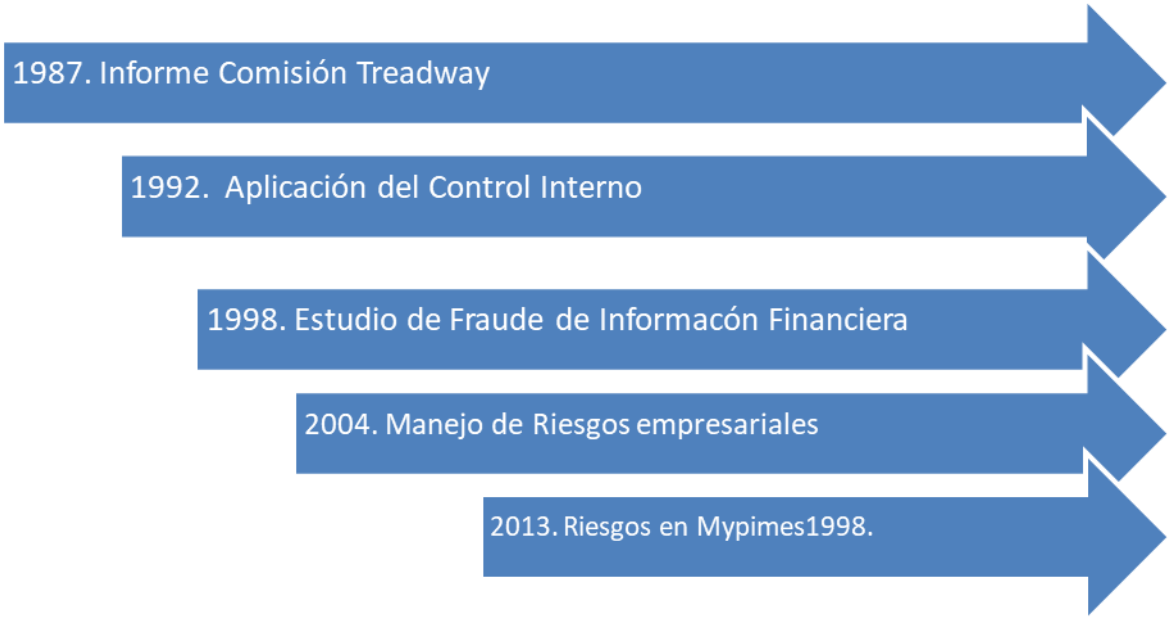

Figura 7. Evolución del modelo COSO
Fuente: Elaboración propia tomado de (Hérnandez D, 2011)

Sin embargo, dada la gran similitud y cercanía que hay entre esta área y los procedimientos de información computarizados, es que resulta importante concebir el alcance y uso de esta norma. Junto a esto son muchas otras las normas que están directa o indirectamente relacionadas con ésta como por ejemplo COBIT (Hérnandez D, 2011, pág. 59).

Coso implementa un ambiente de control asegura transparencia en la información, competitividad en el mercado dado a las eficiencias operativas que conlleva a alinear los sistemas operativos describiendo 26 principios asociados con los componentes clave de control interno tales como evaluación de riesgo, actividad de control, comunicación e información y monitoreo, permitiendo prevenir riesgos reputaciones, perdidas inesperadas o cuestionamientos debido a la ausencia de controles por parte de sus directivos (Rodríguez D & Arevalo J, 2016, pág. 5).

1.8.3.1. Principios y características principales COSO

Los componentes y principios del modelo se entrelazan con sus características principales son (ver figura 8):

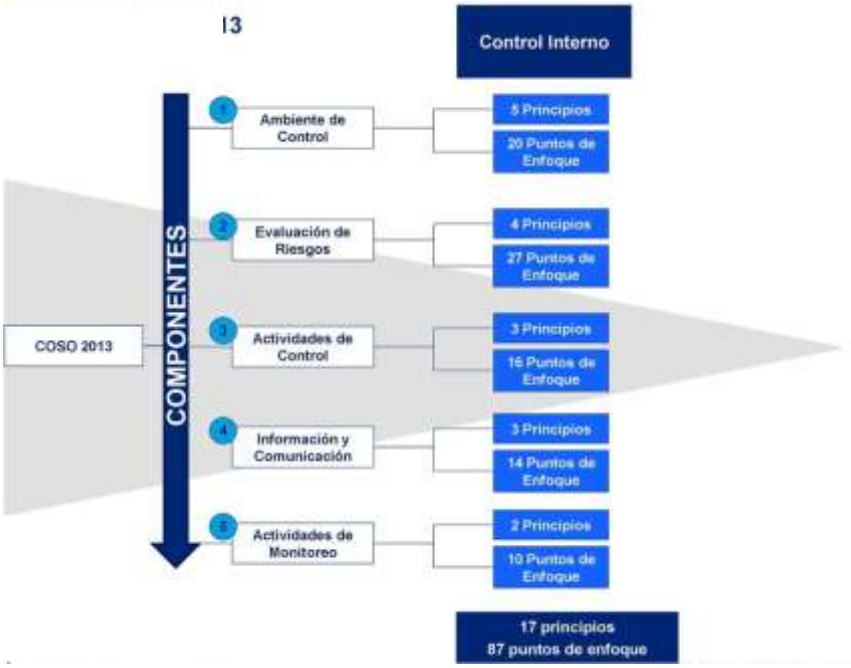

Figura 8. Componentes y principios del modelo COSO
Fuente: (Franco K et al, 2017)

Las características son:

- Forma parte del sistema contable, financiero, de planeación, operaciones y de información
- El representante legal es el responsable de que se establezca, mantenga y perfecciones de acuerdo a la naturaleza, estructura y misión organizacional
- En cada departamento su encargado es responsable del sistema de control interno antes su jefe inmediato
- La auditoría interna se encargará de hacer evaluación independiente del sistema y propondrá recomendaciones al gerente para mejorarlo

- Toda la información se debe registrar en forma exacta, veraz y oportuna para preparar en igual forma informes para asegurar la confiabilidad de la operación, definir y aplicar medidas para prevenir riesgos (Franco K et al, 2017, pág. 16).

1.8.4.2. Modelo COSO

El modelo COSO (ver figura 9) se creó con la finalidad de ayudar a las empresas a alcanzar sus objetivos previamente establecidos desde su constitución, este modelo es una serie de pasos o procedimientos que se penetran en las actividades de la empresa con el fin de minorar los riesgos y cumplir los objetivos (Zamora L & Tamez X, 2019, pág. 354).

Figura 9. Modelo COSO
Fuente: (Zamora L & Tamez X, 2019)

Las principales características del modelo COSO, se basa en 5 componentes (monitoreo, ambiente de control, evaluación de riesgos, actividades de control e información y comunicación) y se encarga de evaluar y determinar riesgos dentro de la organización (Velez S, 2017, pág. 7).

Al aplicar esta norma el proceso realizado por la gerencia, el consejo de administración, o la dirección y el resto del personal de una organización se busca como objetivo facilitar un nivel de seguridad prudente debido al control interno en cada uno de sus procesos cuyo objetivo es el cumplimiento de las leyes, reglamentos y políticas dentro de la infraestructura de la entidad (Tapia G, 2019, pág. 24).

1.8.5. Modelo LEY SOX

Este modelo evoluciona del informe Cadbury a la Ley Sarbanes-Oxley (SOX), de EE.UU. (ver figura 10).

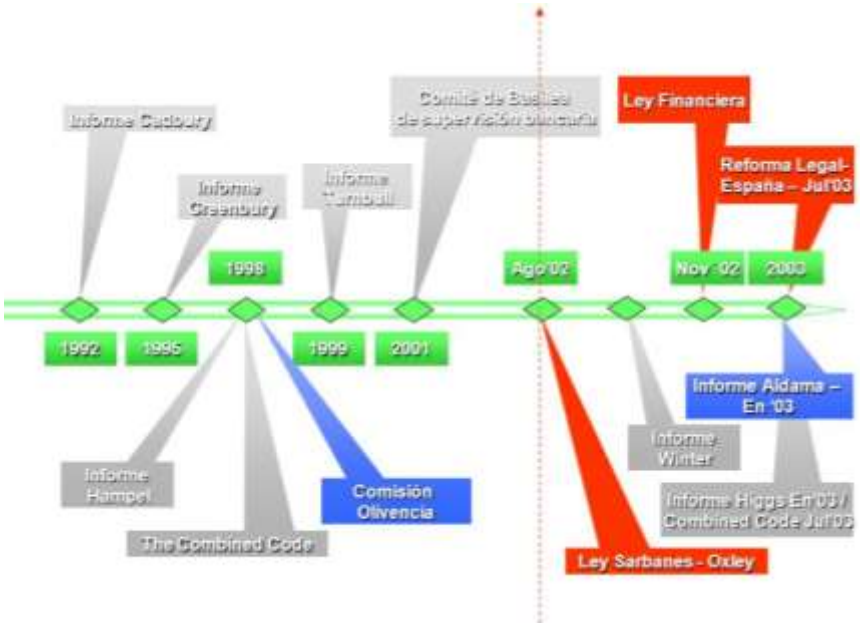

Figura 10. Evolución del modelo LEY SOX
Fuente: (Guerra M, 2015)

Este modelo obliga a las organizaciones públicas nacionales de dicho país, o foráneas suscritas en la Securities and Exchange Comission a acarrear un control y acopio informático preciso de su diligencia. La ley nace producto los problemas bancarios ocurridos en compañías norteamericanas como Enron y Worldcom, durante el año 2002, en los cuales se demostró que la información financiera fue adulterada. Esta ha tenido un alto impacto a nivel mundial en

empresas que transan sus valores en la bolsa de EE. UU (Guerra M, 2015, pág. 25).

1.8.5.2. Principio y características principales del modelo LEY SOX

Loa principios a los que se atiene este modelo son cuatro (ver figura 11):

- Gestión y control interno del riesgo.
- Información de calidad y transparente.
- Responsabilidad de la alta gerencia empresarial.
- Comportamiento ético de los miembros de la organización.

Figura 11. Principios del modelo LEY SOX
Fuente: (Guevara M, 2019)

1.8.5.3. Modelo LEY SOX

En las características principales de este modelo (ver figura 12) se detallan la comprensibilidad de la información donde esta debe ser clara y comprensible para todo tipo de usuario que deseen los datos, la sistematización de un sistema informático útil para obtener los datos ordenados y clasificado, confiabilidad para que la información que se registre no contenga errores y se debe tener un control constante (Guevara M, 2019, págs. 30 - 31).

Figura 12. Modelo LEY SOX
Fuente: (Castillo L, 2018)

La Ley de Sox tiene efectividad en el control interno de la empresa para esto se debe cumplir las características principales tales como controles para evitar o detectar errores y fraudes, segregación de funciones, tener una cultura corporativa, integridad, valores éticos y desarrollar los controles del sistema, accesos lógicos (Castillo L, 2018, pág. 11).

1.8.6. Modelo COCO

El modelo COCO es sencillo y comprensible, evoluciona a partir del año 1995, desarrollado en Canadá ante las dificultades que enfrentaron inicialmente algunas organizaciones en la aplicación COSO.

1.8.6.2. Modelo COCO

Las características principales del modelo COCO (ver figura 13) establece 4 criterios para entender el control de este modelo donde se destaca el propósito,

capacidad, compromiso, monitoreo y aprendizaje donde la información debe de ser confiable tanto interno como externa y el cumplimiento de las leyes, reglamentos y políticas (Álvarez M, 2019, pág. 29).

Figura 13. Modelo COCO
Fuente: Elaboración propia tomado de Álvarez (2019)

Este modelo asegura el cumplimiento de los objetivos de la organización donde el propósito, objetivos deben comunicarse, identificando los riesgo que puedan afectar el logro de las metas, deben procurarse la comunicación y práctica de las políticas ideadas para apoyar la consecución de los objetivos de la empresa, el compromiso mediante valores éticos establecidos y comunicados a todos los miembros de la empresa, la evaluación se debe supervisar el ambiente interno y externo para la identificación de la información, el sistema de información debe evaluarse a medida que cambien los objetivos y precisen la deficiencia de información (Quinaluisa et al, 2018, pág. 278).

1.8.6.3. Características principales COCO

El modelo COCO sus principales características indica que se debe estar escrito sus manuales de forma sencilla, preciso y lógico que permitan garantizar

su aplicabilidad en las tareas y funciones del trabajador, en cuanto al propósito se debe identificar los riesgos internos y externos que pudieran perturbar el provecho de los objetivos, el compromiso y se deben definir y anunciar los valores morales y éticos de la empresa, además sus políticas y habilidades deben ser consistentes con los objetivos de la organización. Así mismo la idoneidad del personal que debe poseer las sapiencias, destrezas y instrumentos que sean necesarias para las acciones de control, las que deben ser delineadas como parte general de la organización (Páramo B, 2013, pág. 17).

1.8.7. Modelo de seguridad CNSS

Este modelo conocido como el McCumber Cube sirve como el estándar para la comprensión de muchos aspectos del estándar nacional de formación de sistemas de información de seguridad, la forma de asegurar la información es mediante tres dimensiones formando un cubo de 3 x 3 x3 con 27 celdas con el objetivo de controlar o salvaguardar la información mediante el uso de tecnologías para proteger el mismo durante su almacenamiento (Espinoza D, 2015, pág. 23).

1.8.7.2. Modelo PHVA aplicado a los procesos de SGSI

El modelo PHVA (ver figura 14) que significa Planificar, Hacer, Verificar, Actuar, estable los requisitos para la elaboración de políticas adecuadas que garanticen la seguridad de la información mediante un plan de buenas prácticas en el uso de los sistemas de información que esta dispuestos para el desarrollo de sus labore para minimizar el riesgo de pérdida, daño o alteración de la información, también tiene la finalidad de actuar en el momento de una violación de seguridad ya sea de una fuente interna o externa (Palacios A, 2015, pág. 18).

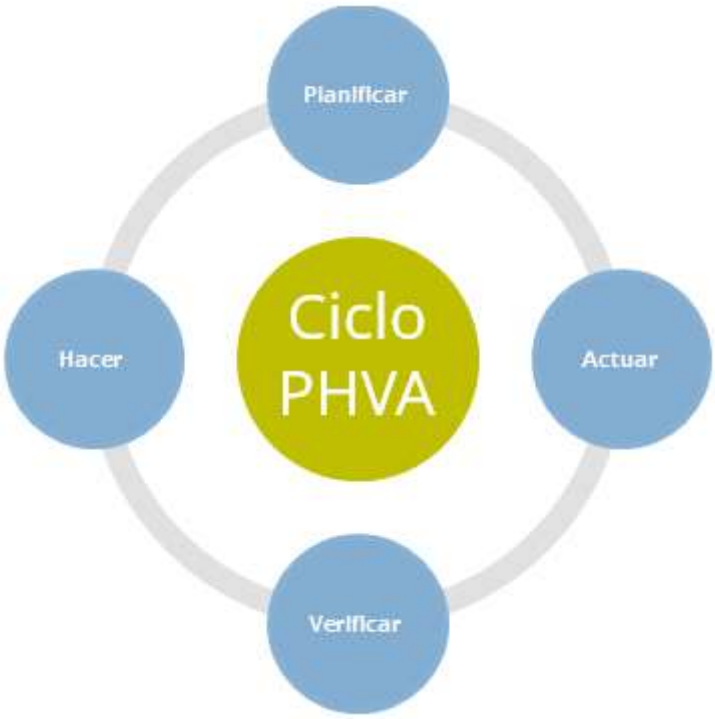

Figura 14. Modelo PHVA
Fuente: Elaboración propia tomado de Palacios (2015)

1.9. Riesgos de seguridad de la información

La valoración y priorización a cada uno de los activos en cuanto a los riesgos de la seguridad de la información, depende la importancia que se dé a la protección de la información y a los activos en la organización, por tanto, se debe establecer estándares para poder evitar la suspensión en las actividades y cumplimiento de sus objetivos (Bedoya M, 2020, pág. 14).

Se debe realizar un análisis de riesgos de seguridad de la información para determinar cuánto es el nivel de seguridad aceptable, de tal manera este análisis tiene un enfoque donde debe ser consistente e integrado y definido en base a la disminución de las ventajas competitivas, daños en la reputación institucional o perdida y robo de los activos de información de los procesos administrativos vinculados a las funciones sustantivas (Heredia H, 2019, pág. 147).

1.9.4. Valoración de riesgos de seguridad de la información

Es fundamenta investigar y analizar los diferentes riesgos que pueden suscitarse y que afecten los procesos que se llevan a cabo en las empresas y aún más si sus procesos cuentan con información relevantes, por tal motivo se debe evaluar si los riesgos son aceptable o infringe las normas institucionales, para lo cual se debe evaluar con un método cualitativo en la que se detallan los activos de la institución, se identifican las amenazas relacionado con cada uno de ellos y las posibilidad de que dichas amenazas se cumplan (Zapata K, 2020, pág. 85).

Una de las medidas importante de una empresa es realizar valoraciones cualitativa y cuantitativa de los riesgos de seguridad de la información demostrando que estas compañías adopten un criterio equilibrado mostrando menos incidentes en este ámbito, si no que obtienen mayor rentabilidad del negocio reduciendo de forma potencial los riesgos (Campos C & León D, 2020, pág. 16).

La valoración de riesgo envuelve la medición del potencial de las pérdidas y la probabilidad de la pérdida categorizando el orden de prioridades, toda organización debe estar a la vanguardia de los procesos de cambio donde se dispone de información continua, confiable y en tiempo (Guzmán G, 2015, págs. 28 - 29).

Capitulo II. Marco metodológico

2.1. Tipo de estudio, alcance y enfoque de la investigación

2.1.1. Tipo de estudio

En esta investigación se han realizado tres tipos de estudios. El primero es el estudio de tipo Exploratorio, donde se profundiza sobre el estado del arte de la temática que se aborda. En tal sentido se consultaron 66 fuentes bibliográficas de mediano y alto impacto, de las cuales el 57,7% corresponden a los últimos cinco años, el 39,3% al periodo del 2011 al 2016 y el 3% restante antes del 2010.

De igual manera se realizó un estudio descriptivo donde se recogió información para conocer la situación real de la empresa sobre los modelos de seguridad de la información, con el objetivo de mejorar la toma de decisiones y evitar los riesgos informáticos.

Por último, se realizó un estudio explicativo con el objetivo de explicar las causas y demostrar mediante las mediciones de las variables las relaciones entre ellas.

2.1.2. Alcance de la investigación

Esta investigación se delimito y centro en la problemática de los riesgos informáticos en el área administrativa de la empresa de operadores logísticos para el comercio exterior en la ciudad de Guayaquil.

2.1.3. Enfoque de la investigación

El enfoque en la presente investigación es de tipo mixto, o sea cualitativo y cuantitativo, se emplean las técnicas de ambos enfoques para medir la relación entre las variables independientes con la variable dependiente. Se realizó la recopilación de datos mediante entrevista y encuesta a los empleados del área del personal administrativo y del personal de sistemas. La composición de ambos (encuesta y entrevista) fue valorado por el método de juicios de expertos (se

valoró la Objetividad y el Contenido) medidas ambas por el Coeficiente de Validez de Coincidencia (CVC) desarrollado por Hernández-Nieto (2002). Este método se resume en la siguiente formula:

$$CVC_t = \sum \left[\left[\frac{\sum S_{xi}/J}{VM_j} \right] - P_{ei} \right] (1/N)$$

$$P_{ei} = \left(\frac{1}{J}\right)^J$$

Donde:

N: Número total de ítems del instrumento de recolección de datos

Sxi: Sumatoria de los puntajes asignados por cada juez *J* a cada uno de los ítems *i*

Pei: Probabilidad del error por cada ítem (probabilidad de concordancia aleatoria entre jueces)

J: Numero de jueces o expertos

El resultado obtenido se debe comparar con el siguiente baremo (ver tabla 1):

Tabla 1*. Baremo para el CVC*

Baremo de CVC	
Menos de 0,4	Validez y Concordancia inaceptable
Igual o mayor a 0,61 y menor o igual a 0,7	Validez y Concordancia Deficiente
Igual o mayor a 0,71 y menor o igual a 0,8	Validez y Concordancia Aceptable
Igual o mayor a 0,81 y menor o igual a 0,9	Validez y Concordancia Buena
Igual o mayor a 0,91 y hasta 1	Validez y Concordancia Excelente

Fuente: Elaboración propia tomado de (Hernández-Nieto, 2002)

La ficha de evaluación para recoger los datos y determinar el modelo se recoge en el anexo 1.

Una vez desarrollados ambos instrumentos se midió la Fiabilidad por el estadístico Alfa de Cronbach. El estadístico Alfa de Cronbach se calcula por la siguiente formula:

$$\alpha = \frac{k}{k-1}\left[1 - \frac{\sum Vi}{Vt}\right]$$

Donde:

k: Número de preguntas (ítems)

Vi: Varianza de cada individuo

Vt: Varianza total

Para su valoración se emplea la siguiente Escala de Consistencia y Confiabilidad

Tabla 2. *Baremo de medición del Alfa de Cronbach*

Baremo de Alfa de Cronbach	
Muy Baja	de 0 a 0.2
Baja	de 0.21 a 0.4
Moderada	de 0.41 a 0.6
Buena	de 0.61 a 0.8
Alta	de 0.81 a 1

Fuente: Elaboración propia tomado de (Landis & Koch, 1977)

Con el instrumento de la entrevista se valora el riesgo de seguridad informática y con la encuesta se demuestran las vulnerabilidades del sistema.

2.2. Métodos de investigación

Método deductivo: Mediante la problemática de la investigación del control de los riesgos informáticos a partir de la aplicación de un modelo teórico para identificar si existen condiciones que determinen el uso de un modelo de un sistema de información mediante un análisis cuantitativa y cualitativa, con esto se determinó la solución del problema.

Método histórico: La presente investigación utilizó una sucesión de hechos y fenómenos que se presentaron en la empresa referente a la seguridad y riesgos informáticos basados en la entrevista al personal administrativo y al personal de sistemas.

Método analítico: Con este método fue de vital importancia descomponer el objeto de estudio en cada una de sus partes para medir sus variables en forma individual.

2.3. Unidad de análisis, población y muestra

En la presente investigación se realizó un análisis de datos a 50 empleados (30 son del personal administrativo, 15 del personal de sistemas y 5 del área gerencial) del Grupo Torres & Torres en la ciudad de Guayaquil, lo que nos permitió analizar un modelo de sistema de información que se ajuste para el control de los riesgos informáticos al debido mantenimiento de los ordenadores, de los servidores, de la correcta capacitación del personal en los ámbitos de seguridad informática; así como un buen seguimiento, control y la actualización de los sistemas de seguridad. En la table 3 se expone el cuadro de operacionalización de variables.

2.4. Variables de la investigación, operacionalización

2.4.1. Cuadro de operacionalización de variables

Tabla 3*. Cuadro de Operacionalización de las variables*

Variable Dependiente	Concepto	Dimensión	Indicador 1	Indicador 2	Indicador 3	Indicador 4	Indicador 5	Indicador 6
Control de los riesgos informáticos en el área administrativa	Es un proceso interactivo e iterativo basado en el conocimiento, evaluación y manejo de los riesgos y sus impactos, con el propósito de mejorar la toma de decisiones organizacionales.	Garantía	Control de la información	Desempeño laboral	Normas ISO			
		Gobernanza	Controles de seguridad	Vulneraciones del sistema	Control de daños			
		Identidad y control de acceso	Control de acceso	Mecanismos de autenticidad	Ataques detectados			
		Gestión de riesgos	Estrategias de mitigación	Monitoreo de la gestión	Efectividad de la gestión			
		Servicio de protección	Numero de servicios	Efectividad de los servicios				
Variables Independientes	**Concepto**	**Dimensión**	**Indicador 1**	**Indicador 2**	**Indicador 3**	**Indicador 4**	**Indicador 5**	**Indicador 6**
Identificación de Activos	Es un código para ordenar y localizar los activos de información dentro de una organización	Riesgo efectivo	Tipo de conexión a la internet	Uso de la internet	Actualización de Softwares	Hardware	Tratamiento le da a la información	
Vulnerabilidades	Denota carencia o ausencia de elementos esenciales para la subsistencia y el desarrollo personal, e insuficiencia de las herramientas necesarias para abandonar situaciones en desventaja, estructurales o coyunturales.	Ataques externos	Detección de actividad anormal	Información de las anormalidades	Antivirus y protecciones	Tipo de amenazas detectadas	Vulnerabilidades detectadas	Riesgos evidenciado
		Errores humanos	Uso de claves de accesos	Uso de claves seguras	Acceso de documentos			
		Desastres naturales	Plan de salva de la información	Sistemas de respaldo de la información	Plan seguro de envió de la información			

Fuente: Elaboración propia

2.4.2. Tipos de Variables

Variable dependiente:

Control de riesgo informático: En la presente investigación esta variable permite determinar el nivel de riesgo informático al que está expuesto la empresa mediante el uso de los modelos de seguridad.

Dimensiones de la VD:

Garantía: Variable para evaluar la seguridad de información fundamentada en la confidencialidad e integridad mediante la validación de una autenticación antes de permitir un acceso.

Gobernanza: Variable para valorar el control de riesgos mediante el modelo de sistema de información aplicada por medio de las Normas ISO.

Identidad y control de acceso: Variable para la identificación de los modelos de información mediante la autenticación, la autorización y las funciones de control de acceso.

Gestión de riesgos: Variable para medir la valoración cuantitativa y cualitativa de los riesgos en la empresa, los procedimientos para el monitoreo continuo del estado de la seguridad de la información sistema mediante los riesgos, las vulnerabilidades y amenazas informáticas.

Servicio: Variable que se utiliza para conocer los servicios que presta los modelos de seguridad en la empresa.

Variables Independientes:

Identificación de Activos: Es la codificación establecida por las organizaciones para localizar y conceptualizar el medio o dispositivo mediante el cual se pueda almacenar, recibir, trasmitir y generar información.

Vulnerabilidades: Es la carencia manifiesta de propiedades que permitan enfrentar determinada situación

Ambas variables cuentan con sus respectivas dimensiones, para la variable independiente de Identificación de Activos se halla el Riesgo efectivo y las dimensiones de la variable Vulnerabilidades se encuentran Ataques Externos, Errores Humanos y Desastres Naturales.

Todas las variables tienen sus diferentes indicadores, de los cuales salen las preguntas respectivas para el instrumento de investigación creado (encuesta y entrevistas)

2.5. Fuentes, técnicas e instrumentos para la recolección de información

Para cumplimentar los objetivos de trabajo de la presente investigación se desarrollaron dos instrumentos de medición, una encuesta y una entrevista.

2.5.1. Encuesta

Mediante esta herramienta se buscó detectar las vulnerabilidades del sistema informático de la empresa de operadores de comercio exterior. Es una encuesta estructurada del tipo test, con casillas de respuesta relacionadas a variables de Likert de cinco apreciaciones, donde 1 es la menor apreciación y 5 la máxima apreciación. Este instrumento cuenta de cinco dimensiones y un total de 15 preguntas. Su estructura fue validad por el método de juicio de expertos y medida su fiabilidad por Alfa de Cronbach. La estructura de la encuesta misma se puede ver en el anexo 2. El formulario fue expuesto en línea por medio de la herramienta de Google Formulario y se accede mediante el siguiente enlace:

https://docs.google.com/forms/d/1xCH2QU3awZxGG33o_CfswovkpLuKpoLZt1RxBIcqEmc/edit?usp=sharing

Dimensiones y las preguntas extraídas de cada indicador son las siguientes:

Dimensión Garantía

- ¿Está de acuerdo con los controles de información?
- ¿Cree que los controles de seguridad pueden garantizar la seguridad informática?
- ¿Cree que un sistema general de calidad en la información podría garantizar la seguridad informática?

Dimensión Gobernanza

- ¿Cree Ud. que los controles de información mejoran su desempeño laboral?
- ¿Cree Ud. que las vulnerabilidades al sistema han disminuido una vez aplicado el modelo de seguridad?

- ¿Se puede valorar el control de daños con el sistema de seguridad establecido?

Dimensión Identidad y Control de acceso

- ¿Cómo valoraría el control de acceso a la información dentro de la empresa Torres y Torres?
- ¿Cree Ud. necesario aplicar mecanismos de autenticidad en los medios informáticos?
- ¿Valora Ud. que las amenazas detectadas han sido neutralizadas?

Dimensión Gestión de riesgos

- ¿Está preparada la empresa para la mitigación de riesgos?

- ¿Se monitorea adecuadamente el estado de seguridad de la información en la empresa?
- ¿Valore Ud. la efectividad de la gestión del riesgo por el modelo usado?

Dimensión Servicio

- ¿Cómo cataloga los servicios que presta el modelo de seguridad en la empresa?
- ¿Existe efectividad de los servicios y disminución de riesgos con el sistema instalado?

Como se puede valorar la encuesta es el instrumento para la medición de la Variable Dependiente de esta investigación.

2.5.2. Entrevistas

Por otra parte, la entrevista se destina para medir las dos variables independientes, específicamente va a ser empleada para valorar los riesgos de seguridad a los que puede estar expuesta la empresa en su dinámica diaria y las vulnerabilidades de la misma. Es una entrevista estructurada con preguntas cerradas y dirigida con los mismos puntos para todos los integrantes de la organización.

Se les entrevista con un test de 17 puntos de las cuales seis son politómicas nominales y 11 abiertas con escala de asignación o variables de Likert de cinco niveles. Este instrumento también fue validado por los cinco expertos anteriores y medida su fiabilidad por Alfa de Cronbach.

La estructura de la validación de la Objetividad y del Contenido por el método de Juicio de expertos de la encuesta y de la entrevista se puede ver en los anexos 3 y 4

Las preguntas presentes para la realización de la entrevista son:

1. ¿Qué tipo de conexión utiliza Ud. en la empresa Torres & Torres para acceder al servicio de internet?
2. ¿Para qué utiliza el internet en sus actividades en la empresa?
3. ¿Están actualizados sus Softwares de uso diario en su PC?
4. ¿Es adecuado el Hardware de su PC para la actividad que realiza?
5. ¿Qué tratamiento le da a la información digital que elabora?
6. ¿Ha detectado Ud. alguna actividad anormal en sus sistemas en el trabajo diario?

7. ¿Informa Ud. de las anormalidades que encuentra en el uso diario de su PC?
8. ¿Están actualizados los antivirus y protecciones de su PC?

9. ¿Qué tipo de amenazas se detectaron en la empresa Torres & Torres?

10. ¿Qué tipo de vulnerabilidades fueron detectadas en la empresa Torres & Torres?
11. ¿Qué tipo de Riesgos se evidenciaron con el modelo instalado en la empresa?
12. ¿Usa Ud. claves en sus accesos a los softwares de uso común?

13. ¿Su máquina o PC está protegida por claves seguras?

14. ¿Accede a sus documentos desde redes públicas sin protección adecuada?
15. ¿Existe plan de salva de la información en lugares seguros para los activos informáticos de su empresa?
16. ¿Cuentan con sistemas de respaldo de la información en servidores seguros y protegidos?
17. ¿En las situaciones actuales de virtualidad ante COVID-19, tienen plan seguro de envió de la información?

2.6. Tratamiento de la información

En la presente investigación el tratamiento de la información se la realizó a través del programa de Excel del paquete informático de Office.

Capitulo III. Análisis, presentación de resultados y diagnostico

3.1. Seleccionar Modelo de Control de los riesgos informáticos.

Para dar cumplimiento al primer objetivo específico se entrega a los integrantes del área de sistemas la documentación detallada de los modelos de Sistemas de Calidad de Seguridad Informática COBIT, ITIL, COSO, LEY SOX, COCO y CNSS.

Esta información establece los métodos y procedimientos de cada uno de ellos y los alcances de su actuación. Pasado una semana se realiza el encuentro para solicitarles completen la información y evalúen los modelos estudiados a su criterio como expertos en la seguridad informática. Este modelo se aprecia en el anexo 1.

Los resultados de la valoración de los expertos por cada modelo se muestran en las tablas 4, 5, 6, 7, 8 y 9. Nótese que cada uno de ellos fueron valorados en dos dimensiones generales, una la calidad de la información y la otra la satisfacción del usuario. Pero cada una de ellas se desagrego en cuatro indicadores la primera (Completamiento o completitud, exactitud, fiabilidad y consistencia) y la segunda valorada en Accesibilidad, velocidad, precisión, visualización y personalización.

Tabla 4*. Coeficiente de coincidencia del modelo COBIT*

Dimensión	Indicador	Especialista 1	Especialista 2	Especialista 3	Especialista 4	Especialista 5	Especialista 6	Especialista 7	Especialista 8	Especialista 9	Especialista 10	Especialista 11	Especialista 12	Especialista 13	Especialista 14	Especialista 15	Especialista 16	Especialista 17	Especialista 18	Especialista 19	Especialista 20	Sxi	Mxi	CVCi	Pei	CVic
Calidad de la información	Completitud	4	4	5	5	5	4	5	4	5	4	5	5	5	4	4	4	5	5	4	5	91	18,2	0,91	0,00000	0,910
	Exactitud	5	5	5	5	4	5	5	5	4	4	4	4	4	5	4	4	5	4	5	5	91	18,2	0,91	0,00000	0,910
	Fiabilidad	4	4	5	4	5	5	5	5	5	4	4	4	5	5	4	5	4	5	5	4	91	18,2	0,91	0,00000	0,910
	Consistencia	5	5	5	4	5	5	5	5	5	5	4	4	4	4	5	5	5	4	5	5	94	18,8	0,94	0,00000	0,940
Satisfacción del usuario	Accesibilidad	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	4	5	4	97	19,4	0,97	0,00000	0,970
	Velocidad	4	4	5	4	5	5	5	5	4	5	4	4	5	4	4	4	5	4	4	4	88	17,6	0,88	0,00000	0,880
	Precisión	5	4	4	4	4	4	4	5	4	5	5	4	5	4	5	5	5	4	5	5	90	18	0,9	0,00000	0,900
	Visualización	5	5	4	4	5	5	4	5	5	5	5	5	5	4	4	4	5	5	4	5	93	18,6	0,93	0,00000	0,930
	Personalización	4	5	5	4	4	4	5	4	4	4	5	5	5	5	5	4	5	5	4	5	91	18,2	0,91	0,00000	0,910
																									CVC Modelo COBIT	**0,918**

Fuente: Elaboración propia

Tabla 5. *Coeficiente de coincidencia del modelo ITIL*

Dimensión	Indicador	Especialista 1	Especialista 2	Especialista 3	Especialista 4	Especialista 5	Especialista 6	Especialista 7	Especialista 8	Especialista 9	Especialista 10	Especialista 11	Especialista 12	Especialista 13	Especialista 14	Especialista 15	Especialista 16	Especialista 17	Especialista 18	Especialista 19	Especialista 20	Sxi	Mxi	CVCi	Pei	CVic
Calidad de la información	Completitud	5	3	5	3	3	5	4	3	5	5	5	5	5	5	4	5	3	3	3	3	82	16,4	0,82	0,00000	0,820
	Exactitud	3	5	5	3	3	5	5	4	4	3	4	5	5	4	3	4	5	4	5	4	83	16,6	0,83	0,00000	0,830
	Fiabilidad	3	3	5	3	4	5	3	3	3	3	4	5	4	3	5	3	5	5	4	3	76	15,2	0,76	0,00000	0,760
	Consistencia	5	5	3	4	4	5	5	4	3	4	4	5	4	5	4	5	3	5	3	5	85	17	0,85	0,00000	0,850
Satisfacción del usuario	Accesibilidad	4	3	4	5	4	3	5	4	3	3	5	3	3	4	4	4	5	4	4	5	79	15,8	0,79	0,00000	0,790
	Velocidad	5	4	4	3	5	3	3	5	4	3	3	4	4	5	4	4	3	4	3	4	77	15,4	0,77	0,00000	0,770
	Precisión	4	3	4	3	4	4	4	5	5	5	5	4	5	4	4	4	4	3	3	4	81	16,2	0,81	0,00000	0,810
	Visualización	3	3	5	4	4	5	3	3	4	4	5	5	4	3	5	4	3	5	5	4	81	16,2	0,81	0,00000	0,810
	Personalización	4	4	3	4	4	4	3	4	4	5	4	5	5	4	4	5	3	3	5	5	82	16,4	0,82	0,00000	0,820
																									CVC Modelo ITIL	**0,807**

Fuente: Elaboración propia

Tabla 6. *Coeficiente de coincidencia del modelo COSO*

Dimensión	Indicador	Especialista 1	Especialista 2	Especialista 3	Especialista 4	Especialista 5	Especialista 6	Especialista 7	Especialista 8	Especialista 9	Especialista 10	Especialista 11	Especialista 12	Especialista 13	Especialista 14	Especialista 15	Especialista 16	Especialista 17	Especialista 18	Especialista 19	Especialista 20	Sxi	Mxi	CVCi	Pei	CVic
Calidad de la información	Completitud	3	3	3	4	3	3	3	4	4	3	3	3	4	3	4	3	3	4	3	3	66	13,2	0,66	0,00000	0,660
	Exactitud	4	4	4	4	4	4	4	4	3	4	3	4	4	3	4	4	3	4	3	3	74	14,8	0,74	0,00000	0,740
	Fiabilidad	4	3	4	4	4	3	3	3	4	4	3	4	3	3	4	3	4	3	3	4	70	14	0,7	0,00000	0,700
	Consistencia	3	4	3	4	3	3	4	3	4	3	3	3	3	3	4	4	4	4	4	4	70	14	0,7	0,00000	0,700
Satisfacción del usuario	Accesibilidad	3	3	4	4	3	3	4	4	3	3	4	3	4	3	4	3	4	3	4	3	69	13,8	0,69	0,00000	0,690
	Velocidad	4	3	4	4	4	4	4	4	4	4	4	3	3	3	4	4	4	3	3	3	73	14,6	0,73	0,00000	0,730
	Precisión	4	3	3	3	4	3	3	3	4	3	3	3	4	3	3	3	4	4	3	4	67	13,4	0,67	0,00000	0,670
	Visualización	4	4	4	3	4	3	4	4	4	3	4	3	4	4	4	4	4	4	4	3	75	15	0,75	0,00000	0,750
	Personalización	3	3	4	4	3	4	3	4	3	4	4	3	3	3	4	3	3	3	4	3	68	13,6	0,68	0,00000	0,680
																									CVC Modelo COSO	**0,702**

Fuente: Elaboración propia

Tabla 7. *Coeficiente de coincidencia del modelo Ley SOX*

Dimensión	Indicador	Especialista 1	Especialista 2	Especialista 3	Especialista 4	Especialista 5	Especialista 6	Especialista 7	Especialista 8	Especialista 9	Especialista 10	Especialista 11	Especialista 12	Especialista 13	Especialista 14	Especialista 15	Especialista 16	Especialista 17	Especialista 18	Especialista 19	Especialista 20	Sxi	Mxi	CVCi	Pei	CVic
Calidad de la información	Completitud	2	3	2	3	4	2	2	5	2	2	5	4	5	5	4	2	5	3	2	3	65	13	0,65	0,00000	0,650
	Exactitud	5	2	2	5	4	5	4	2	4	4	2	3	5	3	4	3	4	5	5	4	75	15	0,75	0,00000	0,750
	Fiabilidad	3	2	3	2	2	2	3	3	2	2	2	3	2	5	5	4	5	5	5	3	63	12,6	0,63	0,00000	0,630
	Consistencia	2	5	4	4	2	5	3	5	3	3	5	3	5	4	4	4	3	3	3	3	73	14,6	0,73	0,00000	0,730
Satisfacción del usuario	Accesibilidad	3	2	3	5	4	5	2	4	3	4	3	4	4	2	5	2	2	5	4	4	70	14	0,7	0,00000	0,700
	Velocidad	3	5	2	3	4	2	4	3	2	2	2	3	3	2	2	4	5	4	4	4	63	12,6	0,63	0,00000	0,630
	Precisión	4	3	2	5	2	5	3	4	4	3	4	3	5	4	4	4	5	5	4	2	75	15	0,75	0,00000	0,750
	Visualización	4	3	5	4	4	5	3	3	2	4	3	3	5	4	3	3	5	4	2	3	72	14,4	0,72	0,00000	0,720
	Personalización	3	4	2	2	4	2	3	2	5	3	3	2	5	4	2	3	2	5	4	2	62	12,4	0,62	0,00000	0,620
																									CVC Modelo LEY SOX	**0,687**

Fuente: Elaboración propia

Tabla 8*. Coeficiente de coincidencia del modelo COCO*

Dimensión	Indicador	Especialista 1	Especialista 2	Especialista 3	Especialista 4	Especialista 5	Especialista 6	Especialista 7	Especialista 8	Especialista 9	Especialista 10	Especialista 11	Especialista 12	Especialista 13	Especialista 14	Especialista 15	Especialista 16	Especialista 17	Especialista 18	Especialista 19	Especialista 20	Sxi	Mxi	CVCi	Pei	CVic
Calidad de la información	Completitud	4	4	3	4	4	5	5	3	3	3	5	5	3	2	5	5	4	3	4	2	76	15,2	0,76	0,00000	0,760
	Exactitud	4	4	3	5	2	3	2	4	2	4	3	3	5	2	2	2	5	4	2	2	63	12,6	0,63	0,00000	0,630
	Fiabilidad	5	5	4	3	2	4	3	4	5	3	4	5	3	2	3	2	3	5	5	2	72	14,4	0,72	0,00000	0,720
	Consistencia	2	3	3	2	2	3	2	4	5	5	2	3	2	2	4	4	4	3	4	5	64	12,8	0,64	0,00000	0,640
Satisfacción del usuario	Accesibilidad	5	4	2	3	2	2	5	3	3	5	5	3	4	2	2	2	2	2	3	2	61	12,2	0,61	0,00000	0,610
	Velocidad	2	2	5	3	4	5	4	4	2	5	2	2	5	4	5	2	2	2	3	4	67	13,4	0,67	0,00000	0,670
	Precisión	2	5	5	5	3	3	3	3	2	4	2	2	4	2	3	4	4	4	5	5	70	14	0,7	0,00000	0,700
	Visualización	2	5	5	2	3	3	3	5	3	5	4	5	5	5	3	5	3	2	3	2	73	14,6	0,73	0,00000	0,730
	Personalización	3	4	5	4	2	5	3	5	3	3	5	5	2	2	2	4	3	3	3	2	68	13,6	0,68	0,00000	0,680
																									CVC Modelo COCO	**0,682**

Fuente: Elaboración propia

Tabla 9*. Coeficiente de coincidencia del modelo CNSS*

Dimensión	Indicador	Especialista 1	Especialista 2	Especialista 3	Especialista 4	Especialista 5	Especialista 6	Especialista 7	Especialista 8	Especialista 9	Especialista 10	Especialista 11	Especialista 12	Especialista 13	Especialista 14	Especialista 15	Especialista 16	Especialista 17	Especialista 18	Especialista 19	Especialista 20	Sxi	Mxi	CVCi	Pei	CVic
Calidad de la información	Completitud	4	4	2	3	4	3	5	2	3	3	3	3	2	3	3	2	5	2	2	3	61	12,2	0,61	0,00000	0,610
	Exactitud	2	2	2	5	2	5	5	4	4	2	4	4	3	3	4	2	2	4	3	2	64	12,8	0,64	0,00000	0,640
	Fiabilidad	3	2	3	5	2	2	4	2	5	3	5	3	2	2	5	3	2	4	5	4	66	13,2	0,66	0,00000	0,660
	Consistencia	4	4	3	4	3	5	2	4	5	4	5	2	2	2	2	4	4	4	2	5	70	14	0,7	0,00000	0,700
Satisfacción del usuario	Accesibilidad	5	4	5	4	3	3	4	2	3	5	2	2	5	2	3	4	3	4	3	3	69	13,8	0,69	0,00000	0,690
	Velocidad	4	4	5	4	4	4	3	3	3	3	5	3	4	5	3	2	2	2	3	3	69	13,8	0,69	0,00000	0,690
	Precisión	2	2	4	5	2	2	2	5	4	3	3	5	3	4	4	3	4	5	5	5	72	14,4	0,72	0,00000	0,720
	Visualización	3	3	2	5	4	5	4	4	2	4	2	4	3	3	2	2	2	3	3	4	64	12,8	0,64	0,00000	0,640
	Personalización	2	3	5	2	4	2	5	4	5	4	4	5	3	5	4	2	4	2	3	5	73	14,6	0,73	0,00000	0,730
																									CVC Modelo CNSS	**0,676**

Fuente: Elaboración propia

Donde:

- *Sxi:* Sumatoria del puntaje de los jueces.

- *Mxi:* Sumatoria del Valor máximo entre máximo total posible de evaluación (5 puntos máximos por 1 categoría a evaluar, total 5) o sea *Sxi/5.*

- *CVCi:* Coeficiente de Validez de Contenido del ítem (Mxi/número de jueces).
- *Pei:* Error asociado al puntaje de los jueces. Se calcula como (1/número de expertos) elevado al número de expertos

- *CVCt:* Coeficiente de Validez de Coincidencias Total por expertos

El resumen del cálculo de la coincidencia entre los expertos del área de sistemas se resume en la siguiente tabla 10.

Tabla 10. *Resumen del CVC de los modelos*

Modelo	**CVC**	Calificación
COBIT	0,918	Excelente
ITIL	0,807	Buena
COSO	0,702	Deficiente
LEY SOX	0,687	Deficiente
COCO	0,682	Deficiente
CNSS	0,676	Deficiente

Fuente: Elaboración propia

De acuerdo a estos resultados se puede valorar que los modelos COBIT e ITIL tienen las mejores puntuaciones de coincidencia entre los expertos, sobresaliendo el modelo COBIT por preferencia con CVC de 0,918, catalogado como excelente al ser comparado con su correspondiente baremo, por lo que se propuso a la dirección de la empresa la aceptación de este modelo en la gestión y el control de la seguridad informática en la organización.

3.2. Identificar las vulnerabilidades en la seguridad de la información.

- **Valoración Juicio de expertos de la encuesta**

Para el cumplimiento de este objetivo específico se desarrolló una encuesta tipo test. La misma fue evaluada antes de ser aplicada por cinco expertos, especialistas en seguridad informática.

Los resultados de la valoración de los expertos se recogieron por los modelos que se presentan en los anexos 3 y 4.

Las preguntas de la encuesta fueron valoradas en Contenido (Suficiencia, Claridad, Coherencia y Relevancia) y Objetividad (Especificidad, Neutralidad, Independencia e Impersonalidad). Los resultados de las respuestas de la encuesta se visualizan en el anexo 5.

En las tablas 11 se expone el resultado de la medición del CVC de la dimensión Contenido valorado por cinco jueces o expertos en la temática.

Tabla 11. *CVC de validez de Contenido de la encuesta*

Ítem	Experto 1	Experto 2	Experto 3	Experto 4	Experto 5	Sxi	Mxi	CVCi	Pei	CVic
P1	20	19	18	19	18	94	4,7	0,94	0,00032	0,940
P2	19	19	19	17	20	94	4,7	0,94	0,00032	0,940
P3	18	17	17	18	20	90	4,5	0,9	0,00032	0,900
P4	19	19	19	16	16	89	4,45	0,89	0,00032	0,890
P5	19	19	18	19	19	94	4,7	0,94	0,00032	0,940
P6	16	18	18	19	16	87	4,35	0,87	0,00032	0,870
P7	17	20	19	19	19	94	4,7	0,94	0,00032	0,940
P8	19	17	19	20	18	93	4,65	0,93	0,00032	0,930
P9	16	18	20	19	20	93	4,65	0,93	0,00032	0,930
P10	19	18	17	14	17	85	4,25	0,85	0,00032	0,850
P11	19	17	19	20	18	93	4,65	0,93	0,00032	0,930
P12	18	17	20	17	17	89	4,45	0,89	0,00032	0,890
P13	18	17	20	18	18	91	4,55	0,91	0,00032	0,910
P14	18	17	20	15	16	86	4,3	0,86	0,00032	0,860
					Promedio del Coeficiente de Validez de Contenido de la Encuesta					**0,91**

Fuente: Elaboración propia

Se aprecia que la coincidencia de estos expertos (CVC) al emitir su juicio es de 0,91, lo que comparando con el baremo correspondiente lo sitúa como una coincidencia de **excelente** por parte de los jueces validando las preguntas de la encuesta como pertinentes en Suficiencia, Claridad, Coherencia y Relevancia.

El cálculo de la coincidencia de los expertos en cuanto a Objetividad se expone en la tabla 12.

Tabla 12. *CVC de validez de Objetividad de la encuesta*

Ítem	Experto 1	Experto 2	Experto 3	Experto 4	Experto 5	Sxi	Mxi	CVCi	Pei	Cvic
P1	0	0	0	0	0	0	0	0	0,00032	0,000
P2	20	19	18	19	18	94	4,7	0,94	0,00032	0,940
P3	19	19	19	17	20	94	4,7	0,94	0,00032	0,940
P4	18	17	17	18	20	90	4,5	0,9	0,00032	0,900
P5	19	19	19	16	16	89	4,45	0,89	0,00032	0,890
P6	19	19	18	19	19	94	4,7	0,94	0,00032	0,940
P7	16	18	18	19	16	87	4,35	0,87	0,00032	0,870
P8	17	20	19	19	19	94	4,7	0,94	0,00032	0,940
P9	19	17	19	20	18	93	4,65	0,93	0,00032	0,930
P10	16	18	20	19	19	92	4,6	0,92	0,00032	0,920
P11	19	18	17	14	16	84	4,2	0,84	0,00032	0,840
P12	19	17	19	20	17	92	4,6	0,92	0,00032	0,920
P13	18	17	20	15	14	84	4,2	0,84	0,00032	0,840
P14	18	17	20	15	14	84	4,2	0,84	0,00032	0,840
								Promedio del Coeficiente de Validez de Objetividad de la Encuesta		**0,84**

Fuente: Elaboración propia

Con este resultado se puede ver que los jueces interpretan que el instrumento es tiene una calificación de **Bueno** (0,84) sobre la dimensión Objetividad que midió la Especificidad, Neutralidad, Independencia e Impersonalidad.

- **Medición de la Fiabilidad de la encuesta**

Una vez respondida la encuesta se procede a la medición de la Fiabilidad de la misma, para lo cual se calcula el coeficiente Alfa con la metodología empleada por Cronbach. El cálculo individual por dimensiones y general de la encuesta de este coeficiente se puede ver en el anexo 6. El resumen de esta medición se puede valorar en la tabla 13.

Tabla 13*. Resultados de la Fiabilidad del instrumento de investigación*

Alfa de Cronbach Resumen	
Alfa Dimensión 1	0,869
Alfa Dimensión 2	0,670
Alfa Dimensión 3	0,740
Alfa Dimensión 4	0,833
Alfa Dimensión 5	0,866
Alfa Instrumento General	0,920

Fuente: Elaboración propia

Como puede apreciarse la Fiabilidad se considera de **Buena** en la Dimensión Gobernanza con 0,67 y la Dimensión Identidad, mientras que en el resto de las dimensiones (Dimensión Garantía, Dimensión Gestión de riesgos y la Dimensión Servicio) y el instrumento en general se cataloga de **Excelente** (0,86, 0,83, 0,86 y 0,92 respectivamente)

- **Análisis de los indicadores de la encuesta**

Una vez corroboradas las mediciones estadísticas de la Fiabilidad se hace el análisis individual de cada indicador por la evaluación de cada pregunta.

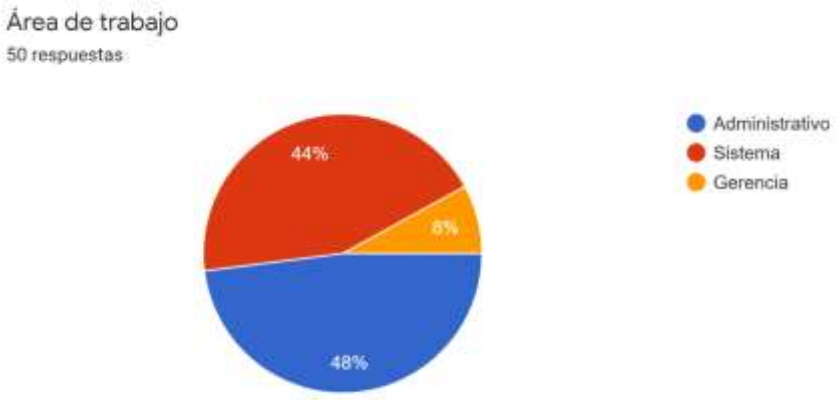

Gráfico 1. Área de desempeño de los encuestados
Fuente: Elaboración propia

Análisis: En esta empresa resalta que su departamento de sistemas es casi del mismo tamaño del departamento administrativo, lo que dice de la importancia en que se trata en esta organización la seguridad informática.

Dimensión Garantía

Gráfico 2. Pregunta 1
Fuente: Elaboración propia

Análisis: Llama la atención que en esta pregunta un 18% no está de acuerdo con los controles de la información en la organización.

Gráfico 3. Pregunta 2
Fuente: Elaboración propia

Análisis: Se refuerza con esta pregunta que existe un 8% que no reconocen al control como medida adecuada para garantizar la seguridad informática.

Gráfico 4. Pregunta 3
Fuente: Elaboración propia

Análisis: Se reafirma que el 20% de los miembros de la organización tienen interés en no reconocer los sistemas de calidad de la información, pues entre los indiferentes y los que están en desacuerdo suman ese porcentaje.

Dimensión Gobernanza

Gráfico 5. Pregunta 4
Fuente: Elaboración propia

Análisis: El 80% de los integrantes si están de acuerdo que este tipo de sistema de control informático les mejora su desempeño laboral, debe entenderse que los operadores informáticos buscan estar siempre protegidos de

las acciones externas que por lo general siempre son formas y métodos de robo de información.

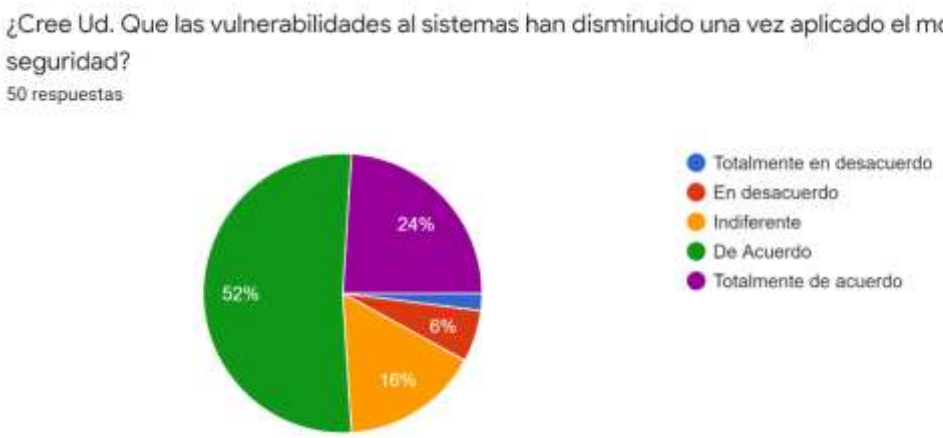

Gráfico 6. Pregunta 5
Fuente: Elaboración propia

Análisis: Al dar respuesta a esta pregunta se evidencia que el 76% dan por sentado que el modelo instaurado si ha hecho que hayan disminuido las vulnerabilidades del sistema informático

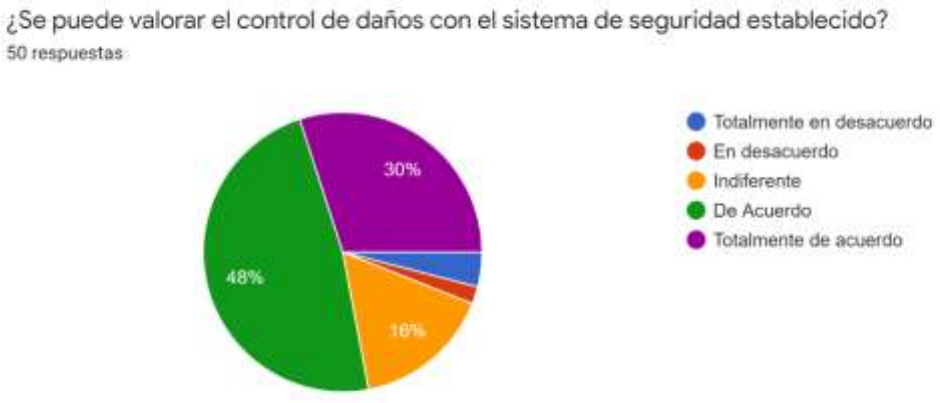

Gráfico 7. Pregunta 6
Fuente: Elaboración propia

Análisis: En sintonía con la pregunta anterior el 78% reconocen que mediante el modelo establecido se pueden valorar los daños al sistema informático, aportando con evidencias en cuanto de las auditorias informáticas.

Dimensión Identidad y Control de acceso

Gráfico 8. Pregunta 7
Fuente: Elaboración propia

Análisis: En este indicador, se puede ver que el 98% aseguran que se ha mejorado el control de acceso a la información dentro de la empresa con este modelo.

Gráfico 9. Pregunta 8
Fuente: Elaboración propia

Análisis: Se reconoce por el 90% de los integrantes de la empresa la necesidad de aplicar los mecanismos de autenticidad en los medios informáticos. Es importante conocer que existe ese 10% que de alguna manera es indisciplinado con las medidas de protección informáticas, por lo que deben prestarse atención al desenvolvimiento de los actores de la empresa de todos los niveles.

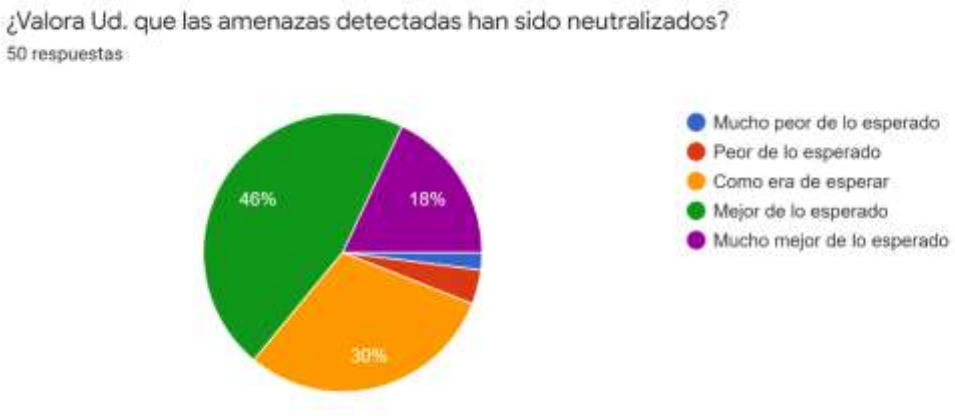

Gráfico 10. Pregunta 9
Fuente: Elaboración propia

Análisis: Se reconoce por el 94% de los miembros de la organización que ha sido efectivo el modelo instalado en la empresa pues ha neutralizado las amenazas que han tratado de vulnerar el sistema

Dimensión Gestión de riesgos

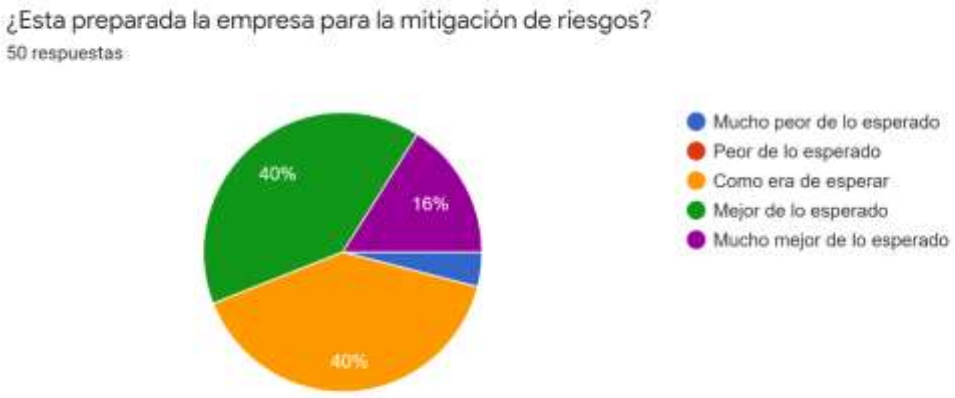

Gráfico 11. Pregunta 10
Fuente: Elaboración propia

Análisis: Existe confianza entre la mayoría de los integrantes de la empresa (96%) pues consideran que la misma está preparada para mitigar los riesgos de violaciones de la seguridad informática de la misma.

Gráfico 12. Pregunta 11
Fuente: Elaboración propia

Análisis: El desempeño del modelo instalado es considerado adecuado pues el 94% reconoce que el mismo monitorea adecuadamente el sistema y la gestión diaria de la organización lo que permite seguridad digital de la misma en sus operaciones en línea.

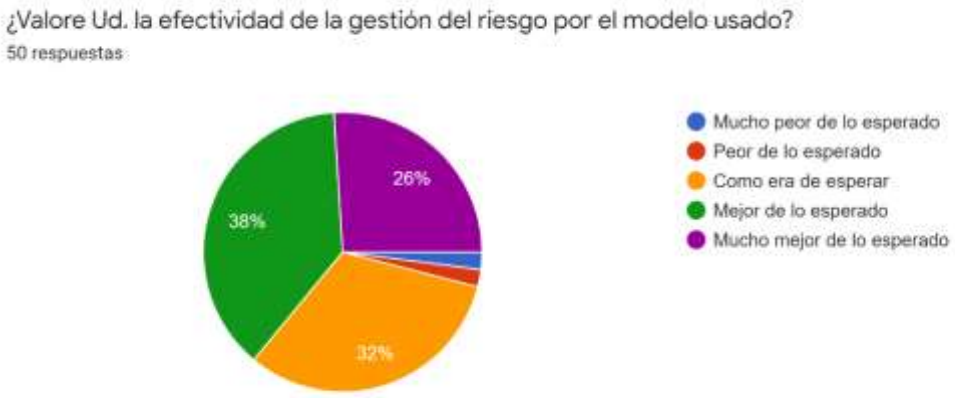

Gráfico 13. Pregunta 12
Fuente: Elaboración propia

Análisis: Al valorar la efectividad del modelo se hace recurrente el que el 96% del personal de la organización lo avale.

Dimensión Servicio

Gráfico 14. Pregunta 13
Fuente: Elaboración propia

Análisis: En la dimensión de servicios se reconoce por el 96% que el mismo es adecuado pues lo valúan entre mucho mejor y como era de esperar con ese porcentaje

Gráfico 15. Pregunta 14
Fuente: Elaboración propia

Análisis: En este indicador de esta dimensión se acentúa que es efectivo el servicio ya que el 98% asegura que disminuye los riesgos al ser instalado este modelo de gestión de la información.

3.3. Analizar de los riesgos de seguridad de la empresa.

Al igual que en el caso de la encuesta, la entrevista estructurada se sometió a la validación de concordancias por el método de juicio de expertos. Para lo cual los mismos expertos que fueron recabados en ambos instrumentos.

Al ser sometidas las 17 preguntas a ser valoradas en validez de Contenido y validez de Objetividad. El resumen de la valoración del Contenido se recoge en la tabla

Tabla 14. *CVC de Contenido de la entrevista*

Ítem	Experto 1	Experto 2	Experto 3	Experto 4	Experto 5	Sxi	Mxi	CVCi	Pei	CVic
P1	16	19	14	17	18	84	4,2	0,84	0,00032	0,840
P2	15	18	15	18	17	83	4,15	0,83	0,00032	0,830
P3	16	19	17	17	18	87	4,35	0,87	0,00032	0,870
P4	17	18	16	19	19	89	4,45	0,89	0,00032	0,890
P5	15	20	13	17	18	83	4,15	0,83	0,00032	0,830
P6	17	18	14	17	17	83	4,15	0,83	0,00032	0,830
P7	20	18	14	17	18	87	4,35	0,87	0,00032	0,870
P8	19	18	15	19	17	88	4,4	0,88	0,00032	0,880
P9	14	19	18	18	19	88	4,4	0,88	0,00032	0,880
P10	14	18	15	19	19	85	4,25	0,85	0,00032	0,850
P11	15	17	16	18	16	82	4,1	0,82	0,00032	0,820
P12	20	16	16	19	18	89	4,45	0,89	0,00032	0,890
P13	16	18	15	18	18	85	4,25	0,85	0,00032	0,850
P14	17	17	16	17	18	85	4,25	0,85	0,00032	0,850
P15	14	19	17	19	17	86	4,3	0,86	0,00032	0,860
P16	13	20	17	19	17	86	4,3	0,86	0,00032	0,860
P17	18	18	15	18	18	87	4,35	0,87	0,00032	0,870
				Promedio del Coeficiente de Validez de Contenido de la Entrevista						**0,86**

Fuente: Elaboración propia

Como se aprecia en el cálculo del coeficiente de coincidencias entre los expertos el contenido (fue evaluado en Suficiencia, Coherencia, Relevancia y Claridad arroja como resultado un valor de 0,86 lo que lo sitúa según el baremo de medición en una concordancia de Buena, lo que califica al instrumento (entrevista) para medir por Contenido las variables que subyacen en el mismo.

De igual manera se procede para valorar la Objetividad de la entrevista. Al tabular los resultados, condensar y calcular se obtienen como resultado lo expuesto en la tabla 15.

Nótese que en el cálculo de los CVC individual de cada ítem hay algunos que su calificación de coincidencia entre los jueces los cataloga de Excelente (ítem 7 y ítem 8) con calificaciones respectivas de 0,91 y 0,94.

En resumen, se valora la Objetividad de la entrevista (valorada en Especificidad, Neutralidad, Independencia e Impersonalidad) en Buena (0,88).

Tabla 15. *CVC de Objetividad de la entrevista*

Ítem	Experto 1	Experto 2	Experto 3	Experto 4	Experto 5	Sxi	Mxi	CVCi	Pei	CVic
P1	18	15	19	19	18	89	4,45	0,89	0,00032	0,890
P2	19	17	18	17	20	91	4,55	0,91	0,00032	0,910
P3	19	15	17	18	20	89	4,45	0,89	0,00032	0,890
P4	16	15	18	16	16	81	4,05	0,81	0,00032	0,810
P5	18	15	19	19	19	90	4,5	0,9	0,00032	0,900
P6	19	17	19	19	16	90	4,5	0,9	0,00032	0,900
P7	18	17	18	19	19	91	4,55	0,91	0,00032	0,910
P8	18	18	20	20	18	94	4,7	0,94	0,00032	0,940
P9	17	14	18	19	20	88	4,4	0,88	0,00032	0,880
P10	17	19	17	14	17	84	4,2	0,84	0,00032	0,840
P11	18	16	18	20	18	90	4,5	0,9	0,00032	0,900
P12	18	17	19	17	17	88	4,4	0,88	0,00032	0,880
P13	19	16	17	18	18	88	4,4	0,88	0,00032	0,880
P14	17	14	20	15	16	82	4,1	0,82	0,00032	0,820
P15	19	16	19	15	16	85	4,25	0,85	0,00032	0,850
P16	20	16	18	15	16	85	4,25	0,85	0,00032	0,850
P17	20	16	17	15	16	84	4,2	0,84	0,00032	0,840
					Promedio del Coeficiente de Validez de Objetividad de la Entrevista					**0,88**

Fuente: Elaboración propia

Para comprobar la Fiabilidad se mide el estadístico Alfa de Cronbach. Los cálculos individuales de cada dimensión del instrumento en general se recogen en el anexo 8. El resumen del dicho calculo se expone en la tabla 16.

Tabla 16. *Resultados de Alfa de Cronbach de la entrevista*

Alfa de Cronbach Entrevista	
Alfa Dimensión 1	0,670
Alfa Dimensión 2	0,773
Alfa Dimensión 3	0,827
Alfa Dimensión 4	0,647
Alfa Instrumento General	0,921

Fuente: Elaboración propia

Como se puede observar la Dimensión 3 y el instrumento (entrevista) en general tienen una calificación de Alta Fiabilidad, el resto de las dimensiones es calificada de Buena

A partir de este punto se pasan a valorar los indicadores de las preguntas cerradas para valorar el estado de los riesgos y las vulnerabilidades del sistema informático de la empresa.

La visualización del Riesgo Efectivo se midió por los ítems 1 y 2 de la entrevista. En el grafico 16 y 17 se muestra su resumen.

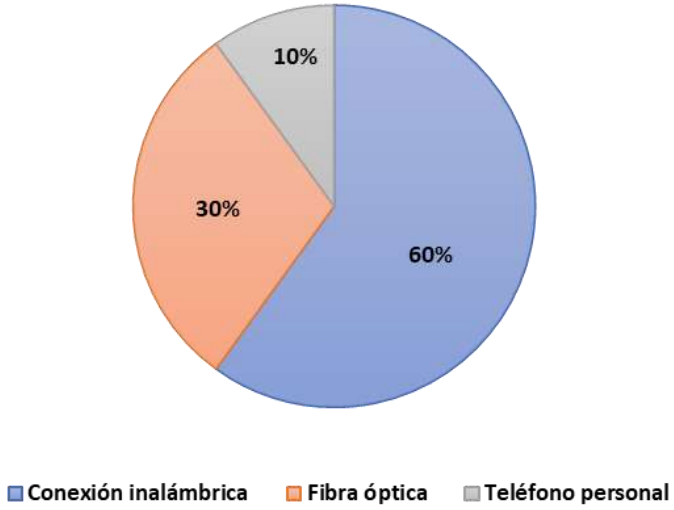

Gráfico 16. Tipo de conexión
Fuente: Elaboración propia

Análisis: Esta variable muestra plenamente el estrato de la empresa, obsérvese que la mayoría usa conexión inalámbrica (60%) y se relaciona directamente con el área administrativa de la organización. La gerencia usa en su trabajo mayoritariamente el teléfono personal (10%) y el área de sistema aprovecha para trabajar una y exclusivamente (30%) sobre la conexión de fibra óptica por las posibilidades que esta da a este departamento.

El segundo ítem (P8) se relaciona Uso de internet, en el grafico 17 se aprecia su resultado.

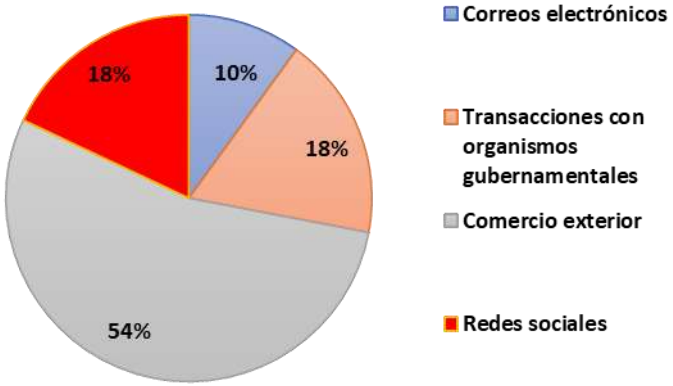

Gráfico 17. Uso de internet
Fuente: Elaboración propia

Se visualiza que el 54% de los integrantes de la organización usan la internet en las actividades de Comercio Exterior, que es en si la medula de la empresa, además el uso de las redes sociales y las transacciones económicas en línea suman junto a la anterior el 90% de su actividad. Este denota la importancia de una correcta gestión de la información en la empresa.

El cuanto al tratamiento de la información generada se valora su manipulación de siguiente forma (ver gráfico 18).

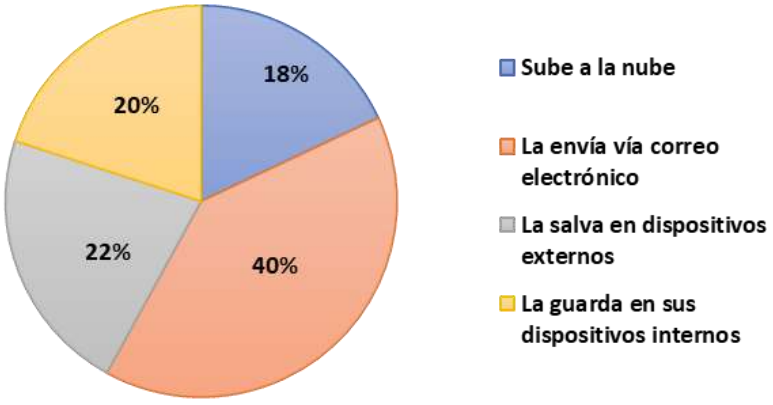

Gráfico 18. Tratamiento de la información
Fuente: Elaboración propia

En cuanto a la Dimensión de Ataques externos se valoran los ítems 9, 10 y 11. El primer indicador es las Amenazas detectadas, que se expone en el gráfico 19.

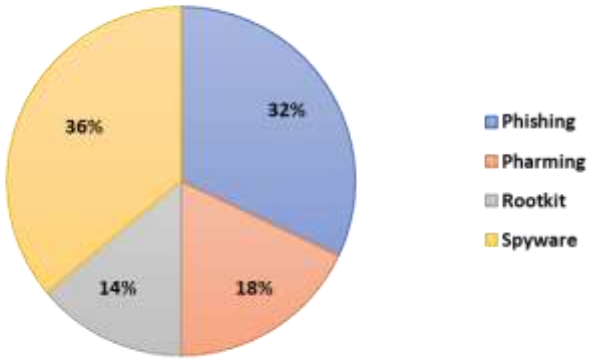

Gráfico 19. Amenazas detectadas
Fuente: Elaboración propia

Entre los ataques tipo Spyware y Phishing se concentra la mayor cantidad de ataques informáticos (68%). El resto de ataques detectados fueron del tipo Pharming (18%) y Rootkit (14%). Es evidente el interés que la empresa causa en los delincuentes informáticos por las actividades que la misma realiza y los montos de capital que maneja.

Se ha podido demostrar que con el sistema instalado se han detectado vulnerabilidades (ver gráfico 20).

Gráfico 20. Vulnerabilidades
Fuente: Elaboración propia

Se pudo evidenciar elementos que pasaban desapercibidos para el personal de control de la información, pues se evidencio que el uso de software no homologado ocupa un 32% del total de las vulnerabilidades, algo que no se estimaba sin la implantación del sistema de seguridad de la información, se evidencio asi mismo que existía mucha promiscuidad entre los empleados de las diferentes áreas de trabajo pues se comprobó una vulnerabilidad del 30% en el acceso al data center, algo que debe ser restringido para el personal que no pertenezca al área de sistemas. Se pudo también comprobar que entre las vulnerabilidades el uso de dispositivos de almacenamiento externo no autorizados era del 22% algo en lo que se debe de trabajar adecuadamente.

Por último, se hicieron evidentes los riesgos al ser instalado el nuevo modelo (ver gráfico 21).

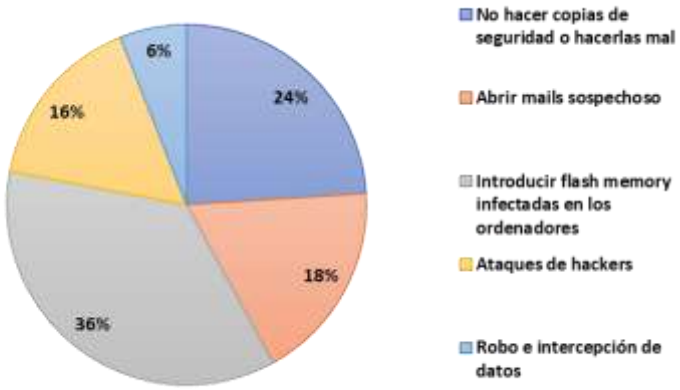

Gráfico 21. Riesgos evidenciados con el nuevo modelo de seguridad
Fuente: Elaboración propia

Como se puede apreciar estos riesgos coinciden con las vulnerabilidades encontradas, se expone que se detectaron un 36% de los mismos por el uso indebido de dispositivos de almacenamiento externo infectados con virus. En cuanto a la organización del trabajo se puede constatar que el 24% no hacia una salva o copia de seguridad de la información que manejan. Como se aprecia también existen riegos por una cultura informática inadecuada al abrir correos

sospechosos (18%), ataques de hackers (16%) y robo de datos (6%) estos últimos mediante la técnica de Spyware y Phishing expuestas en el gráfico 19.

IV. Conclusiones y recomendaciones

4.1. Conclusiones

- Para la selección del modelo adecuado se buscó la valoración de los 20 especialistas del área de sistemas, los cuales después de estudiar y valorar seis modelos de seguridad informática coincidieron con un 91,8% que el mejor modelo a seleccionar es el modelo COBIT, por lo que se propuso a la dirección de la empresa la aceptación de este modelo en la gestión y el control de la seguridad informática en la organización.
- Al buscar identificar las vulnerabilidades en la seguridad de la información se desarrolló una encuesta, su validez fue certificada mediante el instrumento de juicio de expertos (cinco expertos) los que valoran la misma por Contenido con 0,91 (coincidencia excelente) y por Objetividad con 0,84 (buena coincidencia). A su vez después de ser aplicada en línea se calculó la Fiabilidad la que se valoró en Alta (Alfa de Cronbach 0,92). Se midieron cinco Dimensiones y se pudo notar que en todas ellas y en todos los indicadores existe un porcentaje entre el 18 y el 22% que de alguna forma no coincide o no está de acuerdo con la implementación de un sistema de seguridad en la empresa. No obstante, la gran mayoría (más del 80%) lo aprueba.

- Con la valoración cualitativa y cuantitativa (se midió con la entrevista estructurada) de los riesgos de seguridad de la empresa se puede exponer que este instrumento también fue validad mediante el juicio de los cinco expertos anteriores, al tabularse y calcularse el CVC de estos 17 ítems se pudo observar que la coincidencia en el Contenido fue valorada como Buena (0,86) coincidencia, al igual que la Objetividad que punteo 0,88. La Fiabilidad medida de la entrevista se cataloga de Alta (Alfa de Cronbach 0,92). Se pudo evidenciar mediante los indicadores de la misma que después de instalado el sistema escogido se pudieron detectar una serie de vulnerabilidades que anteriormente

se pasaban por alto. Los riesgos se detectaron y se tiene ahora un mejor control de los recursos informáticos y la gestión de la información de la empresa se considera más segura.

4.2. Recomendaciones

- Usar la metodología de selección desarrollada para elegir el modelo a emplear en el sistema de gestión informática, que sean los propios integrantes del área de sistemas que lo escojan pues a la larga serán ellos los encargados de su monitoreo y gestión. En este caso especifico se escoge el modelo COBIT.
- Basándose en los resultados del diagnóstico del sistema empleado se deben realizar los correctivos necesarios para minimizar los riesgos y eliminar las vulnerabilidades detectadas. Se debe prestar atención al hecho de que el 20% de los involucrados no se adaptan al sistema propuesto.
- Al ser valorado cualitativa y cuantitativa de los riesgos de seguridad a los que puede estar expuesta una empresa se recomienda implementar los correctivos necesarios para minimizar los riesgos de seguridad del sistema informático y garantizar el correcto funcionamiento del sistema de la empresa.

Referencias bibliográficas

Acosta C Malambo E & Segura D. (2019). *Formulación de Buenas Prácticas para el Emprendimiento de las Pequeñas Empresas Utilizando las Metodologías de Scrum y Cobit con Base a la Experiencia de Helios T&I S.A.S Bogotá.* Colombia: Tesis de Grado Universidad Cooperativa de Colombia.

Alarcon J. (2016). *Diseño e Implementación de Políticas de Seguridad Informática Red y Virtualización Apoyadas con Software con Software Libre en la Compañía Tecnología y Redes S.A.S.* Colombia: Tesis de Grado Fundación Universitaria los Libertadores.

Altamirano J & Bayona S. (2017). Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento. *Risti*, 115.

Alvarez M. (2019). *Caracterización del Control Interno de las Micro y Pequeñas Empresas del Sector Construcción del Perú: Caso Empresa "Veles Contratistas Generales S.A.C.* Perú: Tesis de Grado Universidad Católica Los ángeles Chimbote.

Baca G. (2016). *Introducción a la Seguridad Informática.* México: Libro Grupo Editorial Patria.

Baygorrea D. (2017). *Propuesta de un Servicio Desk para Mejorar los Procesos de Resolución de Incidencias a Través de ITIL Empresa Cogesa.* Perú: Tesis de Grado Universidad Privada Norbert Wiener.

Bedoya C. (2017). *Diseño de un Instrumento Tipo Escala Likert para la Descripción de las Actitudes Hacia la Tecnología por Parte de los Profesores de un Colegio Público de Bogotá.* Colombia: Tesis de Grado Universidad Distrital Francisco José de Caldas.

Bedoya M. (2020). *Gestión de Riesgo de Tecnología de la Información y la Comunicación de el Gobierno Autónomo Descentralizado Municipal del Cantón Esmeraldas.* Ecuador: Tesis de Grado Pontificia Universidad Católica del Ecuador Sede Esmeraldas.

Caamaño E. (2020). Prevención de Riesgos por Ciberseguridad desde la Auditoria Forense: Conjugando el Talento Humano Organizacional. *Novum*, 63.

Campos C & León D. (2020). *Comparativa de las Metodologías Magerit y Octave para Determinar la más Adecuada en la Gestión de Riesgos de Tecnologías en la Unidad de Red Telemática de la Universidad Nacional Pedro Ruíz Gallo.* Perú: Tesis de Grado Universidad Nacional Pedro Ruíz Gallo.

Cárdenas et al. (2016). Gestión de seguridad de la Información. *El profesional de la información*, 932.

Cárdenas I. (2020). *Diseño de una Política de Seguridad de la Información para la Unidad Educativa Borja 3 Cavanis Basado en la Norma ISO/IEC 27002:2013.* Ecuador: Tesis Maestría Universidad Internacional SEK.

Carpentier J. (2016). *La Seguridad Informática en la Pyme.* España: Libro Ediciones ENI.

Castillo L. (2018). *Importancia de la Implementación del Control Interno para el Cumplimiento de la Ley Sarbanes Oxley en una Empresa del Sector de Generación de Energía Enfocado en el Ciclo de Ingresos.* Perú: Tesis de Grado Universidad de Piura.

Catota X. (2015). *Análisis Diseño e Implementación de un Sistema Informático para Gestionar los Trabajos de Help Desk del Área de Tecnología de la Cooperatica Codesarrollo Basado en Itil y Silverlight.* Ecuador: Tesis de Grado Universidad Politécnica Salesiana Sede Quito.

Chaso H. (2017). *La Gestión de Seguridad Informática y su Incidencia en la Información de la Universidad Técnica de Ambato.* Ecuador: Tesis Maestría Universidad Técnica de Ambato.

Chávez S. (2017). *Plan de Seguridad Informático Basado en el Estándar RFC-2196 y la Gestión Administrativa de los Servicios de Salud del Distrito 12D05 Vinces.* Ecuador: Tesis Maestría Universidad Regional Autónoma de los Andes Uniandes.

Cols C. (2015). Fundamentos de la Seguridad Informática. *Cengace Learning*, 4.

Departamento Juridico Torres and Torres. (2019). *Informe de Vulneravilidades.* Guayaquil.

Domingo A. (2015). *Guía de Implantación de un SGSI Basado en la Norma UNE-ISO/IEC 27001.* España: Tesis de grado Universitat Oberta de Catalunya.

Espinoza D. (2015). *Estudio de la Herramienta de Seguridad Open Source Security Information Management (OSSIM) en la Universidad Tecnológica Empresarial de Guayaquil UTEG.* Ecuador: Tesis de Grado Universidad de Guayaquil.

Estrada et al. (2019). Prácticas de Seguridad de Información del Nivel Ejecutivo de la Policía Nacional de Colombia: Escuela de Policía Simón Bolívar (Tulúa, Colombia). *Logos Ciencias & Tecnología*, 123.

Franco K et al. (2017). *El Sistema de Control Interno Basado en el Modelo COSO y su Inlfuencia en la Profesionalización para la Empresas de Buses Panorámicos en Lima Metropolitana.* Perú: Tesis de Grado Universidad Peruana de Ciencias Aplicadas.

Garcés S. (2015). *Seguridad Informática para la Red de Datos en la Cooperativa de Ahorro y Crédito unión Popular LTDA.* Ecuador: Tesis de Grado Universidad Técnica de Ambato.

García J & Gavilanes M. (2015). *Análisis y Propuesta de Implementación de las Mejores Prácticas de Itil en el Departamento de Sistemas de la Universidad Politécnica Salesiana Sede Guayaquil .* Ecuador: Tesis de Grado Universidad Politécnica Salesiana.

Gil V & Gil J. (2017). Seguridad Informática Organizacional: Un Modelo de Simulación Basado en Dinámica de Sistemas. *Scientia Et Technica*, 194.

Guaylupo J. (2017). *Solución Holística de Seguridad Informática para Mejorar la Gestión de las Tecnologías de la Información y Comunicación en la Dirección Regional de Educación de Piura Departamento de Piura en el Año 2016.* Perú: Tesis Maestría Universidad Católica Los Ángeles.

Guerra M. (2015). Estado del Arte de los Sistemas de Información. *UEES*, 25.

Guevara M. (2019). *La Ley Sox Sección 404 y su Incidencia en el Control de Compras y Ventas de la Empresa de Transporte de Carga Transp Vip Group S.A.C. en la Ciudad de Lima.* Perú: Tesis de Grado Universidad Privada del Norte.

Guevara R. (2017). *Sistema de Gestión de Seguridad de la Información Basados en la Norma ISO/IEC 27001 para el Departamento de Tecnologías de la Información y Comunicación del Distrito 18D01 de Educación.* Ecuador: Tesis de Grado Universidad Técnica de Ambato.

Guzmán A & Taborda C. (2015). *Diseño de un Sistema de Gestión de la Seguridad Informática -SGSI- para Empresas del Área Textil en las Ciudades de Itagui, Medellín y Bogotá D.C. A través de la Auditoría.* Colombia: Tesis de Grado Universidad Nacional Abierta y a Distancia.

Guzmán G. (2015). *Metodología para la Seguridad de Tecnologías de Información y Comunicaciones en la Clínica Ortega.* Perú: Tesis de Grado Universidad Nacional del Centro del Perú.

Heredia H. (2019). *Modelo de Gobierno de Seguridad de la Información para Instituciones de Educación Superior del Ecuador.* Ecuador: Tesis Maestría Universidad Técnica de Amabto.

Hérnandez D. (2011). *Diseño del Sistema de Gestión de Seguridad de la Información en Angelcom S.A.* Colombia: Tesis de Grado Universidad Libre.

Hernández Sampieri, R. (2013). *Metodología de la Investigación.* Ciudad de Mexico, México: Mc Graw Hill Education.

Hernández-Nieto, R. (2002). *El Coeficiente de Validez de Contenido (Cvc) y el Coeficiente Kappa en la determinacion de la validez de contenido de instrumentos de recoleccion de datos.* Merida: Universidad de los Andes.

Hernández-Sampieri, R., & Mendoza Torres, C. (2018). *METODOLOGÍA DE LA INVESTIGACIÓN: LAS RUTAS CUANTITATIVA, CUALITATIVA Y MIXTA* (Primera edición ed.). Ciudad de México: McGRAW-HILL INTERAMERICANA EDITORES, S.A. de C. V.

Landis, J. R., & Koch, G. (1977). An Application of Hierarchical Kappa-type Statistics in the Assessment of Majority Agreement among Multiple Observers. *Biometrics, 33*(2), 363-374. Retrieved from http://www.jstor.org/stable/2529786

López R. (2017). Fundamentos de Seguridad Informática. *Areandina*, 6.

Martelo et al. (2014). Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Informacioón (SGSI). *Información Tecnológica*, 130.

Molina E. (2016). *Análisis Comparativo entre Sistemas OSSTMM y COBIT 5.0 para la Mitigación de Riesgos.* Chile: Tesis de Grado Universidad Gabriela Mistral.

Montaño V. (2011). La Gestión en la Seguridad de la Información según Cobit, Itil e Iso 2700. *Pensamiento Americano*, 21 - 23.

Palacios A. (2015). *Diseño de un Modelo de Políticas de Seguridad Informática para la Superintendencia de Industria y Comercio de Bogotá.* Colombia: Tesis de Grado Universidad Libre de Colombia.

Páramo B. (2013). *Propuesta de Elaboración de un Manual de Control Intenro Basado en el Modelo COCO y Evaluación de la Gestión Operativa al Centro Comercial la Playa Megastore Ubicado en la Ciudad de Azogues en la Provincia de Cañar.* Ecuador: Tesis de Grado Universidad Politécnica Salesiana.

Patiño et al. (2017). Evaluación de Seguridad Informática Basada en ICREA e ISO 27001. *Universidad, Ciencia y Tecnología*, 130.

Pérez B. (2020). Importancia de un Sistema de Gestión de Seguridad de la Información para Empresas de Tecnología. *Re-Pilo*, 7.

Quevedo X & Vintimilla S. (2020). Riesgos de Seguridad de la Información del Departamento de Tecnologías de la Información y Comunicación Hospital Isidro Ayora - Loja. *Polo del Conocimiento*, 366.

Quinaluisa et al. (2018). El Control Interno y sus Herramientas de Aplicación entre Coso y Coco. *Cofín Habana*, 278.

Quiroz S & Macías D. (2017). Seguridad en informática: Consideraciones. *Dominio de las Ciencias*, 687.

Ramos M & Solares P. (2015). Ciencias de la Tecnología de Información. *Ecorfan*, 69 -70.

Reyes D et al. (2016). *Tecnologías de Información y Comunicación en las Organizaciones.* México: Libro UNAM.

Rodríguez D & Arevalo J. (2016). *El Ambiente de Control Interno como Determinante de Buenas Prácticas de Gobierno Corporativo en Multinacionales Caso: Ey.* Colombia: Tesis Maestría CESA.

Rojas J. (2018). *Características y Parámetros de la Seguridad en la Transmisión de Datos para los Dispositivos Smart.* Colombia: Monografía Universidad Nacional Abierta y a Distancia UNAD.

Romero M et al. (2018). Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades. *3Ciencias*, 14.

Ruíz C. (2020). *Auditoria Informática Aplicando la Metodología Cobit 5.0 al Proceso de Recaudación del Modulo de Tesoreria del Sistema Cabildo en el Departamento Financiero del Gobierno Autónomo Descentralizado Municipalidad de Ambato.* Ecuador: Tesis de Grado Universidad Técnica de Ambato.

Sánchez J. (2017). *Análisis de Vulnerabilidades y Diseño de Procesos Correctivos de la página Web de la Dirección de Educación a Distancia y Virtual de la Universidad Técnica de Ambato.* Ecuador: Tesis de Grado Universidad Técnica de Ambato.

Silva M. (2019). Metodología para la Gestión de la Seguridad de los Activos de Información Teniendo como Soporte una Plataforma Web en la Universidad Nacional Santiago Antúnez de Mayolo. *DII UNASAM*, 39.

Solarte et al. (2015). Metodología de Análisis y Evaluación de Riesgos Aplicados a la Seguridad Informática y de Información Bajo la Norma ISO/IEC 27001. *Tecnológica Espol - Rte*, 496.

Suarez G. (2015). *Diseñar un Plan Estrategico de Tecnología de la Información y Comunicaciones para una Empresa de Comercio Electrónico B2B y B2C Aplicando las Mejores Prácticas Basadas en los Lineamientos Aportados por las Metodolofias COBIT 5.0, ITIL e ISO 27001.* Colombia: Tesis de Grado Universidad Distrital Francisco José de Caldas.

Tapia G. (2019). *Propuesta de Mejora de los Factores Relevantes del Control Interno en la Gestión Económica y Financiera de las Empresas Nacionales: Caso Empresa de Transporte America Express S.A. - Chimbote 2019.* Perú: Tesis Universidad Católica Los Ángeles Chimbote.

Tigse J. (2020). *Plan de Gestión de Seguridad Informática Basado en la Norma Iso 27001 para el Departamento de Tecnología de la Información en la*

Empresa Plasticaucho Industrial S.A. Ecuador: Tesis de Grado Universidad Técnica de Ambato.

Torres C. (2020). *Plan de Seguridad Informática Basado en la Norma ISO 27001 para Proteger la Información y Activos de la Empresa Privada Megaprofer S.A.* Ecuador: Tesis de Grado Universidad Técnica de Ambato.

Torres E. (2015). *Políticas de Seguridad de la Información Basado en la Norma ISO/ICE 27002:2013 para la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato.* Ecuador: Tesis de Grado Universidad Técnica de Ambato.

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 2700. *Risti*, 74 -75.

Velez S. (2017). Análisis del Modelo COSO y su Aplicación en una Pyme Ecuatoriana - Laboratorio Químico de Alimentos. *UEES*, 7.

Zamora L & Tamez X. (2019). Riesgos de Auditoría en Control Interno y el Impacto del Modelo COSO. *Eumed*, 354.

Zapata K. (2020). *Ssitema de Gestión de Seguridad de la Información Basado en las Normas ISO/IEC 27001 en el Departamento de Tecnologías de la Información del Gobierno Autónomo Descentralizado de la Municipalidad de Ambato.* Ecuador: Tesis de Grado Universidad Técnica de Ambato.

Anexos

Anexo 1. Modelo recolección de datos del modelo

Resumen Análisis de Selección de modelo de seguridad informática							
Instrucciones de evaluación: Frente a usted se encuentran seis modelos de seguridad informática. Usted debe calificar su preferencia de sus atributos en una escala del 1 al 5 donde 1: Muy poco, 2: Poco, 3: Regular, 4: Aceptable y 5: Muy aceptable							
Dimensión	**Indicador**	**Modelos**					
		COBIT	**ITIL**	**COSO**	**LEY SOX**	**COCO**	**CNSS**
Calidad de la información	Completitud						
	Exactitud						
	Fiabilidad						
	Consistencia						
Satisfacción del usuario	Accesibilidad						
	Velocidad						
	Precisión						
	Visualización						
	Personalización						

Anexo 2. Modelo de encuesta

Universidad Tecnológica Empresarial de Guayaquil

Modelo de seguridad de la información

*Obligatorio

Variables generales

1. Área de trabajo *

Marca solo un óvalo.

- Administrativo
- Sistema
- Gerencia

Dimensión Garantía

2. ¿Está de acuerdo con los controles de información? *

Marca solo un óvalo.

- Totalmente en desacuerdo
- En desacuerdo
- Indiferente
- De Acuerdo
- Totalmente de acuerdo

3. ¿Cree que los controles de seguridad pueden garantizar la seguridad informática? *

Marca solo un óvalo.

- Totalmente en desacuerdo
- En desacuerdo
- Indiferente
- De Acuerdo
- Totalmente de acuerdo

4. ¿Cree que un sistema general de calidad en la información podría garantizar la seguridad informática? *

Marca solo un óvalo.

- Totalmente en desacuerdo
- En desacuerdo
- Indiferente
- De Acuerdo
- Totalmente de acuerdo

Dimensión Gobernanza

5. ¿Cree Ud. que los controles de información mejoran su desempeño laboral? *

Marca solo un óvalo.

- Totalmente en desacuerdo
- En desacuerdo
- Indiferente
- De Acuerdo
- Totalmente de acuerdo

6. ¿Cree Ud. Que las vulnerabilidades al sistemas han disminuido una vez aplicado el modelo de seguridad? *

Marca solo un óvalo.

- Totalmente en desacuerdo
- En desacuerdo
- Indiferente
- De Acuerdo
- Totalmente de acuerdo

7. ¿Se puede valorar el control de daños con el sistema de seguridad establecido? *

Marca solo un óvalo.

- Totalmente en desacuerdo
- En desacuerdo
- Indiferente
- De Acuerdo
- Totalmente de acuerdo

Dimensión Identidad y Control de acceso

8. ¿Cómo valoraría el control de acceso a la información dentro de la empresa Torres y Torres? *

Marca solo un óvalo.

- Mucho peor de lo esperado
- Peor de lo esperado
- Como era de esperar
- Mejor de lo esperado
- Mucho mejor de lo esperado

9. ¿Cree Ud. necesario aplicar mecanismos de autenticidad en los medios informáticos? *

Marca solo un óvalo.

- Totalmente en desacuerdo
- En desacuerdo
- Indiferente
- De Acuerdo
- Totalmente de acuerdo

10. ¿Valora Ud. que las amenazas detectadas han sido neutralizados? *

Marca solo un óvalo.

- Mucho peor de lo esperado
- Peor de lo esperado
- Como era de esperar
- Mejor de lo esperado
- Mucho mejor de lo esperado

Dimensión Gestión de riesgos

11. ¿Esta preparada la empresa para la mitigación de riesgos? *

Marca solo un óvalo.

- Mucho peor de lo esperado
- Peor de lo esperado
- Como era de esperar
- Mejor de lo esperado
- Mucho mejor de lo esperado

12. ¿Se monitorea adecuadamente el estado de seguridad de la información en la empresa? *

Marca solo un óvalo.

- Mucho peor de lo esperado
- Peor de lo esperado
- Como era de esperar
- Mejor de lo esperado
- Mucho mejor de lo esperado

13. ¿Valore Ud. la efectividad de la gestión del riesgo por el modelo usado? *

Marca solo un óvalo.

- Mucho peor de lo esperado
- Peor de lo esperado
- Como era de esperar
- Mejor de lo esperado
- Mucho mejor de lo esperado

Dimensión Servicio

14. ¿Cómo cataloga los servicios que presta el modelo de seguridad en la empresa? *

Marca solo un óvalo.

- Mucho peor de lo esperado
- Peor de lo esperado
- Como era de esperar
- Mejor de lo esperado
- Mucho mejor de lo esperado

15. ¿Existe efectividad de los servicios y disminución de riesgos con el sistema instalado? *

Marca solo un óvalo.

- Mucho peor de lo esperado
- Peor de lo esperado
- Como era de esperar
- Mejor de lo esperado
- Mucho mejor de lo esperado

Anexo 3. Modelo de validación de Objetividad

1	**Validez de Objetividad del Instrumento**			**Fecha:**			
	Método: Juicio de Expertos			**Proyecto:**	Modelos de seguridad de la información para el control de los riesgos informáticos en el área administrativa de una empresa de operadores logísticos de comercio exterior		
	Herramienta: Estadístico Coeficiente de Validación de Concordancias (CVC)						
2	**Indicación:**	Estimado experto, se le solicita su colaboración para que luego de un riguroso análisis de cada elemento, teniendo presente el objetivo de este instrumento y desde su experticia valorar el **Instrumento de Investigación** en el cumplimiento de los atributos que componen la **VALIDEZ DE OBJETIVIDAD** (**Especificidad, Neutralidad, Independencia e Impersonalidad**) necesaria para validar sus resultados.					
3	**Objetivo del Instrumento:**	**Certificación de atributos para Encuesta**					
4	**Metodología de aplicación:**	**Validación de Instrumento de investigación**					
5	**Atributo**	**Descripción**	**Muy Poco (1)**	**Poco (2)**	**Regular (3)**	**Aceptable (4)**	**Muy Aceptable (5)**
6	**Especificidad**	El instrumento a través de sus indicadores permite una definición completa, pertinente, precisa del objeto de investigación, lo que representa objetivamente el criterio de quien lo respondió.					
7	**Neutralidad**	La presentación del instrumento actual no permite la injerencia externa en los juicios de valor que hace un evaluador u otras personas con los resultados de la prueba.					
8	**Independencia**	En el instrumento las medidas y juicio de valor no se ven influidas por otros rasgos, instrumentos o agentes personales o contextuales de quien lo responde.					
9	**Impersonalidad**	Los indicadores permiten expresar la forma en que el asunto en cuestión es observado o percibido por quién responde el instrumento y no como es compartido en el grupo social, cultural, étnico u otro al que pertenece en un momento dado.					
10	**Recomendaciones**						
11	**Nombre y Apellidos**						
12	**Grado Académico**						
13	**Profesión**						**Firma**

Anexo 4. Modelo de validación de Contenido

1	**Validez de Contenido del Instrumento**			**Fecha:**			
	Método: Juicio de Expertos			**Proyecto:**	Modelos de seguridad de la información para el control de los riesgos informáticos en el área administrativa de una empresa de operadores logísticos de comercio exterior		
	Herramienta: Estadístico Coeficiente de Validación de Concordancias (CVC)						
2	**Indicación:**	Estimado experto, se le solicita su colaboración para que luego de un riguroso análisis de cada elemento, teniendo presente el objetivo de este instrumento y desde su experticia valorar el Instrumento de Investigación en el cumplimiento de los atributos de la **VALIDEZ DE CONTENIDO** (**Suficiencia, la claridad, la coherencia y la relevancia**) necesaria para validar sus resultados.					
3	**Objetivo del Instrumento:**	**Certificación de atributos para Encuesta**					
4	**Metodología de aplicación:**	**Validación de Instrumento de investigación**					
5	**Atributo**	**Descripción**	**Muy Poco (1)**	**Poco (2)**	**Regular (3)**	**Aceptable (4)**	**Muy Aceptable (5)**
6	**Suficiencia**	El instrumento a través de sus ítems es suficiente para evaluar de forma precisa del objeto de investigación, lo que representa objetivamente el criterio de quien lo respondió.					
7	**Claridad**	La presentación del instrumento actual es clara, no permite ambigüedades en los juicios de que hace un evaluador u otras personas con los resultados de la prueba.					
8	**Coherencia**	En el instrumento existe la coherencia adecuada en su estructura como un instrumento justo para quien lo responde.					
9	**Relevancia**	Los ítems del instrumento son relevantes y permiten exponer relaciones interesantes entre sus variables, que al ser valoradas expondrán nuevos vínculos y puntos de vistas de aporte a la ciencia.					
10	**Recomendaciones**						
11	**Nombre y Apellidos**						
12	**Grado Académico**						
13	**Profesión**						**Firma**

Anexo 5. Tabulación de los resultados de la encuesta

Encuestados	Área de trabajo	P1	P2	P3	D1	P4	P5	P6	D2	P7	P8	P9	D3	P10	P11	P12	D4	P13	P14	D5	Total
1	Sistema	4	5	4	13	5	4	4	13	3	5	1	9	3	1	4	8	4	4	8	51
2	Gerencia	4	4	4	12	5	4	5	14	4	5	4	13	4	4	3	11	4	5	9	59
3	Administrativo	4	4	4	12	5	4	5	14	4	5	4	13	4	4	4	12	4	4	8	59
4	Administrativo	4	3	4	11	3	4	3	10	3	4	4	11	3	4	3	10	3	3	6	48
5	Administrativo	3	4	4	11	4	4	4	12	3	4	3	10	3	3	3	9	3	3	6	48
6	Administrativo	4	4	4	12	4	4	4	12	4	4	3	11	3	4	4	11	3	3	6	52
7	Gerencia	4	4	4	12	4	4	3	11	3	4	3	10	3	3	3	9	4	3	7	49
8	Administrativo	2	1	1	4	5	3	5	13	5	5	5	15	5	5	5	15	4	4	8	55
9	Administrativo	5	5	5	15	5	5	4	14	5	5	4	14	4	4	4	12	4	5	9	64
10	Administrativo	1	5	5	11	5	5	5	15	5	5	5	15	5	5	5	15	5	5	10	66
11	Administrativo	3	4	3	10	4	4	4	12	4	4	4	12	1	4	3	8	3	3	6	48
12	Administrativo	4	4	4	12	4	4	4	12	3	4	3	10	4	4	4	12	4	4	8	54
13	Administrativo	5	5	5	15	5	4	4	13	4	5	3	12	3	4	3	10	4	3	7	57
14	Administrativo	4	4	4	12	4	3	4	11	3	4	3	10	3	3	3	9	3	3	6	48
15	Administrativo	5	5	5	15	5	5	5	15	4	5	4	13	5	5	5	15	5	5	10	68
16	Administrativo	2	4	4	10	4	2	4	10	3	4	3	10	4	4	4	12	3	3	6	48
17	Sistema	4	4	5	13	3	4	3	10	4	4	4	12	4	5	4	13	4	4	8	56
18	Administrativo	4	4	4	12	4	4	4	12	4	4	4	12	4	4	4	12	4	4	8	56
19	Administrativo	4	4	4	12	4	4	4	12	4	4	4	12	4	4	3	11	4	4	8	55
20	Administrativo	4	3	4	11	4	3	4	11	3	4	4	11	3	4	3	10	4	4	8	51
21	Administrativo	4	5	4	13	3	4	4	11	3	4	3	10	4	3	4	11	3	3	6	51
22	Administrativo	3	5	5	13	5	5	5	15	4	4	4	12	3	4	4	11	4	4	8	59
23	Administrativo	4	4	5	13	4	4	5	13	5	4	5	14	5	5	5	15	5	5	10	65
24	Sistema	1	4	1	6	4	4	4	12	3	4	3	10	3	3	3	9	3	3	6	43
25	Gerencia	3	3	3	9	3	3	3	9	3	3	3	9	3	3	3	9	3	3	6	42
26	Sistema	4	4	4	12	5	2	5	12	3	5	3	11	3	3	4	10	4	4	8	53
27	Sistema	5	4	4	13	5	2	3	10	4	2	5	11	3	4	5	12	4	5	9	55
28	Sistema	5	5	5	15	5	4	3	12	3	4	1	8	4	3	4	11	5	3	8	54
29	Sistema	1	1	1	3	1	5	5	11	5	5	5	15	4	5	5	14	5	5	10	53
30	Sistema	2	4	5	11	4	4	2	10	3	5	3	11	3	3	3	9	3	3	6	47
31	Sistema	4	4	4	12	4	4	5	13	4	4	4	12	4	4	4	12	4	4	8	57
32	Sistema	4	5	5	14	5	5	4	14	4	4	4	12	4	4	4	12	5	5	10	62
33	Sistema	4	3	4	11	3	3	3	9	3	4	4	11	3	3	1	7	3	3	6	44
34	Administrativo	3	4	4	11	4	3	4	11	4	4	4	12	3	4	3	10	4	4	8	52
35	Sistema	4	5	4	13	4	5	4	13	4	4	4	12	5	4	4	13	4	5	9	60
36	Sistema	5	5	5	15	5	5	4	14	4	5	5	14	5	4	5	14	5	5	10	67
37	Sistema	5	4	4	13	4	4	5	13	4	5	4	13	3	4	5	12	4	5	9	60
38	Sistema	1	1	1	3	1	1	1	3	1	1	1	3	1	1	1	3	1	1	2	14
39	Administrativo	1	4	1	6	1	4	1	6	3	1	3	7	3	3	3	9	3	3	6	34
40	Sistema	3	3	3	9	3	3	3	9	3	3	3	9	3	3	3	9	3	3	6	42
41	Administrativo	1	1	1	3	4	3	4	11	3	5	3	11	3	1	3	7	1	3	4	36
42	Sistema	4	5	4	13	4	4	4	12	5	4	4	13	4	4	5	13	4	4	8	59
43	Sistema	5	5	5	15	4	4	4	12	4	4	5	13	4	4	4	12	4	4	8	60
44	Gerencia	4	4	4	12	4	4	4	12	4	4	5	13	4	4	4	12	4	4	8	57
45	Sistema	4	4	5	13	4	5	4	13	3	4	4	11	4	4	5	13	4	5	9	59
46	Sistema	4	5	4	13	4	4	5	13	4	4	4	12	4	3	4	11	4	4	8	57
47	Sistema	4	4	5	13	5	5	5	15	5	4	4	13	4	4	5	13	4	4	8	62
48	Sistema	5	5	5	15	4	5	5	14	5	5	4	14	5	4	4	13	5	4	9	65
49	Administrativo	4	4	4	12	4	4	5	13	5	5	5	15	5	5	5	15	4	5	9	64
50	Administrativo	4	4	4	12	4	5	4	13	3	4	4	11	4	4	5	13	4	4	8	57
Total		**1,44**	**1,12**	**1,43**	**9,48**	**0,96**	**0,81**	**0,90**	**4,83**	**0,68**	**0,79**	**0,93**	**4,73**	**0,79**	**0,85**	**0,91**	**5,73**	**0,73**	**0,76**	**2,63**	**89,71**

Anexo 6. Alfa de Cronbach de dimensiones de la encuesta

Tabla 17. *Alfa de Cronbach Dimensión Garantía*

Alfa Dimensión 1	
k	3
k-1	2
A=k/k-1	1,500
Suma Vi	3,988
Vt	9,484
Suma Vi/Vt	0,420
B	0,580
Alfa D1	**0,869**

Fuente: Elaboración propia

Tabla 18. *Alfa de Cronbach Dimensión Gobernanza*

Alfa Dimensión 2	
k	3
k-1	2
A=k/k-1	1,500
Suma Vi	2,670
Vt	4,826
Suma Vi/Vt	0,553
B	0,447
Alfa D2	**0,670**

Fuente: Elaboración propia

Tabla 19. *Alfa de Cronbach Dimensión Identidad y Control de acceso*

Alfa Dimensión 3	
k	3
k-1	2
A=k/k-1	1,500
Suma Vi	2,397
Vt	4,728
Suma Vi/Vt	0,507
B	0,493
Alfa D3	**0,740**

Fuente: Elaboración propia

Tabla 20. *Alfa de Cronbach Dimensión Gestión de riesgos*

Alfa Dimensión 4	
k	3
k-1	2
A=k/k-1	1,500
Suma Vi	2,548
Vt	5,734
Suma Vi/Vt	0,444
B	0,556
Alfa D4	**0,833**

Fuente: Elaboración propia

Tabla 21*. Alfa de Cronbach Dimensión Servicio*

Alfa Dimensión 5	
k	2
k-1	1
A=k/k-1	2,000
Suma Vi	1,492
Vt	2,630
Suma Vi/Vt	0,567
B	0,433
Alfa D5	**0,866**

Fuente: Elaboración propia

Tabla 22. *Alfa de Cronbach de la encuesta*

Alfa General	
k	14
k-1	13
A=k/k-1	1,077
Suma Vi	13,094
Vt	89,710
Suma Vi/Vt	0,146
B	0,854
Alfa General	**0,920**

Fuente: Elaboración propia

Anexo 7. Tabulación de los resultados de la entrevista (variables de Likert)

Entrevistados	P3	P4	D1	P6	P7	P8	D2	P12	P13	P14	D3	P15	P16	P17	D4	VI
1	3	3	6	5	1	2	8	1	1	3	5	5	2	5	12	31
2	4	3	7	4	1	5	10	2	5	5	12	3	5	3	11	40
3	3	3	6	1	1	5	7	1	2	5	8	3	3	2	8	29
4	3	3	6	1	1	4	6	2	3	1	6	1	4	4	9	27
5	3	3	6	1	1	3	5	3	4	1	8	1	5	3	9	28
6	3	3	6	1	1	1	3	3	4	1	8	1	1	1	3	20
7	3	3	6	1	2	2	5	1	5	1	7	2	1	2	5	23
8	3	3	6	1	2	4	7	1	1	1	3	2	1	5	8	24
9	3	3	6	1	2	1	4	1	1	1	3	2	1	2	5	18
10	3	3	6	1	2	1	4	1	1	2	4	2	1	1	4	18
11	3	3	6	1	2	1	4	1	1	2	4	2	1	3	6	20
12	3	3	6	1	2	1	4	2	1	2	5	2	1	4	7	22
13	3	3	6	1	2	1	4	2	1	2	5	2	2	3	7	22
14	3	3	6	2	2	1	5	2	1	2	5	2	2	1	5	21
15	3	3	6	2	2	1	5	2	1	2	5	2	2	1	5	21
16	3	3	6	2	3	1	6	2	1	2	5	2	2	1	5	22
17	4	3	7	2	3	1	6	2	1	2	5	2	2	1	5	23
18	4	4	8	2	3	1	6	2	1	2	5	3	2	1	6	25
19	4	4	8	2	3	1	6	2	2	2	6	3	3	1	7	27
20	4	4	8	2	3	1	6	2	2	2	6	3	3	1	7	27
21	4	4	8	2	3	2	7	2	2	2	6	3	3	1	7	28
22	4	4	8	2	3	2	7	2	2	2	6	3	3	1	7	28
23	4	4	8	2	3	2	7	2	2	2	6	3	3	1	7	28
24	4	4	8	2	3	2	7	3	2	3	8	3	3	2	8	31
25	4	4	8	3	3	2	8	3	2	3	8	3	3	2	8	32
26	4	4	8	3	4	2	9	3	3	3	9	3	3	2	8	34
27	4	4	8	3	4	3	10	3	3	3	9	4	3	2	9	36
28	4	4	8	3	4	3	10	4	3	3	10	4	4	2	10	38
29	4	4	8	3	4	3	10	4	3	3	10	4	4	3	11	39
30	4	4	8	3	4	3	10	4	3	3	10	4	4	3	11	39
31	4	5	9	3	4	3	10	4	3	4	11	4	4	3	11	41
32	5	5	10	3	4	3	10	4	3	4	11	4	4	3	11	42
33	5	5	10	4	4	3	11	4	4	4	12	4	4	3	11	44
34	5	3	8	4	5	3	12	4	4	4	12	4	4	4	12	44
35	5	3	8	4	5	4	13	4	4	4	12	4	4	4	12	45
36	5	3	8	4	5	4	13	4	4	4	12	4	5	4	13	46
37	5	3	8	5	5	4	14	4	4	4	12	5	5	4	14	48
38	5	3	8	5	5	4	14	4	4	4	12	5	5	4	14	48
39	5	5	10	5	5	4	14	4	4	4	12	5	5	4	14	50
40	5	5	10	5	5	5	15	4	4	4	12	5	5	4	14	51
41	4	5	9	5	5	5	15	5	4	4	13	5	5	4	14	51
42	4	5	9	5	4	5	14	5	5	4	14	5	5	5	15	52
43	4	5	9	5	3	5	13	5	5	4	14	2	5	5	12	48
44	5	5	10	5	3	5	13	5	5	5	15	3	5	5	13	51
45	5	5	10	1	2	5	8	5	5	5	15	5	2	5	12	45
46	5	5	10	1	3	5	9	5	5	5	15	2	2	5	9	43
47	3	5	8	5	5	5	15	2	5	5	12	1	4	5	10	45
48	3	4	7	4	3	5	12	2	5	5	12	2	1	4	7	38
49	5	5	10	5	5	5	15	2	5	5	12	5	4	2	11	48
50	3	4	7	2	4	5	11	4	3	5	12	4	2	4	10	40
Total	**0,61**	**0,67**	**1,92**	**2,24**	**1,65**	**2,38**	**12,94**	**1,65**	**2,14**	**1,73**	**12,30**	**1,52**	**1,92**	**2,01**	**9,59**	**113,83**

Anexo 8. Alfa de Cronbach de dimensiones de la entrevista

Alfa Dimensión 1	
k	2
k-1	1
A=k/k-1	2,000
Suma Vi	1,278
Vt	1,922
Suma Vi/Vt	0,665
B	0,335
Alfa D1	**0,670**

Alfa Dimensión 2	
k	3
k-1	2
A=k/k-1	1,500
Suma Vi	6,274
Vt	12,936
Suma Vi/Vt	0,485
B	0,515
Alfa D2	**0,773**

Alfa Dimensión 3	
k	3
k-1	2
A=k/k-1	1,500
Suma Vi	5,520
Vt	12,300
Suma Vi/Vt	0,449
B	0,551
Alfa D3	**0,827**

Alfa Dimensión 4	
k	3
k-1	2
A=k/k-1	1,500
Suma Vi	5,451
Vt	9,588
Suma Vi/Vt	0,569
B	0,431
Alfa D4	**0,647**

Alfa General	
k	11
k-1	10
A=k/k-1	1,100
Suma Vi	18,522
Vt	113,828
Suma Vi/Vt	0,163
B	0,837
Alfa General	**0,921**