UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS

CARRERA DE CONTADURÍA PÚBLICA E INGENIERÍA EN CONTABILIDAD Y AUDITORÍA

TÍTULO:

EVALUACIÓN DE LA AUDITORIA EN SISTEMAS DE INFORMACIÓN COMO MÉTODO DE PREVENCIÓN DEL FRAUDE EN EL SECTOR DE TELECOMUNICACIONES.

AUTORAS:

Ocampo Gómez, Valeria Ivonne

Piguave Tigua, Zully Esthefani

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN CONTABILIDAD Y AUDITORÍA

TUTOR:

Ing. Delgado Loor, Fabián Andrés, M.B.A.

GUAYAQUIL, ECUADOR

19 de marzo del 2019

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

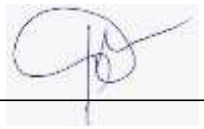
FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS

CARRERA DE CONTADURÍA PÚBLICA E INGENIERÍA EN CONTABILIDAD Y AUDITORÍA

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por: Ocampo Gómez, Valeria Ivonne, y Piguave Tigua, Zully Esthefani, como requerimiento parcial para la obtención del Título de: Ingeniera en Contabilidad y Auditoría.

TUTOR (A)

f. 

Ing. Delgado Loor, Fabián Andrés, M.B.A.

DIRECTOR DE LA CARRERA

f. _____

CPA. Vera Salas, Laura Guadalupe, Ph. D. (c)

Guayaquil, 19 de marzo del 2019

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS

CARRERA DE CONTADURÍA PÚBLICA E INGENIERÍA EN CONTABILIDAD Y AUDITORÍA

DECLARACIÓN DE RESPONSABILIDAD

Nosotras, Ocampo Gómez Valeria Ivonne y Piguave Tigua Zully Esthefani

DECLARAMOS QUE:

El Trabajo de Titulación "**Evaluación de la auditoria en sistemas de información como método de prevención del fraude en el sector de Telecomunicaciones**" previa a la obtención del Título de: Ingeniera en Contabilidad y Auditoría, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de nuestra total autoría.

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

Guayaquil, 19 de marzo del 2019

LOS AUTORES

f. _____ f. _____

Ocampo Gómez Valeria Ivonne Piguave Tigua, Zully Esthefani

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS
CARRERA DE CONTADURÍA PÚBLICA E INGENIERÍA EN CONTABILIDAD Y AUDITORÍA

AUTORIZACIÓN

Nosotras, Ocampo Gómez Valeria Ivonne y Piguave Tigua Zully Esthefani

Autorizamos a la Universidad Católica de Santiago de Guayaquil, la publicación en la biblioteca de la institución del Trabajo de Titulación: "Evaluación de la auditoria en sistemas de información como método de prevención del fraude en el sector de Telecomunicaciones", cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y total autoría.

Guayaquil, 19 de marzo del 2019

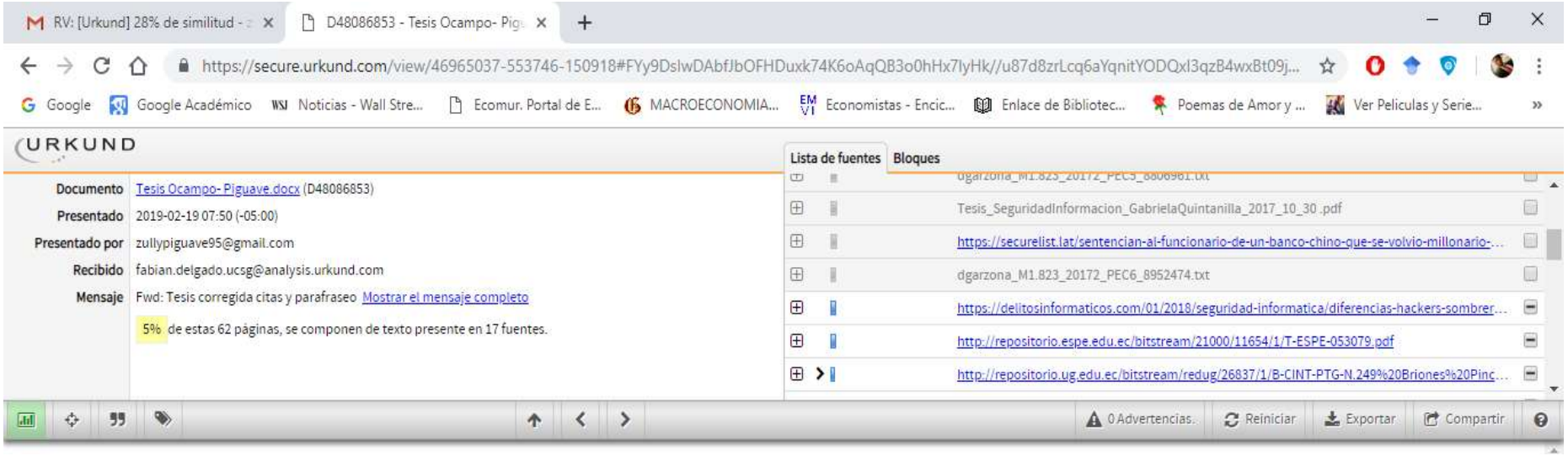
LOS AUTORES

f. _____ f. _____

Ocampo Gómez Valeria Ivonne Piguave Tigua, Zully Esthefani

REPORTE URKUND

https://secure.urkund.com/view/46965037-553746-150918#FdC7TsNAFIThd0m9QvbOXnkVRIEiQCIIkxLx7nwpRl6f+b0zPr+Xn8fl9e0oZzmPpxoNmuU8vc9O3ucq56rkuY9SDzp3qbVRp0GTFpnHPOYxj3nMY958104yb+bduWM7Vk5dzuv5xO9dIidHL9ElZ6VQo+ds0KRF2IqtuIqruDjHWZfoEl2iS3SJLtEluqRhGr7hGk636JaGa7iO0zMd13H6pvM7v/MHf/AHb/CGO4Y7BmZgBmbyp+8nZmLsNf43E2O3mZjlnoWz5yycXWTh7COLb+/Z/M3fKa34Af1V11whfdTRRhE91NBCgXkU8ZKFyhQnTZgsUZKEyFiz2Lqg3cruZY/3cnncvu+3r9v14379vLweL3WsUdcx9kzvM/PvHw==



TUTOR

f. _____

Ing. Delgado Loor, Fabián Andrés, M.B.A.

AGRADECIMIENTO

Por la vida que me has permitido, te agradezco Dios. José Piguave Arteaga y Patricia Tigua Pincay, por la constancia y amor que me han entregado a mí, les agradezco papá y mamá.

El cariño y apoyo que jamás permitieron que me faltara les doy eternamente las gracias a mis hermanas María José y Allison.

A los docentes que forjaron todo este camino lleno de enseñanza y sabiduría para los desafíos profesionales y cotidianos, estoy lista para poner cada consejo en marcha.

Con el pasar de los años y a pesar de la distancia siempre ha estado en cada momento bueno y malo; mi mejor amigo, José Burgos Rangel. A él, por cada adversidad que me enseño y la fortaleza que me demostró que puedo tener. Tampoco puedo dejar de lado a cada verdadera amistad que obtuve en este proceso y todos los buenos momentos vividos, gracias por cada memoria.

Al equipo que armamos para hacer posible esto; mi tutor Ing. Fabián Delgado por cada observación y corrección para un trabajo correcto, y a mi compañera y próxima colega Valeria Ocampo Gómez, por muchos años más de amistad y recuerdos de esta etapa.

Zully Esthefani Piguave Tigua

AGRADECIMIENTO

Dios, gracias por la iluminación y esfuerzo derramado en mí. Agradezco a mi Familia, a mis hermanos. A ustedes papá y mamá por darme este futuro, por estar presente en esta etapa tan importante ofreciéndome y buscando lo mejor para mí. Este logro también es suyo.

No cesan mis ganas de decirte a ti Tyrone que esta meta está cumplida agradeciéndote por ser un pilar fundamental en la culminación de mi carrera.

A mi compañera y futura colega Zully Piguave por su paciencia y apoyo incondicional, agradecida contigo por haber podido realizar y culminar este proyecto juntas.

Valeria Ivonne Ocampo Gómez

DEDICATORIA

El presente trabajo de titulación se lo dedico a mi familia, a mi papá por demostrarme y enseñarme que todo lo que quiero y deseo puede ser posible y que la perseverancia es solo una palabra cuando existe fuerza, voluntad y ganas; a mi mamá, por cada consejo y cada cuidado, por jamás dejarme sola. A mis hermanas; María José, por tu comprensión y alegría constante y a la más pequeña, Allison, porque siempre serás mi orgullo y el motor para lograr todo.

Zully Esthefani Piguave Tigua

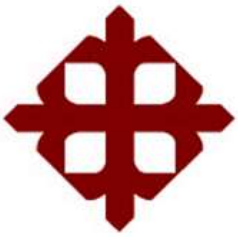
DEDICATORIA

Dedico con todo mi amor y cariño a mis Padres Carlos Ocampo y Gilda Gómez por su sacrificio y esfuerzo, por ser mi inspiración y creer en mi capacidad mostrándome el camino a la superación.

A Tyrone Serrano por ser mi fuente de motivación quien con sus palabras de aliento no me dejaba decaer para que siguiera adelante y siempre sea perseverante y crea en mis ideales.

A mis hermanos Verónica, Carlos y Carlina por el apoyo brindado día a día en el transcurso de cada año de mi Carrera Universitaria.

Valeria Ivonne Ocampo Gómez



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS

CARRERA DE CONTADURÍA PÚBLICA E INGENERÍA EN CONTABILIDAD Y AUDITORÍA

TRIBUNAL DE SUSTENTACIÓN

f. _____

CPA. Vera Salas, Laura Guadalupe MSc.

DIRECTORA DE CARRERA

f. _____

CPA. Jurado Reyes Pedro Omar, MSc. ©

COORDINADOR DEL ÁREA

f. _____

CPA. Rodríguez Samaniego José Antonio, MSc

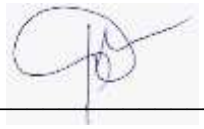
OPONENTE

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS

CARRERA DE CONTADURÍA PÚBLICA E INGENERÍA EN CONTABILIDAD Y AUDITORÍA

CALIFICACIÓN

f. 

Ing. Delgado Loor, Fabián Andrés, MSc
TUTOR

Índice General

Índice de Tablas

Índice de Figuras

RESUMEN

"EVALUACIÓN DE LA AUDITORIA EN SISTEMAS DE INFORMACIÓN COMO MÉTODO DE PREVENCIÓN DEL FRAUDE EN EL SECTOR DE TELECOMUNICACIONES"

En la tesis previa a titulación se estudia la evaluación de la auditoria en sistemas de información, relacionada con las empresas de telecomunicaciones enfocándose en el área de auditoria y la relación que mantiene con el entorno de control tecnológico debido a que dentro de este marco se han detectado problemas que involucran fraudes. A través de la investigación se plantea como meta para el problema inmerso en la auditoria alcanzar la prevención de los delitos ocurridos utilizando de esta manera la evaluación como método a beneficio de futuros casos. El trabajo es realizado bajo la técnica denominada entrevista, dirigida al punto clave del departamento de sistemas de una compañía de telecomunicaciones nacional quien impulsa la búsqueda y análisis de los designados, hackers, crackers y sus derivados siendo estos los usualmente más implicados en los procesos de flaqueo que afectan la auditoria. Considerando la ley de telecomunicación y las regulaciones de ARCOTEL para el correcto proceso analítico de manifiestos y resoluciones que se presentan como ejemplos de los varios agravios del país con referente a los delitos de telecomunicación. Siendo las descripciones de los conceptos, leyes, ejemplos y posturas de autores empleadas de una manera detallada, clara y técnica para facilitar la compresión del método sin desvanecer el foco que presenta cada uno.

Palabras claves: entrevista, hackers, crackers, ARCOTEL, ley de telecomunicación, delito.

Introducción

Formulación del Problema

Desde que el desarrollo tecnológico empezó a manifestarse en la historia de la humanidad, así mismo:

Como parte de los antecedentes nacionales se cita al autor Llangarí Salazar (2016) quien establece en su tesis de grado previo a la obtención del título de Ingeniero en electrónica, redes y comunicación el tema "Análisis de los delitos informáticos y de telecomunicaciones en el Ecuador bajo las nuevas normas jurídicas", mismo que estableció en su investigación como objetivo general: analizar la legislación ecuatoriana relacionada al sector o sectores regulados por las telecomunicaciones; además determinó que los delitos informático y de telecomunicaciones son consideradas como base de interpretaciones, permitiendo establecer comparaciones en las normativas jurídicas que se encuentran establecidas en el país. Además, el autor aplicó la investigación relacionada con las clases de delitos existentes en el ámbito tecnológico y lo tipificado en las leyes vigentes a la fecha en Ecuador, específicamente en el Código Orgánico Integral Penal (COIP) difundido en febrero de 2014 y la Ley Orgánica de Telecomunicaciones (LOT) difundida en febrero de 2015. Por último, como propuesta hubo un planteamiento de procedimientos para garantizar seguridad en entornos de información y comunicación de las instituciones.

Además, Ing.Pulgar Haro (2018) en su trabajo de investigación de la maestría de ingeniería informática empresarial establece el tema: "Auditoría informática y la calidad del servicio de las tecnologías de la información en el distrito de educación 06d04 Colta – Guamote", misma que tuvo como objetivo general: Realizar una Auditoría Informática, para que en base a ella se logre el mejoramiento del servicio de las Tecnologías de la Información en el Distrito de Educación 06D04 Colta – Guamote; por otra parte estableció que el problema relacionado con la calidad del servicio que se da en el distrito se relaciona a la calidad de servicio al usuario, lo que viene proporcionada esencialmente por la

continuidad en el funcionamiento de las tecnologías de información que apoyan los diferentes procesos operativos. Según el estudio dio como resultados sobresalientes, determinar la existencia de la desorganización, asimismo que los equipos se encuentran semi-obsoletos, en cuanto a la conectividad que esta tiene interrupciones y también la inexistencia de una conveniente diligencia administrativa. Por último la recomendación que describe el autor es relacionada a establecer controles aplicados en los procesos, la finalidad es aumentar los estándares en la calidad de los servicios ofrecidos a los usuarios dentro del objeto de estudio y fuera de él, sin exclusión ninguna.

En el artículo presentado en la revista de investigación jurídica por los autores Trejo. M.D.C, Domenech Alvarez, & Ortìz Chimbo. Msc (2015) establecieron como resumen en el tema "La seguridad jurídica frente a los delitos informáticos" el siguiente resumen: el problema de los delitos informáticos que pueden ser considerados como crímenes electrónicos, tan graves que pueden llegar a ser un genérico problema para el avance de la informática. Sin embargo, este puede tener consigo delitos tan graves como el robo, falsificación de documentos, fraudes, chantajes y malversación de caudales públicos.

El Ingeniero Lascano Laica (2016) en su trabajo de investigación como requisito previo a la obtención del título de Magister en informática empresarial definió el tema: "Auditoria informática para mejorar la gestión de las tecnologías de la información en el ministerio del trabajo regional Ambato", mismo que estableció a la auditoría informática que se presentaba durante el estudio permitían establecer como resultado la situación que muestra el equipo tecnológico. Asimismo, el Cobit aplicado como método evaluativo permitió obtener resultados del conjunto de los activos relacionados con el proceso de información. Finalmente se puede definir a la auditoría informática como una medida preventiva para aquellos instrumentos del conjunto físicos (hardware), programas (software) y, por último, sin embargo, no menos importante, la parte lógica, mismos que conjuntamente realizan todos los procesos de la información.

Valencia Duque (2015) planteó como objetivo general: Construir un modelo de Auditoría Continua en el contexto del Control Fiscal Colombiano, acorde a la realidad tecnológica del sector gubernamental, a partir del análisis y cohesión de las relaciones existentes entre los conceptos, paradigmas, estándares, metodologías y prácticas de Auditoría Continua, divulgados por la comunidad científica y profesional, además de establecer como resumen que la Auditoría continua es una tecnología emergente, la cual está basada en Tecnologías de Información y Comunicaciones; y que puede aportar al menos parcialmente, a la problemática que viene aquejando al Control Fiscal Colombiano desde hace varios años. En el cumplimiento de este objetivo y en el marco del control gubernamental, se realiza un profundo análisis bibliográfico, del uso de las Tecnologías de Información, en control y auditoría; como preámbulo al estado del arte de la Auditoría Continua y a los principales modelos existentes, que permiten construir a partir de una propuesta taxonómica y un esquema de homogeneización, un meta modelo, que articulado con las guías de auditoría gubernamental existentes en Colombia.

Se conoce como Tecnología de información y comunicación (TIC) a la utilización de técnicas en computadoras y ordenadores electrónicos para el manejo y procesamiento de información, específicamente la captura, transformación, almacenamiento, protección, y recuperación de datos e investigación. Los orígenes de la TIC son recientes; aunque el nombre de Tecnología de la Información se inicia en la década de 1970. (Acosta Chávez & Navarrete, 2013)

Su utilización en los negocios se remonta a mediados del siglo XX, durante la segunda guerra mundial; sin embargo, es en los últimos 20 años donde alcanza niveles de uso y aplicaciones tan variadas, que se ha convertido en un área de gran amplitud e impacto en todos los aspectos de la vida cotidiana, incluyendo la gerencia de cualquier empresa, en la cual hoy en día es casi indispensable. (Acosta Chávez & Navarrete, 2013)

Planteamiento del problema

El sector de telecomunicaciones debe cumplir con medidas de seguridad que protejan la información debido al aumento de delitos informáticos propios de la era tecnológica, misma que permite realizar con ayuda de los avances y evolución que actualmente existe. El hackeo definido por la Real Lengua Española de la RAE, (2018) define como el "acceder sin autorización a computadoras, redes o sistemas informáticos, o a sus datos", esto ha provocado que, mediante el robo de información como contraseñas, cuentas bancarias y número de identificación, entre otros tipos de información ocasionara que empresas a nivel mundial sean perjudicadas con millones de dólares.

Entre los delitos informáticos más conocido se encuentra: sabotaje informático y piratería informática, en este último se encuentran el hurto de máquinas y apropiación de software, y phreaking. Trejo. M.D.C, Domenech Alvarez, & Ortìz Chimbo. Msc, (2015) afirman que la criminalidad que existe es cada vez mayor permitiendo realizar delitos entre los cuales se encuentra el robo, usurpación de identidad, chantaje, apropiación de software; y "con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados". (p.43)

Ecuador, así como otros países ha sufrido de delitos informáticos de "Transferencia ilícita de dinero, apropiación fraudulenta de datos personales, interceptación ilegal de datos, pornografía infantil, acoso sexual, entre otros" según por Trejo. (M.D.C et all, 2015, p. 46), por ello la seguridad en la navegación que ofrece el sector de las telecomunicaciones juega un papel importante.

Uno de los hechos de especial trascendencia fue el hackeo al sistema de la Agencia Nacional de Transito, la cual represento un perjuicio económico al Estado por más de $ 1,2 millones. La ANT confirmó que su sistema informático fue vulnerado por el ingreso de 99 usuarios externos, quienes otorgaron ilegalmente 15.970 licencias de conducir tipo A, B, C, D, E, F y G. Además, modificaron 14.583 multas por infracciones y devolvieron 26.801 puntos a conductores que violentaron

la ley. Todo esto a través de programas y usuarios no autorizados. Incluso, lo hicieron fuera de horario laboral. Esa tarea ilegal movió más de $ 1’250.000. (Diario El Mercurio, 2018)

Es recién en 2015 que se receptaron denuncias sobre hackeos de páginas o sistemas informáticos de los bancos, por parte de clientes a quienes les debitaron o sustrajeron dineros de sus cuentas. Eso obligó a las entidades crediticias a actuar y tecnificar más sus sistemas de protección informática. De acuerdo a datos de la Fiscalía, en 2017 se presentaron 235 denuncias sobre delitos informáticos, mientras que en el año 2018 hubo 42. El delito informático está actualmente tipificado en el Código Orgánico Integral Penal (COIP). El artículo 232 establece penas de tres a cinco años de prisión para quien sea hallado culpable. (Diario El Mercurio, 2018)

Formulación del problema

Con base en los antecedentes y el planteamiento del problema antes expuesto y pese a contar con herramientas asociadas a la auditoria de sistemas informáticos y entornos tecnológicos, en la actualidad no se cuenta con un estudio que determine en qué medida un factor se encuentra asociado al otro. Por lo que se plantea para el siguiente trabaja la formulación del problema a continuación:

¿En qué medida se relacionan los esquemas de una auditoria de sistemas y el entorno de control tecnológico orientado a la prevención y detección de fraudes en el sector de telecomunicaciones?

Sistematización del problema

Sin embargo, para sistematizar la formulación general y dividirla en segmentos que puedan ser tratados mediante un objetivo de investigación diferente para cada uno, se han formulado las siguientes preguntas de sistematización:

1. ¿Cuáles son los esquemas generales de auditoria y los esquemas específicos de auditoria de sistemas que conciernen a la presente investigación?

2. ¿Qué aspectos relevantes se encuentran asociados al riesgo de fraude en los sistemas informáticos de las empresas de telecomunicaciones?
3. ¿Qué información estadística y de que fuentes primarias se puede realizar análisis acerca de la incidencia de la auditoria informática en entornos tecnológicos de telecomunicaciones?
4. ¿Cuál es el nivel de relación que existe entre la auditoria de sistemas y el entorno de control tecnológico en compañía perteneciente al sector de las telecomunicaciones en Guayaquil?

Justificación

El internet se ha convertido en la base fundamental para la realización de diversos procesos en la sociedad actual, basada en la continua evolución de la tecnología, el sector de telecomunicaciones se ha visto en la necesidad de tener medidas de seguridad informática, misma que puede ser evaluada por medio de la auditoría especializada en "sistemas de información", conocida también como auditoría informática. Debido a las necesidades existentes de establecer una investigación relacionada entre la auditoría en sistemas informáticos y el sector de telecomunicaciones se realiza la presente investigación. El ingeniero Pulgar Haro (2018) afirma lo siguiente:

La auditoría informática es realizada mediante procesos, estos tienen la finalidad de aplicar controles adecuados, los mismos que buscan disminuir su vulnerabilidad. La finalidad es cumplir la entrega de servicios eficientes y con alto nivel de seguridad tecnológica, esto conlleva a cualquier empresa sin distinción del tipo, a mejorar el posicionamiento y acreditación en los procesos, y finalmente lograr el cumplimiento de la visión planteada. (p. 14)

Basada en la cita se puede establecer que la necesidad existente en el sector de telecomunicaciones de cumplir con la seguridad en la información que maneja. Por otra parte, se establece que el objetivo principal de la auditoría informática es ofrecer controles adecuados debido a la vulnerabilidad en las redes, además de la

carencia de conocimiento de los usuarios y nuevas modalidades que representan aumento de riesgos en los servicios que ofrece este sector.

Objetivo General y Específico

Objetivo General

Determinar el nivel de relación entre los esquemas de una auditoria de sistemas y el entorno de control tecnológico orientado a la prevención y detección de fraudes en el sector de telecomunicaciones.

Objetivos Específicos

- Investigar los esquemas generales de auditoria y específicos de auditoria de sistemas.
- Determinar los aspectos relevantes asociados al riesgo de fraude en los sistemas informáticos de las empresas de telecomunicaciones.
- Recopilar información estadística y de fuentes primarias acerca de la incidencia de la auditoria informática en entornos tecnológicos de telecomunicaciones.
- Validar el nivel de relación que existe entre la auditoria de sistemas y el entorno de control tecnológico en compañía perteneciente al sector de las telecomunicaciones en Guayaquil.

Delimitación

Como delimitaciones de la investigación se establece:

Campo: Administración

Área: Auditoría

Tema: Evaluación de la auditoria en sistemas de información como método de prevención del fraude en el sector de Telecomunicaciones

Geografía: Guayas - Guayaquil

Tiempo de investigación: 5 meses

La investigación será realizada en el campo científico de la administración. En el proceso investigativo se recopilarán datos basados en un diseño no experimental. Mediante el mismo se logrará contar con información asociada a los niveles de control en entornos tecnológicos de compañías cuyo giro de negocio se encuentre en el campo de las telecomunicaciones. No existirá un modelo especifico a seguir por lo que previamente se diseñará una herramienta y gran parte de la recopilación de datos obedecerá a un proceso empírico de observación y comparación.

Del mismo modo, se establece como lugar de la investigación aquellas empresas que ofrecen servicios de telecomunicaciones ubicadas en la ciudad de Guayaquil, provincia del Guayas. Finalmente, el tiempo establecido para cumplir con el trabajo investigativo es de 5 meses, siendo establecido por la universidad de acuerdo al cronograma.

Hipótesis

La hipótesis que se presenta en el trabajo de investigación planteado es la siguiente:

La estructuración y desarrollo sistémico de una auditoria de sistemas informáticos, influirá significativamente en el entorno de control y la prevención de fraudes de una compañía del sector de Telecomunicaciones.

Variables

Variable Independiente:

Auditoria de sistemas informáticos

Variable Dependiente:

Entorno de control tecnológico

Capítulo 1: Marco Teórico

Antecedentes de las telecomunicaciones

Historia del sector de telecomunicaciones

Cada vez más las teorías del cambio tecnológico están centrando sus esfuerzos en entender el acoplamiento de las máquinas técnicas con las mega máquinas sociales. Autores pioneros como Marx, Gordon Childe o Mumford ya eran conscientes de esta necesidad. Si dicha conciencia se ha agudizado en los últimos años, ello obedece en buena medida a la insuficiencia de los modelos lineales de explicación a los que esos mismos autores (y otros) apelaron. La articulación de un análisis transversal con otro multilineal y de un punto de vista diacrónico con otro sincrónico (tal como la hemos visto realizada en la propuesta de Serres) revela que los sistemas tecnológicos funcionan como redes complejas, las cuales abarcan elementos procedentes de distintos tipos de tecnología y están articuladas a entornos sociales y naturales con los que guardan múltiples relaciones de retroalimentación. (Ordóñez, 2007, págs. 187 - 210)

La historia de las telecomunicaciones es importante, siendo básica para establecer el conocimiento de los orígenes y saber el proceso que permitió la transformación de un sector que forma parte de la evolución de las formas actuales en que se comunica la sociedad en general, es gracias a esto que se puede establecer una idea dentro del Ecuador y a nivel mundial, sin embargo, el enfoque que se dará a la investigación es prioritario dentro del territorio nacional.

Telecomunicaciones, una palabra de gran significado e importancia en el desarrollo y evolución de los pueblos. Para su apropiada comprensión es necesario una visión retrospectiva desde sus orígenes y un recorrido por cada una de las fases que marcaron hitos históricos, transformaron la vida del hombre y protagonizaron el inicio de nuevas eras a nivel mundial. (Jurado Zevallos, Núñez Sánchez, Cordeor Iñiguez, Uyaguari Uyaguari, & Regladao Iglesias, 2014, pág. 5)

La tecnología y la comunicación como complementos ideales en la socialización surge a inicios de los años 70, momento en que inicia la época digital

originado por la evolución de la electrónica y la informática. En un momento de la década de los 70 llegaron a pensar que la televisión sería insuperable en cuanto a la tecnología, situación que ocurrió en aquel momento de la historia, sin embargo, los ordenadores, el teléfono en conjunto con la televisión conformaron las Tecnologías de la Información y la comunicación, llamadas por sus siglas como las TIC.

Las TIC constantemente evolucionan, basados en la necesidad creciente del ser humano de comunicarse y acortar distancias, sin embargo, esto genera que vaya en aumento y ocurra por medio de la era digital la diferenciación de generaciones.

En un plano más epistemológico y con el propósito de examinar la relación entre las TIC y la nueva sociedad que emerge a raíz de su influencia, en "Comunicación y TIC: de la masa a la red, un cambio de paradigma" Martínez pone al descubierto la evolución de una conciencia social que en el ámbito educativo también está permeando. (Herrera Jiménez, 2015, pág. 3)

Se puede establecer una breve descripción de la evolución de la telefonía en los años setenta, misma que será descrita a continuación:

Tabla 1 **Hechos asociados a las telecomunicaciones en Ecuador**

Año	Evento
1972	Surgió la empresa de telecomunicaciones pública Norte y Sur, apareció la radio como consecuencia de la instalación de cables, propiedad del Estado. Además, Expidió el General Guillermo Rodriguez Lara la primera ley de telecomunicaciones y se creó el Instituto de Telecomunicaciones (IETEL), de este surgió la Dirección Nacional de Frecuencias . Este último tenía las funciones de administrador. Además, en este gobierno surgieron los primeros organismos de control de telecomunicaciones estatal, también fueron eventos retrospectivos importantes dentro del Ecuador.
1972	IETEL generó 1,87 líneas por un total de 100 habitantes, además de emitir 120.542 líneas telefónicas.
1973	Se crea la central telefónica llamada Portete, misma que permitía la emisión de 10.000 líneas.
1974	Se creó la central en el Guasmo misma que permitió la creación de 20.000 líneas. Además, se aplicó los dígitos para comunicarse por regiones, la Sierra tenía el dígito 02 y en la Costa se asignó el 04.
1974	IETEL aumentó la inversión en las ciudades principales del país: Guayaquil y Quito. Se estableció que la zona rural fue un sector que no fue atendido en recibir servicios de telecomunicaciones.
1977	Nació el uso de telefax facilitando el uso de comunicación a nivel regional
1977	Entró en funcionamiento la red Nacional de Télex-Gentex con 700 abonados en Quito y Guayaquil, y 245 en el resto del país; implementación que se realizó junto con la

internacional Siemens, y que incluía una central nodal en Quito, otra en Guayaquil y la central internacional en Quito, las cuales se encontraban comunicadas de manera automática.

Fuente: (Jurado Zevallos et all, 2014, pág. 114)

Ilustración 1 **Equipo de Télex T1200 marca SIEMENS**

Nota. Tomado de (Jurado Zevallos et all , 2014, p. 114)

Se pudo establecer que los años 70 fueron significativos para el sector de las telecomunicaciones, misma que permitió lograr la tecnología que actualmente existe en el Ecuador. Por otra parte, los servicios tecnológicos se encuentran estrechamente relacionados a las telecomunicaciones, se establece dentro del territorio ecuatoriano que el inicio de las empresas que fueron precursores y oferentes de servicios de telecomunicaciones inició en el año 1.993, la empresa Power actualmente conocida como "Claro" puso en marcha sus actividades, luego en el año 1997 ingresó en el mercado la empresa Bellsouth, actualmente conocida como Movistar.

Del mismo modo, Alegro surgió como tercera empresa de servicios de telecomunicaciones, comenzando su operatividad en el año 2003, sin embargo esta tenia poca participación dentro del mercado lo que consecuentemente ponía en riesgo

la continuidad de sus operaciones, a pesar de ofrecer sus servicios a un precio menor que el de sus competidores directos. La empresa Alegro pasó a ser administrada y financiada con fondos del estado, convirtiendola en Corporación Nacional de Telecomunicaciones conocida por sus siglas CNT.

Dentro de los servicios de telecomunicaciones más relevantes que ofrecen a sus usuarios a nivel nacional se encontraban servicios de voz, mensajería de texto y datos para conectividad a internet. A partir del año 2000 Claro tenia el mayor posicionamiento del mercado, seguido por Movistar y finalmente CNT.

Sin duda la tecnología se ve asociada a todos los campos de conocimiento, reflejando un mayor efecto en unos con relación a otros; sin embargo, con el avance y transcendencia de los dispositivos tecnológicos, la especificación es cada vez mayor. Por otra parte, es importante que se establezca la relación de la tecnología desde sus inicios hasta tiempos actuales, estableciendo análisis de la función de las telecomunicaciones con la sociedad actual desde distintas perspectivas. (Herrera Jiménez, 2015, pág. 3)

Asimismo, se estableció que el crecimiento de la tecnología y su evolución gracias a la facilidad que los equipos celulares tenian como caracteristica de permitir el acceso a servicios de internet de manera fácil y ágil como: medios que complementan y fomentan la educación, transacciones on line, trabajos realizados con uso de internet o simplemente compartir eventos importantes con la ayuda de las redes sociales, esto hizo emerger una mayor demanda para cubrir la necesidad del incremento de usuarios de servicios de telecomunicaciones. La Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), (2015) afirmó en su bolentín anual:

(…) las tendencias de uso de tecnologías, accesibilidad y relevancia para potenciales usuarios, crecimiento de número de dispositivos conectados e incremento del número de usuarios de Internet (…) y las conexiones físicas ha crecido de manera exponencial entre 2001 y 2015 a niveles que superan el 300%. (p. 9).

Al igual que el aumento del beneficio de la tecnología, también la utilización de la cantidad de información que se comparte con la ayuda del internet, de acuerdo con los estudios de ARCOTEL afirma que:

"La tendencia de crecimientos de las conexiones móviles que se aplicarán igualmente a la cantidad de conexiones orientadas a lo que se ha denominado Internet de las cosas, que esencialmente es la comunicación entre dispositivos electrónicos para transmitir información crítica a través de la nube de Internet, con el fin de que varias aplicaciones puedan ser monitoreadas remotamente". (p. 9)

Considerando lo anterior, se puede evidenciar que la información es compartida a través de servicios de telecomunicaciones y la importancia en la seguridad e integridad es primordial en las empresas que se dedican a manejar gran cantidad de información.

Por otra parte el uso de conexiones fijas en Ecuador ha tenido un incremento de +396% desde el año 2001 al 2015, esto representado en la siguiente figura:

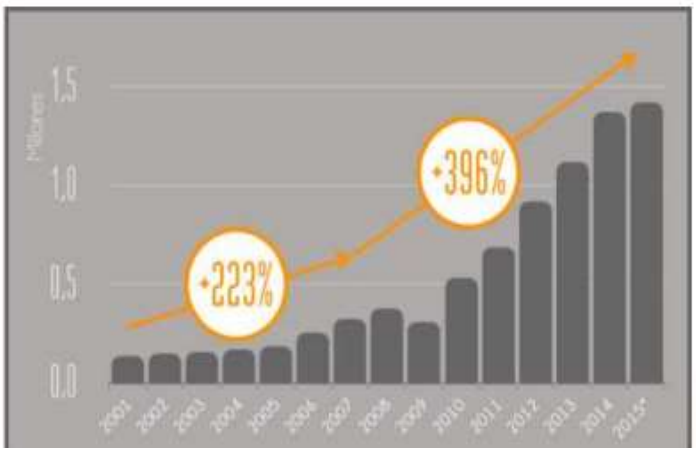


Figura 1. **Crecimiento de uso de conexiones fijas**

Nota: ***Tomado de*** (Agencia de Regulación y Control de las Telecomunicaciones, 2015)

Entre las empresas que conforman el sector de telecomunicaciones que están establecidas en el mercado se encuentran: CNT, CONECEL (Claro), OTECEL (Movistar), SURATEL, ECUADORTELECOM, MEGADATOS, ETAPA EP, PUNTONET S.A., entre otras. Los múltiples beneficios que ofrece este sector han generado que las cifras vayan en aumento al transcurrir los años, hasta la actualidad ARCOTEL establece la siguiente información sobre el número de usuarios:

Tabla 2 **Servicios de telecomunicaciones en Ecuador**

Detalle	**Número**
Líneas activas de telefonía celular	114.497
Cuentas de internet móvil	194.528
Líneas de telefonía fija	379.768
Marcas-modelos de equipos para el Servicio Móvil Avanzado están homologados (verificados), por ARCOTEL	777

Nota. *Tomado de* (ARCOTEL , 2018)

Además, el Instituto Nacional de Estadísticas y Censos (INEC) realizó un estudio sobre la tenencia y uso de la información y comunicación, estableciendo un crecimiento significativo en el año 2016 afirmando que 56 de cada 100 ecuatorianos tenían un equipo celular, comparado con cinco años atrás existe un crecimiento de 6 personas. En la siguiente figura se puede establecer la relación de la tenencia del uso del celular:

Figura 2 **Tenencia de celular año 2016**

Nota. Citado por (ARCOTEL, 2018). **Fuente:** INEC 2016

Basada en la importancia de la información y los avances tecnológicos de acuerdo a las afirmaciones anteriores se evidencia que los servicios que ofrecen las empresas de telecomunicaciones son fundamentales en la vida cotidiana actualmente, esto hace que este sector sea objeto de actos de delitos informáticos.

Si bien es cierto la tecnología actualmente constituye una de las herramientas indispensables en la automatización de procesos, pero por otro lado facilita la realización de fraudes mediante el uso de la información, causando que existan cuantiosas pérdidas económicas sin que sea fácil de detectar e identificar el responsable. Es por ello que los niveles de seguridad informática en relación al hardware y software son una prioridad que debe cumplir el sector de telecomunicaciones. Desde establecer medidas para reducir el riesgo de cometimiento de delitos informáticos hasta aplicar medidas de seguridad como: personal autorizado, contar con terminales de telecomunicaciones, ordenadores y programas que protejan eficientemente la información.

Características de las empresas de Telecomunicaciones

La comunicación surgió debido al uso de implementos tecnológicos, misma que basada en la necesidad de comunicarse de forma fácil, ágil y rápida dentro de la vida del ser humano, además del empresarial. La globalización dio origen a las

empresas dedicadas a ofrecen servicios de telecomunicaciones, sin embargo, la base de los cambios continuos presentes en la era tecnológica hizo que surgiera el activo más importante, la información, asimismo se convirtió en el soporte de la continuidad en los procesos y procedimientos de las empresas, independiente de la actividad económica a la que se dedique.

A continuación, y para ejemplificar y conocer un poco más la estructura organizacional de las empresas de telecomunicaciones, se tomará como punto de referencia una de las compañías más destacadas del sector con presencia en la ciudad de Guayaquil, dicha empresa es CONECEL S.A. CLARO cuyas actividades le son de mucha familiaridad a toda la población. Para ello se analizará en primera instancia su organigrama.

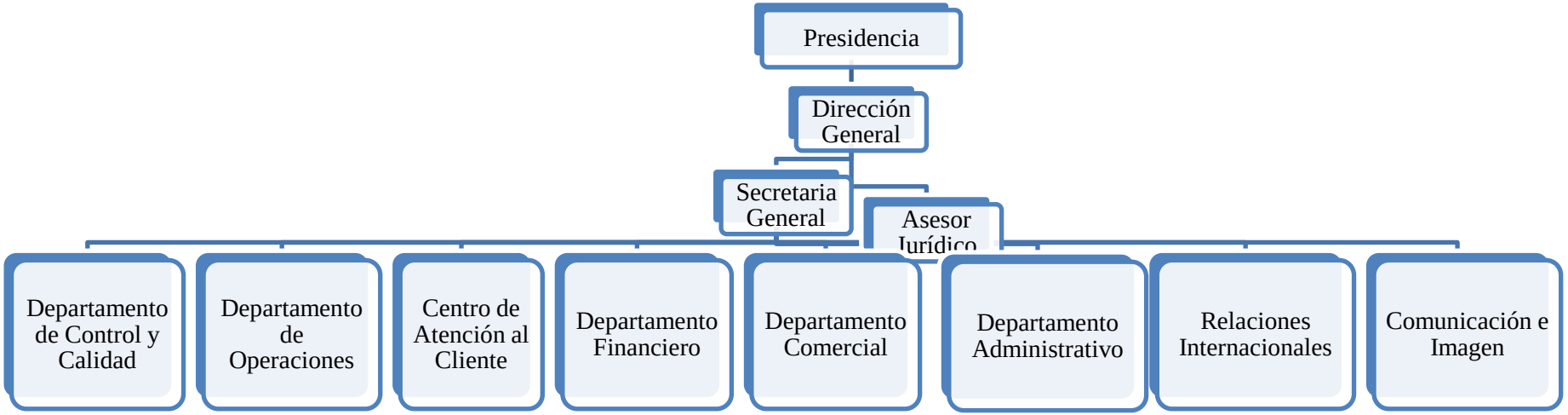


Figura 3. Organigrama de la compañía CONECEL S.A.

Entre los principales cargos y áreas de la compañía se muestran los siguientes:

Presidencia. Su cargo está entre los más altos de la organización y entre sus principales funciones están la de dirigir y controlar el funcionamiento de la compañía, tanto de matriz como de sucursales. Representar a la compañía en las negociaciones surgidas con terceros en relación al objeto de la sociedad. Dirección General. El gerente general es el responsable de la definición de la estrategia de la empresa en la región o país, el uso y fuentes de recursos de la compañía. Da seguimiento a la estrategia de la compañía y a la forma de ejecutar cada una de las fases de la misma. Secretaria General. Encargada de la toma fiel de actas de acuerdos, resoluciones, comunicaciones, mantención y conservación del archivo y todo aquello que se refiera con la preservación de documentos legales de alta importancia para la compañía tanto en su custodia como acceso y difusión. (Valbuena Quebrada, 2016)

Por otra parte, la auditoría en sistema tiene la función de realizar evaluaciones relacionadas a los controles de seguridad para la información, establecidos por medio de mecanismos de seguridad, personal autorizados y demás herramientas y procesos que tienen como objetivo principal el proteger la información. La auditoría en sistemas de información debe cumplir con otro objetivo primordial, como medida de seguridad desde el ámbito legal, detectar y prevenir fraudes mediante uso de la información, aplicando métodos que establecen evaluación de riesgos y lograr reducirlos al mínimo.

Del mismo modo el autor Vinatea Recoba (2011) en el artículo titulado “La Integración de los Servicios de Telecomunicaciones y lo que se requiere para Implementarla” hace referencia a lo siguiente:

En la mayoría de países, más allá de ciertas imperfecciones en algunos de sus mercados, se adoptaron los referidos procesos de liberalización; y hoy el mercado de las telecomunicaciones, en cada una de estas geografías, es un campo de encuentro entre operadores que compiten utilizando todas las herramientas y espacios que tal proceso de liberalización les ha dado. (p. 50)

El sector de telecomunicaciones tiene la característica peculiar relacionada con las actividades que otras empresas ofrecen, siendo los “servicios desagregados”, misma que surge del desglose de cada tipo de servicio de ofrecer, aquellos que son viables para ser vendidos de forma independiente a los usuarios de este sector, que si bien es cierto deben aumentar su competitividad y la optimización de sus recursos, especialmente el tecnológico (incluyendo equipos).

Delitos de telecomunicaciones

Se define como delito informático a toda acción criminal relacionada con robo o hurto, fraudes, estafa y sabotaje, sin embargo, estos evolucionan al igual que la tecnología.

Los propósitos en telecomunicaciones se basan en los mismos que se dan en delitos informáticos, pero también se hace referencia en especial en fraudes ya que afecta a todos los operadores de telecomunicaciones y prestadores de servicios en sus ingresos. Diversas fuentes calculan que las compañías pierden cerca del 10% de sus ingresos por falta de herramientas tecnológicas y procedimientos para contralar el fraude y asegurar sus ingresos. (Llangarí Salazar, 2016)

En China, el fraude de telecomunicaciones se está convirtiendo en un crimen cada vez más común. El año pasado se vieron más de 170.000 casos de fraude de telecomunicaciones que causaron pérdidas de más de 12,5 mil millones de dólares. Por lo general, los estafadores llaman a sus víctimas y las engañan para que transfieran su dinero a un grupo de cibercriminales mediante un cajero automático. Pero hace poco surgió una nueva clase de fraude de telecomunicaciones que combina sitios phishing y troyanos de puerta trasera. La semana pasada, la policía del Departamento Dongcheng de la Oficina de Seguridad Pública de Beijing nos pidió que investigáramos un caso de fraude de telecomunicaciones. La víctima había perdido 100.000 dólares. Después de nuestra investigación, las tácticas de los estafadores quedaron al descubierto. (Kaspersky, 2013)

En otro caso en donde las vulnerabilidades del sistema de información sirvieron para el enriquecimiento ilícito de un funcionario, se tiene lo siguiente. Un tribunal de China ha sentenciado a 10 años y medio de prisión a uno de los programadores del banco Huaxia de Beijing que se volvió millonario explotando una vulnerabilidad en el código de los cajeros automáticos del banco. Qin Qisheng era parte del equipo de programadores del banco y, como tal, recibía acceso a información sobre los sistemas y equipos de la empresa para protegerla. Sin embargo, Qisheng descubrió una vulnerabilidad que decidió explotar en lugar de parchar: un error en el código de los cajeros automáticos que hacía que no se registraran las transacciones realizadas a medianoche. Es decir que un usuario podía retirar dinero de su cuenta y el banco no lo deducía de su saldo. La única traba que tenía el usuario para hacerlo era un mensaje de alerta que salía diciendo que la transacción no podía realizarse, pero Qisheng instaló scripts en los sistemas para que esa notificación no se mostrara. El delincuente aprovechó que era el único que conocía la vulnerabilidad y comenzó a retirar entre 5.000 y 20.000 yuan (entre 740 y 2,965 dólares) cada día a medianoche. De esta manera, el empleado del banco se mantuvo retirando dinero desde noviembre de 2016 hasta enero de 2018. Después de 1.358 transacciones, Qisheng había robado al banco más de 7 millones de yuan, el equivalente a alrededor de 1 millón de dólares. Cuando el banco descubrió la vulnerabilidad la reportó ante las autoridades, que descubrieron el robo de Qisheng en sus investigaciones. Qisheng se defendió diciendo que solamente estaba evaluando la seguridad del banco y tenía el dinero guardado, listo para devolvérselo a su dueño. El banco Huaxia aceptó la explicación y, a pesar de los grandes daños ocasionados a la empresa y a los peligros a los que la expuso, pidió a las autoridades que le permitieran retirar los cargos en su contra luego de que se le devolviera el dinero robado. Sin embargo, las autoridades no confiaron en la explicación de Qisheng y rechazaron la solicitud del banco, por lo que se continuó con el proceso judicial en su contra. El tribunal tampoco creyó en su historia, principalmente porque se demostró que el criminal había retirado el dinero de la cuenta que el banco usa para hacer pruebas y lo había depositado en su cuenta personal. También se demostró que el funcionario no estaba guardando el dinero para devolverlo al banco, sino que lo estaba invirtiendo en acciones de la bolsa. En diciembre de 2018, el tribunal lo

encontró culpable de crímenes cometidos hacia el banco y hace poco el delincuente perdió una apelación para evadir su sentencia. A causa de sus acciones, Qisheng deberá cumplir una sentencia de 10 años y medio en prisión y pagar una multa de 11.000 yuanes, o 1.600 dólares. (Kaspersky, 2019)

Figura 3 **Banco Huaxia lugar del delito**
Fuente: Reuters 2019

En el cuarto trimestre de 2018, los investigadores de seguridad descubrieron una serie de nuevas botnets, entre las cuales no sólo había clones de Mirai. En el otoño (del hemisferio norte), comenzó a hacerse más activo el bot Chalubo, cuyos primeros ataques se registraron a finales de agosto. Aunque este nuevo malware utiliza fragmentos del código Mirai y las mismas técnicas de persistencia que la familia de bots Xor.DDoS, en su mayor parte Chalubo es un producto nuevo diseñado exclusivamente para lanzar ataques DDoS (por ejemplo, uno de los ejemplares detectados era "responsable" de organizar ataques del tipo SYN-flood). En octubre, se hizo más frecuente encontrar a Chalubo "en el mundo real". Los investigadores pudieron detectar versiones diseñadas para diferentes arquitecturas

(ARM de 32 y 64 bits, x86, x86_64, MIPS, MIPSEL, PowerPC), lo que indica con alta probabilidad que ha finalizado el período de prueba. Además, en octubre, se publicó la información sobre la nueva botnet Torii, que los expertos de Avast habían descubierto un mes antes. Esta botnet tiene como blanco una amplia gama de dispositivos y arquitecturas del Internet de las cosas (IoT). Su código es muy diferente al de Mirai, puesto que es un malware más capaz de ocultarse y que garantiza mejor su persistencia, por lo que promete ser mucho más peligroso. Este malware recopila y envía al servidor de comandos información detallada sobre los dispositivos infectados, incluidos el nombre del servidor y el identificador del proceso, pero no está claro con qué propósito lo hace. No se detectaron ataques DDoS con botnets basados en Torii, pero los expertos creen que ocurrirán. Otro bot descrito el pasado trimestre recibió el apodo Demonbot y se caracteriza por capturar los clústeres analíticos de Hadoop utilizando vulnerabilidades en el mecanismo de ejecución remota de comandos de Hadoop YARN. Este bot no es muy complejo desde el punto de vista técnico, pero el peligro está en el blanco que eligió: los clusters de Hadoop tienen a su disposición una potencia considerable, ya que están diseñados para procesar macrodatos. Además, debido a su integración en la nube, pueden aumentar significativamente la potencia de los ataques DDoS. Actualmente, la compañía Radware tiene bajo su vigilancia 70 servidores activos, que realizan hasta un millón de infecciones por día. Demonbot no sólo es compatible con los clusters de Hadoop, sino también con la mayoría de los dispositivos del Internet de las cosas, lo que facilita su reorientación a objetivos más numerosos. En el pasado trimestre, los expertos no se limitaron a advertir sobre las nuevas botnets, sino que también hicieron hincapié en los nuevos mecanismos de ataque. Así, a principios de invierno, quedó claro que FragmentSmack puede tener un uso más amplio de lo que se pensaba. Este ataque explota una vulnerabilidad en la pila de IP, que le permite enviar paquetes defectuosos bajo la apariencia de fragmentos de un mensaje más grande. Como resultado, el recurso atacado intenta recopilar estos paquetes en uno solo o los pone en una cola interminable, con lo que consume todo el poder de cómputo y hace que no se pueda procesar las solicitudes legítimas. El mecanismo de FragmentSmack se consideraba peligroso sólo para los sistemas Linux, pero en diciembre, investigadores de Finlandia descubrieron que también funciona en

ataques contra Windows 7, 8.1, 10, Windows Server y 90 productos de Cisco. Otro método de ataque prometedor para los atacantes es el protocolo CoAP, aprobado para su uso generalizado en 2014. Está diseñado para comunicarse entre dispositivos que tienen poca cantidad de memoria y es ideal para el Internet de las cosas. Dado que CoAP funciona con en el protocolo UDP, tiene todas las "marcas de nacimiento" de este último, lo que significa que se lo puede usar muy fácilmente para potenciar ataques DDoS. Hasta ahora, esto no ha sido un problema mayor, pero los expertos advierten que entre noviembre de 2017 y noviembre de 2018 el número de dispositivos que utilizan CoAP se multiplicó por casi 100 veces, lo que genera gran preocupación. Aparte de los nuevos medios potenciales para organizar ataques, a fines de 2018 apareció una nueva plataforma para lanzar ataques DDoS llamada 0x-booter. El servicio, descubierto el 17 de octubre de 2018, es capaz de lanzar ataques con una capacidad de hasta 420 Gb/s, basándose en un poco más de 16 mil bots infectados con el malware Bushido IoT, una de las versiones modificadas de Mirai. Esta plataforma, compilada sobre el código de un servicio similar, es peligrosa por su simplicidad, bajo costo y poder comparativo: por una cantidad muy pequeña (de 20 a 150 dólares) cualquier persona puede, mediante una simple interfaz, lanzar ataques de varios tipos contra el objetivo seleccionado. Según el análisis de los investigadores, sólo en la segunda mitad de octubre se utilizó este servicio para lanzar más de 300 ataques DDoS. (Kaspersky, 2019)

Otro caso ocurrido en Chile entre los días 28 de diciembre de 2001 y 8 de enero de 2002, un ex empleado de la empresa ATI Chile, realizó diversas intromisiones ilegales al servidor de ésta, alterando, dañando y conociendo indebidamente información contenida en éste. Los sitios Web afectados fueron: www.guestbook.cl y www.metabuscador.cl (Contreras Clunes, 2003)

El imputado era un joven de 19 años, conocido en el Chat IRC con el seudónimo «P0key», el cual habría actuado por «venganza» en contra de la empresa, pues había sido despedido de ésta. (Contreras Clunes, 2003)

El «cracker» al ingresar ilegalmente a estos sitios, alteró el contenido de éstos, creando una nueva página Web (index.html) en reemplazo de la existente, que

mostraba mensajes ofensivos hacia la empresa e indicaba que el sitio había sido hackeado. (Contreras Clunes, 2003)

El administrador del sistema informático procedió a efectuar una inmediata auditoría de todos los archivos «LOG» del servidor y pudo comprobar que dichos sitios habían sido víctima de una serie de ataques e intromisiones, además, la eliminación de algunos archivos de auditoría de transacciones de cuentas de FTP, para borrar rastros desde dónde se efectuaban los ataques. Incluso, mientras se realizaban las auditorías, se pudo comprobar que el «cracker» intentaba ingresar al correo electrónico del gerente general de la empresa, hecho que pudo ser controlado a tiempo. (Contreras Clunes, 2003)

Se pudo comprobar que el 90% de los ataques provenía desde una IP fija, que correspondía a un Ciber Café en el cual el imputado trabajaba como administrador. El resto de los ataques provenía desde cuentas conmutadas de acceso a Internet, fundamentalmente desde el domicilio del imputado. (Contreras Clunes, 2003)

Una vez iniciada la investigación y presentada la querella criminal por delitos informáticos, el caso tomó especial importancia en la prensa de la ciudad de Talca y entre los usuarios del Chat IRC. Aprovechando este momento, el imputado concurrió en forma voluntaria al diario *El Centro* de Talca y entregó una entrevista, siendo portada, bajo el título: «*Yo soy el ciber pirata*». De esta manera lograba la fama y reconocimiento por sus pares, hecho buscado comúnmente entre los «crackers». Incluso ofrecía sus servicios para reparar las fallas de seguridad del sistema. (Contreras Clunes, 2003)

De acuerdo a una publicación realizada por (REVISTA LIDERES, 2016) Las empresas en América Latina se encuentran inmersas en un contexto de negociaciones digitales de carácter global y, como consecuencia, tienen mayor exposición a las ciberamenazas. Pese a que las compañías adoptan una mayor gestión de seguridad, los resultados del estudio ‘Tendencias en Gestión de Ciber-riesgos y Seguridad de la Información en Latinoamérica’, realizado en el 2016 por Deloitte, muestran que el cuidado ante los ciberataques no siempre es prioritario.

En el estudio participaron 89 organizaciones de 13 países y siete industrias diferentes. Por Ecuador fueron consultadas 28 firmas. Los resultados encontraron que el 40% de las firmas encuestadas ha sufrido una brecha de seguridad en los últimos dos años. Oswaldo Bravo, gerente de Evaluación de Riesgos de Deloitte, considera que el dato real tiende a ser muy alto, pero las empresas, por un tema de reputación, no suelen reportarlo. (REVISTA LIDERES, 2016)

Figura 4 **Datos del estudio 'Tendencias en Gestión de Ciber-riesgos y Seguridad de la Información"**
Fuente: Delortte

Según la Fiscalía General del Estado, un caso local sucedió en enero del 2015, cuando un 'malware' o software malicioso se propagó en los computadores de 17 empresas privadas e instituciones públicas de Quito, Guayaquil y Cuenca. Este virus encriptó archivos sensibles e información contable de las entidades. Un error común, según Bravo, es pensar que la seguridad digital se resume en usar un software antivirus. *"Se debe implementar un gobierno de seguridad de la información dentro la empresa",* agrega. Esto implica definir políticas,

procedimientos y un responsable para enfrentar estos riesgos. Sin embargo, los resultados demuestran que a escala regional menos del 10% de las organizaciones cuentan con un tablero con indicadores (kpis), que permita evaluar riesgos de ciberseguridad. (REVISTA LIDERES, 2016)

En Ecuador, según el estudio de Deloitte, el 54% de las firmas cuenta con una estrategia de ciberamenazas y seguridad de la información. De estas empresas, casi todas corresponden al sector bancario. Banco Pichincha cuenta con el portal llamado Banca Segura, que fue implementado en el 2014. Con este, los clientes descargan un aplicativo y generan un canal seguro entre su computador y los servidores del banco. (REVISTA LIDERES, 2016)

Figura 5 **Evaluación de cooperativa de ahorro y crédito**
Fuente: Repositorio ESPE

Actualmente, debido a las medidas de seguridad descritas, la institución logra bloquear el 98,5% de los ataques dirigidos a sus clientes, asegura Juan Carlos Beltrán, gerente de Riesgo Operativo del banco. Por su parte, Banco Guayaquil es la

única entidad financiera del norte de la región que cuenta con la certificación más alta de seguridad, la ISO 27 001. En Ecuador, se suman entidades públicas como CNT y Quito Turismo, y firmas como Telconet y Telefónica. (REVISTA LIDERES, 2016)

En este contexto, las regulaciones de entes de control, como la Superintendencia de Bancos, permiten la aplicación de medidas de seguridad. A nivel del Estado, las empresas públicas se rigen bajo el Acuerdo 166 que obliga la implementación de políticas y procedimientos para salvaguardar la información. Para Bravo, el problema está en el resto de empresas ecuatorianas que "carecen de madurez sobre el tema." Según los empresarios, el mayor obstáculo que afrontan para implementar ciberseguridad es no contar con recursos o con el presupuesto suficiente. El estudio dice que, por primera vez en los últimos cinco años, el 77% de las organizaciones no incrementó o directamente redujo el presupuesto destinado a ciberseguridad. (REVISTA LIDERES, 2016)

Cuando se trata de fraudes y robos de información, las pequeñas y medianas empresas (pymes) suelen ser las más vulnerables. Esto se debe a que no siempre cuentan con presupuestos o el equipo para poder enfrentar estos retos de seguridad. Sin embargo, las empresas pueden acceder a una oferta nacional e internacional de paquetes de seguridad y consejos para que puedan proteger su información. Según la Fiscalía General del Estado, entre enero y mayo del 2016, se registraron 530 delitos informáticos en el país. El 69% de estas denuncias (368) corresponde a una apropiación fraudulenta por medios electrónicos. Las plataformas de pago, los correos en servidores compartidos o las conexiones a Internet gratuito son algunas de las brechas de entrada que facilitan los crímenes de cibernéticos. En el informe 'Evolución de la Gestión de Ciberiesgos y Seguridad de la Información', presentado por consultora Deloitte en julio del 2016, se encontró que cuatro de cada diez empresas sufrieron una brecha de seguridad en los últimos 24 meses. Aproximadamente, un 30% de estas son pymes que no cuentan con sistemas de seguridad satisfactorios.

Licencias de software de seguridad, servidores propios y el análisis de riesgo pueden llegar a costar más de USD 10 000. Estos montos suelen sobrepasar los reducidos presupuestos de las pymes, que en sus primeros años de operaciones tienden a priorizar otros costos. En el mercado, sin embargo, existen opciones más accesibles para las pymes que deseen acceder a servicios de seguridad. Yambuu es una empresa ecuatoriana que se especializa en el desarrollo de productos de seguridad digital.

La auditoría operacional y de control

Definición de Auditoría

El término auditoría hace referencia a revisión de hechos pasados, además de procesos y procedimientos dentro de una organización, del mismo modo evalúa políticas establecidas con el objetivo de permitir la realización de información en el ámbito: tributario, financiero y de operaciones. La finalidad de la auditoría es la verificación y certificación de procesos confiables en base a la optimización de recursos.

La auditoría tiene una variedad de definiciones, sin embargo, con el propósito de aportar a la investigación se establecerá las más relevantes. Los autores Alcívar Cedeño, Brito Ochoa, & Guerrero Carrasco (2016) definen a la auditoría como la sistematización aplicable a procesos determinados que cumple con el objetivo de revisar, verificar y realizar una evaluación de hechos, registros y documentos de una organización. De igual manera en la web se encuentra definida a la auditoría relacionada con la informática como aquella que se

(…) encarga de recoger, agrupar y evaluar evidencias para determinar si un sistema informático salvaguarda activos, mantiene la integridad de los datos, a través del uso eficaz de los fines de la organización y eficiencia de los recursos. Por lo tanto, el objetivo principal de la auditoría informática es proteger los activos y la integridad de datos. (Significado de auditoría , 2016)

Consecuentemente basado en ambos contextos antes mencionados se puede establecer como definición que la auditoría es la evaluación de un determinado proceso con la finalidad de establecer un estudio de los niveles de seguridad de protección aplicada a los activos y recursos, permitiendo emitir un informe de la situación desarrollada dentro de las empresas.

Clasificación de la auditoría

Se establece la clasificación de la auditoría descrita en la siguiente figura:

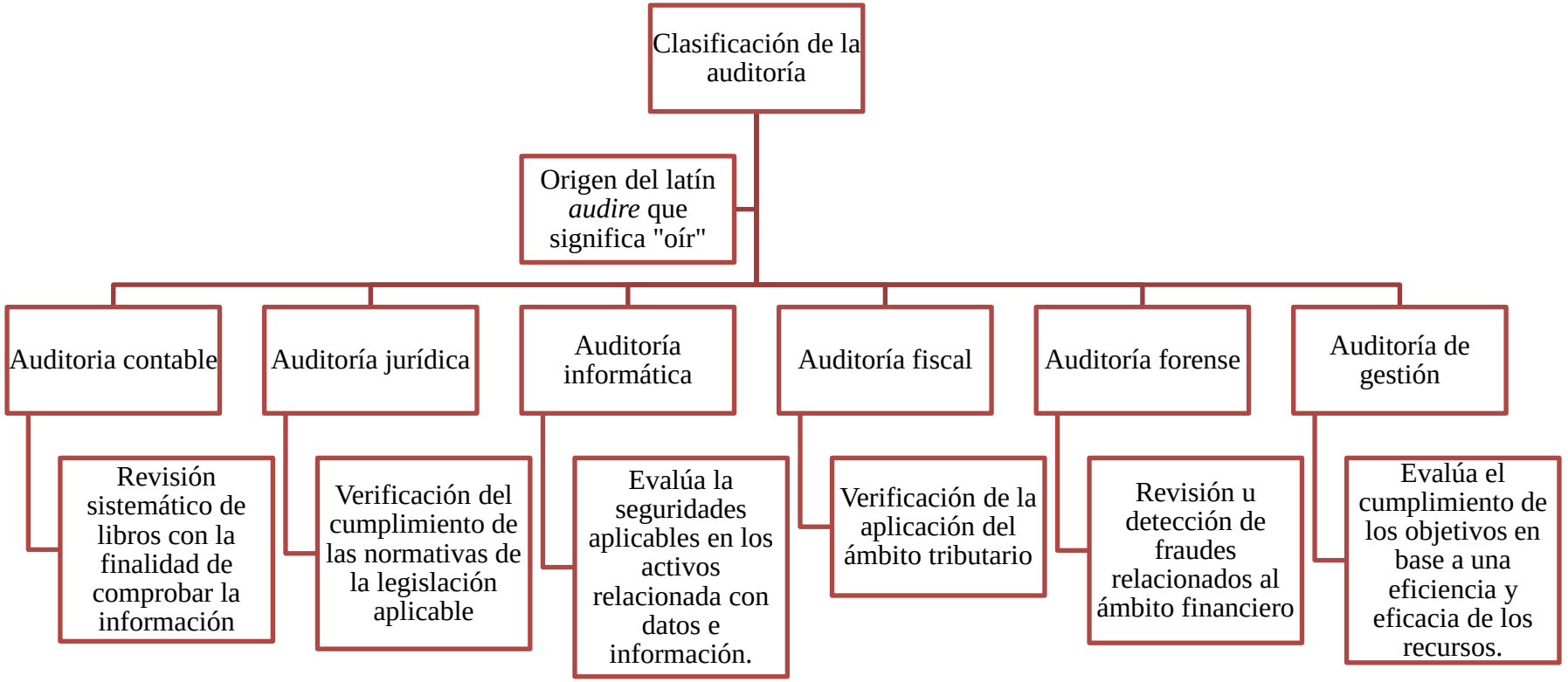


Figura 4 **Clasificación de la auditoría**

Fases de la auditoría

La auditoría tiene una serie de pasos para la realización de una evaluación de hechos, sucesos y seguridades de una determinada organización, estas fases se aplican durante la realización de la auditoría, mismas que primordiales para un correcto desarrollo. Según (Buján Pérez, 2018) afirma que la auditoría requiere de un proceso establecido para la revisión de la información de una empresa en una fecha determinada (…) En elaboración, y necesita de trabajo antes y después de la fecha se requiere de la realización de etapas o fases típicas. La siguiente figura describe las distintas fases aplicables en la auditoría:

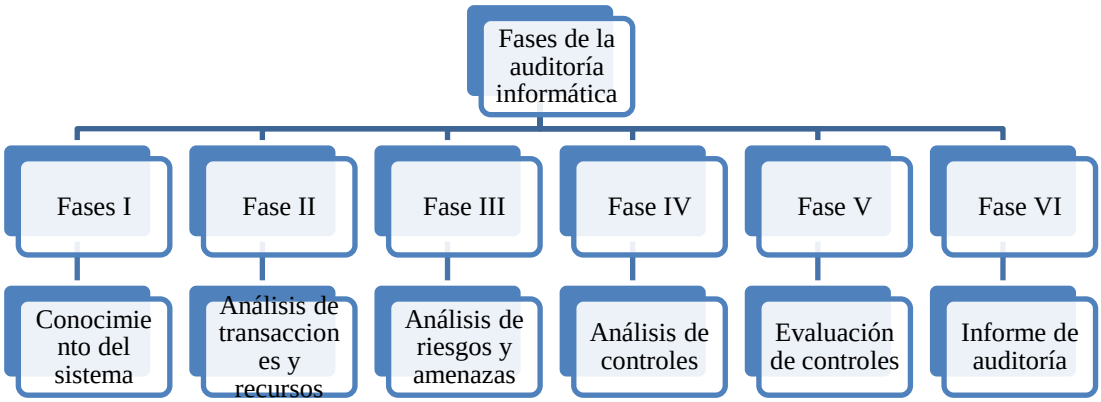


Figura 5 **Fases de la auditoría**

Nota. *Adaptado de* (Martínez, 2014)

Fase I: Conocimientos del Sistema

En esta etapa se establece una revisión de aspectos legales y políticos de la empresa que va a ser auditada. En efecto, se identifica los elementos que componen el sistema que controla la organización que será revisada por el auditor. En este sentido, se puede establecer dentro de la fase I lo siguiente:

- Establecer las características que tiene el sistema operativo, así como también el organigrama del área que hace uso para el funcionamiento.
- Realiza un análisis de los procesos del sistema desde el punto de vista del personal estrechamente relacionado con este, incluyendo el respectivo manual de funciones siempre y cuando exista dentro de la entidad.
- Verificación de si la empresa cuenta con auditorías anteriores.
- Establecer los equipos tecnológicos que conforman la empresa a ser auditada.
- Establecimiento de la forma en que se llevan los procedimientos de los archivos y su respectivo almacenamiento.
- Controles de seguridad aplicables.
- Identificación del personal autorizado en el sistema operativo.

En esta fase una de los puntos que debe ser definido ya que aún el trabajo de auditoria se encuentra en las fases de planificación, es el alcance de auditoria. En el caso de la presente investigación se debe puntualizar que el equipo de auditoria no corresponde al área de especialización técnica de telecomunicaciones y ambientes tecnológicos por lo cual el alcance de la misma queda definido como un trabajo de auditoria convenido entre las partes con base en la NIA 4400 y que se encuentra soportada con los procedimientos, técnicas y diagnósticos usados en una Auditoria de Sistemas.

Fase II: Análisis de transacciones y recursos

En esta etapa es importante establecer la forma en que se relacionado las transacciones y los recursos, a continuación, se establece la relación anterior mencionada:

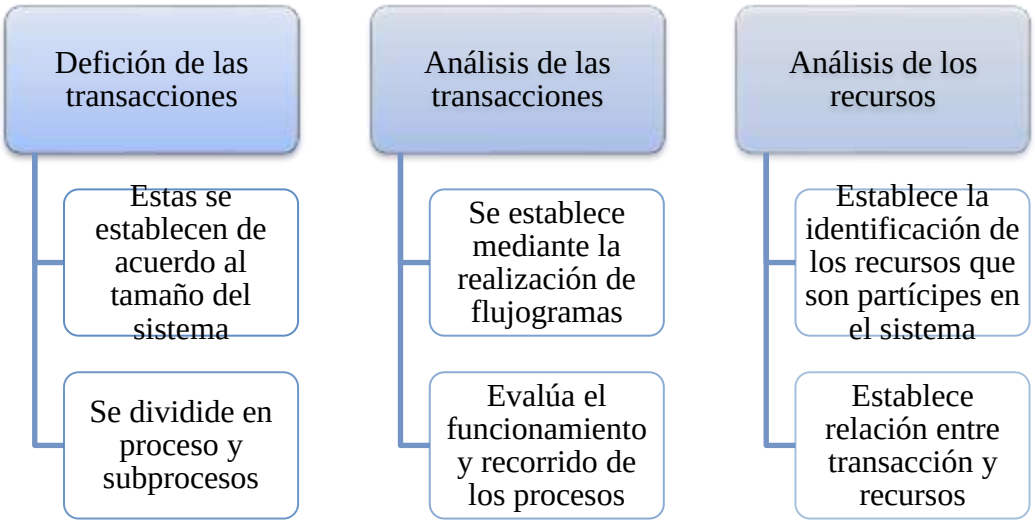


Figura 6. **Fase II Análisis de transacciones y recursos**

Nota. Tomado de (Martínez, 2014)

Fase III: Análisis de riesgos y amenazas

Esta es la fase en que se puede establecer los riesgos y amenazas existentes en el sistema de la empresa auditada. A continuación, se hace una descripción de aquellos riesgos y amenazas más comunes:

Tabla 3 **Riesgos y amenazas de sistemas operativos**

Riesgos	Amenazas
Recursos dañados o destruidos	Existencia de amenazas de equipos tecnológicos
Fraude genera como consecuencia de pérdida de datos	Documentos fuentes amenazados
Pérdida de documentación informes necesarios de respaldo para información	Programas de aplicaciones se encuentran amenazados
Hurto de dispositivos de almacenamiento	
Operaciones ineficientes	
Vulneración de la integridad de datos	
Errores en la información	

Nota. Adaptado de (Martínez, 2014)

Fase IV: Análisis de controles

En esta etapa se encuentra la realización de análisis dentro de los controles aplicables dentro de la empresa u organización, entre las cuales se puede aplicar:

- **Controles codificados**: Es la identificación mediante un código a un determinado recurso, mismo que permite establecer como medida de seguridad y protección.
- **Análisis de cobertura de los controles requeridos:** El auditor tiene el propósito de establecer un análisis en los controles aplicados como medidas de protección, además de establecer el nivel de vulnerabilidad.

Fase V: Evaluación de controles

Los objetivos de esta fase son:

- Realizar la verificabilidad de los controles existentes, es decir establecer si hay controles de acuerdo a los requerimientos de la organización.
- Identificar el nivel operativo de los controles que durante la auditoría hay dentro de la organización, del mismo evaluar si estos cumplen con las necesidades existentes de seguridad.
- Por medio de esta fase se puede establecer el método más acertado para la realización de la auditoría
- Finalmente, se solicita al área auditada aquellos elementos que son necesarios para la aplicación del método de auditoría.

Fase VI: Informe de auditoría

Esta última fase hace referencia al dictamen, informe que contiene la opinión del auditor basado en las evidencias encontradas durante la auditoría. Este informe contiene detallada las recomendaciones, emite las respuestas basadas en la evaluación aplicada y un informe dirigido a la gerencia.

Proceso de Auditoria informática

Auditoría en sistemas informática

La auditoría tiene su clasificación, sin embargo para la presente investigación se realizará la ampliación del estudio de la "auditoría en sistemas de informáticos", tambien conocida como auditoría informática. Con la finalidad de establecer el aporte necesario se planteará definciones de acuerdos a varios autores, tal es el caso de Castello (2016) quien define a la auditoria informática como el estudio aplicado en establecer la comprobación de la fiabilidad de las herramientas informáticas y la forma en que estas son utilizadas dentro una organización (p. 5). Por otra parte, el autor también afirma que el control es importante para lograr cumplir con los objetivos propuestos por una determinada administración.

Otro concepto importante de esta auditoría según el autor; Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utiliza dos en una empresa, sean individuales, compartidos y/o redes, así como a sus instalaciones, telecomunicaciones, mobiliarios, equipos periféricos y demás componentes. Dicha revisión se realiza de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumo necesarios para el funcionamiento del centro de cómputo.

El propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información y la emisión oportuna de sus resultados en la institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas computacionales a la empresa. (Muñoz Razo, 2002)

Bárcenes Mendoza, Riera Riera, Alarcón Muñoz, & Jiménez Zavala (2018) afirma:

Auditorías de tecnología de la información son importantes en la era moderna, donde existen mayormente procesos que son automatizados dentro de la mayoría de las empresas. Las auditorías tienen la finalidad de evaluar la fiabilidad de los sistemas de tecnología de la información. (p. 58)

La Auditoría Informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos. (Piattini & Del Peso, 2001)

La auditoría informática o de sistemas de informáticos tiene la finalidad de revisar con ayuda de aplicación de pruebas y métodos de auditoría los controles, sistemas y procedimientos, enfocándose en establecer un análisis del nivel riesgo en que puede ser afectada la seguridad y su vulnerabilidad relacionada con los

procesadores de información y equipos de soporte, mismos que son fundamentales en las decisiones que debe tomar una organización.

Tipo de auditoría informática

La auditoría informática tiene dos tipos: interna y externa. La auditoría interna es aquella que tiene la característica de hacer uso de recursos de la empresa que es auditada, el auditor es considerado de "planta" debido a que este recibe una remuneración de parte de la organización y se encuentra en la nómina del personal que conforma la misma, además la dirección tiene el control de la forma en que esta es llevada.

La auditoría informática externa es aquella que no tiene pertenencia con la organización que es auditada, es decir no forma parte del personal y además no está en la nómina, sin embargo, este si cubre con los honorarios profesionales por el servicio recibido, este tipo de auditorías son aplicables cuando se busca tener mayor objetividad de la información emitida en el dictamen del auditor.

Tabla 4 **Características del tipo de auditoría informática**

Auditoría Informática Interna	Auditoría Informática Externa
El personal pertenece al equipo de la empresa auditada	El auditor no pertenece a la empresa auditada
Forma parte de la nómina de la empresa auditada, recibe remuneración	No forma parte de la nómina de la empresa auditada, sin embargo, si recibe remuneración
El control es aplicado por la empresa auditada	Ofrece mayor objetividad en el informe emitido por el auditor

Clases de auditoría de sistemas informáticos

La auditoría en sistemas informáticos tiene varias clases, mismos que son descritos a continuación:

Tabla 5 **Clases de auditoría en sistemas informáticos**

Clase de auditoría informática	Descripción
Auditoría Informática de Explotación	Se enfoca en analizar los resultados obtenidos en la informática. La materia prima de esta clase de auditoría son los datos. Mediante un proceso informático se puede transformar en datos. La auditoría tiene como la función de auditor los componentes y las interrelaciones de la productividad de la transformación de datos.
Auditoría Informática de Desarrollo de proyectos	Se enfoca en el desarrollo de programación de sistemas, así como también aplicaciones. Se encarga de evaluar la seguridad aplicable en los programas, además de la ejecución de los mismos. Esta auditoría evalúa las fases del desarrollo de las aplicaciones, la satisfacción de los usuarios y los procesos de programas críticos.
Auditoría Informática de Sistemas	Audita todo lo relacionado con las técnicas de sistemas, incluyendo sus fases. El creciente uso del sector de telecomunicaciones surgió la necesidad de auditar líneas y además de redes que se encuentran en las instalaciones.
Auditoría Informática de Comunicación y Redes	Surgió de la necesidad del aumento del uso de las comunicaciones.

	Evalúa los soportes físico-lógico dentro de la informática Es una auditoría sofisticada que requiere de equipos especializados evaluar las comunicaciones y redes.
Auditoría de la Seguridad Informática	Esta auditoría se enfoca en evaluar el nivel de seguridad física y lógica. Se encarga de identificar la seguridad en hardware y soporte de datos. Verifica el nivel de seguridad en las edificaciones que son parte de las instalaciones del hardware. Debe establecer la seguridad desde distintos contextos en una empresa. Identifica los riesgos potenciales a los cuales están expuestas las empresas.

Beneficios de la auditoría en sistemas informáticos

Según los autores Salgado Soto, Osuna Millán, Sevilla Caro, & Morales Garfias (2017) afirman que la auditoría informática establece como área de interés la tecnología de información, misma que tiene importancia en la forma en que deben ser aplicadas durante la administración estratégica en función de los sistemas informáticos, además de una correcta dirección dentro de una organización y su funcionamiento relacionado con el uso de software, hardware y del mismo modo incluye las telecomunicaciones aplicables en la empresa.

La auditoría en sistemas informáticos se basa en establecer un análisis de las seguridades que una organización, independientemente de su actividad económica, aplica en el activo de la información. Por ende, este tipo de auditoría permite establecer el beneficio de identificar el nivel de riesgo existente en los controles y su

funcionamiento, además de definir si estos pueden ser vulnerados con facilidad para posteriormente ser usado para el cometimiento de delitos informáticos.

Se establece importante identificar los beneficios que conlleva la aplicación de la auditoría en sistemas informáticos para las empresas, quienes deben estar a la vanguardia de evolucionar de acuerdo al avance tecnológico que cambia de forma constante, debido a lo anteriormente mencionado se cita lo siguiente:

La función en Informática da a conocer el funcionamiento de una organización la cual tiene como características el uso del funcionamiento del software, hardware y las telecomunicaciones que hay en la actualidad, y plantea utilizar la información como un arma estratégica de competencia para las empresas y la nueva concepción de la informática en las organizaciones de una manera más activa. (Salgado Soto et all, 2017, p. 6)

Auditoría con informática a Sistemas Contables.

La auditoría con informática a sistemas contables se mide en valores y se encuentra regida por las normas de auditoría. La verificación se realiza desde una posición avanzada, le aporta al auditor los elementos referenciales indispensables, como balances de comprobación, estados financieros, exámenes de registro, estados comparativos o muestras aleatorias, permitiendo realizar los análisis pertinentes, incluso antes de enfrentarse a la documentación primaria. El uso de la computación toca a las puertas de la auditoría con aciertos y riesgos, pero también con la seguridad plena de que rechazarla será imposible. (Alfonso Martínez , Blanco Alfonso , & Loy Marichal , 2012)

En esta Era la información es el activo más importante de las empresas invirtiéndose enormes cantidades de dinero y tiempo en la creación de sistemas de información para obtener la mayor productividad y calidad posibles. (Alfonso Martínez , Blanco Alfonso , & Loy Marichal , 2012)

La utilización de herramientas informáticas para la realización de las auditorías financieras ha provocado que Universidades como Chile, México, España y Argentina, entre otras; cuentan entre sus programas con la asignatura de auditoría informática, comprometidos en la preparación de un profesional más eficiente y preparado para el desarrollo actual. (Alfonso Martínez , Blanco Alfonso , & Loy Marichal , 2012)

En la actualidad las operaciones contables están soportadas mediante sistemas automatizados utilizando las Tecnologías de la Información y las Comunicaciones (TIC), surgiendo la necesidad de incorporar a la auditoría contable un auditor informático y acciones de estas tecnologías en la auditoría. La esencia del auditor informático es la auditoría a sistemas computarizados en explotación auxiliándose de los programas de auditoría, para asegurar que en un sistema no se han cometido ni errores ni fraudes, esto se logra mediante pruebas requeridas que detecte el nivel de confiabilidad del procesamiento de la información del sistema. (Alfonso Martínez , Blanco Alfonso , & Loy Marichal , 2012)

Características de la auditoria en sistemas informáticos

Las características de la auditoría en sistemas informáticos se basan en cumplir con la verificación de los controles que deben tener las organizaciones, con la finalidad de proteger los datos durante los procesos de la información, entre los elementos que conforman el procedimiento que tiene la información se encuentran:

Figura 7 **Proceso de la información**

Nota. Adaptado de (Flores Guirao, 2015)

La información consta de cuatro fases que son: entrada, almacenamiento, procesamiento y salida; durante este proceso es donde deben ser aplicados controles que aumenten la seguridad de la integridad de la información. Con la finalidad de establecer una mejor comprensión se realizará una breve descripción del mismo a continuación:

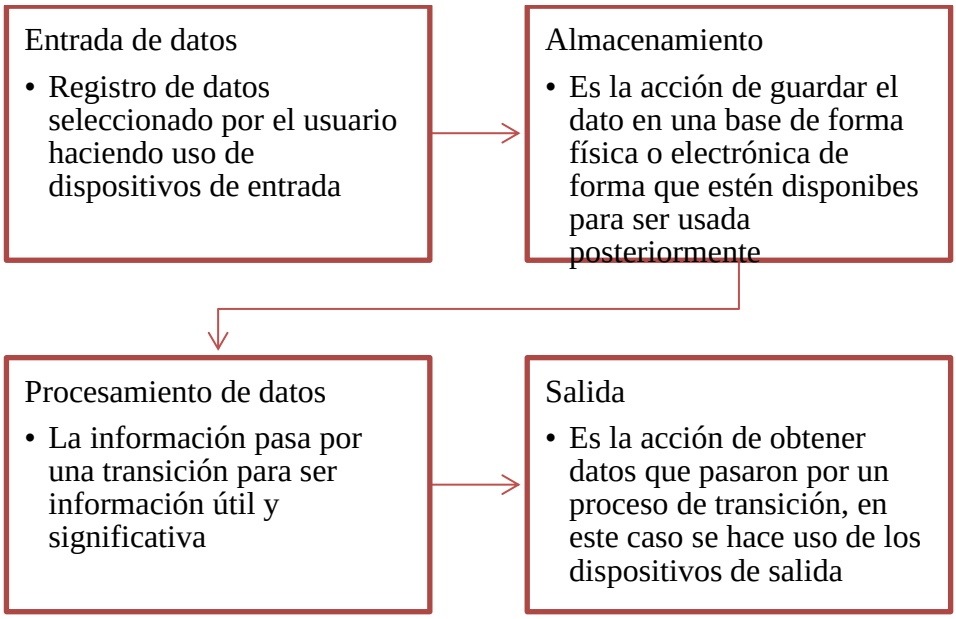


Figura 8. **Descripción del proceso de información**

Nota. Elaboración de los autores

Basado en el proceso de la información antes mencionada en la figura se establece como características de este tipo de auditoría las siguientes:

- Custodiar el activo de la información mediante la aplicación de procesamientos de datos dotados de mecanismos de seguridad que disminuyan el riesgo de robo, destrucción o uso indebido.
- Asegurar la integridad de la información usada por medio de datos.
- Cumplir con los estándares de seguridad de la veracidad de la información para el cumplimiento de metas organizacionales.

Métodos de Auditoria Informática

El auditor, persona que realiza los procesos de auditoría, debe tener una base sustentable de evidencias que le permitan emitir una opinión la cual será detalla en el informe de auditoría, es por ello que debe cumplir con procedimientos que le permitan emitir su opinión mediante: "análisis, características, verificación de resultado del control interno, además de fundamentar su conclusión emitida" (Aguirre Sánchez, 2018). La auditoría en sistemas informáticos cuenta actualmente con tres tipos de métodos aplicables que son:

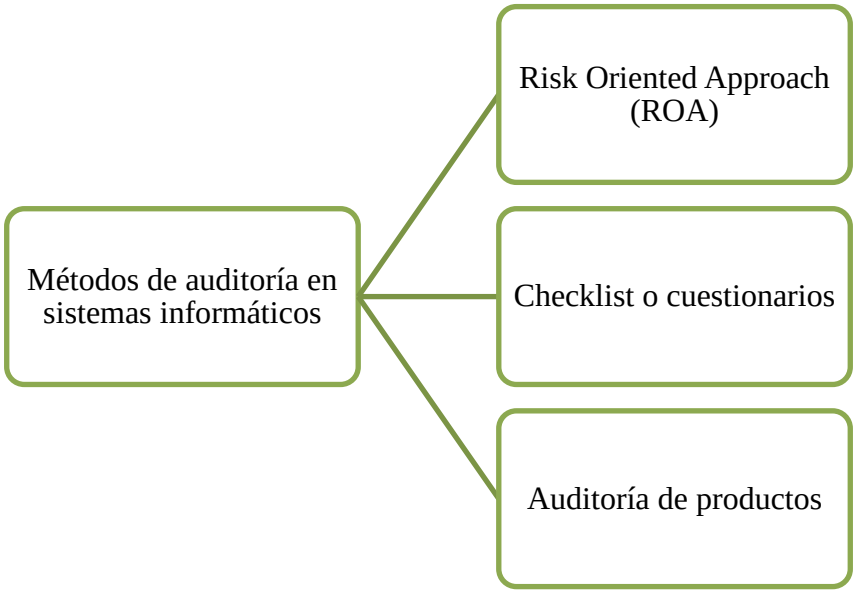


Figura 9 **Métodos aplicables en auditoría informática**

Nota. Adaptado de (Flores Guirao, 2015)

Limitación y alcance de una auditoria informática

La auditoría informática tiene como enfoque la revisión de ámbitos dentro de una organización, el departamento de sistemas es aquel contexto donde se desarrolla la revisión, verificación y análisis de los procesos, del mismo modo también es

aplicada en aspectos técnicos, económicos y administrativos permitiendo aplicar métodos de evaluación de auditoría.

Según Castello (2016) afirma que la auditoría informática tiene como objetivo determinar que la entidad auditada tenga opinión en aspectos como son:

- Determinación del plan informático existente, incluyendo el costo que incurre.
- Conocer el presupuesto que tiene la entidad sobre los servicios informáticos dentro de la misma.
- Conocer y evaluar los métodos aplicados por la dirección.
- Conocer la estructura del personal responsable de la tecnología de información.
- Tener conocimiento de los servicios que presta el área de sistema.

Administración: Es el ámbito en que se enfoca la auditoría aplicada dentro de la administración en el departamento de sistemas. Los aspectos que son evaluados en este ámbito es la forma en aplica la administración, además como realiza el personal sus funciones y procedimientos, por otra parte, identifica y analiza el cumplimiento en la normativa legal correspondiente a la actividad y sector de la empresa.

Explotación u Operaciones: El ámbito de operaciones hace análisis de aquellas actividades relacionada con aquellos servicios prestados del área de sistema, entre los cuales se encuentra considerado la parte de operatividad y la aplicación de la administración del equipamiento, la conectividad de redes de la tecnología de comunicación.

En relación a la operación o ejecución de aplicaciones, es didácticamente conveniente considerar al sector Explotación como una instalación fabril: para realizar procesamiento de datos: se dispone de una materia prima -los datos- que es necesario transformar y que se someten previamente a controles de integridad y

calidad, la transformación se realiza por medio del proceso informático el cual está gobernado por programas. (Castello, 2016, pág. 124)

Delitos informáticos y de telecomunicaciones

El término delito informático se utilizó por primera vez a finales de los años noventa, a medida que Internet se extendía por el mundo. Con el uso del internet, se dio inicio a nuevos problemas por lo que las naciones que conforman el grupo denominado G8, mantuvieron una reunión en Lyon, Francia, con el propósito de estudiar estos problemas emergentes relacionados con la delincuencia que migraron sus actividades al internet. En la reunión se utilizó el término delito informático para describir de forma imprecisa aquellos delitos que se cometieron con el uso de redes informáticas. Al mismo tiempo, y guiado por los participantes en el grupo de Lyon, el Consejo Europeo comenzó a diseñar el Tratado sobre Delito Informático. (Perrin, 2006)

Al delito informático se lo puede definir como cualquier actividad en la cual, a través del uso de las computadoras, para cometer un delito, estos pueden constituirse en nuevas formas penales donde se incluyen como elementos primarios al internet y a la computadora como instrumentos físicos. El delito informático en sus diferentes tipos es un delito susceptible de ser sancionado por el código penal, siempre y cuando la figura antijurídica se encuentre configurada en el tipo y establecida en un cuerpo normativo. (Perrin, 2006)

En el Ecuador las investigaciones realizadas acerca de pericia informática son de bajo interés, una de las causas es el desconocimiento del tema por parte de la sociedad, adicional a la falta de procedimientos registrados de delitos informáticos competentes a las autoridades o entidades gubernamentales. Las fallas principales de la pericia informática en el Ecuador es la carencia de profesionales que tengan conocimientos informáticos adecuados, obteniendo como resultado impunidad de casos, debido a la falta de conocimientos, pocas habilidades idóneas para la utilización de medios tecnológicos en la adquisición de pruebas, y una correcta legislación de acuerdo a los delitos informáticos actuales. (Perrin, 2006)

Tipos de delitos informáticos

De acuerdo a Lara, Martínez & Viollier (2014), se considera para los delitos informáticos las siguientes categorías:

1. El acceso no autorizado: es el acceso sin derecho a un sistema o a una red, donde son violadas las medidas de seguridad, llega también a ser conocido como hacking.
2. El daño a los datos o programas informáticos: es el borrado, descomposición, deterioro o supresión de datos o programas informáticos sin que la persona tenga derecho a realizar esa acción.
3. El sabotaje informático: se refiere a la introducción, alteración, eliminación de datos o programas, la interferencia a los sistemas informáticos con el propósito de ser un obstáculo en el funcionamiento de las redes.
4. La interceptación no autorizada: se refiere a la captación que se realiza sin autorización a través de mecanismos tecnológicos.
5. El espionaje informático: se entiende como la adquisición, revelación, transferencia de información confidencial de tipo comercial sin que se tenga la debida autorización, con el propósito de causar pérdidas económicas o de obtener algún beneficio.

Normas Internacionales de Auditoria

COSO ERM

En 1985 se formó la Comisión Nacional para Emisión de Informes Fraudulentos, conocida como la Treadway Commission, a fin de identificar las causas en la proliferación actual de emisión de informes fraudulentos. En 1987 la Treadway Commission solicitó realizar un estudio para desarrollar una definición común del control interno y marco conceptual. En 1988, el Comité de Organizaciones Patrocinantes de la Comisión Treadway, conocido como COSO, seleccionó a Coopers & Lybrand para estudiar el control interno.

La evolución a lo largo de la historia de la estructura del Sistema COSO ha sido efectiva a partir del año 1992, en cuyo año se denominó Marco del Control Interno (COSO I), para el año 2004 se da a conocer la mejora en el Sistema de

COSO I con el Marco Integral de Riesgos (COSO II ERM), y para el año 2006 se da a conocer el Sistema de COSO III para pequeñas y medianas empresas.

Modelos del Sistema COSO:

COSO I: Contiene los siguientes 5 elementos potenciales: a) ambiente o entorno de control; b) evaluación del riesgo; c) actividades de control; d) información y comunicación y e) supervisión.

COSO II ERM: En este modelo se buscó la mejora en los elementos potenciales, como resultado de ello se integra a 8 elementos potenciales: a) ambiente interno; b) establecimiento de objetivos; c) identificación de eventos; d) evaluación de riesgos; e) respuesta a los riesgos; f) actividades de control; g) información y comunicación y h) supervisión.

COSO III PYMES: En este modelo se simplificó a los 5 primeros elementos potenciales del COSO I, como consecuencia de una búsqueda en la implementación del elemento de Roles y Responsabilidades, el cual al final se reconoció su exclusión del modelo establecido.

Los criterios gerenciales aplicados en una empresa permiten integrar componentes para el monitoreo de las operaciones cotidianas y representadas a través de controles que son planteados y diseñados en base a las necesidades de la directiva y las cuales son revisados por expertos o auditores que establecen los errores y los procedimientos a desarrollar para el accionar de políticas que permitan una correcta presentación de información financiera, evitando así los errores y fraudes que afecten el rendimiento contable de la entidad. (Gaitán, 2016)

Según Eslava (2013) todo proceso de control interno “se somete a una evaluación por parte de una directiva para su implementación y supervisión dentro de las operaciones y actividades realizadas en la empresa”. (p. 55)

El proceso de evaluación del control interno se realiza conforme a las siguientes actividades organizacionales: (a) Diseño, (b) Implementación, (c) Mejoramiento, (d) Diseño, (e) Implementación, (f) Mejoramiento, (g) Evaluación y valoración, (h) Auditoría, (i) Supervisión.

Para evaluar el control interno, la directiva realiza un análisis de los problemas que se dan dentro de un área específica, cuando se identifica el problema, se procede a especificar los resultados que pude ocasionar y las posibles actividades para disminuirlo, ya que de esto depende el éxito ante el cumplimiento de las metas organizacionales de la empresa. Esta etapa garantiza el ahorro de recursos y el manejo de las políticas para afrontar cualquier escenario que se presente, y que quede como antecedente para el desarrollo de las etapas siguientes.

Según Orta (2012) "el proceso de evaluación del control interno debe comprender las siguientes claves: a) Manejar criterios basados en objetividad y conforme a principios internacionales de auditoría, b) Tomar decisiones conforme a las necesidades de la directiva para el despliegue de acciones estratégicas de alta gerencia dentro de cada departamento de la empresa, c) Autorizar la implementación del control interno bajo la responsabilidad de los involucrados y cumpliendo con los criterios de aprobación, d) Consolidar la sociabilización del sistema de control interno implementado en todos los departamentos de la empresa". (p. 88)

En base a la perspectiva del autor es importante proceder con la evaluación del sistema de control interno para su aplicación en la empresa, tomando en cuenta que esta debe cumplir con los criterios de quienes están a cargo de su aprobación e implementación, valorando cada uno de los procedimientos y en relación a los problemas que presentan las áreas que deben ser intervenidas para garantizar el correcto desarrollo de las operaciones cotidianas en aspectos administrativos, contables y operativos.

Ya sea que esté ejecutando una pequeña empresa o una gran corporación, el control interno es una parte importante para asegurar que las operaciones del negocio

sean eficientes y consistentes en general. Los controles internos están diseñados para promover la eficiencia de la empresa, la adhesión a las políticas o valores de la empresa y evitar el fraude, el uso no autorizado o el robo de los activos de una empresa.

Los elementos de un programa de control interno fuerte incluyen la segregación de funciones, procesos de autorización apropiados, inventario y control de activos, buenas prácticas de registro y documentación y supervisión independiente. La empresa debe asegurarse de que incorpora todos estos elementos en el programa de control interno, ya que puede hacer una gran diferencia en la calidad de los productos y servicios que ofrece y en asegurar de que los beneficios de esas actividades están bien protegidos y administrados.

Al dividir la responsabilidad de los diferentes elementos de las actividades relacionadas, las empresas pueden crear un sistema de controles y equilibrios para garantizar que los activos se gestionan adecuadamente y que la empresa cumple con los estándares de calidad, legales y éticos.

Normas Internacionales de Auditoria - NIAs

Las NIAs son emitidas por el International Federation of Accountants (IFAC), hoy International Auditing and Assurance Standards (IAASB) para desarrollar y emitir normas de auditoría. La emisión de estas normas ayuda a mejorar el grado de uniformidad de las prácticas de auditoría y servicios relacionados en todo el mundo. (García, 2016)

El IAASB sigue un riguroso procedimiento. Se recibe opiniones de las partes interesadas, incluido el Grupo Consultivo del IAASB, los organismos emisores de normas de auditoría nacionales, los organismos miembros de IFAC y organismos reguladores y de supervisión, compañías, agencias gubernamentales, inversores. El Consejo de Supervisión del Interés Público (PIOB) supervisa el trabajo del IAASB. (García, 2016)

Las materias que tratan estas normas son evaluación de riesgos y control interno, planificación, evidencia de auditoría, uso de trabajo de otro auditor, importancia relativa, fraude y error, hechos posteriores, etc. Se aprueban a nivel internacional, pero cada país es soberano para decidir si las aplica o no. Un país puede emitir un reglamento que desarrolle esa ley y entre en detalles más técnicos. En el caso de Europa, los países desarrollan su propia ley, pero de acuerdo a la directiva europea sobre auditoría. De este modo, las Normas Internacionales de Auditoría siempre figuran como fuente. La globalización supone cambios para todas las organizaciones. Las Normas Internacionales de Auditoría aportan homogeneidad ante este contexto. (García, 2016)

Aplicación del COBIT en Auditoria de Sistemas

Las empresas poseen un capital activo muy valioso: información y tecnología. Cada vez en mayor medida, el éxito de una empresa depende de la comprensión de ambos componentes. Las buenas prácticas concentradas en el marco de referencia COBIT, permiten que los negocios se alineen con la tecnología de la información para así alcanzar los mejores resultados. La información y la tecnología que la soporta simbolizan los activos más valiosos de muchas empresas, aunque con frecuencia son poco entendidos.

Las empresas exitosas reconocen los beneficios de la tecnología de información y la utilizan para impulsar el valor de sus interesados (stakeholders). Estas empresas también entienden y administran los riesgos asociados, es decir, el aumento en los requerimientos regulatorios, así como también una gran dependencia de muchos de los procesos de negocio en TI. Pero todos estos elementos son clave para el gobierno de la empresa. El valor, el riesgo y el control constituyen la esencia del gobierno de TI. (Santacruz Espinoza, Vega Abad, Pinos Castillo, & Cardenas Villavicencio, 2017)

Gobierno de TI

Fuente: (BIT Company, 2015)

La orientación al negocio que realiza COBIT consiste en vincular las metas del negocio con las metas de TI, brindando métricas y modelos de madurez para medir los logros, e identificando las responsabilidades asociadas de los propietarios de los procesos de negocio y de TI. El enfoque hacia procesos de COBIT se ilustra con un modelo de procesos, el cual subdivide TI en 34 procesos de acuerdo a las responsabilidades de planear (planes de auditoria), construir (Implementar los distintos planes de auditoria), ejecutar (Ejecutar las diferentes planeaciones) y monitorear (verificar y controlar los procesos de ejecución); de esta manera, se ofrece una visión de punta a punta de la TI. El concepto de arquitectura empresarial ayuda a identificar aquellos recursos esenciales para el éxito de los procesos, es decir, aplicaciones, información, infraestructura y personas.

En resumen, para proporcionar la información que la empresa necesita de acuerdo a sus objetivos, los recursos de TI deben ser administrados por un conjunto de procesos agrupados de forma natural que serán controlados a través de la auditoria al momento que se realice implementando el sistema COBIT. (Santacruz Espinoza, Vega Abad, Pinos Castillo, & Cardenas Villavicencio, 2017)

Una respuesta al requerimiento de determinar y monitorear el nivel apropiado de control y desempeño de TI, son los conceptos que COBIT define específicamente:

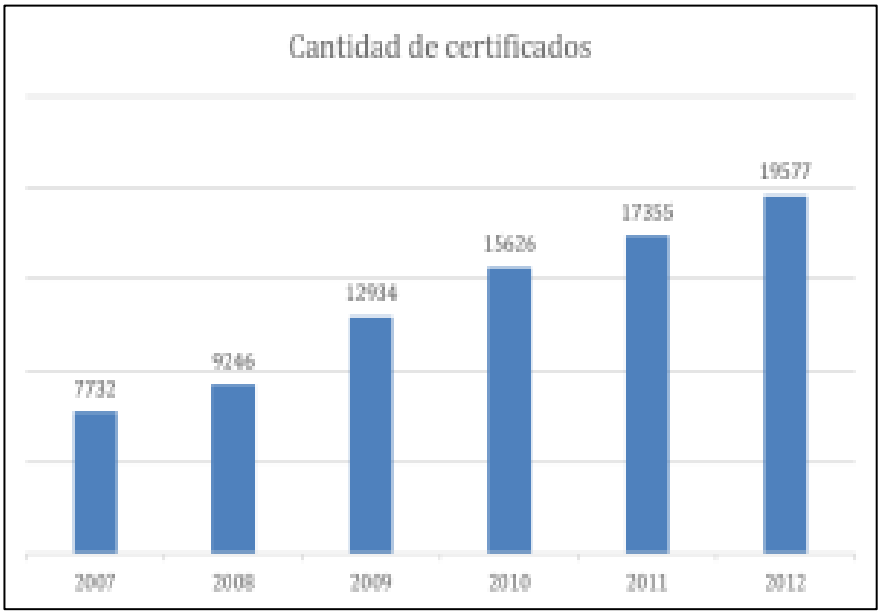
- Benchmarking de la capacidad de los procesos de TI. Son modelos derivados del Modelo de madurez de la Capacidad del Instituto de Ingeniería de Software
- Metas y métricas de los procesos de TI para definir y medir sus resultados y su desempeño, basados en los principios de balanced business Scorecard de Robert Kaplan y David Norton. Es decir, este proceso es para controlar y optimizar el desempeño de las empresas.
- Objetivos de las actividades para controlar estos procesos, con base en los objetivos de control detallados de COBIT. (Santacruz Espinoza, Vega Abad, Pinos Castillo, & Cardenas Villavicencio, 2017)

ISO 27.001 Auditoria de Sistemas de Información

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2. (Segovia, 2018)

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

ISO 27001 se ha convertido en la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento; aquí se puede ver la cantidad de certificados en los últimos años:



Fuente: ISO/IEC 27001:2013

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).

Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

Fuente: ISO/IEC 27001:2013

Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software, pero utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad.

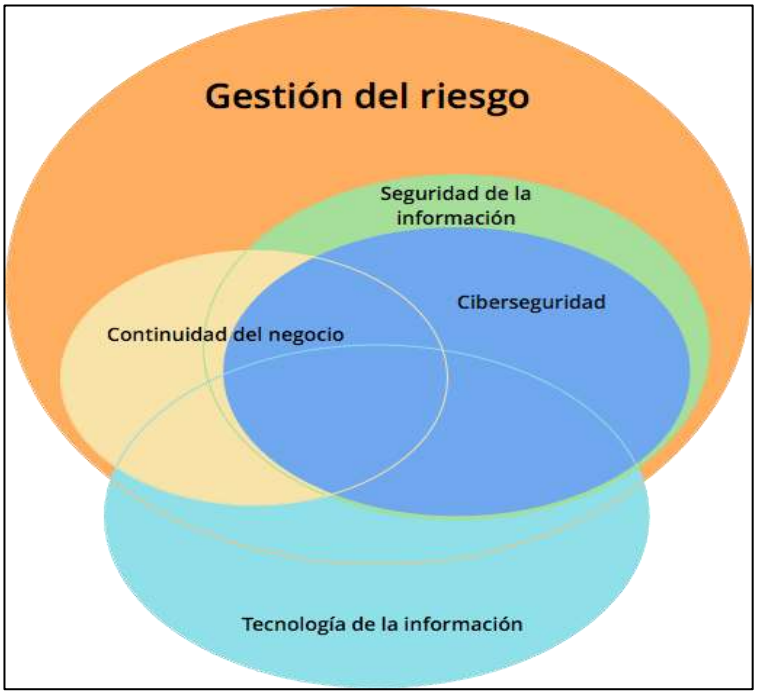
Como este tipo de implementación demandará la gestión de múltiples políticas, procedimientos, personas, bienes, etc., ISO 27001 ha detallado cómo amalgamar todos estos elementos dentro del sistema de gestión de seguridad de la información (SGSI).

Por eso, la gestión de la seguridad de la información no se acota solamente a la seguridad de TI (por ejemplo, cortafuegos, antivirus, etc.), sino que también tiene que ver con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etc.

Ventajas de la implementación de ISO 27.001

Hay 4 ventajas comerciales esenciales que una empresa puede obtener con la implementación de esta norma para la seguridad de la información:

- Cumplir con los requerimientos legales – cada vez hay más y más leyes, normativas y requerimientos contractuales relacionados con la seguridad de la información. La buena noticia es que la mayoría de ellos se pueden resolver implementando ISO 27001 ya que esta norma le proporciona una metodología perfecta para cumplir con todos ellos.
- Obtener una ventaja comercial – si su empresa obtiene la certificación y sus competidores no, es posible que usted obtenga una ventaja sobre ellos ante los ojos de los clientes a los que les interesa mantener en forma segura su información.
- Menores costos – la filosofía principal de ISO 27001 es evitar que se produzcan incidentes de seguridad, y cada incidente, ya sea grande o pequeño, cuesta dinero; por lo tanto, evitándolos su empresa va a ahorrar mucho dinero. Y lo mejor de todo es que la inversión en ISO 27001 es mucho menor que el ahorro que obtendrá.
- Una mejor organización – en general, las empresas de rápido crecimiento no tienen tiempo para hacer una pausa y definir sus procesos y procedimientos; como consecuencia, muchas veces los empleados no saben qué hay que hacer, cuándo y quién debe hacerlo. La implementación de ISO 27001 ayuda a resolver este tipo de situaciones ya que alienta a las empresas a escribir sus principales procesos (incluso los que no están relacionados con la seguridad), lo que les permite reducir el tiempo perdido de sus empleados.



Fuente: ISO/IEC 27001:2013

Marco legal

Ley de Telecomunicaciones del Ecuador

La ley de telecomunicaciones del Ecuador es uno de los instrumentos legales de especial relevancia para el presente trabaja investigativo. En esta ley se pueden extraer los términos tanto técnicos como legales relacionados con la actividad de las telecomunicaciones, el derecho del ciudadano ecuatoriano, el uso de radiofrecuencias, las concesiones y las obligaciones de las compañías encargadas de la prestación de servicios de telecomunicaciones en territorio nacional.

Regulaciones de la Agencia de Regulación y Control de las Telecomunicaciones 2017 - 2018

Tarifa Preferencial SMA. Se emitió la resolución ARCOTEL-2017-1286 que establece los techos tarifarios para tarifas preferenciales en el servicio móvil avanzado, focalizado en mejorar e impulsar la asequibilidad del servicio, por parte de los grupos sociales de atención prioritaria beneficiarias del bono de desarrollo humano (BDH) y pensiones, que se encuentran registradas en el Ministerio de

Inclusión Económica y Social, de manera de favorecer el desarrollo económico del servicio universal. (ARCOTEL, 2017)

Tasa administrativa para el procedimiento de homologación. Se elaboró el modelo de valoración para la determinación de la tasa administrativa para el procedimiento de homologación simplificado de los equipos terminales no homologados del SMA. La medida busca regularizar el pago de la homologación de aquellos equipos no homologados que se encuentren activos en las redes de los prestadores el servicio móvil avanzado. (ARCOTEL, 2017)

Senda Regulatoria. Se emitió una regulación que propende el establecimiento de nuevos cargos de interconexión fijo y móvil, cuyo efecto fue la disminución de cargos de interconexión, de modo de incentivar el mercado con reducción de tarifas al usuario. (ARCOTEL, 2017)

Normativa para la Operación de Equipos Inhibidores de Señal del Servicio Móvil Avanzado (SMA). Regulación para la prohibición de la utilización de equipos inhibidores de señal del SMA en todo el territorio ecuatoriano, excepto en el interior de los centros de rehabilitación social y aquellas instituciones gubernamentales que manejen información de carácter sensible o confidencial. (ARCOTEL, 2017)

Marco conceptual

Sujeto activo

Se llama así a las personas que cometen los delitos informáticos. Son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos. (Delitos Informaticos, 2019)

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que "entra" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes. (Delitos Informaticos, 2019)

Hackers

Aunque en el uso general es frecuente asociar la palabra hacker a 'pirata informático' y, por tanto, a quien usa sus conocimientos con fines ilegales, en el ámbito de la informática se diferencia claramente entre hacker y cracker. Así lo recogen los principales diccionarios de inglés y algunos de español como el de María Moliner, que indica que un hacker es una 'persona con sólidos conocimientos informáticos capaz de introducirse sin autorización en sistemas ajenos para manipularlos, obtener información, etc., o simplemente por diversión'. (Fundeu BBVA, 2017)

Sombrero blanco

Los hackers de sombrero blanco, son personas que utilizan sus conocimientos para hacer el bien; incluso muchas empresas contratan a hacker de sombrero blanco para así poder encontrar las vulnerabilidades de sus plataformas, así evitan que un hacker de sombrero negro pueda vulnerar sus plataformas. Aunque los hackers de sombrero blanco usan los mismos métodos de piratería, ellos se diferencias que ingresan a las plataformas con el permiso de los propietarios, esto hace que todas sus actividades sean legales; así pueden hacer pruebas de seguridad y conocer la vulnerabilidad de las empresas. (Delitos Informaticos, 2019)

Sombrero negro

Los hackers de sombrero negro, son personas que cuentan con un conocimiento amplio para pasar todos los protocolos de seguridad, así pueden ingresar a cualquier red informática, sin ningún problema; además son las personas que realizan malware, así pueden obtener acceso a cualquier ordenador. La

motivación de este hacker es el beneficio personal y financiero, los hackers de sombrero negro, son las personas que se encuentran implicados en los espionajes cibernéticos; estas personas tienen la capacidad para propagar los malware o robar cualquier información financiera. (Delitos Informaticos, 2019)

Sombrero gris

Los hackers de sombrero gris, son las personas que realizan actividades que ejecutan los hackers de sombrero negro y sombrero blanco; los hackers de sombrero gris buscan vulnerabilidad de los sistemas con o sin el permiso de los propietarios de las plataformas. En caso que el hacker consiga un problema en la plataforma se comunica con el propietario, así le solicita una tarifa monetaria, así solucionan el problema de vulnerabilidad, pero si el propietario no cumple, el hacker publica la información al público. Así que la próxima vez que escuches la palabra hackers, no se debe asociar directamente a los ciberdelincuentes. (Delitos Informaticos, 2019)

Cracker

La palabra cracker, en cambio, se aplica a quien, además de ser capaz de entrar en sistemas ajenos, lo hace con fines delictivos, como señala el diccionario de Oxford. (Fundeu BBVA, 2017)

Capítulo 2: Metodología

Diseño de Investigación

Partiendo desde el diseño de la investigación, la misma que es orientada hacia el modelo no experimental, es decir que el investigador deberá realizar la recopilación de la información de fuentes primarias sin que ésta sufra modificaciones o alteraciones que desvíen los criterios y conclusiones acerca de la misma.

Tipo de Investigación

El tipo de investigación seleccionada para el presente proceso investigativo, es de tipo mixto ya que asocia dos de los principales tipos. En la misma confluyen los análisis de tipo descriptivo y los modelos relacionales no estadísticos.

Se usará el tipo descriptivo de investigación ya que al recopilar la información objetivo acerca de la actual situación del entorno de control de las compañías pertenecientes al sector de las telecomunicaciones, se analizará dicha información con fines netamente descriptivos sin establecer esquemas correlativos sobre la cual haya que realizar el cálculo del coeficiente estadístico.

En concordancia con lo mencionado al final del párrafo anterior. Es necesario puntualizar que si bien no se usara técnicas estadísticas para cálculo de coeficientes de correlación. Si se hará énfasis en análisis relacionales de la información bajo el enfoque cualitativo. Esto ya que mediante el instrumento de medición del entorno de control se recopilara información de tipo especifica (tabulada) e información recopilada por medio de respuestas abiertas mediante la cual el entrevistado ofrecerá detalles adicionales de la información solicitada mediante el instrumento de investigación.

Alcance de la Investigación

El alcance de la presente investigación se estructura considerando las empresas pertenecientes al sector de las telecomunicaciones y cuyo domicilio de la matriz u oficina principal se encuentre en la ciudad de Guayaquil. Además, también debe considerarse que la información recopilada mediante el instrumento de

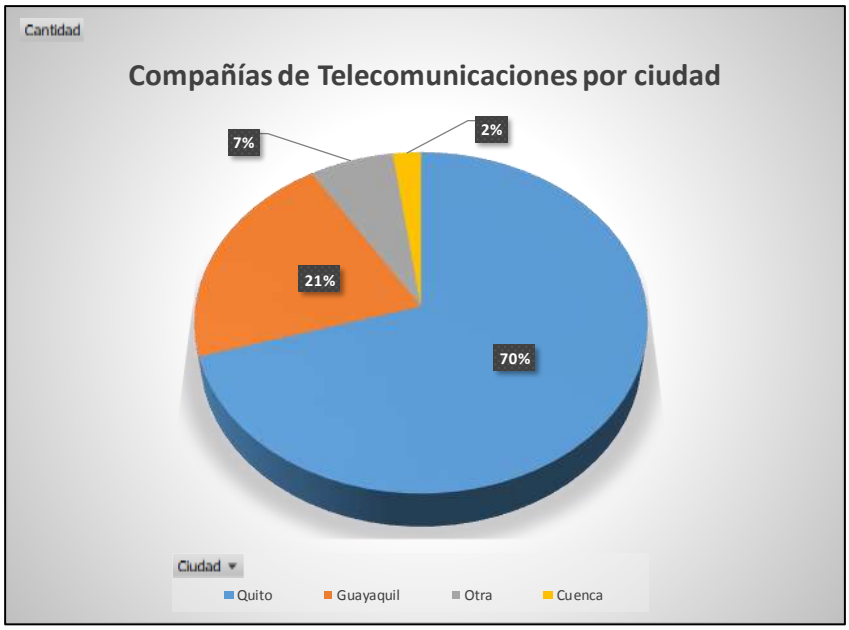
investigación. Hace referencia a únicamente las transacciones, análisis, procesos, métodos o estrategias aplicadas en la compañía durante los dos últimos periodos cerrados, es decir a los años 2017 y 2018.

Población y muestra

Población

Ver anexo de listado completo

Ciudad	Cantidad
Quito	64
Guayaquil	19
Otra	6
Cuenca	2
Total general	**91**



Muestra

Ya que el tamaño de la población objetivo (19 empresas de telecomunicaciones domiciliadas en la ciudad de Guayaquil) no es representativo estadísticamente, el tipo de muestreo seleccionado es el muestreo no probabilístico.

El muestreo no probabilístico es una técnica de muestreo donde las muestras se recogen en un proceso que no brinda a todos los individuos de la población iguales oportunidades de ser seleccionados. A diferencia del muestreo probabilístico, la muestra no probabilística no es un producto de un proceso de selección aleatoria. Los sujetos en una muestra no probabilística generalmente son seleccionados en función de su accesibilidad o a criterio personal e intencional del investigador. (Explorable, 2009)

Muestreo discrecional

El muestreo discrecional es más comúnmente conocido como muestreo intencional. En este tipo de toma de muestras, los sujetos son elegidos para formar parte de la muestra con un objetivo específico. Con el muestreo discrecional, el investigador cree que algunos sujetos son más adecuados para la investigación que

otros. Por esta razón, aquellos son elegidos deliberadamente como sujetos. (Explorable, 2009).

Guayaquil	19
AMERICAN CALL CENTER S.A. (AMERICALL)	1
BONOPRICE C. LTDA.	1
Broadnet S.A.	1
BUSINNESS MARKET S.A. MARKEBUSSI	1
Comsatel S.A.	1
COMUNICACIONES Y TELEFONIA MULTIPLES S.A. MULTICOM – TELEMOVIL	1
Consorcio Ecuatoriano de Telecomunicaciones S.A. Conecel	1
Duocell S.A.	1
EMPRESA DE TELEVISION SATELCOM SA	1
ESPOLTEL S.A.	1
Ingeniería En Radio y Comunicaciones I.R.C. Cia.Ltda.	1
METRO DISTRIBUIDORA METRODIST S. A.	1
Negocios y Telefonía (Nedetel) S.A.	1
Nokia Solutions And Networks Ecuador S.A.	1
PRYSCOM DEL ECUADOR S.A.	1
Soluciones Especializadas de Ingeniería en Telemática S.A.	1
Telconet S.A.	1
Tele - Red, Telecomunicaciones y Redes S.A.	1
UNIVISA S.A.	1

Novedad de lo que se investiga

La presente investigación tiene un gran impacto desde el punto de vista crítico en la rama contable, Auditoría y Control Interno en el país. Ya que las empresas de telecomunicación giran en torno a mercados de los cuales se tienen largos e históricos antecedentes en el Ecuador acerca de los casos de corrupción en los cuales haya tenido participación tanto la empresa privada como el sector público.

Instrumento de investigación

El instrumento de investigación que se usara para la recopilación de la información y aspectos relevantes acerca de entorno de control y seguridad de la información y comunicación, fue estructurado con base a criterios de estándares internacionales como la ISO, COBIT entre otros. Y consiste en reflejar mediante una escala numérica el nivel de cumplimiento de cada uno de los puntos que una organización debe cumplir para poseer una infraestructura tecnológica y sistemas de información y comunicación acorde a los niveles que este tipo de industria requiere.

A continuación, se describen los (7) criterios generales considerados en el cuestionario investigativo.

ID/ITEM	CARGO	ITEM
A	Responsable de SI/Responsable de TICs.	Control de acceso
B	Responsable de SI.	Criptografía
C	Responsable de la seguridad. física/Responsable de SI/Líderes de los procesos.	Seguridad física y del entorno
D	Responsable de TICs Responsable de SI	Seguridad de las operaciones
E	Responsable de TICs Responsable de SI.	Seguridad de las comunicaciones

F	Responsable de SI/Responsable de TICs.	Adquisición, desarrollo y mantenimiento de sistemas
G	Responsable de SI/Responsable de TICs.	Gestión de incidentes de seguridad de la información

---

Estos aspectos generales contienen a su vez varias secciones y finamente las secciones están compuestas por uno o varios aspectos de investigación los cuales son objeto de recopilación de información y medición del entorno de control tecnológico. Estos serán evaluados de menor a mayor en una escala de cumplimiento que consta de cuatro niveles como se muestra a continuación:

Menor --------- Escala de cumplimiento -------- Mayor			
1. Completamente de acuerdo	**2. De acuerdo**	**3. Poco De acuerdo**	**4. En desacuerdo**

En seguida se muestra el detalle del cuestionario por cada uno de los criterios generales mencionados anteriormente.

Resultados de la información recopilada

Resultado en el criterio de: Control de acceso

De acuerdo a los resultados recopilados en las entrevistas realizadas tanto el representante de TELCONET como el representante de CNT E.P. coincidieron en estar completamente de acuerdo en que se debe establecer una política de control de accesos y los dispositivos de control de acceso a redes y a servicios en la red. Sin embargo, ambos coinciden en que, si bien es cierto que la política es prioritaria, en su aplicación se reflejan las siguientes dificultades

Dificultades para su aplicación:

- La política se emite, pero en muchas ocasiones no existe responsable de actualizarla y los criterios quedan obsoletos
- Los medios de difusión de políticas de este tipo (tecnológicos) suceden una única vez al vincular a una persona y desde ahí no se vuelven a difundir
- Los permisos asociados con los usuarios no se revisan con periodicidad sino únicamente cuando sucede un incidente
- Por lo general se tarda mucho tiempo o no se realiza la eliminación o bloqueo de usuarios correspondientes a ex trabajadores de la compañía que ya no laboran en la misma.
- En los presupuestos financieros no se destinan partidas a la adquisición de software de control y monitoreo de este tipo de operaciones.

Resultado en el criterio de Criptografía

Todos los entrevistados coincidieron en que se debe facilitar a la compañía en sus diferentes niveles el uso de criptografía para protección de la información de agentes externos a la misma.

Dificultades para su aplicación:

- Los departamentos de sistemas o tecnología no cuentan con conocimientos idóneos acerca de uso de técnicas de criptografía y protección de ataques cibernéticos.
- En los presupuestos anuales no se considera la asesoría de profesionales externos para fines de niveles de seguridad y protección criptográfica.
- El personal de la compañía indistinto del área, no posee conocimientos en criptografía.

Resultado en el criterio de: Seguridad física y del entorno

Todas las compañías entrevistadas coincidieron al estar completamente de acuerdo en que, en pro de la mejora del control en entornos tecnológicos, se debería definir, establecer, controlar y dar seguimiento para que la compañía cuente con;

Áreas Seguras y Equipos indispensables para prevenir la discontinuidad de las operaciones del negocio.

Dificultades para su aplicación:

- Entre las principales dificultades se encuentra el costo de adquisición, instalación y mantenimiento de infraestructura tecnológica.
- Los departamentos de contabilidad, activos fijos y/o Sistemas, no establecen un sistema para el control de los bienes de la compañía tanto de aquellos comprados por la misma y que forman parte de los activos tecnológicos, como aquellos establecidos de acuerdo a cláusulas contractuales mediante comodato.

Resultado en el criterio de: Seguridad de las operaciones

En el aspecto de la seguridad de las operaciones, todas las compañías entrevistadas indican estar completamente de acuerdo en que las operaciones de la misma deben ser realizadas en entornos tecnológicos seguros que brinden la confiabilidad al giro de negocio y le permitan la exploración segura de nuevas posibilidades, nichos de mercados, rutas de optimización, resultados financieros, etc.

Dificultades para su aplicación:

- Falta de actualización o no contar con manuales de usuarios de sistemas.
- Poca adaptabilidad o actualización de los procedimientos/manuales/instructivos respecto de cambios en las estrategias corporativas y exploración de nuevas líneas de negocio.
- Costos elevados de antivirus y software de protección de la infraestructura tecnológica.
- Costo de análisis técnico de vulnerabilidades.
- Falta de coordinación en actividades de auditoria de sistemas.

Resultado en el criterio de: Seguridad de las comunicaciones

Todas las empresas entrevistadas coincidieron al estar totalmente de acuerdo en que las comunicaciones de la compañía deben realizarse en entornos seguros y mediante equipos e instrumentos que garanticen dicha premisa. Sin embargo, al igual que en los puntos anteriores encontraron dificultades en la práctica.

Dificultades para su aplicación:

- Costos del hardware que garanticen eficientes niveles en la seguridad y control de las comunicaciones.
- Costos elevados de software que contribuyan al control de las comunicaciones.
- Los controles en las comunicaciones por lo general representan tiempos de espera que los niveles ejecutivos los perciben como retrasos en la comunicación.
- Falta de cultura de seguridad cibernética en las comunicaciones por parte de los empleados de la compañía.
- Falta de clasificación y categorización de la información fuente manejada dentro de la compañía.

Resultado en el criterio de Adquisición, desarrollo y mantenimiento de sistemas

A pesar de estar completamente de acuerdo en todos los puntos de este tema, se mencionaron las siguientes dificultades.

Dificultades para su aplicación:

- Falta de estándares y política de clasificación de la información de la compañía.
- Falta de procedimientos autorizados y rutas claras en la adquisición, implementación y mantenimiento de infraestructura tecnológica acorde con los lineamientos mencionados anteriormente.

Resultado en el criterio de: Gestión de incidentes de seguridad de la información.

Los principales obstáculos o dificultades en los cumplimientos de dichos principios s a pesar de estar todos los entrevistados completamente de acuerdo, son los siguientes:

Dificultades para su aplicación:

- Falta de idoneidad para la evaluación integral de incidentes tecnológicos.
- Deficiencia en el manejo de metodologías de mejora continúa para la prevención y/o correcciones de incidentes tecnológicos que afecten la seguridad del entorno de control.

Capítulo 3: Resultados.

Análisis de resultados

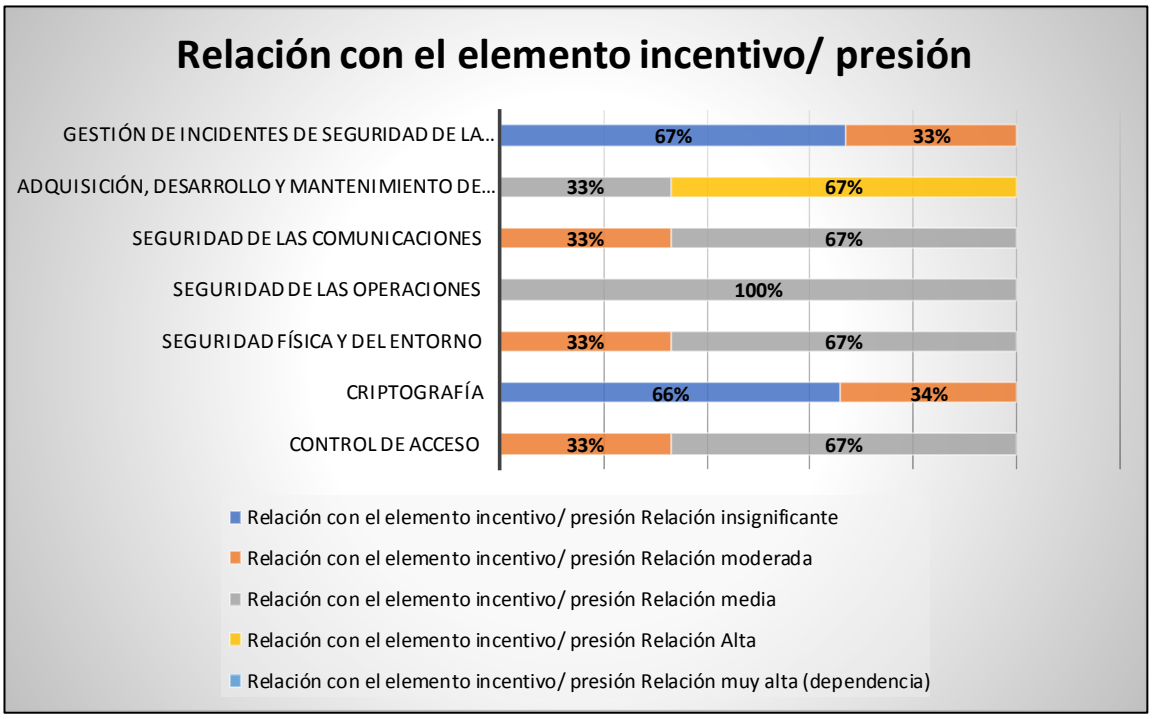
Si bien en la sección anterior se ha realizado el análisis cualitativo de los cuestionarios llenados por las empresas que brindaron la información solicitada, se puede analizar los diferentes entornos de control interno mediante el uso del cuestionario. Sin embargo adicional se solicitó a las empresas encuestadas realizar una estimación considerando la extensa experiencia que los profesionales de auditoría y control interno tienen, llenar una matriz diseñada a partir del conocimiento empírico del giro de negocio y contrastada con la teoría del fraude, es decir el triángulo de condiciones para el cometimiento del fraude empresarial.

Se sabe que las condiciones que deben configurarse para el cometimiento del fraude teóricamente según Cressey (1961), son las siguientes:

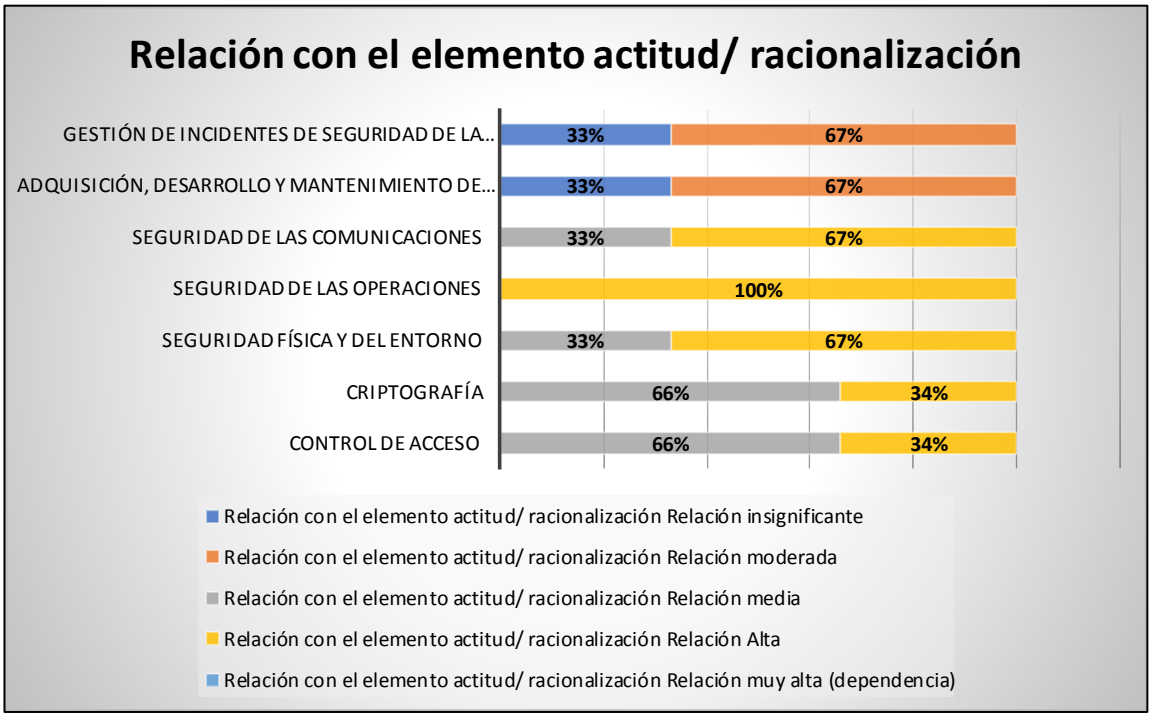
- El elemento incentivo/ presión
- El elemento actitud/ racionalización
- El elemento de la oportunidad

Con base a estos tres postulados que se han analizado ya desde hace varias décadas, se ha procedido al contraste con el supuesto no consentido ambiente de bajo control en los aspectos evaluados mediante el cuestionario de entornos tecnológicos. Los resultados obtenidos fueron los siguientes:

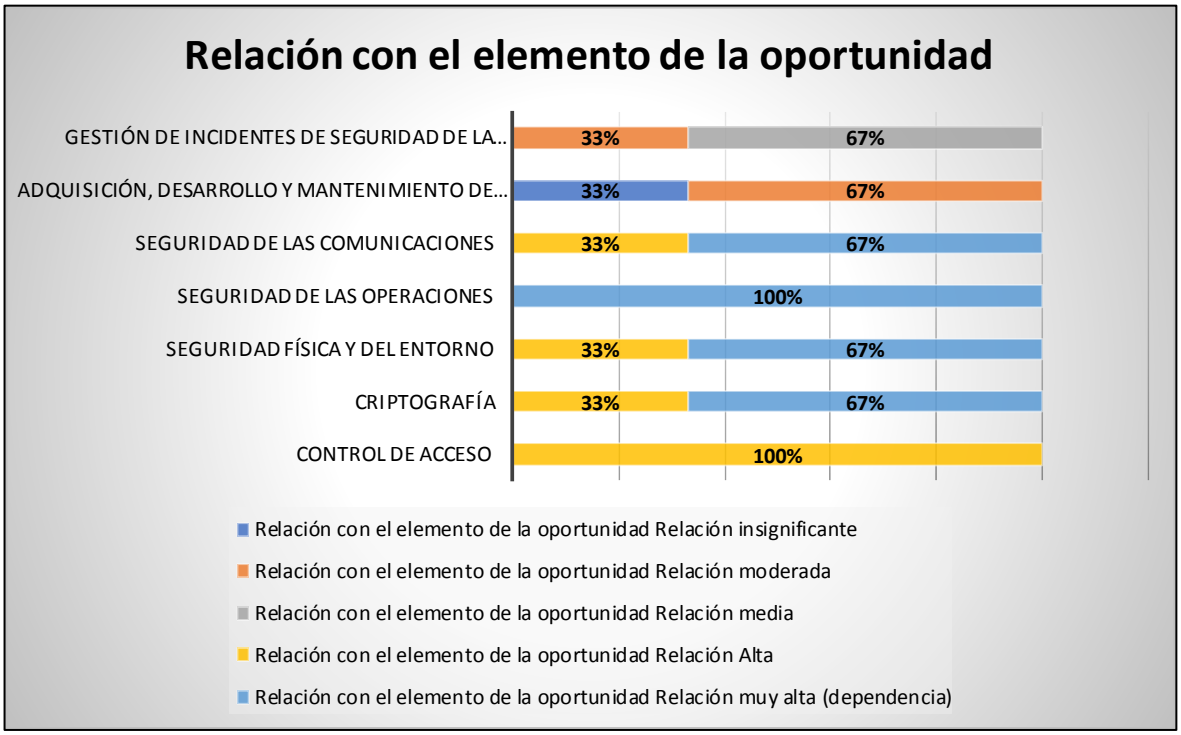
Aspectos del entorno tecnológicos afectados por bajo nivel de control	Relación con el elemento incentivo/ presión				
	Relación insignificante	Relación moderada	Relación media	Relación Alta	Relación muy alta (dependencia)
Control de acceso		33%	67%		
Criptografía	66%	34%			
Seguridad física y del entorno		33%	67%		
Seguridad de las operaciones			100%		
Seguridad de las comunicaciones		33%	67%		
Adquisición, desarrollo y mantenimiento de sistemas			33%	67%	
Gestión de incidentes de seguridad de la información	67%	33%			



Aspectos del entorno tecnológicos afectados por bajo nivel de control	Relación con el elemento actitud/ racionalización				
	Relación insignificante	Relación moderada	Relación media	Relación Alta	Relación muy alta (dependencia)
Control de acceso			66%	34%	
Criptografía			66%	34%	
Seguridad física y del entorno			33%	67%	
Seguridad de las operaciones				100%	
Seguridad de las comunicaciones			33%	67%	
Adquisición, desarrollo y mantenimiento de sistemas	33%	67%			
Gestión de incidentes de seguridad de la información	33%	67%			



Aspectos del entorno tecnológicos afectados por bajo nivel de control	Relación con el elemento de la oportunidad				
	Relación insignificante	Relación moderada	Relación media	Relación Alta	Relación muy alta (dependencia)
Control de acceso				100%	
Criptografía				33%	67%
Seguridad física y del entorno				33%	67%
Seguridad de las operaciones					100%
Seguridad de las comunicaciones				33%	67%
Adquisición, desarrollo y mantenimiento de sistemas	33%	67%			
Gestión de incidentes de seguridad de la información		33%	67%		



De acuerdo a los resultados obtenidos en los tres últimos gráficos y tablas se puede llegar a varias conclusiones preliminares que deberán ser discutidas en el presente capitulo:

Las compañías de telecomunicaciones evaluadas mediante el cuestionario, tienen clara la diferencia entre ambientes tradicionales y ambientes tecnológicos y como esta realidad ha repercutido en los cambios de métodos y estrategias de las direcciones corporativas.

Se evidencia que existe clara conciencia, incluso interés acerca de temas asociados a tecnologías de la información, comunicaciones, dispositivos de control y seguimiento de la información, políticas de seguridad de la información, ciberseguridad, codificación y barreras contra incendios, entro otros aspectos importantes en materia de control y prevención de fraudes.

Uno de los puntos que más destaco en la información recopilada fue el hecho que a pesar de los aspectos de seguridad asociados al control de ambientes tecnológicos eran de idoneidad de los profesionales encargados de las instancias de sistemas, existieron aspectos o puntos específicos que no estaban dentro del dominio de dichos profesionales. La probabilidad que estuvieran dentro del dominio de profesionales de control y auditoria resultaron aun menores. Por lo que es posible evidenciar falta de preparación, capacitación y experiencia en dichos aspectos.

Hallazgos y propuesta

Después de los resultados obtenidos mediante la recopilación de datos en la metodología de investigación. Se ha estructurado la siguiente propuesta investigativa que consiste en el diseño de una metodología de revisión y auditoria operacional de una compañía de telecomunicaciones orientada a la detección de fraudes. La presente metodología cuenta con varias fases y ha sido diseñada con base en la información recopilada de las compañías que contribuyeron en el llenado del cuestionario que consta en la metodología de investigación además de proporcionarnos información

relevante acerca de las dificultades para cumplir con los estándares en seguridad de la información que fueron planteados mediante el mencionado formulario.

La propuesta investigativa puede plantearse de la siguiente forma resumida en el diagrama mostrado a continuación:

Diagnóstico de Control Interno

Para el diagnostico de control interno se tomará como referencia los puntos observados en la metodología de investigación, sin embargo, la escala de cumplimiento de los diferentes puntos en el estándar de control en ambientes tecnológicos ha sido cambiado, con el objetivo de brindar una visión y resultados mucho más claros en la ejecución de dicho diagnóstico.

A continuación, se ha diseñado el formulario en donde el ejecutor o revisor deberá marcar con una (x) de acuerdo a la entrevista realizada en que instancia de cumplimiento la organización refleja el manejo de sus operaciones.

ID/ITEM	ITEM	La administración no tiene conocimiento de este tema	La administración tiene mínimo conocimiento del tema	Se tiene conocimiento medio	Se tiene conocimiento y se está consciente de los riesgos asociados	Se tiene conocimiento y los riesgos han sido medidos al menos una vez al año	Se tiene conocimiento y los riesgos son medidos frecuentemente	Existe medición de riesgos y medidas para mitigarlos	Se revisa frecuentemente los resultados de las medidas tomadas para administrar riesgos	Se cuenta con políticas y procedimientos que se revisar con poca frecuencia	Existe una clara metodología de políticas, procedimientos, instructivos y administración de riesgos.
CONTROL DE ACCESO											
A	**CONTROL DE ACCESO**	**Promedio ponderado del criterio general**									
A.1	**REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO**	**Promedio ponderado de la sección del criterio**									
A.1.1	**Política de control de acceso**										
A.1.2	Acceso a redes y a servicios en red										

A.2	GESTIÓN DE ACCESO DE USUARIOS	**Promedio ponderado de la sección del criterio**									
A.2.1	Registro y cancelación del registro de usuarios										
A.2.2	Suministro de acceso de usuarios										
A.2.3	Gestión de derechos de acceso privilegiado										
A.2.4	Gestión de información de autenticación secreta de usuarios										
A.2.5	Revisión de los derechos de acceso de usuarios										
A.2.6	Retiro o ajuste de los derechos de acceso										

A.3	**RESPONSABILIDAD ES DE LOS USUARIOS**	**Promedio ponderado de la sección del criterio**									
A.3.1	Uso de información de autenticación secreta										
A.3.2	CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	**Promedio ponderado de la sección del criterio**									
A.3.3	Restricción de acceso a la información										
A.3.4	Procedimiento de ingreso seguro										
A.3.5	Sistema de gestión de contraseñas										
A.3.6	Uso de programas utilitarios privilegiados										
A.3.7	Control de acceso a códigos fuente de programas										

ID/ITEM	ITEM	La administración no tiene conocimiento de este tema	La administración tiene mínimo conocimiento del tema	Se tiene conocimiento medio	Se tiene conocimiento y se está consciente de los riesgos asociados	Se tiene conocimiento y los riesgos han sido medidos al menos una vez al año	Se tiene conocimiento y los riesgos son medidos frecuentemente	Existe medición de riesgos y medidas para mitigarlos	Se revisa frecuentemente los resultados de las medidas tomadas para administrar riesgos	Se cuenta con políticas y procedimientos que se revisar con poca frecuencia	Existe una clara metodología de políticas, procedimientos, instructivos y administración de riesgos.
CRIPTOGRAFÍA											
B	**CRIPTOGRAFÍA**	**Promedio ponderado del criterio general**									
B.1	**CONTROLES CRIPTOGRÁFICOS**	**Promedio ponderado de la sección del criterio**									
B.1.1	**Política sobre el uso de controles criptográficos**										
B.1.2	Gestión de llaves										

ID/ITEM	ITEM	La administración no tiene conocimiento de este tema	La administración tiene mínimo conocimiento del tema	Se tiene conocimiento medio	Se tiene conocimiento y se está consciente de los riesgos asociados	Se tiene conocimiento y los riesgos han sido medidos al menos una vez al año	Se tiene conocimiento y los riesgos son medidos frecuentemente	Existe medición de riesgos y medidas para mitigarlos	Se revisa frecuentemente los resultados de las medidas tomadas para administrar riesgos	Se cuenta con políticas y procedimientos que se revisar con poca frecuencia	Existe una clara metodología de políticas, procedimientos, instructivos y administración de riesgos.
SEGURIDAD FÍSICA Y DEL ENTORNO											
C	**SEGURIDAD FÍSICA Y DEL ENTORNO**	**Promedio ponderado del criterio general**									
C.1	**ÁREAS SEGURAS**	**Promedio ponderado de la sección del criterio**									
C.1.1	**Perímetro de seguridad Física**										
C.1.2	Controles físicos de Entrada										
C.1.3	Seguridad de oficinas, recintos e instalaciones										
C.1.4	Protección contra amenazas externas y ambientales										
C.1.5	Trabajo en áreas seguras										
C.1.6	Áreas de despacho y Carga										

C.2	EQUIPOS	Promedio ponderado de la sección del criterio									
C.2.1	Ubicación y protección de los equipos										
C.2.2	Servicios de suministro										
C.2.3	**Seguridad del cableado**										
C.2.4	Mantenimiento de Equipos										
C.2.5	Retiro de activos										
C.2.6	Seguridad de equipos y activos fuera de las instalaciones										
C.2.7	Disposición segura o reutilización de equipos										
C.2.8	Equipos de usuario desatendidos										
C.2.9	Política de escritorio limpio y pantalla limpia										

ID/ITEM	ITEM	La administración no tiene conocimiento de este tema	La administración tiene mínimo conocimiento del tema	Se tiene conocimiento medio	Se tiene conocimiento y se está consciente de los riesgos asociados	Se tiene conocimiento y los riesgos han sido medidos al menos una vez al año	Se tiene conocimiento y los riesgos son medidos frecuentemente	Existe medición de riesgos y medidas para mitigarlos	Se revisa frecuentemente los resultados de las medidas tomadas para administrar riesgos	Se cuenta con políticas y procedimientos que se revisar con poca frecuencia	Existe una clara metodología de políticas, procedimientos, instructivos y administración de riesgos.
SEGURIDAD DE LAS OPERACIONES											
D	**SEGURIDAD DE LAS OPERACIONES**	**Promedio ponderado del criterio general**									
D.1	**PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES**	**Promedio ponderado de la sección del criterio**									
D.1.1	**Procedimientos de operación documentados**										
D.1.2	Gestión de cambios										
D.1.3	Gestión de capacidad										
D.1.4	Separación de los ambientes de desarrollo, pruebas y operación										
D.2	**PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS**	**Promedio ponderado de la sección del criterio**									
D.2.1	Controles contra códigos maliciosos										

D.3	**COPIAS DE RESPALDO**	**Promedio ponderado de la sección del criterio**									
D.3.1	Respaldo de la información										
D.4	REGISTRO Y SEGUIMIENTO	**Promedio ponderado de la sección del criterio**									
D.4.1	**Registro de eventos**										
D.4.2	Protección de la información de registro										
D.4.3	Registros del administrador y del Operador										
D.4.4	Sincronización de relojes										
D.5	CONTROL DE SOFTWARE OPERACIONAL	**Promedio ponderado de la sección del criterio**									
D.5.1	Instalación de software en sistemas operativos										

D.6	GESTIÓN DE LA VULNERABILIDAD TÉCNICA										
D.6.1	Gestión de las vulnerabilidades técnicas										
D.6.2	Restricciones sobre la instalación de software										
D.7	**CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN**	**Promedio ponderado de la sección del criterio**									
D.7.1	Controles sobre auditorías de sistemas de información										

ID/ITEM	ITEM	La administración no tiene conocimiento de este tema	La administración tiene mínimo conocimiento del tema	Se tiene conocimiento medio	Se tiene conocimiento y se está consciente de los riesgos asociados	Se tiene conocimiento y los riesgos han sido medidos al menos una vez al año	Se tiene conocimiento y los riesgos son medidos frecuentemente	Existe medición de riesgos y medidas para mitigarlos	Se revisa frecuentemente los resultados de las medidas tomadas para administrar riesgos	Se cuenta con políticas y procedimientos que se revisar con poca frecuencia	Existe una clara metodología de políticas, procedimientos, instructivos y administración de riesgos.
SEGURIDAD DE LAS COMUNICACIONES											
E	**SEGURIDAD DE LAS COMUNICACIONES**	**Promedio ponderado del criterio general**									
E.1	**GESTIÓN DE LA SEGURIDAD DE LAS REDES**	**Promedio ponderado de la sección del criterio**									
E.1.1	**Controles de redes**										
E.1.2	Seguridad de los servicios de red										
E.1.3	Separación en las redes										
E.2	**TRANSFERENCIA DE INFORMACIÓN**	**Promedio ponderado de la sección del criterio**									
E.2.1	Políticas y procedimientos de transferencia de información										
E.2.2	Acuerdos sobre transferencia de Información										
E.2.3	Mensajería electrónica										
E.2.4	Acuerdos de confidencialidad o de no divulgación										

ID/ITEM	ITEM	La administración no tiene conocimiento de este tema	La administración tiene mínimo conocimiento del tema	Se tiene conocimiento medio	Se tiene conocimiento y se está consciente de los riesgos asociados	Se tiene conocimiento y los riesgos han sido medidos al menos una vez al año	Se tiene conocimiento y los riesgos son medidos frecuentemente	Existe medición de riesgos y medidas para mitigarlos	Se revisa frecuentemente los resultados de las medidas tomadas para administrar riesgos	Se cuenta con políticas y procedimientos que se revisar con poca frecuencia	Existe una clara metodología de políticas, procedimientos, instructivos y administración de riesgos.
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS											
F	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**	**Promedio ponderado del criterio general**									
F.1	**REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN**	**Promedio ponderado de la sección del criterio**									
F.1.1	**Análisis y especificación de requisitos de seguridad de la información**										
F.1.2	Seguridad de servicios de las aplicaciones en redes públicas de red										
F.1.3	Protección de transacciones de los servicios de las aplicaciones										

F.2	**SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE**	**Promedio ponderado de la sección del criterio**									
F.2.1	Política de desarrollo seguro										
F.2.2	Procedimientos de control de cambios en sistemas										
F.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación										
F.2.4	Restricciones en los cambios a los paquetes de software										
F.2.5	Principios de construcción de sistemas seguros										
F.2.6	Ambiente de desarrollo seguro										
F.2.7	Desarrollo contratado externamente										
F.2.8	Pruebas de seguridad de Sistemas										
F.2.9	Prueba de aceptación de sistemas										
F.2.10	**DATOS DE PRUEBA**	**Promedio ponderado de la sección del criterio**									
F.2.11	Protección de datos de prueba										

ID/ITEM	ITEM	La administración no tiene conocimiento de este tema	La administración tiene mínimo conocimiento del tema	Se tiene conocimiento medio	Se tiene conocimiento y se está consciente de los riesgos asociados	Se tiene conocimiento y los riesgos han sido medidos al menos una vez al año	Se tiene conocimiento y los riesgos son medidos frecuentemente	Existe medición de riesgos y medidas para mitigarlos	Se revisa frecuentemente los resultados de las medidas tomadas para administrar riesgos	Se cuenta con políticas y procedimientos que se revisar con poca frecuencia	Existe una clara metodología de políticas, procedimientos, instructivos y administración de riesgos.
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN											
G	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**	**Promedio ponderado del criterio general**									
G.1	**GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN**	**Promedio ponderado de la sección del criterio**									
G.1.1	Responsabilidades y Procedimientos										
G.1.2	Reporte de eventos de seguridad de la información										
G.1.3	Reporte de debilidades de seguridad de la información										
G.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos										
G.1.5	Respuesta a incidentes de seguridad de la información										
G.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información										
G.1.7	Recolección de evidencia										

Medición de Indicadores de Control

Para la medición de indicadores de control se debe tener la conversión de criterios cualitativos en coeficientes cuantitativos, para ello se tomará como guía la siguiente tabla de valores:

Criterio cualitativo	Coeficiente cuantitativo
La administración no tiene conocimiento de este tema	1
La administración tiene mínimo conocimiento del tema	2
Se tiene conocimiento medio	3
Se tiene conocimiento y se está consciente de los riesgos asociados	4
Se tiene conocimiento y los riesgos han sido medidos al menos una vez al año	5
Se tiene conocimiento y los riesgos son medidos frecuentemente	6
Existe medición de riesgos y medidas para mitigarlos	7
Se revisa frecuentemente los resultados de las medidas tomadas para administrar riesgos	8
Se cuenta con políticas y procedimientos que se revisar con poca frecuencia	9
Existe una clara metodología de políticas, procedimientos, instructivos y administración de riesgos.	10

En esta tabla se pueden apreciar los diferentes valores que serán asignados de acuerdo a la marcación obtenida en la tabulación del cuestionario. A continuación, los valores obtenidos en cada ítem deberán ser multiplicados por su peso ponderado para después realizar la sumatoria de las medias ponderadas y obtener el coeficiente de control de cada uno de los factores generales.

ID/ITEM	ITEM	Ponderación asignada por sección del criterio
CONTROL DE ACCESO		
A	**CONTROL DE ACCESO**	**Promedio ponderado del criterio general**
A.1	**REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO**	**Promedio ponderado de la sección del Criterio**
A.1.1	Política de control de acceso	10%
A.1.2	Acceso a redes y a servicios en red	10%
A.2	**GESTIÓN DE ACCESO DE USUARIOS**	**Promedio ponderado de la sección del criterio**
A.2.1	Registro y cancelación del registro de usuarios	5%
A.2.2	Suministro de acceso de usuarios	5%
A.2.3	Gestión de derechos de acceso privilegiado	5%
A.2.4	Gestión de información de autenticación secreta de usuarios	5%
A.2.5	Revisión de los derechos de acceso de usuarios	5%
A.2.6	Retiro o ajuste de los derechos	5%

	de acceso	
A.3	**RESPONSABILIDADES DE LOS USUARIOS**	**Promedio ponderado de la sección del criterio**
A.3.1	Uso de información de autenticación secreta	10%
A.3.2	**CONTROL DE ACCESO A SISTEMAS Y APLICACIONES**	**Promedio ponderado de la sección del criterio**
A.3.3	Restricción de acceso a la información	10%
A.3.4	Procedimiento de ingreso seguro	5%
A.3.5	Sistema de gestión de contraseñas	10%
A.3.6	Uso de programas utilitarios privilegiados	5%
A.3.7	Control de acceso a códigos fuente de programas	10%

ID/ITEM	ITEM	Ponderación asignada por sección del criterio
CRIPTOGRAFÍA		
B	**CRIPTOGRAFÍA**	**Promedio ponderado del criterio general**
B.1	**CONTROLES CRIPTOGRÁFICOS**	**Promedio ponderado de la sección del criterio**
B.1.1	Política sobre el uso de controles criptográficos	50%
B.1.2	Gestión de llaves	50%

ID/ITEM	ITEM	Ponderación asignada por sección del criterio
SEGURIDAD FÍSICA Y DEL ENTORNO		
C	**SEGURIDAD FÍSICA Y DEL ENTORNO**	**Promedio ponderado del criterio general**
C.1	**ÁREAS SEGURAS**	**Promedio ponderado de la sección del criterio**
C.1.1	Perímetro de seguridad física	7%
C.1.2	Controles físicos de entrada	7%
C.1.3	Seguridad de oficinas, recintos e instalaciones	7%
C.1.4	Protección contra amenazas externas y ambientales	7%
C.1.5	Trabajo en áreas seguras	7%
C.1.6	Áreas de despacho y carga	7%
C.2	**EQUIPOS**	**Promedio ponderado de la sección del criterio**
C.2.1	Ubicación y protección de los equipos	5%
C.2.2	Servicios de suministro	5%
C.2.3	Seguridad del cableado	5%
C.2.4	Mantenimiento de equipos	5%

C.2.5	Retiro de activos	10%
C.2.6	Seguridad de equipos y activos fuera de las Instalaciones	10%
C.2.7	Disposición segura o reutilización de equipos	10%
C.2.8	Equipos de usuario desatendidos	5%
C.2.9	Política de escritorio limpio y pantalla limpia	3%

ID/ITEM	ITEM	Ponderación asignada por sección del criterio
SEGURIDAD DE LAS OPERACIONES		
D	**SEGURIDAD DE LAS OPERACIONES**	**Promedio ponderado del criterio general**
D.1	**PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES**	**Promedio ponderado de la sección del criterio**
D.1.1	Procedimientos de operación documentados	5%
D.1.2	Gestión de cambios	5%
D.1.3	Gestión de capacidad	5%
D.1.4	Separación de los ambientes de desarrollo, pruebas y operación	5%
D.2	**PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS**	**Promedio ponderado de la sección del criterio**
D.2.1	Controles contra códigos maliciosos	10%
D.3	**COPIAS DE RESPALDO**	**Promedio ponderado de la sección del criterio**
D.3.1	Respaldo de la información	15%
D.4	**REGISTRO Y SEGUIMIENTO**	**Promedio ponderado de la sección del criterio**
D.4.1	Registro de eventos	5%
D.4.2	Protección de la información de	5%

	registro	
D.4.3	Registros del administrador y del operador	5%
D.4.4	Sincronización de relojes	5%
D.5	**CONTROL DE SOFTWARE OPERACIONAL**	**Promedio ponderado de la sección del criterio**
D.5.1	Instalación de software en sistemas operativos	10%
D.6	**GESTIÓN DE LA VULNERABILIDAD TÉCNICA**	**Promedio ponderado de la sección del criterio**
D.6.1	Gestión de las vulnerabilidades técnicas	10%
D.6.2	Restricciones sobre la instalación de software	10%
D.7	**CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN**	**Promedio ponderado de la sección del criterio**
D.7.1	Controles sobre auditorías de sistemas de Información	5%

ID/ITEM	ITEM	Ponderación asignada por sección del criterio
SEGURIDAD DE LAS COMUNICACIONES		
E	**SEGURIDAD DE LAS COMUNICACIONES**	**Promedio ponderado del criterio general**
E.1	**GESTIÓN DE LA SEGURIDAD DE LAS REDES**	**Promedio ponderado de la sección del criterio**
E.1.1	Controles de redes	15%
E.1.2	Seguridad de los servicios de red	15%
E.1.3	Separación en las redes	15%
E.2	**TRANSFERENCIA DE INFORMACIÓN**	**Promedio ponderado de la sección del criterio**
E.2.1	Políticas y procedimientos de transferencia de información	10%
E.2.2	Acuerdos sobre transferencia de información	10%
E.2.3	Mensajería electrónica	10%
E.2.4	Acuerdos de confidencialidad o de no divulgación	25%

ID/ITEM	ITEM	Ponderación asignada por sección del criterio
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS		
F	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**	**Promedio ponderado del criterio general**
F.1	**REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN**	**Promedio ponderado de la sección del criterio**
F.1.1	Análisis y especificación de requisitos de seguridad de la información	15%
F.1.2	Seguridad de servicios de las aplicaciones en redes Públicas	20%
F.1.3	Protección de transacciones de los servicios de las aplicaciones	15%
F.2	**SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE**	**Promedio ponderado de la sección del criterio**
F.2.1	Política de desarrollo seguro	5%
F.2.2	Procedimientos de control de cambios en sistemas	5%

F.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	5%
F.2.4	Restricciones en los cambios a los paquetes de Software	5%
F.2.5	Principios de construcción de sistemas seguros	5%
F.2.6	Ambiente de desarrollo seguro	5%
F.2.7	Desarrollo contratado externamente	5%
F.2.8	Pruebas de seguridad de sistemas	5%
F.2.9	Prueba de aceptación de sistemas	5%
F.2.10	**DATOS DE PRUEBA**	**Promedio ponderado de la sección del criterio**
F.2.11	Protección de datos de prueba	5%

ID/ITEM	ITEM	Ponderación asignada por sección del criterio
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		
G	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**	**Promedio ponderado del criterio general**
G.1	**GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN**	**Promedio ponderado de la sección del criterio**
G.1.1	Responsabilidades y procedimientos	10%
G.1.2	Reporte de eventos de seguridad de la información	25%
G.1.3	Reporte de debilidades de seguridad de la Información	10%
G.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	10%
G.1.5	Respuesta a incidentes de seguridad de la Información	10%
G.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	10%
G.1.7	Recolección de evidencia	25%

Planificación y Elaboración de pruebas de Auditoria

ID/ITEM	ITEM	Calificación obtenida de la suma ponderada									
		1	2	3	4	5	6	7	8	9	10
A	CONTROL DE ACCESO	Pruebas de detalle de alto alcance			Pruebas de detalle de alcance moderado		Pruebas de detalle de alcance bajo		Pruebas analíticas		
B	CRIPTOGRAFÍA	Pruebas de detalle de alto alcance			Pruebas de detalle de alcance Moderado		Pruebas de detalle de alcance bajo		Pruebas analíticas		
C	SEGURIDAD FÍSICA Y DEL ENTORNO	Pruebas de detalle de alto alcance			Pruebas de detalle de alcance Moderado		Pruebas de detalle de alcance bajo		Pruebas analíticas		
D	SEGURIDAD DE LAS OPERACIONES	Pruebas de detalle de alto alcance			Pruebas de detalle de alcance Moderado		Pruebas de detalle de alcance bajo		Pruebas analíticas		
E	SEGURIDAD DE LAS COMUNICACIONES	Pruebas de detalle de alto alcance			Pruebas de detalle de alcance Moderado		Pruebas de detalle de alcance bajo		Pruebas analíticas		

F	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	Pruebas de detalle de alto alcance	Pruebas de detalle de alcance moderado	Pruebas de detalle de alcance bajo	Pruebas analíticas
G	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Pruebas de detalle de alto alcance	Pruebas de detalle de alcance moderado	Pruebas de detalle de alcance bajo	Pruebas analíticas

Luego de la realización del cálculo ponderado de los coeficientes cuantitativos obtenidos en cada uno de los parámetros evaluados, se tiene el siguiente mapa de pruebas de auditoria que se sugiere realizar para la recopilación de evidencia suficiente y posterior tabulación de resultado.

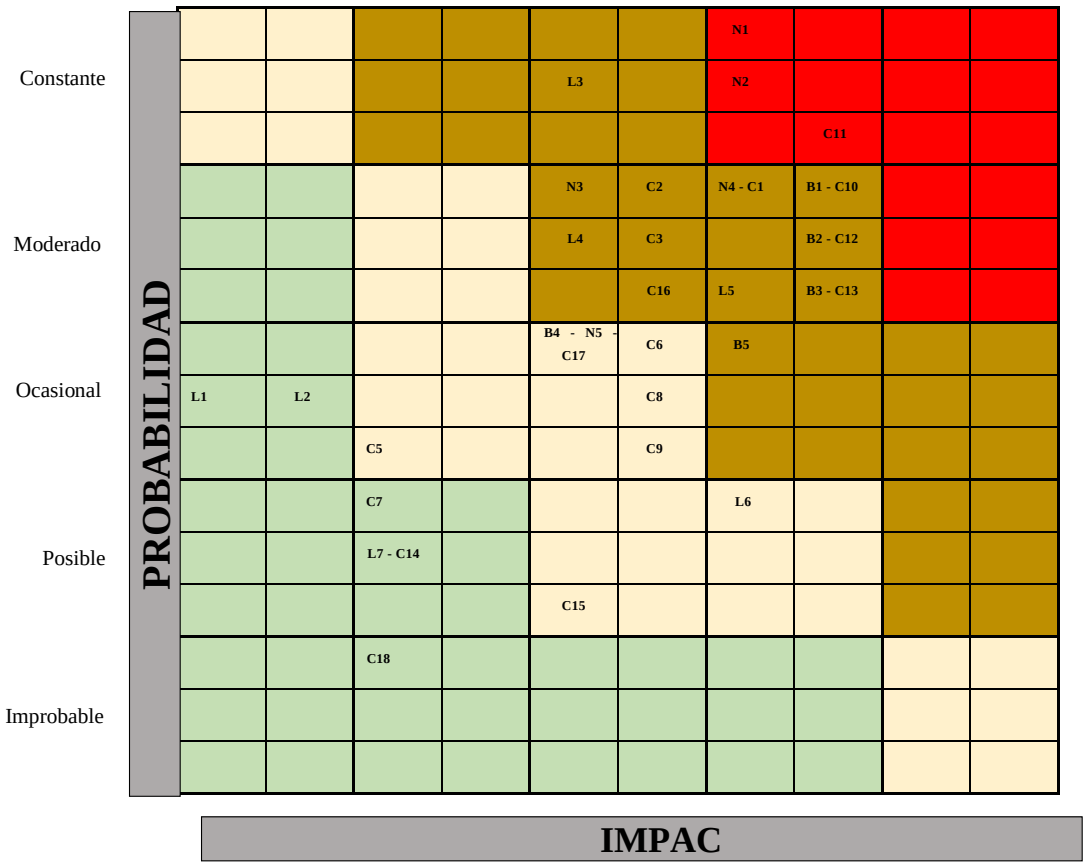
Las pruebas de auditoria deben ser realizadas siguiendo los lineamientos de las Normas Internacionales de Auditoria NIAs y conforme a la práctica profesional para el ejercicio de la auditoria,

Resultados de la Revisión: Matriz de Riesgo de Fraude en Sistemas

Los resultados obtenidos de las pruebas realizadas deben guardar la metodología de observaciones o hallazgos de auditoria y ser tabulados y evidenciados mediante pruebas e información suficiente, incluyendo la probabilidad del hecho evidenciado y el impacto material estimado sobre la presentación de estados financieros y estado de continuidad del negocio. Una vez calculado los parámetros antes mencionados se procederá a realizar la matriz de riesgo de control para la prevención de fraude en entornos tecnológicos, de la siguiente manera.

RIESGO CALCULADO	**NIVEL DE CONTROL ASOCIADO**
Riesgo bajo	Control alto
Riesgo moderado	control Medio
Riesgo alto	control bajo
Riesgo extremo	control bajo

MATRIZ DE RIESGO: (PROBABILIDAD)*(IMPACTO)



Discusión

Con base a los puntos antes expuestos es posible aseverar que el método diseñado y proporcionado contribuirá en gran medida a solucionar los problemas existentes en las dependencias de control y auditoria cuando deban ejecutar revisiones y validaciones de riesgo que deben ser considerados en los planes anuales de auditoria de las compañías de telecomunicaciones.

Sin embargo existe un componente que no se ha analizado con mayor detenimiento y radica en el nivel de preparación e idoneidad de los profesionales de auditoria interna y contraloría en aspectos de tecnologías, control de ambientes tecnológicos, revisiones de integridad de datos y administración de las mismas, entre otros aspectos asociados que por lo general son encargados a un profesional competente pero no necesariamente perteneciente al equipo de auditoria o al staff de auditoria interna de la compañía. Realizar un estudio minucioso de los aspectos asociados para tomar dicha propuesta es un tema de riguroso análisis.

Conclusiones

De acuerdo a la investigación realizada se ha recopilado información suficiente para concluir que los estándares y metodologías de auditorías asociadas a sistemas o entornos tecnológicos se han desarrollado únicamente por medio de marcos normativos asociados a normas internacionales como ISO y COBIT. La prevención de fraude ha sido siempre un esfuerzo conjunto de muchas áreas y no únicamente de la auditoria de sistemas. Sin embargo, también es evidente que en los tiempos actuales los mecanismos de las compañías para la difusión de información, posicionamiento de marca y consecución de objetivos estratégicos, no puede estar desligada de entornos u herramientas tecnológicas. Por ello es de especial importancia de las direcciones de las mismas consideren la evaluación de riesgos tecnológicos que cada una de las acciones que emprenden a fin de evitar potenciales causales de fraude en el mediano plazo.

Entre los aspectos más relevantes asociados al riesgo de fraude en empresas de telecomunicaciones se tienen los siguientes; las compañías no evalúan sus entornos tecnológicos como respuesta a mecanismos de prevención, los mismos obedecen únicamente a eventos puntuales sobre los que se establece una medida correctiva que no necesariamente evita una repercusión o repetición futura. Al menos el 50% de las respuestas obtenidas en la metodología de investigación demostraron que, si bien inicialmente surgió dentro de las compañías el esfuerzo conjunto por la elaboración de políticas de seguridad de la información, esta no ha sido actualizada ni difundida adecuadamente a los nuevos miembros de la compañía los cuales no asocian la importancia de dicho mecanismo de prevención con el código de ética de los empleados de la empresa y por ende subestiman su importancia.

De acuerdo a la información recopilada en empresas de telecomunicaciones mediante la metodología de investigación, los encuestados estuvieron completamente de acuerdo en por lo menos el 95% de los estándares de cumplimientos asociados a; control de accesos, criptografía, seguridad física y del entorno, seguridad de las

operaciones, seguridad de las comunicaciones, adquisición, desarrollo y mantenimiento de sistemas y gestión de incidentes de seguridad de la información. Lo que evidencia que los mandos ejecutivos y el staff de control y revisión están conscientes de la importancia de estos temas. A pesar de ello manifestaron al menos dos dificultades para su mantención y cumplimiento en cada uno de ellos, lo que indicaría finalmente que en caso de ejecutar un diagnostico cuantificado, el coeficiente obtenido en dichas compañías no resultaría tan efectivo.

Por los resultados antes mencionados se puede concluir que el nivel de relación entre la auditoria de sistemas y la prevención de fraudes en las compañías se encuentra altamente relacionado. En la actualidad la auditoria de sistemas ha incorporado varias herramientas que, sin profundizar en los conocimientos técnicos, permite a la dirección de una entidad conocer en detalle y con alta efectividad el riesgo por el cual la institución está atravesando que aumente las probabilidades de futuros entornos perfectos de fraude.

Recomendaciones

Se recomienda tomar en cuenta los aspectos revelados mediante la metodología de investigación a más de considerar en futuras investigaciones una variante del cuestionario utilizado mediante el cual el método de medición resulte más cuantitativo.

Después de los resultados expuestos se recomienda a las instancias de control tomar la propuesta diseñada en el capítulo (3) como punto de partida para la mejora de los resultados en la gestión de administración de riesgos de la compañía. La propuesta contiene un método empírico basado en las mejores prácticas en la actualidad, sin embargo, es aún perfectible y debe ser acoplado a la estructura organización y estrategias de la dirección de cada empresa perteneciente a la industria de telecomunicaciones.

Se recomienda que el aspecto destacado en la discusión sea revisado y tomado como input de futuras investigaciones académicas. Ya que los aspectos concernientes a la idoneidad del profesional de auditoria en relación a temas de ambientes tecnológicos, es una de la necesidad que en la actualidad está ganando

Referencias

Acosta Chávez, D. A., & Navarrete, N. G. (2013). Importancia del uso del software contable en pequeñas y medianas empresas del Catón Portoviejo. *Revista La Tecnica*, 64.

Agencia de Regulación y Control de las Telecomunicaciones. (2015). *Agencia de Regulación y Control de las Telecomunicaciones.* Obtenido de http://www.arcotel.gob.ec/wp-content/uploads/2015/11/Boletin6.pdf

Aguirre Sánchez, Y. (2018). Obtenido de Tema: ropuesta de implantación del área de auditoría en informática en un órgano legislativo: http://olea.org/~yuri/propuesta-implantacion-auditoria-informatica-organo-legislativo/ch03s03.html

Alcívar Cedeño, F. M., Brito Ochoa, M. P., & Guerrero Carrasco, M. J. (julio-septiembre de 2016). *Eumed*. Obtenido de Revista Contribuciones a la Economía ISSN: 1696-8360: http://www.eumed.net/ce/2016/3/auditoria.html

Alfonso Martínez , Y., Blanco Alfonso , B., & Loy Marichal , L. (2012). Auditoría con Informática a Sistemas Contables. . *Revista de Arquitectura e Ingeniería. 2012, vol.6 no.2*, 5.

ARCOTEL . (7 de julio de 2018). *Agencia de regulación y Control de las Telecomunicaciones*. Obtenido de Tema: Crecimiento de los principales servicios de Telecomunicaciones en el Ecuador: http://www.arcotel.gob.ec/crecimiento-de-los-principales-servicios-de-telecomunicaciones-en-el-ecuador/

ARCOTEL. (2017). *Registro oficial* . Obtenido de Registro oficial: http://www.arcotel.gob.ec/wp-content/uploads/2017/04/PROYECTO-DE-REGULACI%C3%93N-DEVOLUCI%C3%93N-DE-SALDOS.pdf

ARCOTEL. (mayo de 2018). *Agencia de Regulación y Controñ de las Telecomunicaciones.* Obtenido de http://www.arcotel.gob.ec/wp-content/uploads/2015/01/BOLETIN-ESTADISTICO-Junio-2018_f.pdf

Bárcenes Mendoza, P. M., Riera Riera, B. A., Alarcón Muñoz, N. E., & Jiménez Zavala, J. D. (septiembre de 2018). *Revista Contribuciones a la Economía (julio-septiembre* . Obtenido de La contabilidad y auditoría: sistemas clave para la gestión eficiente en el sector público y privado: https://eumed.net/rev/ce/2018/3/contabilidad-auditoria.html

Borghi, A. (7 de mayo de 2010). *Coyuntura económica* . Obtenido de https://coyunturaeconomica.com/empresas/resumen-de-la-auditoria

Briones Pincay, G. H., & Hernandez Peñaherrera, E. B. (2018). *Repositorio de la Universidad de Guayaquil.* Obtenido de http://repositorio.ug.edu.ec/bitstream/redug/26837/1/B-CINT-PTG-N.249%20Briones%20Pincay%20Gerson%20Hamner.%20Hern%C3%A1ndez%20Pe%C3%B1a%20herrera%20Erika%20Bel%C3%A9n.pdf

Buján Pérez, A. (14 de junio de 2018). *Enciclopedia Financiera* . Obtenido de https://www.enciclopediafinanciera.com/auditoria/fases-de-la-auditoria.htm

Castello, R. J. (2016). *Auditoría en entornos informáticos* . Creative Commons. Obtenido de I.S.B.N. 950-33-0199-8: https://www.econ.unicen.edu.ar/

Chávez delgado, N. M. (2017). *Tesis de grado: Auditoría informática para el área de gestión de créditos del banco financiero- oficina Chimbote* . Tesis de

grado de Ingeniería de sistemas e informática , Universidad Nacional del Santa , Nuevo Cgimbote .

Chávez Maridueña, W. E. (2015). *Análisis de las principales estrategias de negocios de las empresas de telecomunicaciones del Ecuador periodo 2008-2012.* Tesis de grado de la carrera de Economía, Universidad de Guayaquil , Guayaquil.

Chicano Tejada, E. (2014). *Google books: Auditoría de seguridad informática. IFCT0109.* Antequera. Málaga: IC Editorial . Obtenido de Libro: Auditoría de seguridad informática. IFCT0109. Primera edición : https://books.google.es/books?hl=es&lr=&id=8a3KCQAAQBAJ&oi=fnd&pg=PT4&dq=hallazgos+en+auditoria+informatica&ots=ja1lEFN3Ts&sig=cor7TY1m4JxO0dzSCHH9cB52RtU#v=onepage&q=hallazgos%20en%20auditoria%20informatica&f=false

Contreras Clunes, A. (2003). DELITOS INFORMÁTICOS: UN IMPORTANTE PROCEDENTE. *Ius et Praxis . Año 9 . Nº 1*, 515-521.

Delitos Informaticos. (2019). *Delitos Informaticos*. Obtenido de Delitos Informaticos: https://delitosinformaticos.com/01/2018/seguridad-informatica/diferencias-hackers-sombrero-blanco-sombrero-gris-sombrero-negro

Diario El Mercurio. (23 de 04 de 2018). *Hackers emitieron 15.970 licencias fraudulentas en el país*. Obtenido de Hackers emitieron 15.970 licencias fraudulentas en el país: https://ww2.elmercurio.com.ec/2018/04/23/hackers-emitieron-15-970-licencias-fraudulentas-en-el-pais/

Eslava, J. d. (2013). *La Gestión del Control de la empresa.* Navarra - España: ESIC Editorial.

Explorable. (2009). *Muestreo no probabilístico*. Obtenido de Muestreo no probabilístico: https://explorable.com/es/muestreo-no-probabilistico

Flores Guirao, S. (5 de octubre de 2015). *Gestipolis* . Obtenido de https://www.gestiopolis.com/auditoria-de-sistemas-de-informacion-objetivo-y-razones-para-implementarla/

Fundeu BBVA. (2017). *Fundeu BBVA*. Obtenido de https://www.fundeu.es/recomendacion/hacker-y-cracker-diferencias-de-significado/

Gaitán, R. E. (2016). *Administración de riesgos ERM y la auditoría interna.* Mexico DF: Ecoe Ediciones.

García, D. (5 de 7 de 2016). *Departamento de Comunicación de EALDE Business School.* Obtenido de Departamento de Comunicación de EALDE Business School.: https://www.ealde.es/las-normas-internacionales-de-auditoria-nias/

Herrera Jiménez, A. M. (2015). *Revista Electrónica de Investigación Educativa Vol. 17, Núm. 1.* Obtenido de Tema de artículo: Una mirada reflexiva sobre las TIC en Educación Superior: http://www.scielo.org.mx/pdf/redie/v17n1/v17n1a11.pdf

Ing. Lascano Laica, W. M. (2016). *Universidad Regional Autónoma de los Andes.* Recuperado el 3 de diciembre de 2018, de http://dspace.uniandes.edu.ec/bitstream/123456789/5330/1/PIUAMIE006-2016.pdf

Ing.Pulgar Haro, G. A. (2018). *Repositorio de la Universidad Regional Autónoma de los Andes (ANIANDES).* Recuperado el 3 de diciembre de 2018, de Facultad de Sistemas Mercantiles: http://dspace.uniandes.edu.ec/bitstream/123456789/8655/1/PIUAMIE001-2018.pdf

Jurado Zevallos, J. G., Núñez Sánchez, J., Cordeor Iñiguez, J., Uyaguari Uyaguari, F., & Regladao Iglesias, C. (enero de 2014). *Doc Player.* Recuperado el 2018, de Libro: Historia de las telecomunicaciones en el Ecuador: https://docplayer.es/23358375-Historia-de-las-telecomunicaciones-en-el-ecuador.html

Kaspersky. (2013). *SECURELIST*. Obtenido de Fraude de telecomunicaciones – una combinación de phishing y troyanos: https://securelist.lat/fraude-de-telecomunicaciones-una-combinacin-de-phishing-y-troyanos/65935/

Kaspersky. (7 de 2 de 2019). *Ataques DDoS en el cuarto trimestre de 2018*. Obtenido de SECURE LIST: https://securelist.lat/ddos-attacks-in-q4-2018/88346/

Kaspersky. (2019). *SECURELIST*. Obtenido de https://securelist.lat/sentencian-al-funcionario-de-un-banco-chino-que-se-volvio-millonario-explotando-una-vulnerabilidad-en-los-cajeros-automaticos/88372/

Llangarí Salazar, A. M. (2016). *Repositorio de la Universidad de las Fuerzas Armadas* . Obtenido de Tema de tesis de grado: Análisis de los delitos informáticos y de telecomunicaciones en el Ecuador bajo las nuevas normas jurídicas: http://repositorio.espe.edu.ec/bitstream/21000/11654/1/T-ESPE-053079.pdf

Martínez, R. (18 de noviembre de 2014). *SCRIB* . Obtenido de https://es.scribd.com/document/246947730/Fases-de-La-Auditoria-Informatica

Morales de Rey, A. (2017). *Organización de Estados Americanos* . Obtenido de Tema de Auditoría de Estado: https://www.oas.org/juridico/PDFs/mesicic4_ven_pres_aud_est_ver_doc.pdf

Muñoz Razo, C. (2002). *AUDITORIA EN SISTEMAS COMPUTACIONALES.* MEXICO: PEARSON EDUACION DE MEXICO S.A DE C.V.

Ordóñez, L. (2007). El desarrollo tecnológico en la historia. *Revista cientifica SCIELO*, 187-210.

Orta Pérez, M. (2012). *Fundamentos Teóricos de Auditoría Financiera.* Lima - Perú: Piramide.

Perrin, S. (2006). *VECAM.* Obtenido de VECAM: https://vecam.org/archives/article659.html

Piattini, M., & Del Peso, E. (2001). *Auditoria Informática Un enfoque práctico.* MADRID: AFAOMEGA GRUPO EDITOR S.A.DE C.V.

Quinaluisa Morán, N. V., Ponce Álava, V. A., Muñoz Macías, S. C., Ortega Haro, X. F., & Pérez Salazar, J. A. (ene-jun de 2018). *Revista cielo.* Obtenido de El control interno y sus herramientas de aplicación entre COSO y COCO : http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2073-60612018000100018

Real Lengua Española de la RAE. (2018). *Real Lengua Española de la RAE*. Obtenido de http://dle.rae.es/?id=JxkTJjl

REVISTA LIDERES. (10 de OCTUBRE de 2016). *El delito informático, otra inquietud de las empresas.* Obtenido de https://www.revistalideres.ec/lideres/delito-tecnologia-internet-empresas-fraude.html

Salgado Soto, M. d., Osuna Millán, N. d., Sevilla Caro, M., & Morales Garfias, J. I. (2017). La Auditoría Informática en las organizaciones. *Revista Electrónica sobre Cuerpos Académicos y Grupos de Investigación en Iberoamérica ISSN: 2448 - 6280*, 1-14. Obtenido de http://www.cagi.org.mx/index.php/CAGI/article/view/165/324

Santacruz Espinoza, J., Vega Abad, C., Pinos Castillo, L., & Cardenas Villavicencio, O. (2017). Sistema cobit en los procesos de auditor´ıas de los sistemas informaticos. *JOURNAL OF SCIENCE AND RESEARCH: REVISTA CIENCIA E INVESTIGACIO´ N, E-ISSN: 2528-8083, VOL. 2, NO. 8*, pp 65-68.

Segovia, A. (2018). *Advisera*. Obtenido de https://advisera.com/27001academy/es/que-es-iso-27001/

Significado de auditoría . (8 de septiembre de 2016). *Significados* . Obtenido de https://www.significados.com/auditoria/

Trejo. M.D.C, C., Domenech Alvarez, G., & Ortìz Chimbo. Msc, K. (2015). *Revista de Investigación Jurídica ISSN 2220-2129.* Obtenido de Tema LA SEGURIDAD JURÍDICA FRENTE A LOS DELITOS INFORMÁTICOS: http://revistas.upagu.edu.pe/index.php/AV/article/view/168/120

Valbuena Quebrada, J. (3 de 2 de 2016). *PREZI*. Obtenido de https://prezi.com/wvf1yu1mso4-/organigrama-de-la-empresa-de-telecomunicacionesclaro/

Valencia Duque, F. J. (2015). *La Auditoría Continua, una herramienta para la modernización de la función de auditoría en las organizaciones y su aplicación en el Control Fiscal Colombiano.* Tesis de grado de ingeniería Indutrial , Manizales.

Vinatea Rccoba, L. (2011). *Revista de Derecho & Sociedad N° 36.* Recuperado el 3 de diciembre de 2018, de Tema de artículo: La Integración de los Servicios de Telecomunicaciones y lo que se requiere para Implementarla.: http://revistas.pucp.edu.pe/index.php/derechoysociedad/article/view/13210/13821

Anexos

Anexo A: Empresa de Telecomunicaciones en Guayaquil.

N°	Empresa	Ciudad	Domicilio
1	Corporación Nacional de Telecomunicaciones CNT EP	Quito	Francisco Andrade Marín E6-24 y Av. Eloy Alfaro, Edif. Carolina Millennium, PB – Quito
2	Consorcio Ecuatoriano de Telecomunicaciones S.A. Conecel	Guayaquil	Av. Francisco De Orellana y Alberto Borges, Edif. Centrum – Guayaquil
3	INTEGRALDATA	Quito	Av.10 Agosto N37-288 y Villalengua, Edif. Inteca, piso 9 (edificio esquinero color café) – Quito
4	TOTAL TEK S.A.	Quito	De Los Guarumos 449 y Av. 6 de Diciembre – Quito
5	ECUATRONIX CIA LTDA	Quito	Azcúnaga Oe4-170 y Brasil, Edif. Ecuatronix - Quito Tenis – Quito
6	PUNTONET S.A.	Quito	Av. Amazonas 45-45 y Alfonso Pereira, Edif. Centro Financiero, Piso 4, Of. 401 – Quito
7	Andeantrade S.A.	Quito	Vasco de Contreras N34-180 y Lallement, Edif. Andeantrade – Quito
8	TELECOMAUSTRO	Cuenca	Nicanor Aguilar y Luis Moreno Mora - Cuenca
9	Otecel S.A.	Quito	Av. De los Grandos, Ekopark, Torre 3 – Quito
10	DIRECTV Ecuador C. Ltda.	Quito	Av. Coruña N28-14 y Manuel Iturre, Edif. Santa Fe – Quito
11	AMOVECUADOR S.A.	Quito	Amazonas N44-105 y Río Coca, Edif. Eteco – Quito
12	Telconet S.A.	Guayaquil	Kennedy Norte, Mz. 109 Solar 21 - Guayaquil
13	SERVICIOS DE TELECOMUNICACIONES	Quito	Avenida Eloy Alfaro N44-406 y De las Higueras, Edif. Grupo TV cable - El

	SETEL S.A		Batán – Quito
14	Broadnet S.A.	Guayaquil	Avenida 9 de octubre 100 y Malecón, Edif. La Previsora – Guayaquil
15	Huawei Technologies Cía. Ltda.	Quito	Av. República De El Salvador N34-493 y Portugal, Edif. Torre Gibraltar – Quito
16	MEGADATOS S.A.	Quito	Iñaquito Lote 2 y Corea , Edif. Platinum – Quito
17	ECUADORTELECOM S.A.	Otra	s/d
18	GLOBAL CROSSING COMUNICACIONES ECUADOR S.A.	Quito	Juan Díaz N37-11 - Urbanización Iñaquito Alto – Quito
19	JADARO DISTRIBUCION IMPORTACION & EXPORTACION CIA. LTDA.	Quito	Víctor Mideros N52-119 y Capitán Ramón Borja - Norte – Quito
20	LEVEL 3 ECUADOR LVLT S.A	Otra	s/d
21	MAKROCEL CIA. LTDA	Quito	Avenida Amazonas N26-81 y Pinta - Norte – Quito
22	Road Track Ecuador S A	Quito	Manuel Najas Oe1-81 y Juan De Selis - Quito
23	SIEMENS S. A.	Quito	Manuel Zambrano S/N y Av. 6 de Diciembre – Quito
24	ALCATEL-LUCENT ECUADOR S. A.	Quito	La Pinta 236 y La Rábida , Edificio Alcatel piso 1 - Norte – Quito
25	Nokia Solutions And Networks Ecuador S.A.	Guayaquil	Av. Orellana S/N y Alberto Borgues – Guayaquil
26	AMERICAN CALL CENTER S.A. (AMERICALL)	Guayaquil	Garzota Herradura 6 y Eloy Velásquez - La Garzota – Guayaquil
27	Negocios y Telefonía (Nedetel) S.A.	Guayaquil	Av. Francisco. De Orellana Mz 18 y Km. 1½ Av. Juan Tanca Marengo, Edif. Centro
28	UNIVISA S.A.	Guayaquil	Av. Francisco De Orellana, Mz 110, Solar 30 – Guayaquil
29	SHERLOCTECH	Quito	Av. Colón E2-01 y Av. 10 de Agosto ,

	SOLUTIONS S.A.		Edif. Corporación CFC – Quito
30	Ericsson de Ecuador C.A.	Quito	Av. 12 De Octubre N24-660 y Francisco Salazar – Quito
31	Duocell S.A.	Guayaquil	Cdla. Kennedy Norte. Av. Francisco De Orellana 234,, Edif. Blue Towers - Guayaquil
32	TRANSNEXA S.A. EMA.	Quito	Avenidas Orellana E9-175 y 6 de Diciembre, Edif. Alisal de Orellana – Quito
33	TELEFONICA INTERNATIONAL WHOLESALE SERVICES ECUADOR S.A.	Quito	Mariana de Jesús E7-8 y La Pradera , Edif. Business Plus - La Pradera - Quito
34	Movilcelistic del Ecuador S.A.	Quito	Av. Panamericana Norte Km 12 1/2 , Complejo Industrial Parque Delta Bodega
35	COMPAÑÍA GENERAL DE COMERCIO COGECOMSA S. A.	Quito	Autopista General Rumiñahui entre El Puente Dos y El Puente Tres. Calle Francisco de Orellana L-198 y Hernando de Magallanes. – Quito
36	CABLEUNION S.A	Quito	José María Guerrero N68-44 e Ignacio de Loyola , Urb. Cooperativa 23 de Junio - Cotocollao – Quito
37	DISTRIBUIDORA DICELTECSA S.A.	Quito	- Quito
38	GOTELTELECOM S.A.	Quito	Rumipamba 706 y República, Edif. Borja Páez - La Carolina – Quito
39	Tevecable S.A.	Quito	Av. Eloy Alfaro N44-406 y De Las Higueras – Quito
40	EMPRESA DE TELEVISION SATELCOM SA	Guayaquil	Víctor Emilio Estrada 119 y Bálsamos, Edif. TV Cable - Urdesa – Guayaquil
41	ENERGIA Y PETROLEOS ENERPETROL S.A.	Quito	Calle El Establo y Calle C, Edif. Site Center, Torre 1 - Cumbayá – Quito
42	LUTROL S.A.	Quito	Avenida Edmundo Carvajal y Calle F - Norte – Quito

	SERVICIOS AGREGADOS Y DE TELECOMUNICACIONES		Eloy Alfaro N44-406 e Higuera - El Batán
43	NETWORK SATNET S.A.	Quito	– Quito
	COMPAÑIA BRIGHTCELL		Hernando de la Cruz N31-120 y Mariana
44	S.A	Quito	de Jesús - San Gabriel – Quito
	AT&T GLOBAL NETWORK SERVICES ECUADOR CIA.		REPUBLICA DEL SALVADOR N34-211 y MOSCU , EL FARAON 8 - LA
45	LTDA.	Quito	CAROLINA
			AV. 10 DE AGOSTO 37-288 y
46	TRANSTELCO S. A.	Quito	VILLALENGUA , INTECA 503
			Avenida Naciones Unidas E6-99 y Shyris
47	NEW ACCESS S.A	Quito	- Iñaquito – Quito
	High Telecommunications Sociedad de		Av. Amazonas N36-12 y Japón, Edif.
48	Telecomunicaciones Cía. L	Quito	Unicentro Amazonas – Quito
			Avenida Rumipamba 706 , entre República y Amazonas, Edif. Borja Páez -
49	CODEPRET S.A.	Quito	La Carolina – Quito
50	TERRAMONT S.A.	Otra	Tarqui 2364 y Veloz – Riobamba
			Pasaje Manuel Godoy E12-110 y Juan
51	GYPSO S.A.	Quito	Ramírez - Norte – Quito
			Avenida Orellana E9-195 y 6 de
	MOVILWAY ECUADOR		Diciembre, Edif. Alisal de Orellana - La
52	S.A.	Quito	Paz – Quito
			Avenida Rumipamba 706 - La Carolina -
53	ECUATECHNOLOGIES S.A.	Quito	Quito
	DISTRIBUIDORA DE SERVICIOS DE ENTRETENIMIENTO		Avenida Amazonas 2925 e Inglaterra,
54	DISENTV S.A.	Quito	Edif. Valderrama - Rumipamba – Quito
	Servicios Comunikt Ceher		
55	Sociedad Anónima	Otra	Mera N04-70 y Sucre – Ambato
56	Comsatel S.A.	Guayaquil	Av. Principal "Entre Ríos", Edif. Laxmi –

			Guayaquil
57	La Competencia S.A.	Quito	Pasaje N44B E10-26 Av. 6 De Diciembre entre Río Coca y Shyris – Quito
58	Ciemtelcom Compañía de Telecomunicaciones Satelitales S.A.	Quito	AV. DE LOS SHYRIS N35-174 y SUECIA , RENAZZO PLAZA 6 – BENALCAZAR
59	OLDSTRATEGIC PLANNING, INTERNATIONAL ECUADOR S.A.	Quito	Avenida Occidental N48-188 y Manuel Valdiviezo - El Pinar – Quito
60	CISCOSYSTEM ECUADOR S.A.	Quito	Av. Amazonas N37-29 entre Villalengua y UNP , Edif. Eurocenter Diursa – Quito
61	TELEACCESS S.A.	Quito	Asunción Oe6-12 y Canadá - Santa Prisca – Quito
62	COLOMBIANA DE TELECOMUNICACIONES COLDECON ECUADOR S.A.	Quito	Avenida Galo Plaza OE1-51 y Joaquín Mancheno, Bodegas Wesco - Panamericana Norte Km – Quito
63	TECCELLSA S.A.	Quito	Luis Cordero E10-55 y 12 de Octubre, Edif. Sancho Arias - La Floresta – Quito
64	BT Solutions Limited Cia. Ltda.	Quito	AV. AMAZONAS N21-252 y CARRION , LONDRES 5
65	Telecomunicaciones a su alcance Telalca S.A.	Quito	Calle San Francisco N42-219 y Mariano Echeverría – Quito
66	METRO DISTRIBUIDORA METRODIST S. A.	Guayaquil	Av. 9 de octubre 308 y Pedro Carbo-General Córdova, San Francisco 300 Of. 1 25 - Pedro Carbo – Guayaquil
67	CRONIX CIA. LTDA.	Quito	Avenida 10 de Agosto N34 -601 y Juan Pablo Sanz - Norte – Quito
68	CORPORACION ZEDECUADOR S.A.	Quito	Avenida 12 de Octubre N24-562 y Cordero, Edif. World Trade Center - La Floresta - Quito
69	Iseyco C.A.	Quito	AV. 10 DE AGOSTO N37-288 y VILLALENGUA , INTECA MZ -

			IÑAQUITO
	COMUNICACIONES Y TELEFONIA MULTIPLES S.A. MULTICOM -		Avenida Carlos Julio Arosemena Km. 3
70	TELEMOVIL	Guayaquil	1/2 y 28 de Mayo – Guayaquil
	ACANUMAN		Inglaterra E3-58 y Av. Eloy Alfaro ,
71	COMUNICACIONES S. A.	Quito	Novoa 2 - Mariscal Sucre – Quito
	RAPTORMOBILE SERVICIOS SATELITALES		Av. Amazonas 36-55 y Juan Pablo Sanz,
72	CIA. LTDA.	Quito	Antisana 1 Of. 803 8 - El Batan – Quito
	Audio, Video y Comunicaciones Cía. Ltda.		
73	Advicom	Quito	Paris N43-41 y Emilio Sola Esq. – Quito
			Pasaje Guayas E3-130 y Amazonas -
74	SOLUCINTEGSA S.A.	Quito	Norte – Quito
			Av. Francisco De Orellana, Edif. Blue
	Soluciones Especializadas de		Towers, Cdla. Kennedy Norte. –
75	Ingeniería en Telemática S.A.	Guayaquil	Guayaquil
			Avenida Rodríguez Chávez - Parque
76	BONOPRICE C. LTDA.	Guayaquil	Empresarial Colón – Guayaquil
	Telydata, Telecomunicaciones		N39B José Arizaga E3-37 y Jorge Drom –
77	y Datos Cía. Ltda.	Quito	Quito
			Ruiz de Castilla N763 y Andagoya - Las
78	PANCHONET S.A	Quito	Casas – Quito
			Whymper E7-172 y Diego de Almagro -
79	MESSAGEPLUS S.A.	Quito	Quito
	TELEFONIA CELULAR MIO TECELMIO CIA.		
80	LTDA.	Otra	Av. Atahualpa y 10 De Agosto – Puyo
			Remigio Crespo 2-160 y Agustín Cueva –
81	RUALTIM S.A.	Cuenca	Cuenca
	TELECOMUNICACIONES		Isla Pinzón N43-61 y Emilio Zolá -
82	FULLDATA CIA. LTDA.	Quito	Jipijapa – Quito
83	TELECARRIER S. A.	Quito	REPUBLICA 476 y DIEGO DE

			ALMAGRO , PRESIDENTE 10 - LA PRADERA
	MAKROSECURITY ALARMAS ACTIVAS CIA.		Avenida Amazonas N36-177 y Naciones Unidas , Unicornio, oficinas1106 y 1107 -
84	LTDA.	Quito	Iñaquito – Quito
	Ingeniería En Radio y Comunicaciones I.R.C.		Av. Dr. Miguel Ángel Jijón, Solar 10 y 66
85	Cia.Ltda.	Guayaquil	Ava. – Guayaquil
86	MOVIPHONE CIA. LTDA.	Otra	Tenemaza 5-07 y Luis Cordero – Azogues
	PRYSCOM DEL ECUADOR		Ciudadela Las Garzas y Mz. 11, solar 4 –
87	S.A.	Guayaquil	Guayaquil
88	ESPOLTEL S.A.	Guayaquil	Km. 30½, Vía Perimetral S/N - Guayaquil
	BUSINNESS MARKET S.A.		
89	MARKEBUSSI	Guayaquil	Quito 914 y Hurtado – Guayaquil
			Av. Amazonas E3 -131 y Pasaje Guayas ,
90	Ecisec S.A.	Quito	Edif. Rumiñahui – Quito
	Tele - Red,		
	Telecomunicaciones y Redes		Bálsamos Norte 323 entre Quinta y
91	S.A.	Guayaquil	Primera, Urdesa Central – Guayaquil

Anexo B: Ley de telecomunicaciones del Ecuador

TÍTULO II REDES Y PRESTACIÓN DE SERVICIOS DE TELECOMUNICACIONES

CAPÍTULO I. Establecimiento y explotación de redes

Artículo 9.- Redes de telecomunicaciones.

Se entiende por redes de telecomunicaciones a los sistemas y demás recursos que permiten la transmisión, emisión y recepción de voz, vídeo, datos o cualquier tipo de señales, mediante medios físicos o inalámbricos, con independencia del contenido o información cursada.

El establecimiento o despliegue de una red comprende la construcción, instalación e integración de los elementos activos y pasivos y todas las actividades hasta que la misma se vuelva operativa. En el despliegue de redes e infraestructura de telecomunicaciones, incluyendo audio y vídeo por suscripción y similares, los prestadores de servicios de telecomunicaciones darán estricto cumplimiento a las normas técnicas y políticas nacionales, que se emitan para el efecto.

En el caso de redes físicas el despliegue y tendido se hará a través de ductos subterráneos y cámaras de acuerdo con la política de ordenamiento y soterramiento de redes que emita el Ministerio rector de las Telecomunicaciones y de la Sociedad de la Información.

CAPÍTULO II. Prestación de servicios de telecomunicaciones

Artículo 14.- Formas de Gestión.

Con sujeción a lo dispuesto en la Constitución de la República, los servicios públicos de telecomunicaciones son provistos en forma directa por el Estado, a través de empresas públicas de telecomunicaciones o indirecta a través de delegación a empresas de economía mixta en las cuales el Estado tenga la mayoría accionaria o a la iniciativa privada y a la economía popular y solidaria.

Artículo 15.- Delegación.

La Agencia de Regulación y Control de las Telecomunicaciones, para otorgar títulos habilitantes por delegación, considerará lo siguiente:

a: Para las empresas de economía mixta en las cuales el Estado tenga la mayoría accionaria, el otorgamiento de títulos habilitantes para el uso o explotación del espectro radioeléctrico o para la prestación de servicios públicos de telecomunicaciones, se sujetará al interés nacional y respetará los plazos y límites fijados en esta Ley y en las regulaciones que para el efecto emita la Agencia de Regulación y Control de las Telecomunicaciones.

b. Para el caso de empresas públicas de propiedad Estatal de los países que forman parte de la comunidad internacional, la delegación para el uso o explotación del espectro radioeléctrico o para la prestación de servicios públicos de telecomunicaciones, podrá hacerse en forma directa. En todos los casos, la delegación se sujetará al interés nacional y respetará los plazos y límites fijados en esta Ley y en las regulaciones que para el efecto emita la Agencia de Regulación y Control de las Telecomunicaciones.

c. Para la iniciativa privada y a la economía popular y solidaria, se otorgarán títulos habilitantes para la provisión de servicios públicos de telecomunicaciones y para el uso del espectro radioeléctrico asociado a dicha provisión, en los siguientes casos:

1. Cuando sea necesario y adecuado para satisfacer el interés público, colectivo o general;

2. Cuando la demanda del servicio no pueda ser cubierta por empresas públicas o mixtas en las que el Estado tenga mayoría accionaria;

3. Cuando el Estado no tenga la capacidad técnica o económica;

4. Cuando los servicios de telecomunicaciones se estén prestando en régimen de competencia por empresas públicas y privadas de telecomunicaciones;

5. Cuando sea necesario para promover la competencia en un determinado mercado; y,

6. Para garantizar el derecho de los usuarios a disponer de servicios públicos de telecomunicaciones de óptima calidad a precios y tarifas equitativas.

No se requiere la concurrencia de causas para la delegación.

El otorgamiento de títulos habilitantes y su renovación para servicios de radiodifusión, estará sujeto a lo dispuesto en la Ley Orgánica de Comunicación.

Apéndice C: Entrevista

Menor --------- Escala de cumplimiento -------- Mayor

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	1. Completamente de acuerdo	2. De acuerdo	3. Poco De acuerdo	4. En desacuerdo	Observaciones del encuestado
CONTROL DE ACCESO								
A	**Responsable de SI/Responsable de TICs**	**CONTROL DE ACCESO**		**Promedio ponderado del criterio general**				
A.1	Responsable de SI	**REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO**	**Se debe limitar el acceso a información y a instalaciones de procesamiento de información.**	**Promedio ponderado de la sección del criterio**				**ENTREVISTA REALIZADA A MARIO ALMEIDA, AUDITOR DE TELCONET.**
A.1.1	Responsable de SI	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	X				
A.1.2	Responsable de TICs	Acceso a redes y a servicios en red	Se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	X				
A.2	Responsable de SI	**GESTIÓN DE ACCESO DE USUARIOS**	**Se debe asegurar el acceso de los usuarios autorizados y evitar el acceso no**	**Promedio ponderado de la sección del criterio**				

			autorizado a sistemas y servicios.					
A.2.1	Responsable de SI	Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	X				
A.2.2	Responsable de SI	Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	X				
A.2.3	Responsable de SI	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	X				
A.2.4	Responsable de SI	Gestión de información de autenticación secreta de usuarios	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	X				
A.2.5	Responsable de SI	Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	X				
A.2.6	Responsable de SI	Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben		X			

			ajustar cuando se hagan cambios.					
A.3	**Responsable de SI**	**RESPONSABILIDADES DE LOS USUARIOS**	**Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.**	**Promedio ponderado de la sección del criterio**				
A.3.1	Responsable de SI	Uso de información de autenticación secreta	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	X				
A.3.2	Responsable de SI	**CONTROL DE ACCESO A SISTEMAS Y APLICACIONES**	**Se debe evitar el acceso no autorizado a sistemas y aplicaciones.**	**Promedio ponderado de la sección del criterio**				
A.3.3	Responsable de SI	Restricción de acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.	X				
A.3.4	Responsable de SI	Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	X				
A.3.5	Responsable de TICs	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	X				

A.3.6	Responsable de TICs	Uso de programas utilitarios privilegiados	Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.	X				
A.3.7	Responsable de TICs	Control de acceso a códigos fuente de programas	Se debe restringir el acceso a los códigos fuente de los programas.	X				
ID/ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**Completamente de acuerdo**	**De acuerdo**	**Poco De acuerdo**	**En desacuerdo**	**Observaciones del encuestado**
CRIPTOGRAFÍA								
B	**Responsable de SI**	**CRIPTOGRAFÍA**		**Promedio ponderado del criterio general**				
B.1	**Responsable de SI**	**CONTROLES CRIPTOGRÁFICOS**	**Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.**	**Promedio ponderado de la sección del criterio**				
B.1.1	Responsable de SI	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	X				
B.1.2	Responsable de SI	Gestión de llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.	X				

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	Completamente de acuerdo	De acuerdo	Poco de acuerdo	En desacuerdo	Observaciones del encuestado
SEGURIDAD FÍSICA Y DEL ENTORNO								
C	**Responsable de la seguridad física/Responsable de SI/Líderes de los procesos**	**SEGURIDAD FÍSICA Y DEL ENTORNO**		**Promedio ponderado del criterio general**				
C.1	**Responsable de la seguridad física**	**ÁREAS SEGURAS**	**Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.**	**Promedio ponderado de la sección del criterio**				
C.1.1	Responsable de la seguridad física	Perímetro de seguridad física	Se debe definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.	X				
C.1.2	Responsable de SI	Controles físicos de entrada	Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	X				
C.1.3	Líderes de los procesos	Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, recintos e	X				

			instalaciones.					
C.1.4	Responsable de SI	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	X				
C.1.5	Responsable de SI	Trabajo en áreas seguras	Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.	X				
C.1.6	Responsable de la seguridad física	Áreas de despacho y carga	Se debe controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	X				
C.2	**Responsable de SI**	**EQUIPOS**	**Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.**	**Promedio ponderado de la sección del criterio**				
C.2.1	Responsable de SI	Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	X				
C.2.2	Responsable de TICs	Servicios de suministro	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en	X				

			los servicios de suministro.					
C.2.3	Responsable de TICs	Seguridad del cableado	El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debe estar protegido contra interceptación, interferencia o daño.	X				
C.2.4	Responsable de TICs	Mantenimiento de equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	X				
C.2.5	Responsable de TICs	Retiro de activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	X				
C.2.6	Responsable de SI	Seguridad de equipos y activos fuera de las instalaciones	Se debe aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	X				
C.2.7	Responsable de TICs	Disposición segura o reutilización de equipos	Se debe verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reusó.	X				

C.2.8	Responsable de SI	Equipos de usuario desatendidos	Los usuarios deben asegurarse de que a los equipos desatendidos se les dé protección apropiada.	X				
C.2.9	Responsable de SI	Política de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	X				
ID/ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**Completamente de acuerdo**	**De acuerdo**	**Poco de acuerdo**	**En desacuerdo**	**Observaciones del encuestado**
SEGURIDAD DE LAS OPERACIONES								
D	**Responsable de TICs/Responsable de SI**	**SEGURIDAD DE LAS OPERACIONES**		**Promedio ponderado del criterio general**				
D.1	**Responsable de TICs**	**PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES**	**Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.**	**Promedio ponderado de la sección del criterio**				
D.1.1	Responsable de TICs	Procedimientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.	X				
D.1.2	Responsable de TICs	Gestión de cambios	Se debe controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad	X				

			de la información.					
D.1.3	Responsable de TICs	Gestión de capacidad	Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.	X				
D.1.4	Responsable de TICs	Separación de los ambientes de desarrollo, pruebas y operación	Se debe separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	X				
D.2	**Responsable de SI**	**PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS**	**Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.**	**Promedio ponderado de la sección del criterio**				
D.2.1	Responsable de SI	Controles contra códigos maliciosos	Se debe implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	X				
D.3	**Responsable de TICs**	**COPIAS DE RESPALDO**	**Proteger contra la pérdida de datos.**	**Promedio ponderado de la sección del criterio**				
D.3.1	Responsable de TICs	Respaldo de la información	Se debe hacer copias de respaldo de la información, del software e imágenes	X				

			de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.					
D.4	**Responsable de SI**	**REGISTRO Y SEGUIMIENTO**	**Registrar eventos y generar evidencia.**	**Promedio ponderado de la sección del criterio**				
D.4.1	Responsable de SI	Registro de eventos	Se debe elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	X				
D.4.2	Responsable de SI	Protección de la información de registro	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	X				
D.4.3	Responsable de SI	Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	X				
D.4.4	Responsable de SI	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia	X				

			de tiempo.					
D.5	**Responsable de TICs**	**CONTROL DE SOFTWARE OPERACIONAL**	**Asegurar la integridad de los sistemas operacionales.**	**Promedio ponderado de la sección del criterio**				
D.5.1	Responsable de TICs	Instalación de software en sistemas operativos	Se debe implementar procedimientos para controlar la instalación de software en sistemas operativos.	X				
D.6	**Responsable de SI**	**GESTIÓN DE LA VULNERABILIDAD TÉCNICA**	**Prevenir el aprovechamiento de las vulnerabilidades técnicas.**	**X**				
D.6.1	Responsable de SI	Gestión de las vulnerabilidades técnicas	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas	X				

			para tratar el riesgo asociado.					
D.6.2	Responsable de TICs	Restricciones sobre la instalación de software	Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	X				
D.7	**Responsable de TICs**	**CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN**	**Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.**	**Promedio ponderado de la sección del criterio**				
D.7.1	Responsable de TICs	Controles sobre auditorías de sistemas de información	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se debe planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	X				

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	Completamente de acuerdo	De acuerdo	Poco de acuerdo	En desacuerdo	Observaciones del encuestado
SEGURIDAD DE LAS COMUNICACIONES								
E	**Responsable de TICs/Responsable de SI**	**SEGURIDAD DE LAS COMUNICACIONES**		**Promedio ponderado del criterio general**				
E.1	**Responsable de TICs**	**GESTIÓN DE LA SEGURIDAD DE LAS REDES**	**Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.**	**Promedio ponderado de la sección del criterio**				
E.1.1	Responsable de TICs	Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	X				
E.1.2	Responsable de SI	Seguridad de los servicios de red	Se debe identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya	X				

			sea que los servicios se presten internamente o se contraten externamente.					
E.1.3	Responsable de TICs	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	X				
E.2	**Responsable de TICs**	**TRANSFERENCIA DE INFORMACIÓN**	**Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.**	**Promedio ponderado de la sección del criterio**				
E.2.1	Responsable de TICs	Políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones	X				

			de comunicación.					
E.2.2	Responsable de TICs	Acuerdos sobre transferencia de información	Los acuerdos deben tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.	X				
E.2.3	Responsable de TICs	Mensajería electrónica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	X				
E.2.4	Responsable de SI	Acuerdos de confidencialidad o de no divulgación	Se debe identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	X				

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	Completamente de acuerdo	De acuerdo	Poco de acuerdo	En desacuerdo	Observaciones del encuestado
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS								
F	**Responsable de SI/Responsable de TICs**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**		**Promedio ponderado del criterio general**				
F.1	**Responsable de SI**	**REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN**	**Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.**	**Promedio ponderado de la sección del criterio**				
F.1.1	Responsable de SI	Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos	X				

			sistemas de información o para mejoras a los sistemas de información existentes.					
F.1.2	Responsable de SI	Seguridad de servicios de las aplicaciones en redes públicas	La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	X				
F.1.3	Responsable de SI	Protección de transacciones de los servicios de las aplicaciones	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de	X				

			mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.					
F.2	**Responsable de SI**	**SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE**	**Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.**	**Promedio ponderado de la sección del criterio**				
F.2.1	Responsable de SI	Política de desarrollo seguro	Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.	X				
F.2.2	Responsable de TICs	Procedimientos de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben	X				

			controlar mediante el uso de procedimientos formales de control de cambios.					
F.2.3	Responsable de TICs	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	X				
F.2.4	Responsable de TICs	Restricciones en los cambios a los paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	X				

F.2.5	Responsable de TICs	Principios de construcción de sistemas seguros	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	X				
F.2.6	Responsable de TICs	Ambiente de desarrollo seguro	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	X				
F.2.7	Responsable de TICs	Desarrollo contratado externamente	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados	X				

			externamente.					
F.2.8	Responsable de SI	Pruebas de seguridad de sistemas	Durante el desarrollo se debe llevar a cabo pruebas de funcionalidad de la seguridad.	X				
F.2.9	Responsable de TICs	Prueba de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se debe establecer programas de prueba para aceptación y criterios de aceptación relacionados.	X				
F.2.10	Responsable de SI	**DATOS DE PRUEBA**	**Asegurar la protección de los datos usados para pruebas.**	**Promedio ponderado de la sección del criterio**				
F.2.11	Responsable de SI	Protección de datos de prueba	Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.	X				
ID/ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**Completamente de acuerdo**	**De acuerdo**	**Poco de acuerdo**	**En desacuerdo**	**Observaciones del encuestado**
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN								

G	**Responsable de SI/Responsable de TICs**	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**		**Promedio ponderado del criterio general**				
G.1	**Responsable de SI**	**GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN**	**Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.**	**Promedio ponderado de la sección del criterio**				
G.1.1	Responsable de SI	Responsabilidades y procedimientos	Se debe establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	X				
G.1.2	Responsable de SI	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se deben informar a través de los	X				

			canales de gestión apropiados, tan pronto como sea posible.					
G.1.3	Responsable de SI	Reporte de debilidades de seguridad de la información	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	X				
G.1.4	Responsable de SI	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	X				
G.1.5	Responsable de SI	Respuesta a incidentes de seguridad de la	Se debe dar respuesta a los	X				

		información	incidentes de seguridad de la información de acuerdo con procedimientos documentados.					
G.1.6	Responsable de TICs	Aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	X				
G.1.7	Responsable de TICs	Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	X				

Declaración y Autorización

Yo, Piguave Tigua Zully Esthefani con C.C: #0931759070 autora del trabajo de titulación: "**EVALUACIÓN DE LA AUDITORIA EN SISTEMAS DE INFORMACIÓN COMO MÉTODO DE PREVENCIÓN DEL FRAUDE EN EL SECTOR DE TELECOMUNICACIONES",** previo a la obtención del título de Ingeniero en Contabilidad y Auditoría, en la Universidad Católica de Santiago de Guayaquil.

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

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

Guayaquil, 19 marzo del 2019

f. _____

Nombre: Piguave Tigua, Zully Esthefani

C.C: 0931759070

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	Evaluación de la auditoria en sistemas de información como método de prevención del fraude en el sector de telecomunicaciones.		
AUTOR(ES)	Piguave Tigua Zully Esthefani		
REVISOR(ES)/TUTOR(ES)	Delgado Loor Fabián Andrés		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Ciencias Económicas y Administrativas		
CARRERA:	Contabilidad y Auditoría		
TITULO OBTENIDO:	Ingeniero en Contabilidad y Auditoría		
FECHA DE PUBLICACIÓN:	19 marzo del 2019	**No. DE PÁGINAS:**	154
ÁREAS TEMÁTICAS:	Auditoria 1, Sistemas de Información, Auditoría en Sistemas.		
PALABRAS CLAVES/ KEYWORDS:	Entrevista, hackers, crackers, ARCOTEL, ley de telecomunicación, delito.		

RESUMEN/ABSTRACT:

En la tesis previa a titulación se estudia la evaluación de la auditoria en sistemas de información, relacionada con las empresas de telecomunicaciones enfocándose en el área de auditoria y la relación que mantiene con el entorno de control tecnológico debido a que dentro de este marco se han detectado problemas que involucran fraudes. A través de la investigación se plantea como meta para el problema inmerso en la auditoria alcanzar la prevención de los delitos ocurridos utilizando de esta manera la evaluación como método a beneficio de futuros casos. El trabajo es realizado bajo la técnica denominada entrevista, dirigida al punto clave del departamento de sistemas de una compañía de telecomunicaciones nacional quien impulsa la búsqueda y análisis de los designados, hackers, crackers y sus derivados siendo estos los usualmente más implicados en los procesos de flaqueo que afectan la auditoria. Considerando la ley de telecomunicación y las regulaciones de ARCOTEL para el correcto proceso analítico de manifiestos y resoluciones que se presentan como ejemplos de los varios agravios del país con referente a los delitos de telecomunicación. Siendo las descripciones de los conceptos, leyes, ejemplos y posturas de autores empleadas de una manera detallada, clara y técnica para facilitar la compresión del método sin desvanecer el foco que presenta cada uno.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593-4-263166/ +593 996790734	**E-mail:** zullypiguave95@gmail.com
CONTACTO CON LA INSTITUCIÓN (COORDINADOR DEL PROCESO UTE):	**Nombre:** Lorena Bernabé Argandoña	
	Teléfono: +593-4- 3804600 ext.1635	
	E-mail: lorena.bernabe @cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	

Declaración y Autorización

Yo, Ocampo Gómez Valeria Ivonne con C.C: # 0930001094 autora del trabajo de titulación: "**EVALUACIÓN DE LA AUDITORIA EN SISTEMAS DE INFORMACIÓN COMO MÉTODO DE PREVENCIÓN DEL FRAUDE EN EL SECTOR DE TELECOMUNICACIONES",** previo a la obtención del título de Ingeniero en Contabilidad y Auditoría, en la Universidad Católica de Santiago de Guayaquil.

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

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

Guayaquil, 19 marzo del 2019

f. _____

Nombre: Ocampo Gómez, Valeria Ivonne

C.C: 0930001094

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	Evaluación de la auditoria en sistemas de información como método de prevención del fraude en el sector de telecomunicaciones.		
AUTOR(ES)	Ocampo Gómez Valeria Ivonne		
REVISOR(ES)/TUTOR(ES)	Delgado Loor Fabián Andrés		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Ciencias Económicas y Administrativas		
CARRERA:	Contabilidad y Auditoría		
TITULO OBTENIDO:	Ingeniero en Contabilidad y Auditoría		
FECHA DE PUBLICACIÓN:	19 marzo del 2019	**No. DE PÁGINAS:**	154
ÁREAS TEMÁTICAS:	Auditoria 1, Sistemas de Información, Auditoría en Sistemas.		
PALABRAS CLAVES/ KEYWORDS:	Entrevista, hackers, crackers, ARCOTEL, ley de telecomunicación, delito.		

RESUMEN/ABSTRACT:
En la tesis previa a titulación se estudia la evaluación de la auditoria en sistemas de información, relacionada con las empresas de telecomunicaciones enfocándose en el área de auditoria y la relación que mantiene con el entorno de control tecnológico debido a que dentro de este marco se han detectado problemas que involucran fraudes. A través de la investigación se plantea como meta para el problema inmerso en la auditoria alcanzar la prevención de los delitos ocurridos utilizando de esta manera la evaluación como método a beneficio de futuros casos. El trabajo es realizado bajo la técnica denominada entrevista, dirigida al punto clave del departamento de sistemas de una compañía de telecomunicaciones nacional quien impulsa la búsqueda y análisis de los designados, hackers, crackers y sus derivados siendo estos los usualmente más implicados en los procesos de flaqueo que afectan la auditoria. Considerando la ley de telecomunicación y las regulaciones de ARCOTEL para el correcto proceso analítico de manifiestos y resoluciones que se presentan como ejemplos de los varios agravios del país con referente a los delitos de telecomunicación. Siendo las descripciones de los conceptos, leyes, ejemplos y posturas de autores empleadas de una manera detallada, clara y técnica para facilitar la compresión del método sin desvanecer el foco que presenta cada uno.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593-958650224	**E-mail:** Valeria.ocampog94@hotmail.com
CONTACTO CON LA INSTITUCIÓN (COORDINADOR DEL PROCESO UTE):	**Nombre:** Lorena Bernabé Argandoña	
	Teléfono: +593-4- 3804600 ext.1635	
	E-mail: lorena.bernabe @cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	