



**ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO**  
**FACULTAD DE ADMINISTRACIÓN DE EMPRESAS**  
ESCUELA DE CONTABILIDAD Y AUDITORÍA  
CARRERA: INGENIERÍA EN CONTABILIDAD Y AUDITORÍA CPA.

## **TRABAJO DE TITULACIÓN**

Previa a la obtención del título de:

**INGENIERO EN CONTABILIDAD Y AUDITORÍA CPA.**

TEMA:

“AUDITORÍA INFORMÁTICA A LA GESTIÓN DE LAS TIC DEL DEPARTAMENTO DE SISTEMAS DE LA EMPRESA IRCOSTEL CÍA. LTDA. DE LA CIUDAD DE RIOBAMBA PROVINCIA DE CHIMBORAZO, PERIODO 2014.

AUTOR:

**MILTON FERNANDO MOROCHO LEMA**

RIOBAMBA - ECUADOR

2016

## **CERTIFICACIÓN DEL TRIBUNAL**

Certificamos que el presente trabajo de titulación ha sido desarrollado por el Sr. MILTON FERNANDO MOROCHO LEMA, ha cumplido con las normas de investigación científica y una vez analizado su contenido, se autoriza su presentación.

Ing. Espindola Lara Oscar Omar

**DIRECTOR**

Ing. Cando Zumba Ana del Rocío

**MIEMBRO**

## **DECLARACIÓN DE AUTENTICIDAD**

Yo, Milton Fernando Morocho Lema, declaro que el presente trabajo de titulación es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente, están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este trabajo de titulación.

Riobamba, 14 de junio del 2016

Milton Fernando Morocho Lema

CC: 060493622-9

## **DEDICATORIA**

Primeramente a Dios por ser mi guía, brindarme fortaleza, salud, sabiduría para enfrentar todas las adversidades y culminar con satisfacción esta etapa importante de mi vida profesional, a mis padres quienes son parte fundamental y mi motivo para seguir adelante, gracias por sus consejos, por su apoyo incondicional en todo momento, a mis hermanos por ser parte importante en mi diario vivir por esas palabras de aliento y por estar siempre a mi lado en los buenos y malos momentos.

A toda la Familia Morocho Lema por estar siempre apoyándome en mi vida en todos los momentos por creer en mí, a mis amigos William Orozco y Kathy Girón que siempre me ayudaron y apoyaron en el transcurso de la vida estudiantil politécnica, gracias por su valiosa compañía.

**Milton**

## **AGRADECIMIENTO**

A Dios, por darme la vida, salud y fortaleza para poder culminar con éxito este objetivo de mi vida estudiantil y con este proyecto de tesis con la mayor satisfacción posible.

A la Escuela Superior Politécnica de Chimborazo, Facultad Administración de Empresas, Escuela de Contabilidad y Auditoría, al grupo de docentes que durante todos estos años de estudio me han brindado sus conocimientos, ayudándome a plasmarlos en el presente trabajo de investigación

A IRCOSTEL CIA LTDA., por permitir desarrollar mi proyecto de tesis en la Gerencia a Jorge Calle, y a todo su personal por brindarme el apoyo incondicional para poder realizar y culminar con el mismo.

Un amplio y sincero agradecimiento a la Doctora Roció Cando y al Ingeniero Oscar Espíndola que con su colaboración oportuna y pertinente han logrado que cumpla con mi sueño de ser profesional.

A mis padres por su esfuerzo y consejos, a mis hermanos por su ayuda, apoyo y comprensión en todo lo que he realizado en mi vida y sobre todo en la culminación de mi profesión sin esperar nada a cambio con ejemplo de lucha, perseverancia, responsabilidad y humildad.

A mis amigos y familia que escogí, que son mi compañía caminando juntos en todas las circunstancias de la vida y a pesar de todos los obstáculos hemos permanecido juntos.

*Milton*

## ÍNDICE GENERAL

Portada.....	i
Certificación del tribunal .....	ii
Declaración de autenticidad.....	iii
Dedicatoria.....	iv
Agradecimiento.....	v
Índice General.....	vi
Índice de Gráficos.....	x
Índice de Anexos .....	xi
Resumen ejecutivo.....	xii
Summary.....	xiii
INTRODUCCIÓN .....	1
CAPÍTULO I: EL PROBLEMA.....	2
1.1. PLANTEAMIENTO DEL PROBLEMA .....	2
1.1.1. Formulación del Problema .....	2
1.1.2. Delimitación del Problema.....	2
1.2. JUSTIFICACIÓN .....	3
1.3. OBJETIVOS .....	3
1.3.1. Objetivo General .....	3
1.3.2. Objetivos Específicos .....	4
CAPÍTULO II: MARCO TEÓRICO .....	5
2.1. ANTECEDENTES INVESTIGATIVOS .....	5
2.1.1. Antecedentes Históricos.....	5
2.2. FUNDAMENTACIÓN TEÓRICA .....	6
2.2.1. Auditoría .....	6
2.2.1.1. Clasificación de Auditoría.....	6

2.2.2.	Tipos de Informes .....	10
2.2.2.1.	Control Interno .....	11
2.2.2.2.	Objetivos del Control Interno .....	11
2.2.2.3.	Importancia del Control Interno .....	12
2.2.2.4.	COSO II o ERM .....	12
2.2.2.5.	Componentes .....	12
2.2.2.6.	Papeles de trabajo .....	14
2.2.2.7.	Programas de auditoría .....	15
2.2.2.8.	Referencias y marcas .....	15
2.2.2.9.	Archivo Corriente .....	16
2.2.2.10.	Archivo Permanente .....	16
2.2.2.11.	Pruebas de auditoría .....	16
2.2.2.12.	Clasificación de las pruebas de auditoría .....	17
2.2.2.13.	Evidencia .....	17
2.2.2.14.	Requisitos de la evidencia .....	17
2.2.2.15.	Clasificación de la evidencia .....	18
2.2.2.16.	Hallazgo.....	19
2.2.2.17.	Atributos .....	19
2.2.2.18.	Auditoría Informatica .....	20
2.2.2.19.	Auditor Informático .....	20
2.2.2.20.	Auditoría de los Sistemas de Gestión en las Tecnologías de la Información y Comunicación (TIC) .....	22
2.2.2.21.	Importancia de la auditoría informática.....	23
2.2.2.22.	Alcance de la auditoría informática .....	24
2.2.2.23.	Objetivos de la auditoría informática.....	26
2.2.2.24.	Tipos de Auditoría Informática.....	27

2.2.2.25. Controles .....	29
2.2.2.26. Control de datos fuente y manejo de cifras de control .....	30
2.2.2.27. Control de Operación.....	30
2.2.2.28. Control de Asignación de Trabajo .....	31
2.2.2.29. Controles de Almacenamiento Masivo.....	31
2.2.2.30. Control de Mantenimiento .....	32
2.2.2.31. Control Interno Informático.....	32
2.2.2.32. Clases de Control Interno Informático.....	33
2.2.2.33. Sistema de Control Interno Informático .....	33
2.2.2.34. Tipos de Riesgos en Informática .....	40
2.2.2.35. Fases de la Auditoría Informática.....	41
2.2.2.36. Elementos Informáticos .....	47
2.3. IDEA A DEFENDER .....	50
<b>CAPÍTULO III: MARCO METODOLÓGICO.....</b>	<b>51</b>
3.1. MODALIDAD DE LA INVESTIGACIÓN .....	51
3.2. TIPOS DE INVESTIGACIÓN .....	51
3.3. POBLACIÓN Y MUESTRA.....	51
3.4. MÉTODOS, TÉCNICAS E INSTRUMENTOS .....	52
3.4.1. Métodos.....	52
3.4.2. Técnicas.....	52
3.4.3. Instrumentos .....	53
<b>CAPÍTULO IV: MARCO PROPOSITIVO.....</b>	<b>54</b>
4.1. TÍTULO .....	54
4.2. CONTENIDO DE LA PROPUESTA.....	54
4.2.1. Archivo Permanente .....	54
2.2.2. Archivo Corriente .....	64

2.2.2.1.FASE I .....	66
2.2.2.2.FASE II .....	77
2.2.2.3.FASE III.....	127
CONCLUSIONES .....	133
RECOMENDACIONES.....	133
BIBLIOGRAFÍA .....	135
ANEXOS .....	137

## ÍNDICE DE TABLAS

Cuadro N° 1: Comparaciones entre Auditoría de Cuentas y Auditoría Informática .....	21
Cuadro N° 2: Principales Funcionarios .....	57
Cuadro N° 3. Recursos Materiales .....	75
Cuadro N° 4. Cronograma de Trabajo.....	63
Cuadro N° 5. Resumen de Hallazgo.....	65

## ÍNDICE DE GRÁFICOS

Gráfico N° 1: Clasificación de Auditoría .....	7
Gráfico N° 2: Componentes COSO II .....	12
Gráfico N° 3. Sistema de Gestión de TIC .....	23
Gráfico N° 4. Tipo de Auditoría Informática.....	27
Gráfico N° 5. Fases de la Auditoría Informática Razo (2002) .....	41
Gráfico N° 6. Fases de la Auditoría Informática Echenique (2001) .....	42
Gráfico N° 7. Estructura Organizacional .....	58
Gráfico N° 8. Ubicación Geográfica.....	59
Gráfico N° 9. Logotipo .....	59

## ÍNDICE DE ANEXOS

Anexo N° 1. Registro de la Superintendencia de Companias.....	137
Anexo N° 2. Registro de los Socios o Accionistas .....	138
Anexo N° 3. Departamentos de la Empresa Ircostel Cía. Ltda.....	140
Anexo N° 4. Departamento de Sistemas Ircostel Cía. Ltda.....	142

## **RESUMEN EJECUTIVO**

La presente investigación de Auditoría Informática a la Gestión de las TIC se realizó en el departamento de sistemas de la Empresa IRCOSTEL CÍA. LTDA., de la ciudad de Riobamba, para contribuir en el mejoramiento de la seguridad y confiabilidad en el manejo de los recursos tecnológicos del sistema informático. La metodología utilizada para el desarrollo de la auditoría informática consta de cuatro fases, en la planificación se detalla el programa de trabajo, entrevista al Gerente, visita previa a las instalaciones, y el memorándum de planificación., La evaluación al sistema informático se realizó aplicando los ocho componentes del COSO II con la finalidad de analizar el nivel de riesgo y confianza resultante de los cuestionarios utilizados.

En el análisis de áreas críticas se elaboró indicadores de eficiencia, eficacia y seguridad del área informática, y se identificó los principales hallazgos, que se detectaron en la Empresa IRCOSTEL CÍA. LTDA., desde el inicio de sus actividades podemos citar que se ha manejado con funciones básicas sin implementar Manuales de Ética, Programas de Capacitación, Seguridad e Higiene y políticas de manejo de los recursos tecnológicos de la información, poniendo en riesgo la integridad, seguridad y disponibilidad de los recursos informáticos. Por lo que se recomienda a los Directivos de la Empresa IRCOSTEL CÍA. LTDA., diseñar Manuales de Ética, Programas de Capacitación, Seguridad e Higiene y políticas de manejo de los recursos tecnológicos de la información, que serán adecuados a los requerimientos de la Empresa, que brinden seguridad, confianza y protección de los recursos tecnológicos.

**Palabras clave:** AUDITORÍA DE INFORMATICA, INDICADORES DE GESTIÓN INFORMATICOS, SEGURIDAD FÍSICA Y LÓGICA , CONTROL INTERNO, COSO II.

Ing.: Espindola Lara Oscar Omar

**DIRECTOR DEL TRABAJO DE TITULACIÓN**

## **EXECUTIVE SUMMARY**

The objective of the present investigation is to develop Informatics Auditing to the TIC Management, which was made in the System Department of the Enterprise IRCOSTEL (Ltd. Co.), of the city of Riobamba to contribute in the improvement of the safety and trust in the management of the technological resources of the informatics system. The evaluation to the informatics system was made by applying the eight components of the COSO II with the aim to analyze the risk level and trust resulting of the surveys used.

Within the analysis of the critical areas indicators of efficiency, efficacy and safety were elaborated in the informatics area and the main findings were identified, from the beginning of its activities basic functions has been managed without implementing manuals of Ethics, Training Programs, Safety and Hygiene and Policies of Management of Information Technological Resources, by risking the integrity, safety and availability of the informatics resources. That is why is recommended to the executives of the Enterprise to desing manuals of Ethics, Training Programs, Safety and Hygiene and Policies of Management of Information Technological Resources, Which will be adequate to the Enterprise requirements that brings safety, trust, and protection of the technological resources.

**Key Words:** Informatics Auditing, Informatics Management Indicators, Physical and Logical Safety, Internal Control, COSOII.

## INTRODUCCIÓN

La Empresa Ircostel Cía. Ltda., se constituye legalmente el 30 de octubre del 2009 mediante escritura pública otorgada ante el notario cuarto del Cantón Riobamba. Dr. Carlos Marcelo Aúlla Erazo, aprobada mediante resolución N° SC.DIC. A. 09. 00315 y legalmente inscrita en el Registro Mercantil el 06 de noviembre del 2009 bajo el número 1619, se encuentra ubicada en la provincia de Chimborazo, en la ciudad de Riobamba en las calles Primera Constituyente y Juan Larrea y está bajo el control de la Súper Intendencia de Compañías, la finalidad de la empresa es la comercialización y servicio de la telefonía Claro a toda la ciudadanía.

IRCOSTEL CÍA. LTDA., desde el inicio de sus actividades se ha manejado con funciones básicas sin implementar Manuales de Ética, Programas de Capacitación, Seguridad e Higiene y políticas de manejo de los recursos tecnológicos de la información, poniendo en riesgo la integridad, seguridad y disponibilidad de los recursos informáticos.

El objetivo de la presente investigación es desarrollar una herramienta completa que permita realizar una auditoría informática, permitiendo proponer soluciones para contrarrestar los problemas que aparecen por la inadecuada utilización de los recursos tecnológicos, por ello se desarrolla cuatro capítulos detallados a continuación.

CAPÍTULO I: denominado El Problema donde se analiza los antecedentes, formulación, delimitación, objetivos y la justificación que respalda el desarrollo de la presente investigación.

CAPÍTULO II: Se refiere al Marco Teórico donde se desarrolla la fundamentación teórica realizada mediante conceptos, leyes y modelos que ayudan al análisis y solución del problema encontrado.

CAPÍTULO III: Marco Metodológico donde se identificaron los métodos, técnicas e instrumentos que se utilizó para recolectar información.

CAPÍTULO IV: El Marco Propositivo que consta de los archivos: Corriente y Permanente, y también la Planificación de la Auditoría que se ejecutó en base a cuatro fases que son: Planificación Preliminar, Evaluación del Control Interno, Análisis de Áreas Críticas e Informe.

# CAPÍTULO I: EL PROBLEMA

## 1.1. PLANTEAMIENTO DEL PROBLEMA

El Ircostel Cía. Ltda., es una empresa dedicada al servicio de la telefonía CLARO, al igual que otras empresas presenta múltiples deficiencias en cuanto a su organización, a la presente fecha no se ha realizado una Auditoría Informática que da a conocer una visión más amplia de la organización en especial del departamento de sistemas con respecto a la gestión de las TIC que contribuya a tomar decisiones oportunas y salvaguardar los recursos tecnológicos.

Entre las principales debilidades encontradas, citamos las siguientes:

- ZETALIBRA – Versión 2.3.50 no cumple con los requerimientos de la empresa.
- La inadecuada utilización en el manejo de los recursos tecnológicos y la falta de mantenimiento, provoca pérdida y daños severos a los equipos que afecta a los requerimientos del personal administrativo y consecuentemente al servicio que la empresa brinda a los clientes.
- No posee instalaciones adecuadas lo que dificulta el desarrollo normal de los recursos tecnológicos de la empresa.

### 1.1.1. Formulación del Problema

¿Cómo incide la realización de una auditoría informática a la gestión de las TIC del departamento de sistemas de la empresa IRCOSTEL CÍA. LTDA., en el manejo de los recursos tecnológicos del sistema informático?

### 1.1.2. Delimitación del Problema

Campo: Auditoría Informática.  
Área: Departamento de Sistemas  
Temporal: Período 2014  
Espacial: Empresa Ircostel Cía. Ltda.

## **1.2. JUSTIFICACIÓN**

La presente investigación permitirá, evidenciar errores y/o falencias en el manejo de los recursos tecnológicos de la Empresa Ircostel Cía. Ltda., en primer lugar se ha observado que el sistema informático zeta libre versión 2.3.50 no cumple con los requerimientos de la empresa, datos inconsistentes para generar la contabilidad, la inadecuada utilización en el manejo de los recursos tecnológicos y la falta de mantenimiento, provocando pérdida y daños severos a los equipos que afecta a los requerimientos del personal administrativo y consecuentemente al servicio que la empresa brinda a los clientes.

Otro aspecto desfavorable es que no posee instalaciones lo que dificulta el desarrollo normal de los recursos tecnológicos de la empresa.

La aplicación de la Auditoría Informática permitirá identificar las falencias en el sistema Zetalibre, el inadecuado manejo de los recursos tecnológicos y la falta de mantenimiento e instalaciones adecuadas para evitar en el futuro el deterioro, pérdida total o parcial de los recursos tecnológicos que posee la entidad para la ejecución de sus funciones, tareas y atención eficiente y eficaz a todos sus usuarios.

La presente investigación permitirá poner en evidencia los conocimientos adquiridos durante la etapa de aprendizaje como estudiante de la ESPOCH, y lograr un aporte a la sociedad la cual servirá de guía o mejora para las siguientes investigaciones.

## **1.3.OBJETIVOS**

### **1.3.1. Objetivo General**

Realizar una Auditoría Informática a la Gestión de las TIC del departamento de sistemas de la empresa IRCOSTEL CIA. LTDA., de la ciudad de Riobamba, para mejorar la seguridad y confiabilidad en el manejo de los recursos tecnológicos del sistema informático.

### **1.3.2. Objetivos Específicos**

- Elaborar el marco teórico que permita desarrollar la Auditoría de Sistemas Informáticos.
- Evaluar el sistema de control interno a través de la normativa vigente.
- Emitir un informe que contenga conclusiones y recomendaciones para la toma de decisiones oportunas.

## **CAPÍTULO II: MARCO TEÓRICO**

### **2.1. ANTECEDENTES INVESTIGATIVOS**

#### **2.1.1. Antecedentes Históricos**

En la actualidad La presente investigación se realizará a la Empresa IRCOSTEL CIA LTDA. mediante el lineamiento de investigaciones posteriores, basada en la Auditoría Informática de la Superintendencia de Telecomunicaciones elaborada por la Ing. Verónica Karina Quintuña Rodríguez en la ciudad de Cuenca, en cuanto al modelo empleado para la planeación y ejecución de la auditoría informática a la Superintendencia de Telecomunicaciones, se puede afirmar que además de ser una herramienta de auditoría es un marco de gobierno de TI, ya que permite asegurar que los procesos y recursos tecnológicos, contribuyen al logro de los objetivos institucionales y la satisfacción de los clientes.

Auditoría Informática de los Sistemas Tecnológicos de Información realizada a la Cooperativa de Ahorro y Crédito “Alianza del Valle”. Ltda. Utilizando COBIT 4.0 Elaborada por la Ing. Andrea Cadena Marten, Ing. Gabriela Barros Marcillo en la ciudad de Quito, el análisis de los Objetivos de Control con COBIT debe ser de carácter objetivo e independiente, crítico, basado en evidencia, sistemático, bajo normas y metodologías aprobadas a nivel internacional, que seleccione políticas, normas, prácticas, funciones, procesos, procedimientos e informes relacionados con los sistemas de información computarizados, que permiten obtener una opinión profesional e imparcial enfocada en aspectos como: criterios de información y prácticas requeridas que ayuden a determinar con eficiencia el uso de los recursos informáticos, validez de la información y efectividad de los controles establecidos.

Las dos tesis citadas anteriormente nos servirán como guía para la elaboración de nuestra investigación, logrando identificar las falencias existentes en el manejo de los recursos tecnológicos del sistema informático.

## **2.2. FUNDAMENTACIÓN TEÓRICA**

### **2.2.1. Auditoría**

“Mantilla (2009) define a la auditoría como la evaluación de una persona, organización, sistema, proceso, producto o proyecto, realizada para determinar la validez y la confiabilidad de la información, y también proporcionar una evaluación del sistema de control interno.

Auditoría es el proceso estructurado que:

- a) Con lleva la aplicación de habilidades analíticas, juicio profesional y escepticismo profesional;
- b) Usualmente es realizado por un equipo de profesionales, dirigido con habilidades directivas;
- c) Usa formas apropiadas de tecnología y se adhiere a una metodología;
- d) Cumple con todos los estándares técnicos relevantes tales como los Estándares Internacionales de Auditoria (ISAs), los Estándares Internacionales de Control de Calidad (ISQCs), los Estándares Internacionales de Información Financiera (IFRS), los Estándares Internacionales de Contabilidad del Sector Público (IPSAS), y otros equivalentes internacionales, nacionales o locales;
- e) Cumple con los estándares requeridos de ética profesional.

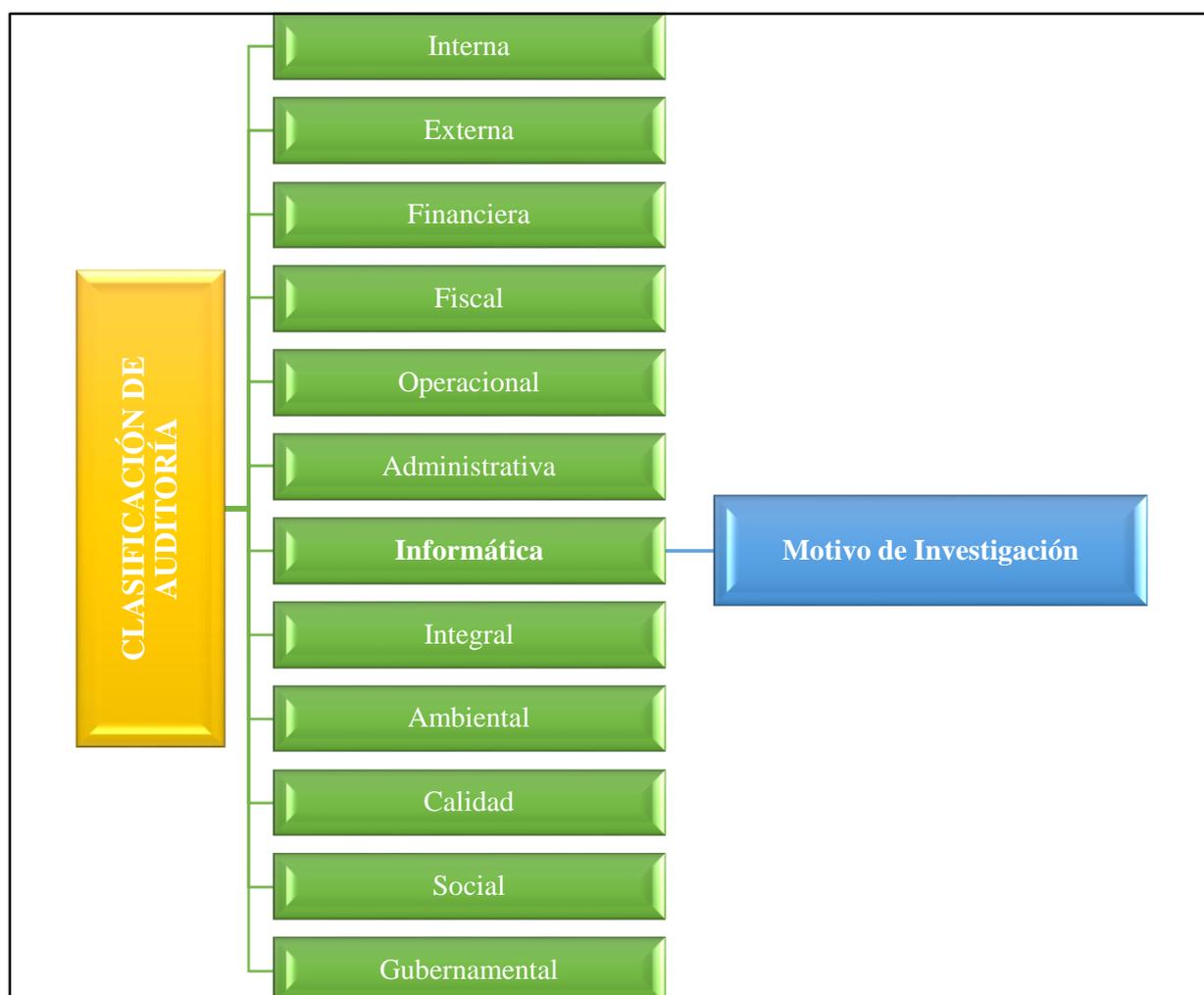
Según Blanco (2012) sostiene que la Auditoría es un proceso sistemático, que consiste en obtener y evaluar objetivamente evidencias sobre las afirmaciones relativas a los actos o eventos de carácter económico – administrativo, con el fin de determinar el grado de correspondencia entre esas afirmaciones y los criterios establecidos, para luego comunicar los resultados a las personas interesadas.

#### **2.2.1.1. Clasificación de Auditoría**

“Existe Cuellar (2010), Finkowsky (2007), Piattini (2009), Blanco (2012) manifiesta el campo de acción del auditor puede ser muy amplio o bien restringido a determinados fines, según instrucciones recibidas de sus mandatos o clientes.

Esto da origen a distintas clases de auditoría como lo podemos observar en el grafico 1

Gráfico N° 1 Clasificación de Auditoría



Fuente: Elaboración propia con información Cuellar (2010); Finkowsky (2007); Piattini (2009); Blanco (2012)

**Auditoría Financiera.-** Cuellar (2010), manifiesta que la auditoría financiera examina a los estados financieros y a través de ellos las operaciones financieras realizadas por el ente contable, con la finalidad de emitir una opinión técnica y profesional.

Consiste en el examen de los registros, comprobantes, documentos y otras evidencias que sustentan los estados financieros de una entidad u organismo, efectuado por el auditor para formular el dictamen respecto de la razonabilidad con que se presentan los resultados de las operaciones, la situación financiera, los cambios operados en ella y en el patrimonio; para determinar el cumplimiento de las disposiciones legales y para formular comentarios, conclusiones y recomendaciones tendientes a mejorar los procedimientos relativos a la gestión financiera y control interno.

Para que el auditor esté en condiciones de emitir su opinión en forma objetiva y profesional, tiene la responsabilidad de reunir los elementos de juicio suficientes que le permitan obtener una certeza razonable sobre:

1. La autenticidad de los hechos y fenómenos que reflejan los estados financieros.
2. Que son adecuados los criterios, sistemas y métodos utilizados para captar y reflejar en la contabilidad y en los estados financieros dichos hechos y fenómenos.
3. Que los estados financieros estén preparados y revelados de acuerdo con los Principios de Contabilidad Generalmente Aceptados, las Normas Ecuatorianas de Contabilidad y la normativa de contabilidad

**Auditoría Fiscal.-** Cuellar, (2010) afirma que es una inspección de la situación tributaria de una persona o de una empresa para verificar si cumplen con sus obligaciones.

La auditoría fiscal, por lo tanto, es un proceso que consiste en la obtención y evaluación de evidencias acerca de los hechos vinculados a los actos de carácter tributario. El auditor debe comparar las declaraciones y los pagos de impuestos con las finanzas del ente auditado para determinar si todo está en regla.

**Auditoría Operacional.-** según Cuellar, (2010) es una revisión y evaluación parcial o total de las operaciones y procedimientos adoptados en una empresa, con la finalidad principal de auxiliar a la dirección a eliminar las deficiencias por medio de la recomendación de medidas correctivas. Comprende además de la financiera, el examen y evaluación de la planeación, organización, dirección y control interno administrativo; de la eficiencia, eficacia y economía con que se han empleado los recursos humanos, materiales y financieros; y de los resultados de las operaciones programadas para saber si se han logrado o no los objetivos propuestos.

**Auditoría Administrativa.-** según Finkowsky (2007) que es la revisión analítica total o parcial de una organización con el propósito de precisar su nivel de desempeño y perfilar oportunidades de mejora para innovar el valor y lograr una ventaja competitiva sustentable.

**Auditoría Informática.-** Piattini, Peso y Peso (2008) sostiene que 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. De este modo la auditoría informática sustenta y confirma la consecuencia de los objetivos tradicionales de la auditoría.

**Auditoría Integral.-** Blanco (2012) se refiere como el proceso de obtener y evaluar objetivamente, en un período determinado, evidencia relativa a la siguiente temática: la información financiera, la estructura del control interno, el cumplimiento de las leyes pertinentes y la conducción ordenada en el logro de las metas y objetivos propuestos; con el propósito de informar sobre el grado de correspondencia entre la temática y los criterios o indicadores establecidos para su evaluación.

**Auditoría Ambiental.-** según Cuellar (2010) examina los procesos e impactos industriales en el medio ambiente y recursos materiales, con base en los lineamientos de normatividad oficiales de la autoridad federal y estatal en la materia.

**Auditoría Calidad.-** Cuellar, (2010) estudia la evaluación de la calidad consiste en un examen minucioso del producto o servicio que ofrece la organización (privada o pública), así como de los procesos que la integran. Dicha evaluación requiere certificación de los resultados.

**Auditoría Social.-** Cuellar, (2010) sostiene que la auditoría social representa un examen del comportamiento social del negocio, lo cual incluye las acciones emprendidas y la manera en que han repercutido en la sociedad de su localidad, de su país e internacionalmente. Algunos de los aspectos que se consideran son: salud, vivienda, obras viales, escolares, seguridad y programas de tipo social en las comunidades

**Auditoría Gubernamental.-** Manifiesta Cuellar, (2010) es un mecanismo disponible en la actualidad para los diversos órganos de control y vigilancia, así como, para las máximas autoridades de las diferentes entidades que componen el sector público, ya que permite el ejercicio de funciones de revisión, control y fiscalización de manera independiente

### 2.2.2. Tipos de Informes

**Piattini, Peso y Peso (2008)** menciona que las opiniones pueden clasificarse por el tipo de trabajo y por los resultados del trabajo.

Por el tipo de trabajo, como ya se ha comentado, las opiniones se pueden expresar de forma positiva o negativa.

Según los resultados del trabajo los tipos de opiniones básicas generalmente aceptadas en auditoría son cuatro.

1. **Favorable:** si se concluye que el sistema es satisfactorio, el auditor emitirá una opinión favorable.
2. **Desfavorable:** si el auditor considera que el sistema es un desastre, su opinión sería desfavorable.
3. **Con salvedades:** el sistema es satisfactorio, aunque contiene ciertas debilidades o incumplimientos que no lo invalidan, opinión con salvedades.
4. **Denegación de opinión:** también podría ocurrir que el auditor no tenga suficientes elementos de juicio para poder opinar; en ese caso no opinaría y a tipo de opinión se le denomina denegación de opinión.

#### **Recomendaciones de los Informes.**

Cuando el auditor, durante la realización de la auditoría, detecte debilidades, debe comunicarlas al auditorio con la mayor prontitud posible, un esquema, generalmente aceptado, de cómo presentar las debilidades es el siguiente:

- Describir la debilidad.
- Indicar el criterio o instrumento de medida que se ha utilizado.
- Indicar los efectos que puede tener en el sistema de información.
- Describir la recomendación con la que esa debilidad se podrá eliminar.
- Respuesta a los directivos.

### **2.2.2.1.Control Interno**

Según la Contraloría General del Estado. (2012) el control interno constituye un proceso aplicado por la máxima autoridad, la dirección y el personal de cada institución, que proporciona seguridad razonable de que se protegen los recursos públicos y se alcancen los objetivos institucionales.

Constituyen elementos del control interno: el entorno de control, la organización, la idoneidad del personal, el cumplimiento de los objetivos institucionales, los riesgos institucionales en el logro de tales objetivos y las medidas adoptadas para afrontarlos, el sistema de información, el cumplimiento de las normas jurídicas y técnicas; y, la corrección oportuna de las deficiencias de control.

El control interno será responsabilidad de cada institución del Estado y tendrá como finalidad primordial crear las condiciones para el ejercicio del control externo a cargo de la Contraloría General del Estado.

### **2.2.2.2.Objetivos del Control Interno**

**Fonseca. (2011)** establece como objetivos del control interno los siguientes:

- Asegurar que los procesos, actividades, recursos y operaciones se realicen de acuerdo a criterios de efectividad, eficiencia, economía, transparencia y calidad.
- Prevenir o detectar la utilización deficiente o perjudicial de bienes y recursos de la empresa, operaciones no autorizadas, actos o decisiones que conlleven egresos antieconómicos, apropiaciones indebidas, así como en general todas aquellas actuaciones que podrían significar pérdidas tangibles o potenciales para la organización, incluyendo los casos de despilfarro e irregularidades en el uso de recursos.
- Asegurar que los actos y operaciones que realiza, así como la utilización de los recursos, se sujeten y sean acordes con las disposiciones establecidas en las disposiciones legales y administrativas vigentes.

- Asegurar que la información financiera y de gestión elaborada por la empresa es válida y confiable, así como que sea revelada razonablemente en los informes correspondientes.
- Fomentar una cultura sólida y el ejemplo, que adopta la dirección y personal de la empresa para lograr el respeto de la colectividad a la que sirve y un clima institucional favorable al cumplimiento cabal de su misión.

### 2.2.2.3.Importancia del Control Interno

Según Mantilla. (2009) dice que el control interno es importante porque facilita la efectividad y la eficiencia de las operaciones, ayuda a asegurar la confiabilidad del proceso de presentación de reportes internos y externos y ayuda al cumplimiento de las leyes y regulaciones.

### 2.2.2.4.COSO II o ERM

Según Fonseca (2011) el ERM ofrece una mejor oportunidad de supervivencia a las organizaciones mediante la adopción de acciones para: identificar, mitigar, evitar y responder ante los riesgos que podría afrontar en el presente y en el futuro.

### 2.2.2.5.Componentes

Gráfico N° 2 Componentes COSO II



Fuente: Elaboración propia con información Fonseca (2011)

1. **Ambiente Interno:** comprende el todo de la organización que influye en la conciencia de sus empleados, con relación al riesgo y establece la base para el resto de componentes de la gestión de riesgos corporativos, proporcionando estructura y disciplina.
2. **Establecimiento de Objetivos:** los objetivos de la organización se fijan en el nivel estratégico, estableciendo con ellos una base para la identificación de los objetivos operacionales, de información y de cumplimiento. Cada organización confronta una variedad de riesgos procedentes de fuentes externas e internas y una condición previa para la identificación eficaz de eventos, la evaluación de sus riesgos y la respuesta a ellos consiste en fijar los objetivos alineados con el riesgo aceptado por la organización, lo que a su vez orienta los niveles de tolerancia al riesgo.
3. **Identificación de Eventos:** la gerencia identifica los eventos potenciales que, de ocurrir, podrían afectar a la organización y determina si representan oportunidades o si, podrían afectar negativamente su capacidad para implementar la estrategia y lograr los objetivos con éxito. Los eventos que tienen un impacto negativo representan riesgos que requieren evaluación y respuesta. Los eventos que tienen un impacto positivo representan oportunidades, que la gerencia debería aprovechar para reorientar la estrategia y el proceso de diseño de los objetivos.
4. **Evaluación de Riesgos:** la evaluación de riesgos permite a la organización considerar la amplitud con que los eventos potenciales podrían impactar en el logro de sus objetivos. La gerencia evalúa estos acontecimientos desde un doble ángulo: probabilidad e impacto. Los impactos positivos y negativos de los eventos potenciales, deberían examinarse en forma individual o por categoría en la organización.
5. **Respuesta al Riesgo:** una vez que la gerencia ha evaluado los riesgos importantes, debería determinar cómo hacerles frente, ya sea evitando, reduciendo, compartiendo y/o aceptando el riesgo. Al considerar su respuesta la gerencia evalúa su efecto y la probabilidad de impacto del riesgo, así como los costos y beneficios involucrados,

seleccionando aquella que ubique el riesgo residual dentro de las tolerancias al riesgo establecidas por la organización.

- 6. Actividades de Control:** están constituidas por políticas y procedimientos que aseguran que se llevan a cabo las respuestas de la gerencia ante los riesgos. Las actividades de control se desarrollan a través de toda la organización, en todos los niveles y funciones, e incluyen una gran variedad de actividades entre otras: aprobaciones, autorizaciones, verificaciones, conciliaciones, revisiones operativas, salvaguarda de activos y segregación de funciones.
  
- 7. Información y Comunicación:** la información se identifica, obtiene y comunica de una forma y en un marco de tiempo que permite a las personas llevar a cabo sus responsabilidades. Los sistemas de información utilizan datos generados internamente y otros datos de fuentes externas y su salida facilita la gestión de riesgos y la toma de decisiones con relación a los objetivos. Del mismo modo, existe una comunicación eficaz fluyendo en todas las direcciones de la organización.
  
- 8. Monitoreo:** la gestión de los riesgos corporativos se monitorea, revisando la presencia y funcionamiento de sus componentes en el tiempo mediante evaluaciones continuas y evaluaciones independientes. El monitoreo se ejecuta en el curso normal de las actividades de gestión, en tanto que la frecuencia de las evaluaciones independientes está condicionada a la evaluación de riesgos. Del mismo modo, las deficiencias en la gestión de riesgos se comunican, transfiriendo los asuntos importantes para la consideración de la gerencia y la junta de directores.

#### **2.2.2.6. Papeles de trabajo**

Según Piattini, Peso y Peso (2008) indica como la documentación de la auditoría de los sistemas de información es el registro del trabajo de auditoría realizado, y la evidencia que sirve de soporte a las debilidades encontradas y las conclusiones a las que ha llegado el auditor. Esos documentos genéricamente se denominan papeles de trabajo. Los papeles de trabajo se deben diseñar y organizar según las circunstancias y las necesidades del auditor. Estos han de ser completos, claros y concisos. Todo el trabajo de auditoría debe quedar reflejado en papeles de trabajo por los siguientes motivos:

- ❖ Recogen la evidencia obtenida a lo largo del trabajo.
- ❖ Ayudan al auditor en el desarrollo de su trabajo.
- ❖ Ofrecen un soporte del trabajo realizado para, así, poder utilizarlo en auditorías sucesivas.
- ❖ Permiten que el trabajo pueda ser revisado por terceros.

#### **2.2.2.7. Programas de auditoría**

Según Blanco (2007) señala al programa de auditoría como el plan detallado o listado de procedimientos a ser ejecutados, con el objeto de comparar los sistemas y controles existentes con criterios de auditoría y, recolectar evidencias para sustentar las observaciones. La preparación efectiva de los programas de auditoría proporciona;

- a) Un plan sistemático para cada fase del trabajo, el que puede comunicarse a todo el personal involucrado en la auditoría;
- b) Una base apropiada de asignación de labores para el supervisor, auditor encargado, auditores y asistentes;
- c) Medio para comparar el rendimiento del equipo de auditoría con relación a los planes aprobados y normas complementarias establecidas;
- d) Ayuda al entrenamiento de personal sin experiencia en auditoría;
- e) Sirve al supervisor para disminuir el trabajo de supervisión sobre el personal en forma directa.

#### **2.2.2.8. Referencias y marcas**

Según Peña (2011) define como referencia y marcas:

Se denominan referencias de las hojas de trabajo a los caracteres alfanuméricos que las identifican y que van a permitir ordenar los papeles de trabajo de una forma lógica facilitando, de esta manera su manejo y archivo.

Por su parte se denominan tildes o marcas de comprobación a una serie de símbolos que se emplean en las hojas de trabajo para:

- Explicar la documentación examinada.
- Explicar la procedencia de datos.

- Evidenciar el trabajo realizado.
- Para llevar al lector de la hoja de una parte a otra de la misma.

Es imprescindible explicar en la propia hoja el significado de los símbolos utilizados en su elaboración para que un tercero que no ha participado en su elaboración pueda comprender el trabajo efectuado y las conclusiones alcanzadas.

#### **2.2.2.9. Archivo Corriente**

Las Cardozo (2006) afirma como archivo corriente: Este archivo recoge todos los papeles de trabajo relacionados con la auditoría específica de un período; Los tipos de información que se incluyen en el archivo presente son: programas de auditoría, información general, balance de comprobación de trabajo, asientos de ajuste y reclasificación y cédulas de apoyo; La cantidad de legajos o carpetas que forman parte de este archivo de un período dado varía de una auditoría a otra y aun tratándose de la misma entidad auditada.

.

#### **2.2.2.10. Archivo Permanente**

Dávalos (1990) indica como archivo permanente:

Contiene la documentación elemental de la información obtenida en un trabajo de auditoría que se considera útil para la ejecución de exámenes posteriores con el propósito de contar con una fuente de datos permanentes sobre la naturaleza y objetivos del ente examinado, evitando pérdida de tiempo y la duplicación de esfuerzos en obtener en cada caso, información sobre el mismo organismo sujeto a control.”

#### **2.2.2.11. Pruebas de auditoría**

Son técnicas o procedimientos que se utiliza para la obtención de evidencia que compruebe y fundamente su dictamen u opinión de la auditoría. (Enrique Franklin, Auditoría Administrativa; Evaluación y diagnóstico empresarial, 2013, pp.15-16)

### **2.2.2.12. Clasificación de las pruebas de auditoría**

#### **Pruebas de control**

Están relacionadas con el grado de efectividad del control interno imperante.

#### **Pruebas analíticas**

Se utilizan haciendo comparaciones entre dos o más estados financieros o haciendo un análisis de las razones financieras de la entidad para observar su comportamiento.

#### **Pruebas de cumplimiento**

Consiste en recolectar evidencia con el propósito de probar el cumplimiento de una organización con procedimientos de control.

#### **Pruebas sustantivas**

Se refiere en la que la evidencia se recoge para evaluar la integridad de transacciones individuales, datos u otra información.

### **2.2.2.13. Evidencia**

Según La Norma Internacional de Auditoría (2013) señala que la información utilizada por el auditor para alcanzar las conclusiones en las que basa su opinión. La evidencia de auditoría es necesaria para sustentar la opinión y el informe de auditoría. Es de naturaleza acumulativa y se obtiene principalmente de la aplicación de procedimientos de auditoría en el transcurso de la auditoría

### **2.2.2.14. Requisitos de la evidencia**

Finkowsky (2013) señala que los requisitos de la evidencia son:

**Suficiente:** Debe ser necesaria para sustentar los hallazgos, conclusiones y recomendaciones del auditor.

**Competente:** Debe ser consistente, convincente, confiable, y haber sido validada.

**Relevante:** Debe aportar elementos de juicio para demostrar o refutar un hecho en forma lógica y convincente.

**Pertinente:** Debe existir congruencias entre las observaciones, conclusiones y recomendaciones de la auditoría.

### **2.2.2.15. Clasificación de la evidencia**

Finkowsky (2013) clasifica a la evidencia de la siguiente manera:

#### **Evidencia Física**

- **Inspección:** Es el examen físico de activos tangibles con objeto de asegurarse de su existencia.
- **Observación:** Consiste en presenciar un determinado proceso o procedimiento efectuado por el personal de la entidad auditada.”

#### **Evidencia Documental**

- **Revisión de documentos:** Consiste en la revisión de la documentación que soporta a los registros contables.
- **Obtención de certificaciones:** Consiste en la obtención de documentos donde se certifique por alguna autoridad la realidad de determinados hechos.”

#### **Confirmaciones de Terceros**

- **Confirmación mediante circularización:** Mediante este procedimiento se trata de contrastar la información contenida en los registros contables, u otro tipo de información, con las afirmaciones de un tercero, normalmente ajeno a la empresa.”

#### **Evidencia Verbal**

- **Cuestionarios:** Tiene por objeto obtener de manera estructurada determinado tipo de información bien del personal de la propia empresa o bien de terceros.

- **Conversaciones:** Consiste en obtener información a través de conversaciones o de comentarios efectuados por el personal de la propia entidad auditada que pueda poner de manifiesto la existencia de determinados problemas organizativos o personales.”

### **Evidencia Analítica**

- **Comparaciones:** Consiste en comparar determinadas partidas de las cuentas anuales, con cifras de referencia significativas para el auditor.
- **Cálculos:** El auditor comprueba la exactitud de los cálculos realizados por la empresa con el fin de pronunciarse sobre la razonabilidad de determinadas partidas.

#### **2.2.2.16. Hallazgo**

Maldonado. (2011) establece que el hallazgo en la auditoría tiene el sentido de la obtención y síntesis de información sobre una operación, actividad, proyecto, unidad administrativa u otro asunto evaluación y que los resultados sean de intereses para los funcionarios de la empresa auditada. La evidencia de los hallazgos de auditoría deberá ser evaluada en términos de suficiencia, importancia, confiabilidad y eficacia; El concepto de “hallazgo de auditoría” implica que este tenga 4 atributos: Condición, criterio, causa, efecto.

#### **2.2.2.17. Atributos**

Maldonado. (2011) indica como atributos del hallazgo los siguientes:

**Condición:** es la situación actual encontrada por el auditor con respecto a una operación, actividad o transacción. La condición refleja el grado en que los criterios están siendo logrados. Es importante que la condición se refiera directamente al criterio o unidad de medida porque el objetivo de la condición es describir lo bien que se comporta la organización en el logro de las metas expresadas como criterios.”

**Criterio:** son las metas que la entidad está tratando de lograr o las normas relacionadas con el logro de las metas. Necesariamente son unidades de medida que permiten la evaluación de la condición actual.

**Causa:** es la razón fundamental (o razones fundamentales) por la cual ocurrió la condición, o es el motivo por el que no se cumplió el criterio o norma. La simple aseveración en el informe de que el problema existe porque alguien no cumplió las normas es insuficiente para hacer convincente al lector.”

**Efecto:** es el resultado adverso, real o parcial que resulta de la condición encontrada. Normalmente representa la pérdida en dinero o en efectividad causada por el fracaso en el logro de las metas

#### **2.2.2.18.Auditoría Informática**

Piattini, Peso y Peso (2008) señala que 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.

Echenique (2001) manifiesta la Auditoría Informática como un conjunto importante de tareas, realizadas y materializadas por profesionales especialmente capacitados para el efecto, y que consiste en recolectar, agrupar y evaluar evidencias, para poder saber si un sistema informático salvaguarda el activo empresarial, si mantiene la integridad de los datos, si utiliza eficientemente los recursos y si cumple con las leyes y regulaciones establecidas.

#### **2.2.2.19.Auditor Informático**

Piatinni, Peso y Peso (2008) manifiesta que la tecnología de la información y las comunicaciones (TIC) están creando nuevos canales y herramientas para la gestión de los negocios. El auditor tradicional, esto es, el auditor de cuentas, no se encuentra capacitado en términos de formación para afrontar los nuevos riesgos derivados de la utilización de las tecnologías. De ahí que se haga imprescindible la existencia de la auditoría de sistemas informáticos.

Entre las características del auditor destaca la independencia. Podemos definir la dependencia del auditor como la ausencia de intereses o influencias que permite al auditor

actuar con libertad respecto a su juicio profesional, para la cual debe estar libre de cualquier predisposición que impida su imparcialidad en la consideración objetiva de los hechos. Los problemas pueden clasificarse en tres grupos principales:

La compatibilidad de la práctica de la auditoría con las asesorías legales, el interlocutor del auditor dentro de la empresa auditada y la rotación del auditor.

Tabla N° 1 Comparaciones entre Auditoría de Cuentas y Auditoría Informática

<b>AUDITOR</b>	<b>AUDITORÍA DE CUENTAS</b>	<b>AUDITORÍA INFORMÁTICA</b>
<b>FUNCIÓN</b>	ANALIZAR:	ANALIZAR:
	INFORMACIÓN ECONÓMICA	INFORMACIÓN ENTORNOS INFORMÁTICOS
	FINANCIERA	DEDUCIDA
	DEDUCIDA DE DOCUMENTOS	REVISIÓN Y CONTROL DE LOS MISMOS
	CONTABLES	
<b>INFORME</b>	EMITIR INFORME:	EMITIR INFORME:
	MANIFESTANDO SU OPINIÓN	MANIFESTANDO SU OPINIÓN
	RESPONSABLE	RESPONSABLE
	SOBRE LA FIABILIDAD DE LA INFORMACIÓN PARA QUE SE CONOSCA Y VALORE POR TERCEROS	SOBRE LA FIABILIDAD DE LA INFORMACIÓN PARA QUE SE CONOSCA Y VALORE POR TERCEROS
<b>REGLAMENTACIÓN</b>	SUJETO A:	SUJETO A:
	REQUISITOS	REQUISITOS
	FORMALIDADES	FORMALIDADES
	LEY	NORMAS DE LA PROFESIÓN
	REGLAMENTO	CÓDIGO DE CONDUCTA DE LA PROFESIÓN

Fuente: Elaboración propia con información Piatinni, Peso y Peso (2008)

### **2.2.2.20. Auditoría de los Sistemas de Gestión en las Tecnologías de la Información y Comunicación (TIC)**

Piattini, Peso y Peso (2008) afirma acerca de los sistemas de gestión pretende centrarse en el análisis de los mismos desde las perspectiva de la gestión del conocimiento.

Podemos afirmar que el ciclo de Deming-con el acrónimo PDCA es un ciclo de mejora continua, donde cabe distinguir las siguientes fases:

**Plan:** planificación de objetivos y procesos necesarios para alcanzar los resultados de acuerdo a las políticas de la empresa.

**Do:** implantación de los procesos.

**Check:** revisión y monitorización de los procesos.

**ACT:** ejecutar acciones para mejorar continuamente los procesos.

Los ámbitos donde el PDCA pueden considerarse como el auténtico motor y el conocimiento de las TIC es muy variado: va desde la seguridad de los sistemas de información pasando por la ingeniería del software, hasta la calidad en los servicios TIC.

El conocimiento vendría a ser la guía de buenas prácticas que, desde la perspectiva de los sistemas de información, lo definimos como repositorio o base de datos de controles.

Los dos sistemas de gestión del sector de las TIC que están siendo más implantados por las empresas ya sean grandes corporaciones o PYMES son los denominados:

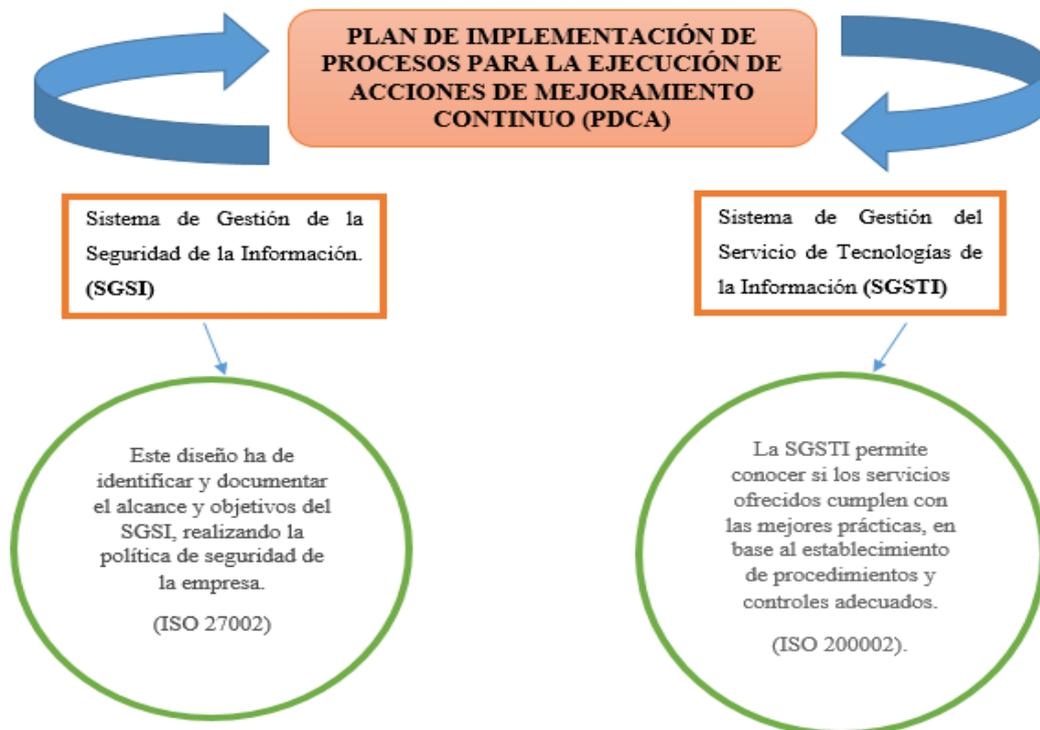
**SGSI:** Sistema de Gestión de la Seguridad de la Información.

**SGSTI:** Sistema de Gestión del Servicio de Tecnologías de la Información.

Las principales ventajas que presenta estos sistemas de gestión en las TIC la constituye su capacidad de integración con otros sistemas ya muy difundidos en las empresas, como son los sistemas de gestión de calidad, y el sistema medio ambiental, etc.

Por este motivo con su implementación se logra que las TIC queden integradas y alineadas con otros procesos de negocios.

Gráfico N° 3 Sistema de Gestión de TIC



Fuente: Elaboración propia con información Piattini, Peso y Peso (2008)

### 2.2.2.21. Importancia de la auditoría informática

Según Gallo (2010) Señala la importancia de la Auditoría Informática se ha extendido en los últimos años, debido al gran interés de las organizaciones por el aumento de errores dentro de los sistemas de información conforme pasa el tiempo, siendo necesario solventar problemas y adelantarse a ellos, para ganar efectividad y estabilidad en las empresas.

Muñoz (2002) señala que la evaluación a los sistemas computacionales, a la administración del centro de cómputo, al desarrollo de proyectos informáticos, a la seguridad de los sistemas computacionales y a todo lo relacionado con ellos, será considerada bajo los siguientes objetivos:

- Hacer una evaluación sobre el uso de los recursos financieros en las áreas del centro de información, así como del aprovechamiento del sistema computacional, sus equipos periféricos e instalaciones.

- Evaluar el uso y aprovechamiento de los equipos de cómputo, sus periféricos, las instalaciones y mobiliario del centro de cómputo, así como el uso de sus recursos técnicos y materiales para el procesamiento de información.
- Evaluar el aprovechamiento del sistema operativo, programas, software de producción disponible.
- Evaluar el cumplimiento de planes, programas, estándares, políticas, normas y lineamientos que regulan las funciones y actividades de las áreas y de los sistemas de procesamiento de información, así como de su personal y de los usuarios del centro de información.

Evaluar la disponibilidad de seguridades necesarias a fin de proteger y salvaguardar los equipos de tecnología disponibles para el desarrollo de actividades.

#### **2.2.2.22. Alcance de la auditoría informática**

López (2011) se refiere a definir con precisión el entorno y los límites en que va a desarrollarse la auditoría informática, se complementa con los objetivos de ésta. El alcance figurará expresamente en el Informe Final,

El campo de aplicación o alcance de la auditoría responde al conjunto de necesidades del cliente y debe quedar bien definido. El alcance especificará las instalaciones y unidades que van a ser cubiertas, así como áreas de estudio que van a ser tratadas, por lo que puede centrarse en un único puesto de trabajo, en un procedimiento o conjunto de procedimientos.

Echenique, (2001) el campo de acción de la Auditoría Informática es:

- La evaluación administrativa del área informática.
- La evaluación de los sistemas y procedimientos, y de la eficacia que se tiene en el uso de la información. La evaluación de la eficiencia y eficacia con la que se trabaja.
- La evaluación del proceso de datos de los sistemas y de los equipos de cómputo (software, hardware, redes, bases de datos, comunicaciones).

- Seguridad y confidencialidad de la información.
- Aspectos legales de los sistemas y de la información.

Para lograr los puntos antes señaladas se necesita:

- a) Evaluación administrativa del departamento de informática. Esto comprende la evaluación de:
- Los objetivos del departamento, dirección o gerencia.
  - Metas, planes, políticas, procedimientos de procesos electrónicos estándares.
  - Organización del área y su estructura orgánica.
  - Funciones y niveles de autoridad y responsabilidad del área de procesos electrónicos.
  - Integración de los recursos materiales y técnicos.
  - Dirección.
  - Costos y controles presupuestales.
  - Controles administrativos del área de procesos electrónicos.
- b) Evaluación de los sistemas y procedimientos, y de la eficiencia y eficacia que se tiene en el usos de la información, lo cual comprende:
- Evaluación del análisis de los sistemas y sus diferentes etapas.
  - Evaluación del diseño lógico del sistema.
  - Evaluación del desarrollo físico del sistema.
  - Facilidades para la elaboración de los sistemas.
  - Control de proyectos.
  - Control de sistemas y programación.
  - Instructivos y documentación.
  - Formas de implantación.
  - Seguridad física y lógica de los sistemas.
  - Confidencialidad de los sistemas.
  - Controles de mantenimiento y forma de respaldo de los sistemas.
  - Utilización de los sistemas.
  - Prevención de factores que pueda causar contingencias seguros y recuperación en caso de desastre.
  - Productividad

- Derechos de autor y secretos industriales.
- c) Evaluación del procesos de datos y de los equipos de cómputo que comprende:
- Controles de los datos fuente y manejos de cifras de control.
  - Control de operación.
  - Control de asignación de trabajo.
  - Control de medios de almacenamiento masivos.
  - Control de otro elemento de cómputo.
  - Control de medios de comunicación.
  - Orden en el centro de computo
- d) Seguridad:
- Seguridad física y lógica.
  - Confidencialidad
  - Respaldos.
  - Seguridad del personal
  - Seguros.
  - Seguridad en la utilización de los equipos.
  - Plan de contingencia y procedimientos de respaldo para casos de desastre.
  - Restauración de equipos y sistemas.

### **2.2.2.23.Objetivos de la auditoría informática**

Gallo (2010) señala como objetivos los siguientes:

- ❖ Evaluar los controles de la función informática
- ❖ Analizar la eficiencia de los sistemas informáticos
- ❖ Verificar el cumplimiento de las políticas y procedimientos de la empresa
- ❖ Revisar que los recursos materiales y humanos del área informática se utilicen eficientemente.

Echenique, (2001) los principales Objetivos de la auditoria informática son los siguientes:

- ❖ Salvaguardar los activos. Se refiere a la protección de hardware, software y recursos humanos.
- ❖ Integridad de datos. Los datos deben mantener consistencia y no duplicarse.
- ❖ Efectividad de sistemas. Los sistemas deben cumplir con los objetivos de la organización.
- ❖ Eficiencia de sistemas. Que se cumplan los objetivos con los menores recursos.
- ❖ Seguridad y confidencialidad.

#### 2.2.2.24. Tipos de Auditoría Informática.

Gráfico N° 4 Tipo de Auditoría Informática



Fuente: Elaboración propia con información Rodríguez (2009)

De acuerdo a Rodríguez (2009) se refiere a los tipos de Auditoría Informática:

- **Auditoría de la Gestión:** Referido a la contratación de bienes y servicios, documentación de los programas, etc.

- **Auditoría Legal del Reglamento de Protección de Datos:** Cumplimiento legal de las medidas de seguridad exigidas por el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos.
- **Auditoría de los Datos:** Clasificación de los datos, estudio de las aplicaciones y análisis de los flujogramas.
- **Auditoría de las Bases de Datos:** Controles de acceso, de actualización, de integridad y calidad de los datos. Esta auditoria se encarga de manera fundamental de la seguridad de la base de datos sus objetivos se encuentran :
  - ❖ Evitar el acceso externo.
  - ❖ Imposibilitar el acceso interno a los usuarios no autorizados.
  - ❖ Autorizar el acceso solo a los usuarios autorizados.
- **Auditoría de la Seguridad:** Referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.
- **Auditoría de la Seguridad Física:** Referido a la ubicación de la organización, evitando ubicaciones de riesgo, y en algunos casos no revelando la situación física de esta. También está referida a las protecciones externas (arcos de seguridad, CCTV, vigilantes, etc.) y protecciones del entorno.

La Seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc. Igualmente, a este ámbito pertenece la política de Seguros.

- **Auditoría de la Seguridad Lógica:** La seguridad lógica se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.

- **Auditoría de las Comunicaciones:** La creciente importancia de las Comunicaciones ha determinado que se estudien separadamente del ámbito de Técnica de Sistemas. Naturalmente, siguen siendo términos difíciles en los conceptos generales de Sistemas y de Arquitecturas de los Sistemas Informáticos. Se ha producido un cambio conceptual muy profundo en el tratamiento de las comunicaciones informáticas y en la construcción de los modernos Sistemas de Información, basados en Redes de Comunicaciones muy sofisticadas.
  
- **Auditoría de la Seguridad en Producción:** consiste en auditar un proceso concreto para obtener información precisa y real. La auditoría de la seguridad en producción significa planear organizar coordinar dirigir y controlar las actividades relacionadas a mantener y garantizar la integridad física de los recursos implicados en la función informática, así como el resguardo de los activos de la empresa.

#### **2.2.2.25. Controles**

Echenique, (2001) afirma que los datos son uno de los recursos más valiosos de las organizaciones, y, aunque son intangibles, necesitan ser controlados y auditados con los mismos cuidados que los demás inventarios de organización, por lo cual se debe tener presente:

- La responsabilidad de los datos es compartida conjuntamente por alguna función determinada de la organización y la dirección de la informática.
- Un problema que se debe considerar es el que se origina por la duplicidad de los datos, el cual consiste en poder determinar los propietarios o usuarios posibles (principalmente en casos de redes y banco de datos) y la responsabilidad de su actualización y consistencia.
- Se debe relacionar los elementos de los datos con las bases de datos donde están almacenados así como los reportes y grupos de procesos donde son generados.

En todo centro de informática se debe contar con una serie de políticas que permita la mejor operación de sistemas. Estas políticas son evaluadas durante el transcurso de la auditoría.

### **2.2.2.26. Control de datos fuente y manejo de cifras de control**

La mayoría de los delitos por computadora son cometidos por modificaciones de datos fuente al:

- Suprimir u omitir datos.
- Adicionar datos.
- Alterar datos.
- Duplicar procesos.

Esto es de suma importancia en caso de sistemas en línea, en los que los usuarios son los responsables de la captura y modificación de la información. Por ello, se debe tener un adecuado control, con señalamiento de responsables de los datos ( uno de los usuarios debe ser el único responsable de determinado dato ), con claves de acceso de acuerdo a niveles.

### **2.2.2.27. Control de Operación**

La eficiencia y el costo de la operación de un sistema de cómputo se ven fuertemente afectados por la calidad e integridad de la documentación requerida para el proceso en la computadora.

Debemos considerar la operación de los sistemas en línea, los cuales deben estar residentes en todo momento, con sus correspondientes sistemas de comunicación, mientras que en cuanto a los sistemas en lote (batch) se debe planear y programar su operación. Para lograr esto existen instalaciones que tienen equipos de computación y comunicación dedicados exclusivamente a los sistemas en línea.

Se debe verificar que el instructivo de información contenga los siguientes datos:

- Diagramas.
- Mensajes y su explicación.
- Parámetro y su explicación.
- Fórmulas de verificación.
- Observaciones e instrucciones en caso de error.

- Calendario de procesos y de entrega de resultados.

#### **2.2.2.28. Control de Asignación de Trabajo**

Esta parte se relaciona con la dirección de las operaciones de la computadora en términos de la eficiencia y la satisfacción de los usuarios. Esta sección debe ser comparada con la opinión del usuario. La función clave del personal de cargas de máquina está relacionada con el logro eficiente y efectivo de varios aspectos:

- Satisfacer las necesidades de tiempo del usuario.
- Ser compatible con los programas de recepción y transcripción de datos.
- Permitir niveles efectivos de utilización de los equipos y sistemas de operación.
- Volver la utilización de los equipos en línea.
- Entregar a tiempo y correctamente los procesos en lotes (batch).

La experiencia muestra que los mejores resultados se logran en organizaciones que utilizan sistemas formales de programación de actividades, los cuales intentan balancear los factores y medir resultados.

#### **2.2.2.29. Controles de Almacenamiento Masivo**

Los dispositivos de almacenamiento representan, para cualquier centro de cómputo archivos extremadamente importantes, cuya pérdida total o parcial podrían tener repercusiones muy serias no solo en la unidad en informática, sino en la dependencia en la cual se presta servicios.

Una dirección de informática bien administrada debe tener perfectamente protegidos en estos dispositivos de almacenamiento, de modo que sirva de base a los programas de limpieza (borrado de información), principalmente en el caso de las cintas.

Además, se debe tener perfectamente identificados físicamente los archivos para reducir la posibilidad de utilización errónea o destrucción de la información.

### **2.2.2.30. Control de Mantenimiento**

Existen básicamente tres tipos de control de mantenimiento. El contrato de mantenimiento total, que incluye el mantenimiento correctivo y preventivo el cual a su vez puede dividirse en aquel que incluye las partes del contrato y el que no las incluye. Este tipo de contrato es normalmente el más caro, pero se deja al proveedor la responsabilidad total del mantenimiento a excepción de daños por negligencia en la utilización de los equipos.

El segundo tipo de mantenimiento es por llamada el cual se llama al proveedor en caso de descompostura y este cobra de acuerdo a una tarifa y al tiempo que se requiera para componerla.

El tercer tipo de mantenimiento es el que se conoce como en banco, y es aquel en el cual el cliente lleva a las oficinas del proveedor el equipo, y este hace una cotización de acuerdo con el tiempo necesario para su compostura más las refacciones.

Al evaluar el mantenimiento debemos primero analizar cuál de los tres tipos es el que más nos conviene, y el segundo lugar pedir los contratos y analizar con detalle que las cláusulas estén perfectamente definidas que no existan subjetividad y que haya penalización en caso de incumplimiento, para evitar contratos que sean parciales hacia el proveedor.

### **2.2.2.31. Control Interno Informático**

**Piattini, Peso y Peso (2008)** indica que los controles internos que se utilizan en el entorno informático continúan evolucionando hoy en día a medida que los sistemas informáticos se vuelven complejos. Los progresos que se producen en la tecnología de soportes físicos y de software han modificado de manera significativa los procedimientos que se empleaban tradicionalmente para controlar los procesos de aplicaciones y para gestionar los sistemas de información.

Para asegurar la integridad, disponibilidad y eficacia de los sistemas se requieren complejos mecanismos de control, la mayoría de los cuales son automáticos. Resulta

interesante observar, sin embargo, que hasta en los sistemas servidor/cliente avanzados, aunque algunos controles son completamente automáticos, otros son completamente manuales, y muchos dependen de una combinación de elementos de software y procedimientos.

### **2.2.2.32. Clases de Control Interno Informático**

**Piattini, Peso y Peso (2008)** señala los siguientes tipos de control:

**Controles preventivos:** para tratar de evitar el hecho, como un software de seguridad que impida los accesos no autorizados al sistema.”

**Controles detectivos:** cuando fallan los preventivos para tratar de conocer cuanto antes el evento. Por ejemplo, el registro de intentos de accesos no autorizados, el registro de la actividad diaria para detectar errores u omisiones.”

**Controles correctivos:** facilitan la vuelta a la normalidad cuando se han producido incidencias. Por ejemplo, la recuperación de un fichero dañado a partir de las copias de seguridad.

### **2.2.2.33. Sistema de Control Interno Informático**

**Piattini, Peso y Peso (2008)** define como sistema de control interno:

Se puede definir el control interno como cualquier actividad o acción realizada manual o automáticamente para prevenir corregir errores o irregularidades que pueden afectar al funcionamiento de un sistema para conseguir sus objetivos.

Los controles cuando se diseñen, desarrollen e implanten han de ser al menos completos simples, fiables, revisables, adecuados y rentables. Respecto a este último habrá que analizar el coste riesgo de su implantación.

Los controles internos que se utilizan en el entorno informático continúan evolucionando hoy en día a medida que los sistemas informáticos se vuelven complejos los progresos que se producen en la tecnología de soportes físicos y de software han modificado de

manera significativa. Para asegurar la integridad disponibilidad y eficacia de los sistemas se requieren complejos mecanismos de control la mayoría de los cuales son automáticos. Implantación de un sistema de controles internos informáticos.

Los controles pueden implantarse a varios niveles diferentes. La evolución de los controles de la tecnología de la información exige analizar diversos elementos interdependientes. Por ello es importante llegar a conocer bien la configuración del sistema con el objeto de identificar los elementos, productos y herramientas que existen para saber dónde puedan implantarse los controles, así como para identificar posibles riesgos. Para llegar a conocer a configuración del sistema es necesario documentar los detalles de la red así como los distintos niveles de control y elementos relacionados:

Entorno de red: esquema de red, descripción de la configuración hardware de comunicaciones, descripción del software que se utiliza como acceso las telecomunicaciones, control de red, situación general de los ordenadores de entornos de base que soportan aplicaciones críticas y consideraciones relativas a la seguridad de la red.

Configuración del ordenador base: configuración del soporte físico entorno del sistema operativo, software con particiones, entornos, pruebas y real, bibliotecas de programa y conjunto de datos.

Entorno de aplicaciones: procesos de transacciones, sistema de gestión de base de datos y entornos de procesos distribuidos.

Productos y herramientas: software para desarrollo de programas software de gestión de bibliotecas y para operaciones automáticas.

Seguridad del ordenador base: identificar y verificar usuarios, control de acceso, registro e información, integridad del sistema, controles de supervisión.

Para la implantación de un sistema de controles internos informáticos habrá que definir:

Gestión de sistemas informáticos: políticas, pautas y normas técnicas que sirvan de base para el diseño y la implantación de los sistemas de información y de los controles correspondientes.

Administración de sistemas: controles sobre la actividad de los centros de datos y otras funciones de apoyo al sistema, incluyendo la administración de redes.

Seguridad: incluye las tres clases de controles fundamentales implantados en el software del sistema, integridad del sistema confidencialidad control de acceso y disponibilidad.

Gestión del cambio: separación de las pruebas y la producción a nivel de software y controles de procedimientos para la migración de programas de software aprobados y probados.

- Dirección de negocio o dirección de sistemas de información: han de definir la política y/o directrices para los sistemas de información en base a las exigencias del negocio, que podrán ser internas o externas.
- Dirección de informática: han de definir las normas de funcionamiento del entorno informático y de cada una de las funciones de informática mediante la creación y publicación de procedimientos, estándares metodología y normas aplicables a todas las áreas de informática así como a los usuarios que establezcan el marco de funcionamiento.
- Control interno informático: ha de definir los diferentes controles periódicos a realizar en cada una de las funciones informáticas, de acuerdo al nivel de riesgo de cada una de ellas y diseñarlos conforme a los objetivos de negocio y dentro del marco legal aplicable. Estos se plasmarán en los oportunos procedimientos de control interno y podrán ser preventivos o de detección.
- Auditor interno / externo Informático: ha de revisar los diferentes controles internos definidos en cada una de las funciones informáticas y el cumplimiento de normativa interna y externa de acuerdo al nivel de riesgo, conforme a los objetivos definidos por la Dirección de Negocio y la Dirección de Informática.

A continuación Piattini, Peso y Peso (2008) indican algunos controles internos:

### **1) Controles generales organizativos**

- ❖ Políticas: deberían de servir de base para la planificación, control y evaluación por la Dirección de las actividades del Departamento de Informática.
- ❖ Planificación:
  - Plan Estratégico de Información, realizado por los órganos de la Alta Dirección de la Empresa donde se definen los procesos corporativos y se considera el uso de las diversas tecnologías de información así como las amenazas y oportunidades de sus usos o de su ausencia.
  - Plan Informático, realizado por el Departamento de Informática, determina los caminos precisos para cubrir las necesidades de la Empresa plasmándolas en proyectos informáticos.
  - Plan General de Seguridad física y lógica, que garantice la confidencialidad, integridad y disponibilidad de la información.
  - Plan de emergencia ante desastres, garantice la disponibilidad de los sistemas ante eventos.
- ❖ Estándares: que regulen la adquisición de recursos, el diseño, desarrollo y modificación y explotación de sistemas.
- ❖ Procedimientos: que describan la forma y las responsabilidades de ejecutoria para regular las relaciones entre el Departamento de Informática y los Departamentos usuarios.
- ❖ Organizar el Departamento de Informática en un nivel suficientemente superior de estructura organizativa como para asegurar su independencia de los departamentos usuarios.
- ❖ Descripción de las funciones y responsabilidades dentro del Departamento con una clara separación de las mismas.
- ❖ Políticas de personal: selección, plan de formación, plan de vacaciones y evaluación y promoción.

- ❖ Asegurar que la Dirección revisa todos los informes de control y resuelve las excepciones que ocurran.
- ❖ Asegurar que exista una política de clasificación de la información para saber dentro de la Organización qué personas están autorizadas y a qué información.
- ❖ Designar oficialmente la figura de Control Interno Informático y de Auditoría Informática.

## **2) Controles de desarrollo, adquisición y mantenimiento de sistemas de información.**

Para que permitan alcanzar la eficacia del sistema, economía y eficiencia, integridad de los datos, protección de los recursos y cumplimiento con las leyes y regulaciones:

- ❖ Metodología del ciclo de vida del desarrollo de sistemas: su empleo podrá garantizar a la alta Dirección que se alcanzaran los objetivos definidos para el sistema:
  - La alta Dirección debe publicar una normativa sobre el uso de la metodología de ciclo de vida del desarrollo de sistemas y revisar esta periódicamente.
  - Plan de validación, verificación y pruebas.
  - Estándares de prueba de programas, prueba de sistemas.
  - Plan de conversión; prueba de aceptación final.
  - La contratación de programas de servicios de programación a medida ha de estar justificada mediante una petición escrita de un director de proyecto.
  - Deberán prepararse manuales de operación y mantenimiento como parte de todo proyecto de desarrollo o modificación de sistemas de información, así como manuales de usuario.

## **3) Controles de explotación de sistemas de informaron.**

- ❖ Planificación y Gestión de recursos: definir el presupuesto operativo del Departamento, Plan de adquisición de equipos y gestión de la capacidad de equipos.
- ❖ Controles para usar, de manera efectiva, los recursos en ordenadores.
- ❖ Procedimientos de selección del software del sistema, de instalación de mantenimiento de seguridad y control de cambios.
- ❖ Seguridad física y lógica:
- ❖ Definir un grupo de seguridad de la información siendo una de sus funciones la administración y gestión del software de seguridad, revisar periódicamente los informes de violaciones y actividad para identificar y resolver incidentes.
- ❖ Instalación de medidas de protección contra e fuego.
- ❖ Normas que regulen el acceso a los recursos informáticos.

#### **4) Controles en aplicaciones**

- ❖ Control de entrada de datos: procedimientos de conversión y de entrada validación y corrección e datos.
- ❖ Controles de tratamientos de datos para asegurar que no se dan de alta, modifican o borran no autorizados para garantizar la integridad de los mismos mediante procesos no autorizados.
- ❖ Controles de salida de datos: sobre el cuadro y reconciliación de salidas, procedimientos de distribución de salidas, de gestión d e errores en las salidas.

#### **5) Controles específicos de ciertas tecnologías**

- ❖ Controles en Sistema de Gestión de Bases de Datos:
- ❖ El software de gestión de base de datos para prever el accesos a la estructuración de y el control sobre los datos compartidos deberá instalarse y mantenerse de modo tal que asegure la integridad del software, las bases de datos y las instrucciones de control que definen el entorno.

- ❖ Controles sobre el acceso a datos y de ocurrencia.
- ❖ Controles en informática distribuida y redes:
  - Planes adecuados de implantación, conversión y pruebas de aceptación para la red.
  - Existencia de un grupo de control de red.
  - Procedimientos que definan las medidas y controles de seguridad a ser usados en la red de informática en conexión.
  - Considerar circuitos de conmutación que usen rutas alternativas para diferentes paquetes de información provenientes del mismo mensaje; esto ofrece una forma de seguridad en caso de que alguien intercepte los mensajes.
- ❖ Controles sobre ordenadores personales y redes de área local.
  - Políticas de adquisición y utilización.
  - Normativas y procedimientos de desarrollo y adquisición de software de aplicaciones.
  - Procedimientos de seguridad física y lógica.
  - Inventario actualizado de todas las aplicaciones de la Entidad.
  - Controles para evitar la introducción de un sistema operativo a través de disquete que pudiera vulnerar el sistema de seguridad establecido.

## **6) Controles de calidad**

- ❖ Existencia de un plan general de calidad basado en el plan de la entidad a largo plazo y el plan a largo plazo de tecnología. Este plan general de calidad debe promover la filosofía de mejora continua y debe dar respuestas a preguntas básicas de qué quién y cómo.
- ❖ Compatibilidad de la revisión de garantía de calidad con las normas y procedimientos habituales en las distintas funciones de Informática.
- ❖ Actualización de la metodología de desarrollo de sistemas respecto a Cambios Tecnológicos.
- ❖ Pruebas piloto o en paralelo: la metodología desarrollo de sistemas de la entidad debe definir las circunstancias bajo las cuales se efectuaran Pruebas Piloto o en Paralelo de programas o sistemas.

❖ Evaluación del cumplimiento de Garantía de Calidad de las Normas de Desarrollo.

#### 2.2.2.34. Tipos de Riesgos en Informática

**Piattini, Peso y Peso. ( 2008)** indica los siguientes tipos de riesgo:

**Riesgo en la continuidad del proceso:** son aquellos riesgos de situaciones que pudieran afectar a la realización del trabajo informático o incluso que pudieran llegar a paralizarlo, y, por ende, llegar a perjudicar gravemente a la empresa o incluso también a paralizarla.

**Riesgos en la eficacia del servicio informático:** se entiende como eficacia del servicio a la realización de los trabajos encomendados. Así pues, los riesgos en la eficacia serán aquellos que alteren dicha realización o que afecten a la exactitud de los resultados ofrecidos por el servicio informático.

**Riesgo en la eficiencia del servicio informático:** se entiende como eficiencia del servicio a la mejor forma de realizar los procesos o trabajos, ya sea a nivel económico o técnico, pretendiendo con el análisis de estos riesgos mejorar la calidad de servicio. Hay que matizar en este aspecto que determinados controles podría resultar una mejora considerable de la eficiencia del servicio pero igualmente podrían resultar económicamente poco rentables sobre todo para pequeñas empresas. La valoración de dichos controles deberá ser analizada por los responsables de la empresa en cuya mano estará la decisión de aplicación de los mismos.

**Riesgos económicos directos:** en cuanto a estos riesgos se analizarán aquellas posibilidades de desembolsos directos inadecuados, gastos varios que no deberían producirse, e incluso aquellos gastos derivados de acciones ilegales con o sin consentimiento de la empresa que pudieran transgredir la normativa de la empresa o las leyes vigentes.

**Riesgos de la seguridad lógica:** como riesgos en seguridad lógica se entiende a todos aquellos que posibiliten accesos no autorizados a la información mecanizada mediante técnicas informáticas o de otros tipos. Incluyendo aquellos inherentes a transmisiones,

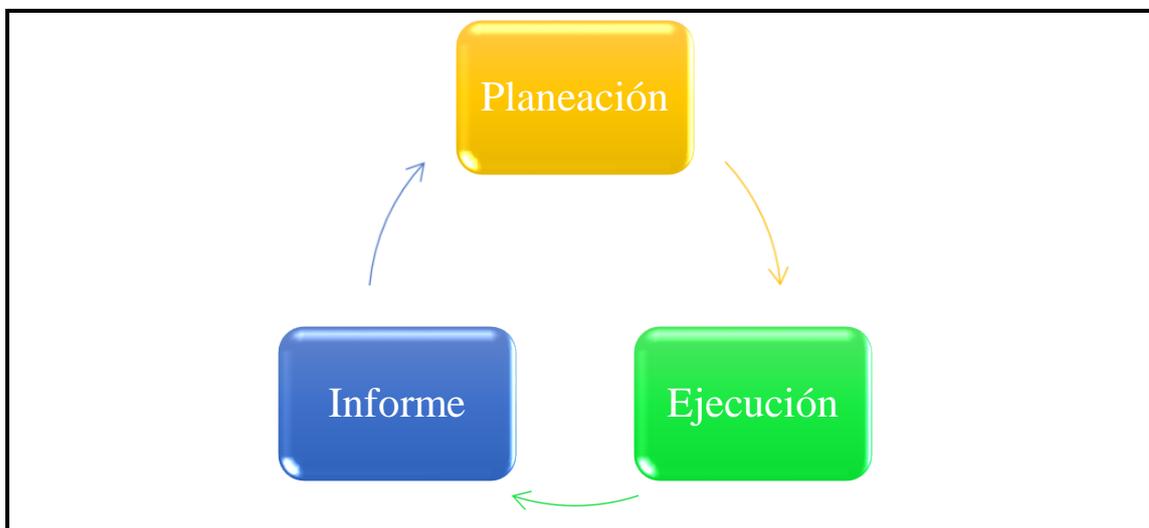
pese a que quizá en determinados ámbitos de aplicación podrían constituir un área independiente pero que se anexan con el fin de compactar el sistema de análisis.

**Riesgos de la seguridad física:** los riesgos en cuanto a seguridad física comprenderán todos aquellos que actúen sobre el deterioro o apropiación de elementos de información de una forma meramente física.

### 2.2.2.35. Fases de la Auditoría Informática

**Razo (2002)** manifiesta las siguientes fases:

Gráfico N° 5 Fases de la Auditoría Informática Razo (2002)



Fuente: Elaboración propia con información de Razo (2002)

#### Planeación

- ✓ Identificar el origen de la auditoría.
- ✓ Realizar una visita preliminar al área que será evaluada.
- ✓ Establecer los objetivos de la auditoría.
- ✓ Determinar los puntos que serán evaluados en la auditoría.
- ✓ Elaborar planes, programas y presupuestos para realizar la auditoría.
- ✓ Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoría.

- ✓ Contar los recursos y sistemas computacionales para la auditoría.

### **Ejecución**

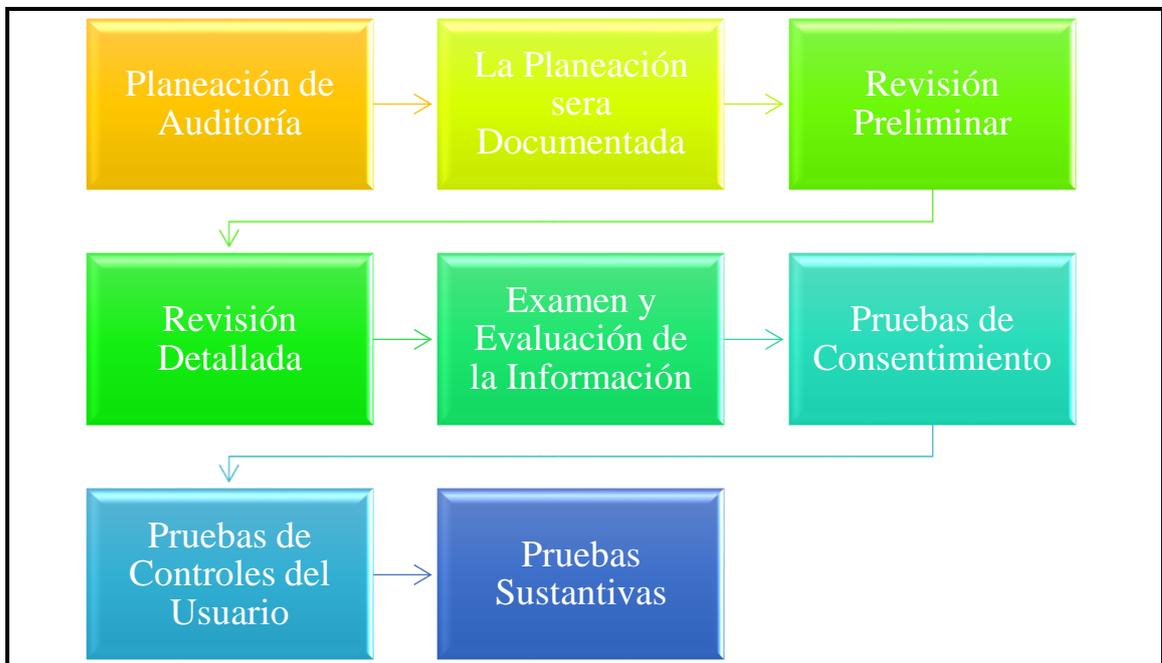
- ✓ Realizar las acciones programadas para la auditoría.
- ✓ Aplicar los instrumentos y herramientas para la auditoría.
- ✓ Identificar y elaborar los documentos de desviaciones encontradas.
- ✓ Elaborar el dictamen preliminar y presentarlo a discusión.
- ✓ Integrar el legajo de papeles de trabajo de la auditoría.

### **Informe.**

- ✓ Analizar la información y elaborar un informe de situaciones detectadas.
- ✓ Elaborar el dictamen final.
- ✓ Presentar el informe de auditoría.

**Echenique (2001)** manifiesta las siguientes fases:

Gráfico N° 6 Fases de la Auditoría Informática Echenique (2001)



**Fuente:** Elaboración propia con información de Echenique (2001).

La auditoría en informática es el proceso de recolección y evaluación de evidencias para determinar cuando son salvaguardados los activos de los sistemas computarizados, de qué manera se mantiene la integridad de los datos y como se logran los objetivos de la organización eficazmente y se usan los recursos consumidos eficientemente.

La auditoría informática sigue los objetivos tradicionales de la auditoría aquella que son de la auditoría externa, de salvaguarda de los activos y la integridad de datos, y los objetivos gerenciales, aquellos propios de la auditoría interna que no solo logran los objetivos señalados sino también los de eficiencia y eficacia.

#### **a). Planeación de la auditoría informática**

Para hacer una adecuada planeación de la auditoría en informática hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características del área dentro del organismo a auditar, sus sistemas, organización y equipo. Con ello podemos determinar el número y características del personal de auditoría las herramientas necesarias, el tiempo y costo, así como definir los alcances de la auditoría para, en caso necesario, poder elaborar el contrato de servicios.

#### **b). La planeación deberá ser documentada e incluirá:**

- El establecimiento de los objetivos y el alcance del trabajo
- La obtención de información de apoyo sobre las actividades que se auditarán.
- La determinación de los recursos necesarios para realizar la auditoría.
- La preparación por escrito del programa de auditoría.
- La determinación de cómo, cuándo y a quién se le comunicarán los resultados de la auditoría.
- La obtención de la aprobación del plan de trabajo de la auditoría.

En el caso de la auditoría informática, la planeación es fundamental pues habrá que hacerla desde el punto de vista de varios objetivos:

- Evaluación administrativa de la rea de procesos electrónicos.
- Evaluación de los sistemas y procedimientos.
- Evaluación de los equipos de cómputo.
- Evaluación del proceso de datos, de los sistemas y de los equipos de cómputo (software, hardware, redes, base de datos, comunicaciones)

- Seguridad y confidencialidad de la información.
- Aspectos legales de los sistemas y de la información.

Para lograr una adecuada planificación, lo primero que se requiere es obtener información general sobre la organización y sobre la función de informática a evaluar. Para ello es preciso hacer una investigación preliminar y algunas entrevistas previas, y con base en esto planear el programa de trabajo, el cual deberá incluir tiempos, costos, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la auditoría.

El proceso de planeación comprende el establecer:

- Metas
- Programas de trabajo de auditoría
- Planes de contratación de personal y presupuesto financiero.
- Informes de actividades.

### **c). Revisión preliminar**

El primer paso en el desarrollo de la auditoría, después de la planeación es la revisión preliminar del área de informática. El objetivo de la revisión preliminar es el de obtener la información necesaria para que el auditor pueda tomar la decisión de cómo proceder en la auditoría. Al terminar la revisión preliminar el auditor puede proceder en uno de los tres caminos siguientes:

- Diseño de la auditoría. Puede haber problemas debido a la falta de competencia técnica para realizar la auditoría.
- Realizar una revisión detallada de los controles internos de los sistemas con la esperanza de que se deposite la confianza en los controles de los sistemas.
- Decidir en no confiar en los controles internos del sistema. Existen dos razones posibles para esta decisión. Primero puede ser más eficiente desde el punto de vista de costo beneficio el realizar pruebas sustantivas directamente. Segundo, los controles del área de informática pueden duplicar los controles existentes en el área del usuario.

#### **d). Revisión detallada**

Los objetivos de la fase detallada son los de obtener la información necesaria para que el auditor tenga un profundo entendimiento de los controles usados dentro del área de informática.

El auditor debe decidir si debe de continuar elaborando pruebas de consentimiento, con la esperanza de obtener mayor confianza por medio del sistema de control interno, o proceder directamente a la revisión con los usuarios (pruebas compensatorias), o a las pruebas sustantivas. En algunos casos el auditor puede, después de hacer un análisis detallado, decidir que controles internos se tiene suficiente confianza y en otros casos que los procedimientos alternos de auditoría pueden ser más apropiadas.

En la fase de evaluación detallada es importante para el auditor identificar las causas de las perdidas existentes dentro de las instalaciones y los controles para reducir las pérdidas y los efectos causados por estos. Al terminar la revisión detallada el auditor debe evaluar en qué momento los controles establecidos reduce las pérdidas esperadas a un nivel aceptable. Los métodos de obtención de información al momento de la evaluación detallada son los mismos usados en la investigación preliminar, y lo único que difiere es la profundidad con que se obtiene la información y se evalúa.

#### **e). Examen y evaluación de la información.**

Los auditores internos deberán obtener, analizar, interpretar y documentar la información para apoyar los resultados de la auditoría.

El proceso de examen y evaluación de la información es el siguiente:

- Se debe obtener la información de todos los asuntos relacionados con los objetivos y alcance de la auditoría.
- La información deberá ser suficiente, competente, relevante y útil para que proporcione base sólida en relación con los hallazgos y recomendaciones de la auditoría. La información suficiente significa que está basada en hechos, que es adecuado y convincente, de tal manera que una persona prudente e informada puede llegar a las mismas conclusiones que el auditor. La información competente significa

que es confiable y puede obtenerse de la mejor manera, usando las técnicas de auditoría apropiadas. La información relevante apoya los hallazgos y recomendaciones de auditoría.

- Los procedimientos de auditoría, incluyendo el empleo de las técnicas de pruebas selectivas y el muestreo estadístico, deberán ser elegidos con anterioridad, cuando esta se a posible, y ampliarse o modificarse cuando las circunstancias lo requieran.
- El proceso de recabar, analizar, interpretar y documentar la información deberá supervisarse para proporcionar una seguridad razonable de que la objetividad del auditor se mantuvo y que las metas de auditoría se cumplieron.
- Los documentos de trabajo de la auditoría deberán ser preparados por los auditores y revisados por la gerencia de auditoría. Estos documentos deberán registrar la información obtenida y el análisis realizado, y deben apoyarlas bases de los hallazgos de auditoría y recomendaciones.

Los auditores internos realizaran el seguimiento de las recomendaciones para asegurarse que se tomaron las acciones apropiadas sobre el hallazgo.

El director de auditoría en informática deberá establecer un programa para seleccionar y desarrollar los recursos:

- Descripciones de puestos por cada nivel de auditoría en informática.
- Selección de individuos calificados y competentes.
- Entrenamiento y oportunidad de capacitación profesional continuo para todos y cada uno de los auditores.

#### **f). Pruebas de consentimiento**

El objetivo de la fase de prueba de consentimiento es el de determinar si los controles internos operan como fueron diseñados para operar. El auditor debe determinar si los controles declarados en realidad existen y si realmente trabajan confiablemente.

Además de las técnicas manuales de recolección de evidencia, muy frecuentemente el auditor debe recurrir a técnicas de recolección de información asistidas por computadora, para determinar la existencia y confiabilidad de los controles.

### **g). Pruebas de controles del usuario**

En algunos casos el auditor puede decidir el no confiar en los controles internos dentro de las instalaciones informáticas, porque el usuario ejerce controles que compensan cualquier debilidad dentro de los controles internos de informática. Estas pruebas que compensan las deficiencias de los controles internos se pueden realizar mediante cuestionarios entrevistas, vistas y evaluaciones hechas directamente por los usuarios.

### **h). Pruebas sustantivas**

El objetivo de la fase de pruebas sustantivas es obtener evidencia suficiente que permita al auditor emitir su juicio en las conclusiones acerca de cuándo pueden ocurrir pérdidas materiales durante el procesamiento de la información. El auditor externo expresará este juicio en forma de opinión sobre cuándo puede existir un proceso equivocado o falta de control de la información.

- Pruebas para identificar errores en el procesamiento o de falta de seguridad o confidencialidad.
- Pruebas para asegurar la calidad de los datos.
- Pruebas para identificar la inconsistencia de los datos.
- Pruebas para comparar con los datos o contadores físicos.
- Confirmación de datos con fuentes externas.
- Pruebas para confirmar la adecuada comunicación.
- Pruebas para determinar falta de seguridad.
- Pruebas para determinar problemas de legalidad.

### **2.2.2.36.Elementos Informáticos**

**Activos Informáticos** según Aguilera (2010) Son los recursos que pertenecen al propio sistema de información o que están relacionados con este. La presencia de los activos facilita el funcionamiento de la empresa u organización y la consecución de sus objetivos.

**Amenaza** según Aguilera (2010) Es la presencia de uno o más factores de diversa índole (personas, máquinas o sucesos) que de tener la oportunidad atacarían al sistema produciéndole daños aprovechando de su nivel de vulnerabilidad

**Auditor** dice Global (2007) El auditor es la persona calificada y autorizada para dirigir, planificar y actuar como interlocutor principal al informar de las desviaciones encontradas y evaluar las acciones correctivas.

**Auditoría** manifiesta Finkowsky (2013) Es un examen crítico que se realiza con el fin de asegurar la salvaguarda de los activos de los sistemas computacionales, mantener la integridad de los datos y lograr los objetivos de una organización en forma eficaz y eficiente

**Auditoría Informática** de acuerdo Gallo (2010) Es una serie de exámenes periódicos o esporádicos de un sistema informático cuya finalidad es analizar y evaluar la planificación, el control, la eficacia, la seguridad, la economía y la adecuación de la infraestructura informática de la empresa.

**Datos** define Aguilera (2010) Constituyen el núcleo de toda organización, hasta tal punto que se tiende a considerar que el resto de los activos están al servicio de la protección de los datos. Normalmente están organizados en bases de datos y almacenados en soportes de diferente tipo.

**Eficiencia** de acuerdo a Maldonado (2011) se refiere a la relación entre los insumos (recursos) consumidos y los productos obtenidos. La eficiencia aumenta a medida que se produce un mayor número de unidades de producto para una unidad dada de insumo. Sin embargo, la eficiencia de una operación se encuentra influenciada no sólo por la cantidad de producción sino también por la calidad y otras características del producto o servicio ofrecido.

**Eficacia** Maldonado (2011) Señala el grado en que son alcanzados, en forma continua, los objetivos de los programas y los efectos esperados de una entidad.

**Fortuito** según Aguilera (2010) Son errores cometidos accidentalmente por los usuarios, accidentes, cortes de fluido eléctrico, averías los sistemas, catástrofes naturales, etc.

**Fraudulento** sostiene Aguilera (2010) Como daños causados por software malicioso intrusos o por la mala voluntad de algún miembro del personal con acceso al sistema, robo o accidentes provocados.

**Hardware** asimismo Aguilera (2010) Se trata de los equipos (servidores y terminales) que contienen las aplicaciones y permiten su funcionamiento, a la vez que almacenan los datos del sistema de información.

**Información** dice Aguilera (2010) Es el conjunto de datos organizados que tienen un significado. La información puede estar contenida en cualquier tipo de soporte.

**Informática** según Ibanez (2009) La informática es la ciencia que se dedica al procesamiento automático de datos o información por medio de computadoras para una aplicación específica.

**Programa de trabajo** afirma Sotomayor (2008) Es el documento formal que utiliza el auditor como guía metodológica en la realización de sus labores; éste incluye el nombre y objetivo del programa, los procedimientos apropiados, así como la calendarización prevista y el personal involucrado.

**Papeles de trabajo** de acuerdo a Hurtado (2011) Es el registro del trabajo de auditoría realizado, y la evidencia que sirve de soporte a las debilidades encontradas y las conclusiones a las que ha llegado el auditor. Los papeles de trabajo se deben diseñar y organizar según las circunstancias y las necesidades del auditor.

**Recursos** según Aguilera (2010) Pueden ser físicos, como ordenadores, componentes, periféricos, y conexiones, recursos informáticos; y lógicos, como sistemas operativos y aplicaciones informáticas.

**Seguridad Informática** para Hurtado (2011) Es un conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información en un sistema informático e intentar reducir las amenazas que pueden afectar al mismo. Dentro de la seguridad informática se puede encontrar elementos y técnicas tanto hardware, como software, así como dispositivos físicos y medios humanos.

**Sistema Informático** según Aguilera (2010) Está constituido por un conjunto de elementos físicos (hardware, dispositivos, periféricos y conexiones), lógicos (sistemas operativos, aplicaciones, protocolos entre otros) y con frecuencia se incluyen también los elementos humanos (personal experto que maneja el software y el hardware).

**Software** afirma Aguilera (2010) Son los sistemas operativos y el conjunto de aplicaciones instaladas en los equipos de un sistema de información que reciben y gestionan o transforman los datos para darles el fin que se tenga establecido.

### **2.3. IDEA A DEFENDER**

La realización de una auditoría informática a la gestión de las (TIC) del Departamento de Sistemas de la Empresa IRCOSTEL CÍA. LTDA., en la ciudad de Riobamba período 2014, permitirá mejorar la seguridad y confiabilidad en el manejo de los recursos tecnológicos del sistema informático.

## CAPÍTULO III: MARCO METODOLÓGICO

### 3.1. MODALIDAD DE LA INVESTIGACIÓN

En la presente investigación se aplicará las modalidades:

**Cualitativa:** se utilizará entrevistas, técnicas de observación al personal del departamento de sistemas informáticos para evaluar el manejo de los recursos tecnológicos de información.

**Cuantitativa:** permitirá recoger o identificar antecedentes generales, números y cifras respecto al problema de investigación..

### 3.2. TIPOS DE INVESTIGACIÓN

**Descriptiva.-** Se detallarán las características que se identifiquen en los diferentes componentes, delimitados al trabajo de investigación.

**De Campo.-** Se obtendrá información concisa en la empresa Ircostel Cía. Ltda. con el fin de obtener un panorama de la unidad Informática.

**Bibliográfico.-** Se utilizará libros, tesis, para obtener información.

**Explicativa.-** Se explicará las diferentes causas y/o efectos de la inadecuada gestión de la unidad informática, en caso de serlo.

**Linkográfica:** páginas web. que tiene relación causal; no sólo persigue describir o acercarse a un problema, sino que intenta encontrar las causas del mismo. Existen diseños experimentales y no experimentales.

### 3.3. POBLACIÓN Y MUESTRA

La presente investigación se aplicará a toda la población por que no es necesario determinar la muestra, entre funcionarios de libre remoción, empleados y trabajadores.

DESCRIPCIÓN	N#
Representante de Toma	41
<b>TOTAL</b>	<b>41</b>

Muestra: 41

### 3.4.MÉTODOS, TÉCNICAS E INSTRUMENTOS

#### 3.4.1. Métodos

En la presente investigación se aplicará los siguientes métodos:

##### ➤ **Método Inductivo**

Es un proceso analítico – sintético mediante el cual se parte del estudio de hechos o fenómenos particulares para llegar al descubrimiento de un principio o ley general que los rige. Es aquel que de la observación de los hechos y casos particulares para llegar a ley general; en otras palabras, va de sus partes al todo.

##### ➤ **Método Deductivo**

El método deductivo sigue un proceso sintético – analítico, es decir contrario al anterior; se presenta conceptos, definiciones, leyes o normas generales, de las cuales se extraen conclusiones o consecuencias en las que se aplican; o se examinan casos particulares sobre las base de las afirmaciones generales presentadas. Es aquel que va de lo general a lo particular, del todo de las partes.

##### ➤ **Método Sintético:** Se podrá obtener información de la empresa para obtener las conclusiones de la auditoría.

#### 3.4.2. Técnicas

Las técnicas que se utilizarán en la investigación son las siguientes:

Las técnicas de auditoría más usuales para la recopilación de datos son: técnicas verbales, oculares, documentarias y físicas.

**Técnicas Verbales.-** Estas técnicas se subdividen en: indagación y encuestas.

- **Indagación:** Se obtendrá información por medio del contacto directo con el personal de la Empresa, mediante la realización de entrevistas que son el medio más idóneo para llevar a cabo el levantamiento de información.
- **Encuestas:** Se diseñará formularios específicos a todo el personal involucrado con la unidad Informática de la empresa Ircostel Cía. Ltda.

**Técnicas Oculares.-** Estas técnicas se subdividen en observación y comparación.

- **Observación directa.-** Se efectuara visitas a las instalaciones de la empresa Ircostel Cía. Ltda., con el objeto de obtener una apreciación directa de las actividades y registrar los datos observados, analizarlos e interpretarlos.

.

### **3.4.3. Instrumentos**

- **Cuestionarios.-** Se utilizará formulario impreso, destinado a obtener respuestas sobre el problema en estudio.
- **Cédula de Entrevista.-** Se diseña un documento para medir opiniones sobre eventos o hechos específicos.
- **Check list.-** Se realizará preguntas complementarias para el desarrollo de la investigación.

## CAPÍTULO IV: MARCO PROPOSITIVO

### 4.1. TÍTULO

“Auditoría Informática a la gestión de las Tic del Departamento de Sistemas de la Empresa Ircostel Cía. Ltda”

### 4.2. CONTENIDO DE LA PROPUESTA



#### 4.2.1. Archivo Permanente

## ARCHIVO PERMANENTE

<b>ENTIDAD:</b>	Empresa Ircostel Cía. Ltda.
<b>DIRECCIÓN:</b>	Primera Constituyente y Larrea
<b>NATURALEZA DEL TRABAJO:</b>	AUDITORÍA INFORMÁTICA
<b>PERÍODO:</b>	2014

**ÍNDICE**

**EMPRESA IRCOSTEL CÍA. LTDA**

**ARCHIVO PERMANENTE**

<b>ARCHIVO PERMANENTE</b>	<b>AP</b>
<b>INFORMACIÓN GENERAL</b>	<b>IG</b>
Reseña Histórica	<b>AP-IG</b>
Misión	<b>AP-IG</b>
Visión	<b>AP-IG</b>
Principios y Valores	<b>AP-IG</b>
Principales Funcionarios	<b>AP-IG</b>
Estructura Organizacional	<b>AP-IG</b>
Ubicación Geográfica	<b>AP-IG</b>
Logotipo	<b>AP-IG</b>
Productos y Servicios	<b>AP-IG</b>
Base Legal	<b>AP-IG</b>
Hoja de Marcas y Referencias	<b>AP-HMR</b>

<b>Elaborado por:</b> <a href="#">M.F.M.L</a>	<b>Fecha:</b> 10/04/2016
<b>Aprobado por:</b> <a href="#">O.E.R.C</a>	<b>Fecha:</b> 10/04/2016

## Antecedentes

La Empresa Ircostel Cía. Ltda., se constituye legalmente el 30 de octubre del 2009 mediante escritura pública otorgada ante el notario cuarto del Cantón Riobamba. Dr. Carlos Marcelo Aúlla Erazo, aprobada mediante resolución N° SC.DIC. A. 09. 00315 y legalmente inscrita en el Registro Mercantil el 06 de noviembre del 2009 bajo el número 1619, se encuentra ubicada en la provincia de Chimborazo, en la ciudad de Riobamba en las calles Primera Constituyente y Juan Larrea y está bajo el control de la Ley de Compañías, la finalidad de la empresa es la comercialización y servicio de la telefonía Claro a toda la ciudadanía.

Sus principales actividades comerciales son la venta al por mayor y menor de:

Chips, teléfonos, tarjetas, planes telefónicos, servicio de televisión satelital, servicio y atención al cliente. La empresa se encuentra actualmente entre las mejores a nivel de la ciudad, y es líder a nivel regional como distribuidora Claro, La empresa cuenta con una sucursal en Ambato, cuenta con asesores comerciales internos y externos en Machala, Latacunga y Riobamba los cuales cubren todos los cantones promocionando los diferentes productos.

## Misión

Mediante la comercialización y distribución de aparatos de comunicación telefónica, proporcionar a nuestros clientes productos y servicios de calidad, con una óptima satisfacción al consumidor, con estándares de responsabilidad, talento humano capacitado y comprometido a brindar un servicio rápido eficiente y personalizado.

## Visión

Ser una empresa líder a nivel de la zona centro, en la distribución y comercialización de productos y servicios de telecomunicación móvil, satisfaciendo a nuestros clientes y así llegar al crecimiento y fortalecimiento de la empresa con excelente calidad y eficiencia en el servicio.

Elaborado por: M.F.M.L	Fecha: 10/04/2016
Aprobado por: O.E.R.C	Fecha: 10/04/2016

**Valores**

- Liderazgo
- Creatividad
- Transparencia
- Servicio al Cliente
- Trabajo en Equipo

**Principales Funcionarios**

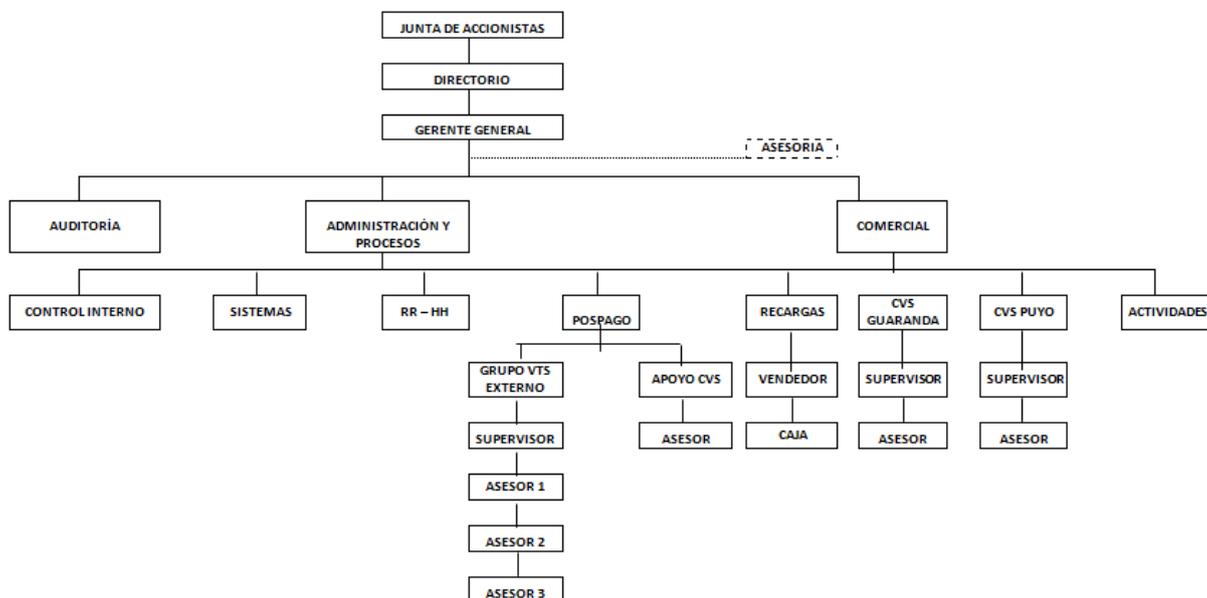
**Tabla N° 2 Principales Funcionarios**

NOMBRE	CARGO
Jorge Luis Calle	PRESIDENTE
Jorge Calle	GERENTE
Franco Costales	SUPÉRVISOR DE VENTAS
Verónica Quintana	RECURSOS HUMANOS
Hemilton Nolivos	TÉCNICO EN SISTEMAS

Elaborado por: M.F.M.L	Fecha: 10/04/2016
Aprobado por: O.E.R.C	Fecha: 10/04/2016

## Estructura Organizacional

Grafico N° 7 Estructura Organizacional



Fuente: Ircostel Cía. Ltda.

### Ubicación Geográfica

La Empresa Ircostel Cía. Ltda., se encuentra ubicado:

**Provincia:** Chimborazo

**Ciudad:** Riobamba

**Dirección:** Primera Constituyente y Larrea

**Teléfonos:** 032946966

**Página Web:** w.w.w.movilcentro.com.ec

<b>Elaborado por:</b> M.F.M.L	<b>Fecha:</b> 10/04/2016
<b>Aprobado por:</b> O.E.R.C	<b>Fecha:</b> 10/04/2016



## Productos y Servicios

AP-IG 5/6

- Venta directa de recargas telefonía Claro
- Chips
- Teléfonos
  - Samsung
  - Huawei
  - Alcatel
  - LG
  - Sony
  - Yezz
- Tarjetas
  - \$ 1
  - \$ 3
  - \$ 5
  - \$ 10
- Planes Telefónicos.
  - Mi Claro \$ 18
  - Mi Claro \$ 19
  - Mi Claro \$ 20
  - Mi Claro \$ 29
  - Mi Claro sin límite \$ 25
  - Mi Claro sin límite \$ 38
  - Mi Claro Tablet \$ 22
  - Mi Claro Tablet \$ 25
  - Mi Claro Tablet \$ 30
  - Mi Router \$ 25
  - Mi Netbook \$40
- Planes Línea Propia
  - Mi Claro \$ 15

- Mi Claro \$ 20
- Mi Claro \$ 25
- Mi Claro \$ 30
- Mi Claro \$ 35
- Televisión Satelital.
  - Mi Claro TV \$ 15
  - Mi Claro TV \$ 23
  - Mi Claro TV \$ 33
- Servicio y atención al cliente.
  - Pago de planes
  - Otorgamiento de planes
  - Garantías

### **Base Legal**

La Empresa Ircostel Cía. Ltda., se constituye legalmente el 30 de octubre del 2009 mediante escritura pública otorgada ante el notario cuarto del Cantón Riobamba. Dr. Carlos Marcelo Aúlla Erazo, aprobada mediante resolución N° SC.DIC. A. 09. 00315 y legalmente inscrita en el Registro Mercantil el 06 de noviembre del 2009 bajo el número 1619.

- La Constitución Política de la República del Ecuador
- Ley de Compañías.
- Ley Orgánica del Régimen Tributario Interno y su Reglamento.
- Reglamento de Comprobantes de Ventas, Retención y Documentos Complementarios.
- Código de trabajo.

Elaborado por: <a href="#">M.F.M.L</a>	Fecha: <a href="#">10/04/2016</a>
Aprobado por: <a href="#">O.E.R.C</a>	Fecha: <a href="#">10/04/2016</a>

## Hojas de Marcas y Referencias

## MARCAS

MARCAS	DESCRIPCIÓN
*	Hallazgo de Auditoría

## REFERENCIAS

ABREVIATURAS	SIGNIFICADO
<b>AC</b>	Archivo Corriente
<b>AP</b>	Archivo Permanente
<b>MFML</b>	Milton Fernando Morocho Lema
<b>RC</b>	Rocío Cando
<b>OE</b>	Oscar Espíndola
<b>CP</b>	Carta de Presentación
<b>CC</b>	Carta de Compromiso
<b>CPFA</b>	Carta de Presentación de la Firma Auditora
<b>CSP</b>	Contrato de Servicios Profesionales
<b>MP</b>	Memorando de Planificación
<b>CT</b>	Cronograma de Actividades
<b>PA</b>	Programas de auditoría

<b>CCI</b>	Cuestionarios Control Interno
<b>HA</b>	Hoja de Hallazgos
<b>IA</b>	Informe de Auditoría
<b>CHL</b>	Check List
<b>IG</b>	Indicadores de Gestión Informáticos

<b>Elaborado por:</b> M.F.M.L	<b>Fecha:</b> 10/04/2016
<b>Aprobado por:</b> O.E.R.C	<b>Fecha:</b> 10/04/2016

### 2.2.2. Archivo Corriente

<b>ENTIDAD:</b>	EMPRESA IRCOSTEL CÍA LTDA.
<b>DIRECCIÓN:</b>	Primera Constituyente y Larrea
<b>NATURALEZA DEL TRABAJO:</b>	AUDITORÍA INFORMÁTICA
<b>PERÍODO:</b>	2014

## ÍNDICE

### EMPRESA IRCOSTEL CIA. LTDA.

### ARCHIVO CORRIENTE

<b>ARCHIVO CORRIENTE</b>	<b>AC</b>
<b>FASE I PLANIFICACIÓN PRELIMINAR</b>	
Planificación de la Auditoría	<b>PA</b>
Carta de presentación	<b>CP</b>
Carta de compromiso	<b>CC</b>
Carta de presentación de la firma Auditora	<b>CPFA</b>
Contrato de Servicios Profesionales	<b>CSP</b>
Memorando de Planificación	<b>MP</b>
Cronograma de Actividades	<b>CT</b>

<b>FASE II EJECUCIÓN DE LA AUDITORÍA</b>	
Programa de Auditoría	<b>PA</b>
<b>FASE III COMUNICACIÓN DE RESULTADOS</b>	
Carta de Presentación	<b>CP</b>
Informe de Auditoría Informática	<b>II</b>

<b>Elaborado por:</b> M.F.M.L	<b>Fecha:</b> 11/04/2016
<b>Aprobado por:</b> O.E.R.C	<b>Fecha:</b> 11/04/2016

### **2.2.2.1.FASE I**

#### **Planificación Preliminar**

En la presente investigación se consideró la información generada durante el año 2014 de la empresa IRCOSTEL Cía. Ltda., Sus principales actividades comerciales son la venta al por mayor y menor de recargas y tarjetas electrónicas en establecimientos especializados, chips, teléfonos, tarjetas, planes telefónicos, servicio de televisión satelital, servicio y atención al cliente; obteniendo la información para la elaboración del programa de auditoría; cumpliendo con la evaluación del control interno, aplicación de indicadores, mediante la utilización del método COSO II.

#### **Conocimiento Preliminar.**

Este punto tuvo como propósito realizar una revisión y recopilación de la información, a través de la visita previa a la empresa permitirá identificar las actividades que se ejecutan, y determinar la pertinencia y oportunidad de realizar una acción de control.

La Auditoría de Sistemas Informáticos tiene como objetivo mejorar la seguridad y confiabilidad en el manejo de los recursos tecnológicos del sistema informático.

Para la realización de la auditoría de Sistemas Informáticos, se realizó el estudio previo de la información contenida en los archivos de la empresa Ircostel Cía. Ltda., que se incluyó en la Planificación Preliminar, que servirá para determinar las áreas críticas, los riesgos mediante la aplicación de los papeles de trabajo y la emisión del correspondiente informe de auditoría como un aporte para el mejoramiento de la toma de decisiones.

#### **Designación del Equipo de Trabajo.**

Para la ejecución de la Auditoría se contará con el apoyo de los administradores de la Empresa Ircostel Cía. Ltda., para la recopilación de la información suficiente y competente para el desarrollo del programa de auditoría; también se necesitará la colaboración de las personas responsables del departamento de sistemas con los conocimientos sobre el manejo del sistema informático quien será una ayuda idónea.

#### **Tiempo Utilizado.**

El presente examen de auditoría de Sistemas Informáticos se estimó hacerlo en un tiempo promedio de 30 días laborables, período considerado suficiente para analizar y evaluar los distintos procesos que se ejecutan en la Empresa Ircostel Cía. Ltda.

<b>Elaborado por:</b> M.F.M.L	<b>Fecha:</b> 11/04/2016
<b>Aprobado por:</b> O.E.R.C	<b>Fecha:</b> 11/04/2016

**Carta de presentación**

Riobamba, 11 de Abril del 2016

Señor Ing.  
Jorge Calle  
Gerente General  
Presente.-

De nuestra consideración:

Mediante la presente expresamos un atento un cordial saludo de quienes conformamos la Firma de Auditoría “MOROCHO AUDITORES INDEPENDIENTES” la misma que tiene como propósito confirmar lo convenido para llevar a cabo una Auditoría Informática a la empresa Ircostel Cía. Ltda., correspondiente al período 2014, con la finalidad de generar un informe la cual se fundamentará en las respectivas normas y reglamentos de auditoría que contengan conclusiones y recomendaciones que contribuyan al mejoramiento de la seguridad y confiabilidad en el manejo de los recursos tecnológicos del sistema informático de la entidad.

La responsabilidad estará a cargo de los Auditores, Dra. Rocío Cando como supervisor de la Auditoría y Milton Morocho como Sénior quienes realizarán el examen de acuerdo a las respectivas normas y reglamentos respectivos.

Por la atención a la presente, anticipo mi sincero agradecimiento.

Atentamente,



Milton Morocho  
(Auditor Independiente)

<b>Elaborado por:</b> M.F.M.L	<b>Fecha:</b> 11/04/2016
<b>Aprobado por:</b> O.E.R.C	<b>Fecha:</b> 11/04/2016

## Carta de compromiso

AC-CC 1/1

Riobamba, 11 de Abril del 2016

Señor Ing.  
Jorge Calle  
Gerente General  
Presente.-

De nuestra consideración:

Reciba un atento y cordial saludo queremos expresarle nuestro agradecimiento por la aceptación para realizar una Auditoría Informática a la entidad que acertadamente dirige.

Nuestro trabajo está enmarcado en las Normas Ecuatorianas de Auditoría (NEA) en las Normas de Auditoría Generalmente Aceptadas (NAGA), las que determinan que tipo de Auditoría será aplicada diseñada para obtener una certeza razonable sobre:

- El grado de cumplimiento de la seguridad y confiabilidad en el manejo de los recursos tecnológicos del sistema informático.

Por la atención a la presente, anticipo mi sincero agradecimiento y reitero mi compromiso para el cumplimiento del trabajo a cabalidad.

Atentamente,



Milton Morocho  
(Auditor Independiente)

Elaborado por: M.F.M.L	Fecha: 11/04/2016
Aprobado por: O.E.R.C	Fecha: 11/04/2016

## Carta de Autorización de la Firma de Auditoría

Riobamba, 11 de Abril del 2016

Señor Ing.  
Jorge Calle  
Gerente General  
Presente.-

De nuestra consideración:

Reciba un cordial saludo, quienes conformamos “MOROCHO AUDITORES INDEPENDIENTES”, agradeciéndole la oportunidad para la ejecución de la Auditoría Informática para la entidad del periodo que corresponde 2014.

Particular por la atención que concede del presente anticipamos nuestros más sinceros agradecimientos y reiteramos los sentimientos de alta consideración y estima.

Atentamente,



Milton Morocho  
(Auditor Independiente)

Elaborado por: M.F.L.M	Fecha: 11/04/2016
Aprobado por: O.E.R.C	Fecha: 11/04/2016

## Contrato de Servicios Profesionales

En la ciudad de Riobamba a los 11 días de mes de Abril del 2014, comparece a la celebración del presente contrato de presentación de servicios profesionales que celebran por una parte la Empresa Ircostel Cía. Ltda. A quién se lo denominara EL CLIENTE representado por el Ing. Jorge Calle Gerente General, y por la otra **MOROCHO AUDITORES INDEPENDIENTES**, representado por la Sr: Milton Fernando Morocho Lema al que en adelante se denominara “EL AUDITOR”.

### CLAUSULAS

**PRIMERA.- EL AUDITOR** declara que:

- a) Que tiene la capacidad jurídica para contratar y reúne todas las condiciones técnicas y económicas para obligarse a la prestación de servicios profesionales.
- b) Las partes celebraran el presente contrato que se consigna en las siguientes cláusulas:

**SEGUNDA.-** EL AUDITOR asume el costo de los recursos, físicos, humanos, técnicos y materiales que se presenten en desarrollo de Auditoría Informático debido que el mismo servirá para obtener el Título Profesional.

**TERCERA.-** “EL AUDITOR “se obliga a iniciar su trabajo, el día lunes 11 de Abril del año del 2016; el mismo que se realizará de manera eficaz y eficiente en el lapso de un mes.

**CUARTA.** “EL AUDITOR” conviene que no podrá divulgar por medio de publicaciones, informes, conferencia o cual quiera otra forma los datos y los resultados obtenidos de los trabajos sin la autorización por escrito del CLIENTE pues dicho datos y resultados son propiedad única y exclusivamente de este último.

**QUINTA.-** Para la interpretación y cumplimiento de este contrato así como todo aquello que nos este expresamente consignado en el mismo las partes se someten a la jurisdicción de los tribunales de la Provincia de Chimborazo renunciando al dominio que le pueda

corresponderles por razón de su domicilio presente, futuro o por cualquier otra causa los otorgantes firman y multiplican en las cláusulas precedentes y para constancia firman tres ejemplares de igual tenor.



**Señor Ing. Jorge Calle**  
**GERENTE IRCOSTEL CÍA. LTDA**



**Milton Morocho**  
**REPRESENTATE LEGAL DE LA FIRMA DE AUDITORÍA**

<b>Elaborado por:</b> M.F.M.L	<b>Fecha:</b> 11/04/2016
<b>Aprobado por:</b> O.E.R.C	<b>Fecha:</b> 11/04/2016

**Memorando de planificación**

Riobamba, 11 de Abril del 2016

**ENTIDAD:** Empresa Ircostel Cía. LTDA**NATURALEZA DEL TRABAJO:** Auditoría Informática**PERÍODO:** 2014**1. Antecedentes**

La Auditoría Informática en la Empresa Ircostel Cía. Ltda., se realizará por primera vez a cargo del equipo de “MOROCHO AUDITORES INDEPENDIENTES” quienes se han comprometido a ejecutar el trabajo con ética y responsabilidad para entregar un informe final que contribuya al mejoramiento del manejo de los recursos tecnológicos del sistema informático.

**2. Motivo de la auditoría**

La Auditoría Informática, será aplicada a toda la entidad para verificar el cumplimiento de la seguridad y confiabilidad en el manejo de los recursos tecnológicos del sistema informático, con el propósito de recomendar las falencias y corregir acciones detectadas.

**3. Objetivos de la auditoría****a) Objetivo General**

Efectuar una Auditoría Informática a la Empresa Ircostel Cía. Ltda., en el periodo 2014, que contribuya al mejoramiento y cumplimiento de la seguridad y confiabilidad en el manejo de los recursos tecnológicos del sistema informático.

**b) Objetivos Específicos**

- ❖ Elaborar el marco teórico que permita desarrollar la auditoría de sistemas informáticos.

<b>Elaborado por:</b> M.F.M.L	<b>Fecha:</b> 11/04/2016
<b>Aprobado por:</b> O.E.R.C	<b>Fecha:</b> 11/04/2016

- ❖ Obtener la información necesaria para la ejecución de la Auditoría Informática
- ❖ Evaluar el sistema de control interno a través de la normativa vigente con la aplicación del COSO II que contribuye al desarrollo del programa de Auditoría.
- ❖ Emitir un informe final que contenga conclusiones y recomendaciones para la toma de decisiones oportunas.

#### 4. Alcance

La Auditoría Informática se realizará a la Empresa Ircostel Cía. Ltda., del período a examinar comprende del 1 de enero al 31 de diciembre del 2014.

#### 5. Personal encargado

Cargo		Nombre
Supervisor	→	Dra. Rocío Cando
Auditor	→	Milton Morocho

#### 6. Tiempo Estimado

Tiempo estimado	Fecha de inicio	Fecha final
30 días	11/04/2016	11/05/2016

#### 7. Metodología a utilizar

- Entrevistas con las autoridades.
- Cuestionarios a los administrativos y personal involucrado.
- Observación directa.
- Obtención de evidencia documentaria.
- Se emitirá su informe respectivo.

Elaborado por: M.F.M.L	Fecha: 11/04/2016
Aprobado por: O.E.R.C	Fecha: 11/04/2016

## 8. Recursos Materiales para realizar la Auditoría Administrativa

**Tabla N° 3 Recursos Materiales**

<b>RECURSOS MATERIALES</b>	<b>COSTO</b>
250 Impresiones	\$ 85,00
Lápiz bicolor	\$ 2,00
3 CD'S	\$ 5,00
Servicio de Internet	\$ 60,00
<b>TOTAL</b>	<b>\$ 152,00</b>



Milton Morocho

(Auditor Independiente)

<b>Elaborado por:</b> M.F.M.L	<b>Fecha:</b> 11/04/2016
<b>Aprobado por:</b> O.E.R.C	<b>Fecha:</b> 11/04/2016

**Cronograma de Trabajo****ENTIDAD:** Empresa Ircostel Cía. Ltda.**NATURALEZA DEL TRABAJO:** Auditoría Informática**PERÍODO:** 2014**RESPONSABLE:** Milton Morocho**Tabla N° 4 Cronograma de Trabajo**

N°	ACTIVIDADES	Abril				Mayo			
		1	2	3	4	1	2	3	4
1	<b>FASE I</b> Planificación Preliminar y recopilación de información.								
2	<b>FASE II</b> Ejecución de la Auditoría Informática								
3	<b>FASE III</b> Informe de Auditoría								

Elaborado por: <b>M.F.M.L</b>	Fecha: <b>11/04/2016</b>
Aprobado por: <b>O.E.R.C</b>	Fecha: <b>11/04/2016</b>

**2.2.2.2.FASE II****EJECUCIÓN DE LA AUDITORÍA****Programa de Auditoría****ENTIDAD:** Empresa Ircostel Cía. Ltda.**NATURALEZA DEL TRABAJO:** Auditoría Informática**PERÍODO:** Año 2014**OBJETIVO GENERAL**

Realizar una evaluación a las actividades que realiza el Departamento de Sistemas mediante la aplicación de instrumentos investigativos que permita detectar el cumplimiento de la seguridad y confiabilidad en el manejo de los recursos tecnológicos del sistema informático.

**OBJETIVOS ESPECÍFICOS**

1. Examinar si está cumpliendo la seguridad y confiabilidad en el manejo de los recursos tecnológicos del sistema informático.
2. Formular conclusiones y recomendaciones para la toma de decisiones oportunas, cuya finalidad es el mejoramiento y cumplimiento de la seguridad y confiabilidad en el manejo de los recursos tecnológicos del sistema informático.

N°	PROCEDIMIENTOS	REF – PT	ELABORADO POR	FECHA
1	Efectúe una visita a las instalaciones de la empresa Ircostel Cía. Ltda.	VIC	M.F.M.L	13/04/2016
2	Realice una matriz de evaluación de medios internos y externos – FODA a la entidad.	MEF	M.F.M.L	13/04/2016

<b>Elaborado por:</b> M.F.M.L	<b>Fecha:</b> 13/04/2016
<b>Aprobado por:</b> O.E.R.C	<b>Fecha:</b> 13/04/2016

N°	PROCEDIMIENTOS	REF – PT	ELABORADO POR	FECHA
3	Realice una entrevista al responsable del Departamento de Sistemas.	EJS	M.F.M.L	13/04/2016
4	Realice un Check list al Departamento de Sistemas	CHL	M.F.M.L	13/04/2016
5	Realice la Matriz de Control de Áreas Críticas.	ARC	M.F.M.L	14/04/2016
3	Diseñe Indicadores de Gestión Informáticos	IG	M.F.M.L	14/04/2016
4	Efectúe una evaluación de Control Interno a través del método COSO II, mediante cuestionarios.	CCI	M.F.M.L.	15/04/2016
5	Elabore la Hoja de Hallazgos	HA	M.F.M.L	20/04/2016
6	Elabore el Informe de Auditoría	IA	M.F.M.L	24/04/2016

Elaborado por: M.F.M.L	Fecha: 13/04/2016
Aprobado por: O.E.R.C	Fecha: 13/04/2016

**Visita a las Instalaciones de la Empresa****EMPRESA IRCOSTEL CÍA. LTDA.  
ENTREVISTA INICIAL  
AUDITORÍA INFORMÁTICA****➤ DENOMINACIÓN**

Claro

**➤ DOMICILIO**

Primera Constituyente y Larrea

**➤ TELÉFONO**

032 942 797

**➤ HORARIO DE ATENCIÓN**

Mañana: 8h30 – 13h30

Tarde: 15h30 – 18h30

**➤ OBJETIVO PRINCIPAL DE LA ENTIDAD**

Obtener rentabilidad económica que permite la sostenibilidad y permanencia de la entidad en el tiempo.

Elaborado por: M.F.M.L	Fecha: 13/04/2016
Aprobado por: O.E.R.C	Fecha: 13/04/2016

**Matriz de Evaluación de Medios Internos y Externos FODA**

**EMPRESA IRCOSTEL CÍA. LTDA**  
**NATURALEZA DEL TRABAJO:** Auditoría Informática

**PERÍODO:** Año 2014

El análisis FODA es una herramienta que permitirá conocer y evaluar cuatro conceptos con respecto a la entidad dos internos, Fortalezas - Debilidades y dos externos, Oportunidades – Amenazas.

**MATRIZ FODA**

<b>ANÁLISIS INTERNO</b>	<b>FORTALEZAS:</b>	<b>OPORTUNIDADES:</b>	<b>ANÁLISIS EXTERNO</b>
	<ul style="list-style-type: none"> <li>➤ La comunicación es cordial entre los directivos y el personal.</li> <li>➤ Existe un buen ambiente laboral</li> <li>➤ Buen nivel de información y atención al cliente.</li> <li>➤ Incremento de ventas mensualmente, al cumplir con las metas.</li> <li>➤ Transporte propio.</li> <li>➤ Otorgación de Créditos.</li> </ul>	<ul style="list-style-type: none"> <li>➤ La empresa se encuentra en una ubicación geográfica favorable en el mercado.</li> <li>➤ Acceso a nuevas provincias del país.</li> <li>➤ Servicio de telefonía Internet en el sector rural.</li> <li>➤ Clientes potenciales.</li> <li>➤ Publicidad a través de redes sociales.</li> </ul>	

<b>Elaborado por:</b> M.F.M.L	<b>Fecha:</b> 13/04/2016
<b>Aprobado por:</b> O.E.R.C	<b>Fecha:</b> 13/04/2016

<b>ANÁLISIS INTERNO</b>	<b>DEBILIDADES:</b>	<b>AMENAZAS:</b>	<b>ANÁLISIS EXTERNO</b>
	<ul style="list-style-type: none"> <li>➤ No cuenta con Planificación Estratégica.</li> <li>➤ No cuenta con un Reglamento Interno.</li> <li>➤ Carece de un Manual de capacitación y adiestramiento.</li> <li>➤ No cuenta un Manual de Seguridad e Higiene.</li> <li>➤ No cuenta con un espacio físico adecuado.</li> <li>➤ El sistema informático contable no cumple con los requerimientos de la empresa.</li> </ul>	<ul style="list-style-type: none"> <li>➤ Precios menores de la competencia.</li> <li>➤ Alta competencia para la expansión de mercados.</li> <li>➤ Inestabilidad Laboral.</li> <li>➤ Falta de mantenimiento de los recursos de la empresa.</li> <li>➤ Riesgo en las Importaciones.</li> <li>➤ Tendencia continúa en la subida de precios.</li> </ul>	

**Fuente:** Investigación de Campo

**Elaborador por:** Milton Morocho

<b>Elaborado por:</b> M.F.M.L	<b>Fecha:</b> 13/04/2016
<b>Aprobado por:</b> O.E.R.C	<b>Fecha:</b> 13/04/2016

**AUDITORÍA INFORMÁTICA**

**MATRIZ PONDERACIÓN FACTORES INTERNOS**

En el análisis de la Matriz FODA, es importante ponderar y calificar cada uno de los factores internos, con el fin de conocer si la posición de Ircostel Cía. Ltda., es fuerte o débil.

La calificación de los medios internos se realizó en base a la siguiente escala:

1	Gran Debilidad
2	Debilidad
3	Equilibrio
4	Fortaleza
5	Gran Fortaleza

La ponderación se obtiene al asignar un valor (entre 1 y 5) a cada variable (fortalezas y debilidades) en función de su importancia.

<b>Elaborado por:</b> M.F.M.L	<b>Fecha:</b> 13/04/2016
<b>Aprobado por:</b> O.E.R.C	<b>Fecha:</b> 13/04/2016

**MATRIZ PONDERACIÓN FACTORES INTERNOS**

Factores Internos Claves		Ponderación	Calificación	Resultado Ponderado
F1	La comunicación es cordial entre los directivos y el personal.	0.15	5	0.76
F2	Un buen ambiente laboral.	0.12	4	0.48
F3	Buen nivel de información de la atención al cliente.	0.09	3	0.27
F4	Incremento de ventas mensualmente, al cumplir con las metas.	0.12	4	0.48
F5	Transporte propio.	0.12	4	0.48
F6	Otorgación de Créditos.	0.09	3	0.27
<b>Total Fortalezas</b>				<b>2.74</b>
D1	No cuenta con Planificación Estratégica.	0.03	1	0.03
D2	No cuenta con un Reglamento Interno.	0.06	2	0.12
D3	Carece de un Manual de capacitación y adiestramiento.	0.06	2	0.12
D4	No cuenta un Manual de Seguridad e Higiene.	0.06	2	0.12
D5	No cuenta con un espacio físico adecuado.	0.03	1	0.03
D6	El sistema informático contable no cumple con los requerimientos de la empresa.	0.03	1	0.03
<b>Total Debilidades</b>				<b>0.45</b>
<b>Total</b>		<b>1</b>	<b>33</b>	<b>3.19</b>

**Análisis.**

Luego de obtener el resultado ponderado de la matriz de evaluación de factores internos, se generó un resultado ponderado de 3,19 cifra que se encuentra arriba del punto de equilibrio el mismo que es de 2,50 por lo que se puede decir que la Empresa Ircostel Cía. Ltda., se encuentra estable.



**EMPRESA IRCOSTEL CÍA. LTDA.**

**MPFI 1/2**

**AUDITORÍA INFORMÁTICA**

**MATRIZ PONDERACIÓN FACTORES EXTERNOS**

En el análisis de la Matriz FODA, es importante ponderar y calificar cada uno de los factores externos, con el fin de conocer si la posición de Ircostel Cía. Ltda., es fuerte o débil.

La calificación de los medios externos se realizó en base a la siguiente escala:

1	<b>Gran Amenaza</b>
2	Amenaza
3	Equilibrio
4	Oportunidad
5	Gran Oportunidad

La ponderación se obtiene al asignar un valor (entre 1 y 5) a cada variable (oportunidades y amenazas) en función de su importancia.

<b>Elaborado por:</b> M.F.M.L	<b>Fecha:</b> 13/04/2016
<b>Aprobado por:</b> O.E.R.C	<b>Fecha:</b> 13/04/2016

### MATRIZ PONDERACIÓN FACTORES EXTERNOS

Factores Externa Claves		Ponderación	Calificación	Resultado Ponderado
O1	La empresa se encuentra en una situación geográfica favorable en el mercado.	0.16	5	0.81
O2	Acceso a nuevas provincias del país.	0.13	4	0.52
O3	Servicio de telefonía Internet en el sector rural.	0.10	3	0.29
O4	Clientes potenciales.	0.13	4	0.52
O5	Publicidad a través de redes sociales.	0.16	5	0.81
<b>Total Oportunidades</b>				<b>2.95</b>
A1	Precios menores al de la competencia.	0.06	2	0.13
A2	Crecimiento de la Competencia	0.03	1	0.03
A3	Inestabilidad Laboral.	0.06	2	0.13
A4	Falta de mantenimiento de los recursos de la empresa.	0.06	2	0.13
A5	Riesgo en las importaciones	0.03	1	0.03
A6	Tendencia continúa de subida de precios.	0.06	2	0.13
<b>Total Amenazas</b>				<b>0.58</b>
<b>Total</b>		<b>1</b>	<b>31</b>	<b>3.53</b>

#### Análisis.

El resultado de la ponderación de los medios externos (oportunidades y amenazas) es de 3.53; lo que indica que Ircostel Cía. Ltda., tiene más oportunidades que amenazas, lo que representa que las fuerzas externas son favorables para la empresa.

**Entrevista al Gerente General de la Empresa Ircostel Cía. Ltda.****Nombre del entrevistado:** Ing. Jorge Calle**Cargo:** Gerente General de la Empresa Ircostel Cía. Ltda.**Entrevistador:** Milton Morocho**Día previsto:** lunes 14 de abril del 2016**Hora solicitada:** 10h00 am**Lugar:** Oficina Gerente General de la empresa Ircostel Cía. Ltda.**Tiempo estimado:** 25 minutos**OBJETIVO DE LA ENTREVISTA**

Con el propósito de desarrollar el trabajo de investigación titulada AUDITORÍA INFORMÁTICA A LA GESTIÓN DE LAS TIC DEL DEPARTAMENTO DE SISTEMAS DE LA EMPRESA IRCOSTEL CÍA. LTDA. EN LA CIUDAD DE RIOBAMBA, PROVINCIA DE CHIMBORAZO EN EL PERIODO 2014, dígnese en contestar las preguntas citadas con la mayor veracidad posible.

**1. ¿La empresa tiene definido claramente los objetivos?**

La empresa si tiene objetivos definidos ya que se cumplen metas mensualmente.

**2. ¿La Empresa cuenta con una misión y visión?**

Si contamos con una misión y visión porque toda institución debe tener establecido la meta hacia donde se propone llegar.

**3. ¿Conoce usted que es una Auditoría Informática?**

Sí, tengo conocimiento que la Auditoría informática está directamente relacionada con los recursos tecnológicos e informáticos.

<b>Elaborado por:</b> M.F.M.L	<b>Fecha:</b> 13/04/2016
<b>Aprobado por:</b> O.E.R.C	<b>Fecha:</b> 13/04/2016

**4. ¿Está de acuerdo que se realice una Auditoría informática?**

Estoy de acuerdo que se realice este tipo de investigación, para saber si estoy utilizando adecuadamente los recursos tecnológicos e informáticos.

**5. ¿Cree usted que la Auditoria Informática en la institución contribuirá para la toma de decisiones oportunas?**

Sí, porque mediante esta investigación me ayudará a corregir las falencias encontradas y así lograr cumplir los objetivos institucionales con respecto al mejoramiento de os recursos tecnológicos del sistema informático.

**6. ¿Existe un organigrama estructural bien establecido?**

Si, contamos con un organigrama estructural en donde la organización de la empresa se detalla cada cargo que debe cumplir.

**7. ¿La empresa cuenta con un sistema informático eficiente?**

La empresa cuenta con el programa Zetalibra versión 2.3.50 para el registro adecuado y control de las operaciones diarias.

<b>Elaborado por:</b> M.F.M.L	<b>Fecha:</b> 13/04/2016
<b>Aprobado por:</b> O.E.R.C	<b>Fecha:</b> 13/04/2016

**Entrevista al responsable del Departamento de Sistemas de la Empresa Ircostel  
Cía. Ltda.**

**Nombre del entrevistado:** Ing. Hemilton Nolivos

**Cargo:** Jefe del Departamento de Sistemas.

**Entrevistador:** Milton Morocho

**Día previsto:** Lunes 14 de abril del 2016

**Hora solicitada:** 11h00 am

**Tiempo estimado:** 25 minutos

**OBJETIVO DE LA ENTREVISTA**

Con el propósito de desarrollar el trabajo de investigación titulada AUDITORÍA INFORMÁTICA A LA GESTIÓN DE LAS TIC DEL DEPARTAMENTO DE SISTEMAS DE LA EMPRESA IRCOSTEL CÍA. LTDA. EN LA CIUDAD DE RIOBAMBA, PROVINCIA DE CHIMBORAZO EN EL PERIODO 2014, dígnese en contestar las preguntas citadas con la mayor veracidad posible.

**1. ¿Se cumple las actividades del Departamento de Sistemas con eficiencia y eficacia?**

Si ( ) No (X )

**2. ¿El Departamento de Sistemas cuenta con una estructura adecuada para el desarrollo de las actividades?**

Si ( ) No (X )

**3. ¿El Departamento de Sistemas cuenta con políticas internas establecidas?**

Si ( ) No (X )

Elaborado por: M.F.M.L	Fecha: 13/04/2016
Aprobado por: O.E.R.C	Fecha: 13/04/2016

4. **¿Las funciones del Departamento de Sistemas se desarrolla mediante el control permanente del sistema informático?**

Si (X ) No ( )

5. **¿El Departamento de Sistemas cuenta con un número adecuado de empleados para el cumplimiento de sus funciones?**

Si (X ) No ( )

6. **¿El responsable del Departamento de Sistemas está capacitado para resolver problemas del sistema?**

Si (X ) No ( )

7. **¿Las claves de acceso al sistema informático se cambia con frecuencia?**

Si ( ) No ( X)

8. **¿Los empleados manejan la información de manera confidencial?**

Si ( X ) No ( )

9. **¿Con que frecuencia se realiza el manteniendo a los recursos tecnológicos?**

- Cada 15 días ( )
- Cada mes ( )
- Cada 3 meses ( )
- Cada año (X )

Elaborado por: M.F.M.L	Fecha: 13/04/2016
Aprobado por: O.E.R.C	Fecha: 13/04/2016

## **Análisis de la Evaluación al Departamento de Sistemas**

La Empresa Ircostel Cía. Ltda., no cuenta con políticas para la renovación de claves del sistema informático para evitar la malversación de la información por terceras personas, El Departamento de Sistemas no posee un espacio físico adecuado que permita el cumplimiento de las funciones, falta de mantenimiento periódicamente para evitar fallas en el sistema con la finalidad de salvaguardar los recursos tecnológicos, adicional no posee políticas internas establecidas en el Departamento de Sistemas.

**CHECK LIST**

CHECK LIST	CUMPLE		OBSERVACIONES
	SI	NO	
<b>RIESGO</b>			
Condiciones Ambientales		X	
Incendios accidentales, tormentas e inundaciones		X	
Amenazas ocasionadas por el hombre	X		
Sabotaje externo e interno	X		
<b>SEGURIDAD FÍSICA-HARDWARE</b>			
Alarmas de seguridad y guardianía	X		
Existe seguridad física a través de puertos USB	X		
Políticas de mantenimiento de hardware, correctivo y preventivo		X	
<b>SEGURIDAD LOGICA –SOFTWARE</b>			
Claves de acceso individual	X		
Sistemas biométricos		X	
Roles de Usuarios	X		
Antivirus	X		

Políticas para la renovación de claves.		X	
VPN o Red Privada Virtual	X		
Sistemas operativos cuenta con licencias originales.	X		
<b>INFRAESTRUTURA</b>			
Existe lugares de acceso restringido	X		
Las instalaciones del Departamento de Sistemas son óptimas para el funcionamiento correcto de las actividades.		X	
Existe sistemas de emergencia		X	
<b>SISTEMA INFORMÁTICO</b>			
Sistema Informático que poseen actualmente cuenta con soporte	X		
En caso que existiera nuevos requerimientos el sistema es flexible.	X		
Existe backup (respaldo de información)	X		

Fuente: Elaboración propia con información del Departamento de Sistemas de Ircostel Cía. Ltda.

Elaborado por: <b>M.F.M.L</b>	Fecha: <b>13/04/2016</b>
Aprobado por: <b>O.E.R.C</b>	Fecha: <b>13/04/2016</b>

**Indicadores de Gestión de los Recursos Tecnológicos de la Información**

Actividad	Nombre del Indicador	Unidad de Medida	Fórmula	Frecuencia	Interpretación	Brecha	Análisis
Costo	Gasto Total del Sistema	%	Gasto del Sistema informático /Gasto Total de la Empresa	Anual	\$360.000/\$8900	3%	El total de los gastos anuales de la empresa, solo el 3% se estima para el sistema informático.
	Costo de la actualización del sistema informático	%	Costo de actualización del software/Costo total del Sistema Informático	Anual	\$400/\$8900	4%	El 4% del costo total del sistema representa la inversión de la actualización del software
	Costo del Sistema Informático por el número de máquinas existentes	\$	Costo Total de Sistema / El Número de Máquinas	Anual	\$8900/30	\$297.67	El costo individual por máquina del sistema informático es de \$297,67
	Costo Total de las Licencias	\$	Costo Total Licencias * Total de Maquinas	Anual	\$40*30	\$1200	El costo total de la licencia de antivirus Nod es de \$ 1200
	Costo Total del Sistema Informático	\$	Total Costo del Sistema + Fibra Óptica+mantenimiento+actualización	Anual	\$2500+\$4800+\$1200+\$400	\$8900	El costos total del sistema informático es de \$8900

Infraestructura	Número Total de Maquinas	#	Número de Maquinas / Número de Empleados	Anual	30/44	1	El número promedio de máquina por empleado es de 1
	Número de Impresoras por Departamento	#	Número de Impresoras / Número de Departamentos	Anual	21/7	3	El número estimado por departamento es de 3 impresoras.
Atención al cliente	Tiempo de Demora en la Atención al Cliente	Tiempo	Tiempo Aproximado / Tiempo Real	Diario	10/16	63%	El tiempo real es de 16 minutos lo cual representa el 63% de demora en la atención de los clientes
Seguridad	Incidencias Atendidas	Unidad	Incidencias atendidas/ Número de incidencias	Mensual	60/80	75%	Las incidencias atendidas en la empresa es del 75%

**Fuente:** Elaboración propia con información del Departamento de Sistemas de Ircostel Cía. Ltda.

<b>Elaborado por:</b> M.F.M.L	<b>Fecha:</b> 14/04/2016
<b>Aprobado por:</b> O.E.R.C	<b>Fecha:</b> 14/04/2016

## Matriz de Control de Áreas Críticas

### COSO II



**ARC1/5**

**ÁREAS CRÍTICAS**

<b>ORGANIZACIÓN AUDITADA</b>	<b>IRCOSTEL CÍA. LTDA.</b>
<b>Área</b>	<b>Riesgo</b>
<b>Prioridad</b>	<b>Descripción</b>
1	La Empresa Ircostel Cía. Ltda., no cuenta con un Manual de seguridad e higiene que dirija al cumplimiento de metas u objetivos.
2	La Empresa no está apta para afrontar condiciones ambientales, que pongan en riesgo sus recursos tecnológicos.

Fuente: Elaboración propia con información Ircostel Cía. Ltda.

Elaborado por: <a href="#">M.F.M.L</a>	Fecha: <a href="#">14/04/2016</a>
Aprobado por: <a href="#">O.E.R.C</a>	Fecha: <a href="#">14/04/2016</a>

**ÁREAS CRÍTICAS**

<b>ORGANIZACIÓN AUDITADA</b>	<b>IRCOSTEL CÍA. LTDA.</b>
<b>Área</b>	<b>Seguridad Física y Hardware</b>
<b>Prioridad</b>	<b>Descripción</b>
1	La empresa Ircostel Cía. Ltda. no realiza periódicamente mantenimiento a los recursos lo que provoca amenazas en el buen funcionamiento de sus equipos.

**Fuente:** Elaboración propia con información Ircostel Cía. Ltda.

<b>Elaborado por:</b> M.F.M.L	<b>Fecha:</b> 14/04/2016
<b>Aprobado por:</b> O.E.R.C	<b>Fecha:</b> 14/04/2016

**AREAS CRÍTICAS**

<b>ORGANIZACIÓN AUDITADA</b>	<b>IRCOSTEL CÍA. LTDA.</b>
<b>Área</b>	<b>Seguridad Lógica y Software</b>
<b>Prioridad</b>	<b>Descripción</b>
1	<p>Ircostel CÍA. Ltda. cuenta con seguridad lógica, pero es necesario implementar algunas medidas de seguridad tales como:</p> <ol style="list-style-type: none"> <li>1. Sistemas Biométricos.</li> <li>2. Políticas para la renovación de claves.</li> <li>3. Utilizar soporte externo de datos</li> </ol>

**Fuente:** Elaboración propia con información Ircostel Cía. Ltda.

<b>Elaborado por:</b> M.F.M.L	<b>Fecha:</b> 14/04/2016
<b>Aprobado por:</b> O.E.R.C	<b>Fecha:</b> 14/04/2016



**ARC 4/5**

**ÁREAS CRÍTICAS**

<b>ORGANIZACIÓN AUDITADA</b>	<b>IRCOSTEL CÍA. LTDA.</b>
<b>Área</b>	<b>Infraestructura</b>
<b>Prioridad</b>	<b>Descripción</b>
1	El Departamento de Sistemas no cuenta con instalaciones adecuadas para el funcionamiento de las actividades.
2	No cuenta con un Plan de Contingencia para contrarrestar riesgos internos y externos.

Fuente: Elaboración propia con información Ircostel Cía. Ltda.

<b>Elaborado por:</b> M.F.M.L	<b>Fecha:</b> 14/04/2016
<b>Aprobado por:</b> O.E.R.C	<b>Fecha:</b> 14/04/2016



ARC 5/5

**ÁREAS CRÍTICAS**

<b>ORGANIZACIÓN AUDITADA</b>	<b>IRCOSTEL CÍA. LTDA.</b>
<b>Área</b>	<b>Sistema Informático</b>
<b>Prioridad</b>	<b>Descripción</b>
1	Zeta libre versión 2.3.50 no cumple con los requerimientos de la empresa.

Fuente: Elaboración propia con información Ircostel Cía. Ltda.

<b>Elaborado por:</b> M.F.M.L	<b>Fecha:</b> 14/04/2016
<b>Aprobado por:</b> O.E.R.C	<b>Fecha:</b> 14/04/2016

Entidad:	EMPRESA IRCOSTEL CÍA. LTDA.				
Área Evaluada:	Toda la Empresa				
Tipo de Auditoría:	Auditoría Informática				
Componente:	Ambiente de Control				
Alcance:	Todos los Departamentos de la Empresa				
N.-	PREGUNTAS	RESPUESTAS			OBSERVACIÓN
		SI	NO	N.A	
1	¿Cuenta con un Código de Ética?		41		Diseñar un código de ética para las empresa *
2	¿Dispone de un Organigrama Estructural?	41			
3	¿La empresa fomenta los valores éticos y la conducta moral?	31	10		
3	¿Cuenta con políticas de desempeño?	41			
5	¿Las funciones y responsabilidades de los directivos es eficiente?	39	2		
6	¿Se evalúa al personal que trabaja en la empresa?	35	6		
7	¿El personal que trabaja en la empresa es contratado mediante concurso o pruebas?	8	33		
8	¿El personal que trabaja en la empresa tiene el perfil idóneo al cargo que desempeña?	20	21		
9	¿Cuenta con un manual de capacitación y adiestramiento informático para sus empleados?		41		
	Total	215	154		

Elaborado por: M.F.M.L	Fecha: 15/04/2016
Aprobado por: O.E.R.C	Fecha: 15/04/2016

**Donde;**

NC= Nivel de Confianza

CP= Ponderación total

CT= Calificación total

**CCI 2/17**

**COMP 1**

$$\text{Fórmula: } CF = \frac{CP}{CT} * 100$$

$$\text{NIVEL CONFIANZA} = \frac{215}{369} * 100$$

NIVEL DE CONFIANZA = **58%**

NIVEL DE RIESGO= **42%**

### **CRITERIO**

NIVEL DE CONFIANZA		
BAJO	MODERADO	ALTO
15% - 50%	51 - 75%	76% - 95%
NIVEL DE RIESGO		
ALTO	MODERADO	BAJO
85% - 50%	49% - 25%	24% - 5%

### **Análisis**

El componente Ambiente de Control se puede evidenciar a través de la aplicación del cuestionario del Control Interno con un Nivel de Confianza Moderado del 58% y un Nivel de Riesgo Moderado del 42%, lo que señala que la Empresa Ircostel Cía. Ltda. se encuentra equilibrada.

Elaborado por: <b>M.F.M.L</b>	Fecha: <b>15/04/2016</b>
Aprobado por: <b>O.E.R.C</b>	Fecha: <b>15/04/2016</b>

Entidad:	EMPRESA IRCOSTEL CÍA. LTDA.				
Área Evaluada:	Toda la Empresa				
Tipo de Auditoría:	Auditoría Informática				
Componente:	Establecimiento de Objetivos				
Alcance:	Todos los Departamentos de la Empresa				
N.-	PREGUNTAS	RESPUESTAS			OBSERVACIÓN
		SI	NO	N.A	
10	¿La empresa cuenta con indicadores de eficiencia y eficacia (Informáticos)?		41		Implementar Indicadores Informáticos.*
11	¿Los objetivos son claros y concisos?	30	11		
12	¿Las actividades que desempeñan están acorde con los objetivos establecidos?	36	5		
13	¿Los objetivos institucionales son informados al personal?	6	35		
14	¿Los objetivos son rediseñados anualmente?	35	6		
15	¿Dentro de los objetivos institucionales se ha considerado salvaguardar los recursos tecnológicos de la información?	35	6		
16	¿Los objetivos se cumplen corto plazo?	39	2		
17	¿Existen riesgos para el cumplimiento de los objetivos?	35	6		
	Total	216	112		

Elaborado por: M.F.M.L	Fecha: 15/04/2016
Aprobado por: O.E.R.C	Fecha: 15/04/2016

**Donde;**

**CCI 4/17**

NC= Nivel de Confianza

CP= Ponderación total

CT= Calificación total

**COMP 2**

$$\text{Fórmula: } CF = \frac{CP}{CT} * 100$$

$$\text{NIVEL CONFIANZA} = \frac{216}{328} * 100$$

NIVEL DE CONFIANZA = **66%**

NIVEL DE RIESGO= **44%**

### **CRITERIO**

NIVEL DE CONFIANZA		
BAJO	MODERADO	ALTO
15% - 50%	51 - 75%	76% - 95%
NIVEL DE RIESGO		
ALTO	MODERADO	BAJO
85% - 50%	49% - 25%	24% - 5%

### **Análisis**

El componente analizado Establecimiento de Objetivos refleja que la Empresa Ircostel Cía. Ltda. se encuentra en un nivel de confianza y riesgo moderado, debido al cumplimiento de los objetivos a mediano y corto plazo.

<b>Elaborado por:</b> M.F.M.L	<b>Fecha:</b> 15/04/2016
<b>Aprobado por:</b> O.E.R.C	<b>Fecha:</b> 15/04/2016



CUESTIONARIO DE CONTROL INTERNO

**C.C.I 5/17  
Comp.3**

Entidad:	EMPRES IRCOSTEL CÍA. LTDA.				
Área Evaluada:	Toda la empresa				
Tipo de Auditoría:	Auditoría Informática				
Componente:	Identificación de Eventos				
Alcance:	Todos los Departamentos de la Empresa				
N.-	PREGUNTAS	RESPUESTAS			OBSERVACIÓN
		SI	NO	N.A	
18	¿Los riesgos que se presentan son resueltos inmediatamente?	34	7		
19	¿Identificado el riesgo se corrige de acuerdo al impacto o categorización que provoca?	35	6		
20	¿Los riesgos se categorizan de acuerdo a su importancia?	6	35		
21	¿Los riesgos externos e internos se encuentran debidamente identificados a los recursos tecnológicos?	6	35		
22	¿Los riesgos existentes provoca el incumplimiento de los objetivos?	20	21		
23	¿Se identifica todos los riesgos posibles que la empresa puede enfrentarse?	11	30		
24	¿Existen acciones correctivas oportunas para dar solución al riesgo?	35	6		
25	¿La empresa cuenta con apoyo gerencial para la identificación de eventos?	32	9		
	Total	179	149		

Elaborado por: M.F.M.L	Fecha: 15/04/2016
Aprobado por: O.E.R.C	Fecha: 15/04/2016

**Donde;**

NC= Nivel de Confianza

CP= Ponderación total

CT= Calificación total

$$\text{Fórmula: } CF = \frac{CP}{CT} * 100$$

$$\text{NIVEL CONFIANZA} = \frac{179}{328} * 100$$

NIVEL DE CONFIANZA = **54%**

NIVEL DE RIESGO= **46%**

### CRITERIO

NIVEL DE CONFIANZA		
BAJO	MODERADO	ALTO
15% - 50%	51 - 75%	76% - 95%
NIVEL DE RIESGO		
ALTO	MODERADO	BAJO
85% - 50%	49% - 25%	24% - 5%

### Análisis

El componente Identificación de Eventos tiene un nivel de confianza y riesgo moderado, debido que la Empresa tiene identificado los riesgos a los que están expuestos.

Elaborado por: <a href="#">M.F.M.L</a>	Fecha: <a href="#">15/04/2016</a>
Aprobado por: <a href="#">O.E.R.C</a>	Fecha: <a href="#">15/04/2016</a>

Entidad:	EMPRESA IRCOSTEL CÍA. LTDA.				
Área Evaluada:	Departamento Ejecutivo, Administrativo y Sistemas.				
Tipo de Auditoría:	Auditoría Informática				
Componente:	Evaluación de Riesgos				
Alcance:	Área Ejecutiva, Administrativa, Sistemas				
N.-	PREGUNTAS	RESPUESTAS			OBSERVACIÓN
		SI	NO	N.A	
26	¿Se ha identificado riesgos continuos en los recursos tecnológicos de la empresa?	2	1		
27	¿Se ha considerado el grado de daño que ocasiona dicho riesgo?	2	1		
28	¿Existe procedimientos para evaluar los riesgos?	2	1		
29	¿Existe controles que permiten medir los cambios?	2	1		
30	¿El personal está capacitado para enfrentar los posibles riesgos que se presentan?	1	2		
31	¿Se considera importante el impacto que genera el riesgo a la empresa?	2	1		
32	¿Cree usted que los riesgos identificados pueden afectar al cumplimiento de los objetivos institucionales?	2	1		
	Total	13	8		

Elaborado por: M.F.M.L	Fecha: 15/04/2016
Aprobado por: O.E.R.C	Fecha: 15/04/2016

**Donde;**

NC= Nivel de Confianza

CP= Ponderación total

CT= Calificación total

**CCI 8/17**

**COMP 4**

$$\text{Fórmula: } CF = \frac{CP}{CT} * 100$$

$$\text{NIVEL CONFIANZA} = \frac{13}{21} * 100$$

NIVEL DE CONFIANZA = **62%**

NIVEL DE RIESGO= **38%**

### **CRITERIO**

NIVEL DE CONFIANZA		
BAJO	MODERADO	ALTO
15% - 50%	51 - 75%	76% - 95%
NIVEL DE RIESGO		
ALTO	MODERADO	BAJO
85% - 50%	49% - 25%	24% - 5%

### **Análisis**

El componente identificado Evaluación de Riesgos, se puede evidenciar un Nivel de Confianza Moderado del 62% y un Nivel de Riesgo Moderado del 38%, debido a que la Empresa se encuentra en un punto de equilibrio con respecto a los riesgos.

Elaborado por: <b>M.F.M.L</b>	Fecha: <b>15/04/2016</b>
Aprobado por: <b>O.E.R.C</b>	Fecha: <b>15/04/2016</b>

Entidad:	EMPRESA IRCOSTEL CÍA. LTDA.				
Área Evaluada:	Departamento Ejecutivo, Administrativo y Sistemas.				
Tipo de Auditoría:	Auditoría Informática				
Componente:	Respuesta a los riesgos				
Alcance:	Área Ejecutiva, Administrativa, Sistemas				
N.-	PREGUNTAS	RESPUESTAS			OBSERVACIÓN
		SI	NO	N.A	
33	¿Existen medidas correctivas ante los riesgos encontrados?	2	1		
34	¿Los recursos tecnológicos son de suma importancia para la prevención de riesgos?	2	1		
35	¿Ante las posibles pérdidas de información existen medidas de precaución?	2	1		
36	¿Cuentan con un plan de contingencia para contrarrestar los riesgos?		3		Implementar una matriz de riesgo. *
37	¿Existen herramientas que apoyen las decisiones tomadas para contrarrestar los riesgos?	2	1		
	Total	8	7		

Elaborado por: M.F.M.L	Fecha: 15/04/2016
Aprobado por: O.E.R.C	Fecha: 15/04/2016

**Donde;**

**CCI 10/17**

**COMP 5**

NC= Nivel de Confianza

CP= Ponderación total

CT= Calificación total

$$\text{Fórmula: } CF = \frac{CP}{CT} * 100$$

$$\text{NIVEL CONFIANZA} = \frac{8}{15} * 100$$

NIVEL DE CONFIANZA = **53%**

NIVEL DE RIESGO= **46%**

### **CRITERIO**

NIVEL DE CONFIANZA		
BAJO	MODERADO	ALTO
15% - 50%	51 - 75%	76% - 95%
NIVEL DE RIESGO		
ALTO	MODERADO	BAJO
85% - 50%	49% - 25%	24% - 5%

### **Análisis**

La Empresa Ircostel Cía Ltda. al evaluar su componente Respuesta al Riesgo ha identificado un nivel de confianza y riesgo moderado, debido a la inexistencia de acciones correctivas.

Elaborado por: <b>M.F.M.L</b>	Fecha: <b>15/04/2016</b>
Aprobado por: <b>O.E.R.C</b>	Fecha: <b>15/04/2016</b>

Entidad:	EMPRESA IRCOSTEL CÍA. LTDA.				
Área Evaluada:	Departamento de Sistemas				
Tipo de Auditoría:	Auditoría Informática				
Componente:	Actividades de Control				
Alcance:	Área Informática				
N.-	PREGUNTAS	RESPUESTAS			OBSERVACIÓN
		SI	NO	N.A	
	<b>Seguridad Física</b>				
38	¿Se han establecido políticas de mantenimiento de hardware, correctivo y preventivo?	0	1		Diseñar políticas correctivas, preventivas.*
39	¿Existen medidas de seguridad para el cuidado de la seguridad informática?	1	0		
40	¿Cuentan con una persona encargada para el cuidado de los recursos tecnológicos de la empresa?	1	0		
41	¿La empresa ha realizado estudios de los posibles riesgos como incendios, tormentas e inundaciones, accidentes laborales y robos a lo que se puede presentar la empresa?	0	1		Implementar un manual de Seguridad e Higiene.*
42	¿Existen procedimientos y barreras para la extracción de información?	1	0		
	<b>Seguridad Lógica</b>				
43	¿Se realiza la actualización del sistema informático constantemente?	0	1		
44	¿Existen políticas para la renovación de claves?	0	1		Crear políticas de renovación de claves.*
	<b>Total</b>	3	4		

Elaborado por: M.F.M.L	Fecha: 15/04/2016
Aprobado por: O.E.R.C	Fecha: 15/04/2016

Entidad:	EMPRESA IRCOSTEL CÍA. LTDA.				
Área Evaluada:	Departamento de Sistemas				
Tipo de Auditoría:	Auditoría Informática				
Componente:	Actividades de Control				
Alcance:	Área Informática				
N.-	PREGUNTAS	RESPUESTAS			OBSERVACIÓN
		SI	NO	N.A	
45	¿Existen restricción para el acceso de páginas web?	1			
46	¿Cuenta con claves de acceso para las distintas áreas?	1			
47	¿La protección de datos cuenta con respaldo en caso de una falla del sistema?	1			
48	¿Existe dispositivos móviles con acceso al sistema de la empresa?	1			
	<b>Infraestructura</b>				
49	¿El cableado de los equipos está debidamente instalado?	1	0		
50	¿Existe lugares de acceso restringido?	1	0		
51	¿El área donde se encuentra los recursos tecnológicos es adecuada?	0	1		Ampliar el espacio físico. *
	<b>Sistema Informático</b>				
52	¿El sistema es flexible en caso que se presenten nuevos requerimientos?	1	0		
53	¿El sistema es de fácil manejo?	1	0		
54	¿Las advertencias que se presentan en el sistema son de ayuda?	1	0		
	<b>Total</b>	9	1		

Elaborado por: M.F.M.L	Fecha: 15/04/2016
Aprobado por: O.E.R.C	Fecha: 15/04/2016

**Donde;**

NC= Nivel de Confianza

CP= Ponderación total

CT= Calificación total

**CCI 13/16**

**COMP 5**

**Fórmula:**  $CF = \frac{CP}{CT} * 100$

NIVEL CONFIANZA =  $\frac{12}{17} * 100$

NIVEL DE CONFIANZA = **71%**

NIVEL DE RIESGO= **29%**

### **CRITERIO**

NIVEL DE CONFIANZA		
BAJO	MODERADO	ALTO
15% - 50%	51 - 75%	76% - 95%
NIVEL DE RIESGO		
ALTO	MODERADO	BAJO
85% - 50%	49% - 25%	24% - 5%

### **Análisis**

Evaluado el Componente Actividades de Control, se obtuvo un Nivel de Confianza y Nivel de Riesgo moderado, en razón de que la Empresa no cuenta con políticas, manuales y procedimientos que describan las actividades a desarrollar en el Departamento de Sistemas.

Elaborado por: <b>M.F.M.L</b>	Fecha: <b>15/04/2016</b>
Aprobado por: <b>O.E.R.C</b>	Fecha: <b>15/04/2016</b>

Entidad:	EMPRESA IRCOSTEL CÍA. LTDA.				
Área Evaluada:	Toda la empresa				
Tipo de Auditoría:	Auditoría Informática				
Componente:	Información y Comunicación				
Alcance:	Todos los departamentos de la empresa				
N.-	PREGUNTAS	RESPUESTAS			OBSERVACIÓN
		SI	NO	N.A	
55	¿Se evalúa periódicamente los recursos tecnológicos y los sistemas de información?	11	30		
56	¿La información que genera la empresa es oportuna para la toma de decisiones?	28	13		
57	¿La información es socializada a nivel general?	20	21		
58	¿La información es utilizada como mecanismo de supervisión?	28	13		
59	¿Se cruza información de clientes, proveedores, reguladores y otras partes relacionadas externas?	39	2		
	<b>Total</b>	126	79		

<b>Elaborado por:</b> M.F.M.L	<b>Fecha:</b> 15/04/2016
<b>Aprobado por:</b> O.E.R.C	<b>Fecha:</b> 15/04/2016

**Donde;**

NC= Nivel de Confianza

CP= Ponderación total

CT= Calificación total

**CCI 15/17**

**COMP 7**

$$\text{Fórmula: } CF = \frac{CP}{CT} * 100$$

$$\text{NIVEL CONFIANZA} = \frac{126}{205} * 100$$

NIVEL DE CONFIANZA = **61%**

NIVEL DE RIESGO= **39%**

### **CRITERIO**

NIVEL DE CONFIANZA		
BAJO	MODERADO	ALTO
15% - 50%	51 - 75%	76% - 95%
NIVEL DE RIESGO		
ALTO	MODERADO	BAJO
85% - 50%	49% - 25%	24% - 5%

### **Análisis**

El componente Información y Comunicación tiene un Nivel de Confianza y Nivel de Riesgo Moderado, debido a que no existen procedimientos que permitan evaluar la información interna y externa que afecten el cumplimiento de los objetivos.

<b>Elaborado por:</b> M.F.M.L	<b>Fecha:</b> 15/04/2016
<b>Aprobado por:</b> O.E.R.C	<b>Fecha:</b> 15/04/2016

Entidad:	EMPRESA IRCOSTEL CÍA. LTDA.				
Área Evaluada:	Toda la empresa				
Tipo de Auditoría:	Auditoría Informática				
Componente:	Monitoreo				
Alcance:	Área Ejecutiva, Administrativa, Sistemas				
N.-	PREGUNTAS	RESPUESTAS			OBSERVACIÓN
		SI	NO	N.A	
60	¿Se da seguimiento al cumplimiento de las normas y leyes que rigen a la empresa?	2	1		
61	¿Se realiza inventarios periódicos de los recursos tecnológicos de la información?	2	1		
63	¿Se evalúa periódicamente el cumplimiento de objetivos y metas?	2	1		
64	¿La gerencia toma en cuenta las recomendaciones emitidas?	2	1		
	<b>Total</b>	8	4		

Elaborado por: <b>M.F.M.L</b>	Fecha: <b>15/04/2016</b>
Aprobado por: <b>O.E.R.C</b>	Fecha: <b>15/04/2016</b>

**Donde;**

NC= Nivel de Confianza

CP= Ponderación total

CT= Calificación total

**CCI 17/17**

**COMP 8**

**Fórmula:**  $CF = \frac{CP}{CT} * 100$

NIVEL CONFIANZA =  $\frac{8}{12} * 100$

NIVEL DE CONFIANZA = **67%**

NIVEL DE RIESGO= **33%**

### **CRITERIO**

NIVEL DE CONFIANZA		
BAJO	MODERADO	ALTO
15% - 50%	51 - 75%	76% - 95%
NIVEL DE RIESGO		
ALTO	MODERADO	BAJO
85% - 50%	49% - 25%	24% - 5%

### **Análisis**

La Empresa al evaluar el componente Monitoreo obtuvo un Nivel de Confianza y un Nivel de Riesgo Moderado, porque no se realizan seguimientos continuos de los procedimientos y actividades.

<b>Elaborado por:</b> M.F.M.L	<b>Fecha:</b> 15/04/2016
<b>Aprobado por:</b> O.E.R.C	<b>Fecha:</b> 15/04/2016

## Hoja de Hallazgo



### AUDITORÍA DE SISTEMAS INFORMÁTICOS HALLAZGOS

HA 1/9

ENTIDAD: Empresa Ircostel Cía. Ltda.

COMPONENTE: Ambiente de Control

#### TÍTULO DEL HALLAZGO

La Empresa no cuenta con un Código de Ética.

#### CONDICIÓN

La Empresa no cuenta con un código de ética donde se estipule los principios, normas y valores que direccionen al personal y directivos en el cumplimiento de sus actividades.

#### CRITERIO

Implementación de un Código de Ética para el cumplimiento de las normas que regulan el comportamiento de la empresa.

#### CAUSA

- Falta de compromiso por parte de los directivos de la empresa en diseñar un código de ética
- Desconocimiento por parte de la gerencia en realizar normas de comportamiento.

#### EFECTO

El incumplimiento de las normas de comportamiento, puede ocasionar que el personal puede ser sujeto a sobornos, estafas en el desarrollo de sus actividades.

Elaborado por: M.F.M.L	Fecha: 20/04/2016
Aprobado por: O.E.R.C	Fecha: 20/04/2016

**CONCLUSIÓN**

La Empresa no cuenta con un Código de Ética en donde se estipule las normas de comportamiento para todo el personal de la empresa, debido a la falta de compromiso por parte de los directivos de la empresa.

**RECOMENDACIÓN****Directivos**

Es necesario la implementación de un Código de Ética donde consten todos los principios, normas y valores de comportamiento.

**Gerencia**

Sugerir al Departamento de talento humano y dar a conocer al personal de la empresa la creación del Código de Ética.

Elaborado por: M.F.M.L	Fecha: 20/04/2016
Aprobado por: O.E.R.C	Fecha: 20/04/2016



AUDITORÍA DE SISTEMAS  
INFORMÁTICOS  
HALLAZGOS

HA 3/9

ENTIDAD: Empresa Ircostel Cía. Ltda.  
COMPONENTE: Ambiente de Control

**TÍTULO DEL HALLAZGO**

Programas de Capacitación y Adiestramiento Informático

**CONDICIÓN**

La Empresa no cuenta con un programas de capacitación y adiestramiento para contar con el personal óptimo e idóneo para el desarrollo de las actividades.

**CRITERIO**

Implementación de un programa de capacitación y adiestramiento que permita la descripción clara, del desarrollo personal, profesional e institucional que brinde eficiencia y eficacia en los diferentes servicios.

**CAUSA**

Falta de compromiso por parte de los directivos de la empresa en diseñar programas de capacitación y adiestramiento

**EFECTO**

- El talento Humano no está capacitado para poder solucionar los presentes inconvenientes que se presenten en la ejecución de sus actividades.
- La empresa pierde clientes.
- Pérdidas Económicas.

**CONCLUSIÓN**

La Empresa no cuenta con un programas de capacitación y adiestramiento en donde se defina detalladamente los manuales de capacitación para todo el personal de la empresa, debido a la falta de compromiso por parte de los directivos de la empresa.

**RECOMENDACIÓN**

**Gerencia**

Tomar las medidas necesarias para la elaboración de programas de capacitación que se ajuste a las necesidades de la empresa, para contar con personal eficiente e idóneo.

Elaborado por: M.F.M.L	Fecha: 20/04/2016
Aprobado por: O.E.R.C	Fecha: 20/04/2016



AUDITORÍA DE SISTEMAS  
INFORMÁTICOS  
HALLAZGOS

HA 4/9

ENTIDAD: Empresa Ircostel Cía. Ltda.  
COMPONENTE: Establecimiento de Objetivos

TÍTULO DEL HALLAZGO  
Indicadores de Gestión Informáticos.

**CONDICIÓN**

La Empresa no cuenta con indicadores de gestión lo cual ayude a medir objetivamente sus recursos tecnológicos de información.

**CRITERIO**

Diseñar e implementar indicadores lo cual ayudará a medir el nivel de eficiencia y eficacia de los recursos tecnológicos de información.

**CAUSA**

- Desconocimiento de la importancia de los indicadores
- Falta de interés por parte del Gerente.

**EFECTO**

- Oportunidades de mejora.
- Incumplimiento con las metas establecidas.
- Diagnosticar problemas.

**CONCLUSIÓN**

La Empresa no ha diseñado indicadores, para medir objetivamente el grado de eficiencia y eficacia de los recursos tecnológicos de información.

**RECOMENDACIÓN**

**Gerencia**

Diseñar indicadores de corto plazo, para lograr detectar problemas y así cumplir con las metas establecidas.

Elaborado por: M.F.M.L	Fecha: 20/04/2016
Aprobado por: O.E.R.C	Fecha: 20/04/2016

ENTIDAD: Empresa Ircostel Cía. Ltda.  
COMPONENTE: Respuesta a los Riesgos

TÍTULO DEL HALLAZGO  
Matriz de Riesgos.

### CONDICIÓN

La Empresa IRCOSTEL. CÍA. LTDA no cuenta con una matriz de riesgos que permita medir u evaluar el impacto que genera los riesgos.

### CRITERIO

Mediante la elaboración de una matriz de riesgos se podrá contrarrestar los riesgos identificados y por ende cumplir con los objetivos de la empresa.

### CAUSA

- No se ha medido el impacto que generaría riesgos potenciales.
- No dispone de procedimientos para identificar los riesgos que pueda enfrentar la empresa

### EFECTO

- Gastos perjudiciales que generan pérdidas a la empresa.
- Pérdida de los recursos materiales, tecnológicos y financieros de la empresa.

### CONCLUSIÓN

La Empresa no tiene un matriz de riesgos que permita mitigar y evaluar el impacto que genera y así poder cumplir con sus objetivos planteados.

### RECOMENDACIÓN

#### Directivos

Diseñar una matriz de riesgos que permita eliminar los posibles eventos que pongan en peligro a la empresa.

#### Gerencia

El Gerente debe informar a toda la empresa la implementación de la matriz de riesgos.

Elaborado por: <a href="#">M.F.M.L</a>	Fecha: 20/04/2016
Aprobado por: <a href="#">O.E.R.C</a>	Fecha: 20/04/2016



AUDITORÍA DE SISTEMAS  
INFORMÁTICOS  
HALLAZGOS

HA6/9

ENTIDAD: Empresa Ircostel Cía. Ltda.

COMPONENTE: Actividades de Control.

**TÍTULO DEL HALLAZGO**

Políticas de Control Preventiva y Correctiva (mantenimiento)

**CONDICIÓN**

La Empresa no cuenta con una matriz en donde se establezca las políticas de prevención y corrección en del mantenimiento de sus recursos tecnológicos de información.

**CRITERIO**

Crear un matriz en donde se enfatice las políticas de prevención y corrección.

**CAUSA**

Falta de planificación por parte de la persona responsable del departamento, para evitar el daño de los equipos y la pérdida de información.

**EFECTO**

- Daños a sus equipos tecnológicos
- Falla del sistema
- Pérdida de información

**CONCLUSIÓN**

Por falta de Planificación no se ha diseñado un matriz de prevención y corrección del mantenimiento de los recursos tecnológicos de información.

**RECOMENDACIÓN**

**Departamento de Sistemas**

Evaluar y diseñar políticas de prevención y corrección para salvaguardar los recursos tecnológicos de información de la empresa.

Elaborado por: M.F.M.L	Fecha: 20/04/2016
Aprobado por: O.E.R.C	Fecha: 20/04/2016

ENTIDAD: Empresa Ircostel Cía. Ltda.  
COMPONENTE: Actividades de Control

### TÍTULO DEL HALLAZGO

Manual de Seguridad e Higiene

### CONDICIÓN

Ircostel Cía. Ltda. no cuenta con un manual de seguridad e higiene que ayude a prevenir y controlar los accidentes de trabajo y enfermedades profesionales.

### CRITERIO

Elaborar un manual de seguridad e higiene que permita evitar eventos no deseados y garantizar la protección a los empleados, que con el seguimiento del manual podrán llevar una coordinación y orden de las actividades de la empresa.

### CAUSA

- Desconocimiento y la falta de importancia de implementar el manual de seguridad e higiene.
- Falta de compromiso de los directivos en diseñar el manual de seguridad e higiene.
- Falta de recursos financieros

### EFECTO

- El personal que labora no realiza sus actividades laborales con eficiencia.
- No exista un ambiente de trabajo donde el empleado se sienta seguro.
- El personal está expuesto a accidentes, enfermedades o la muerte

### CONCLUSIÓN

Ircostel Cía. Ltda. no cuenta con un manual de seguridad e higiene debido a la falta de recursos financieros, a la falta de interés de los funcionarios de la empresa.

### RECOMENDACIÓN

#### Directivos y Gerencia

Diseñar el manual de seguridad e higiene q garantice a los empleados condiciones de seguridad, salud y bienestar en un ambiente de trabajo adecuado y propicio.

Elaborado por: M.F.M.L	Fecha: 20/04/2016
Aprobado por: O.E.R.C	Fecha: 20/04/2016



AUDITORÍA DE SISTEMAS  
INFORMÁTICOS  
HALLAZGOS

HA 8/9

ENTIDAD: Empresa Ircostel Cía. Ltda.  
COMPONENTE: Actividades de Control.

TÍTULO DEL HALLAZGO  
Renovación de Claves

**CONDICIÓN**

Los empleados no han realizado cambio de contraseñas desde el momento que ingresaron a trabajar

**CRITERIO**

Realizar cambios de contraseñas periódicamente con un nivel de seguridad medio.

**CAUSA**

- Inexistencia de un adecuado control de verificación de claves, para saber si estas son o no seguras.
- Falta de una política, por ende no se ha realizado ese control.

**EFECTO**

- Robo de información
- Manipulación de la información por terceros.

**CONCLUSIÓN**

Los empleados de la empresa no han realizado cambio de sus claves de acceso durante un tiempo prolongado.

**RECOMENDACIÓN**

**Departamento de sistemas**

Crear políticas de renovación de claves de acceso de forma frecuente para aumentar el nivel de seguridad.

Elaborado por: M.F.M.L	Fecha: 20/04/2016
Aprobado por: O.E.R.C	Fecha: 20/04/2016



AUDITORÍA DE SISTEMAS  
INFORMÁTICOS  
HALLAZGOS

HA 9/9

ENTIDAD: Empresa Ircostel Cía. Ltda.

COMPONENTE: Actividades de Control

**TÍTULO DEL HALLAZGO**

Espacio Físico Inadecuado

**CONDICIÓN**

La Empresa no posee un adecuado espacio físico para el departamento de sistemas que dificulta el desarrollo de sus actividades.

**CRITERIO**

Los directivos deberán realizar un estudio para la ampliación o renovación del espacio físico donde funciona el departamento de sistemas y de sus recursos tecnológicos.

**CAUSA**

- Falta de recursos financieros.
- La inadecuada infraestructura donde se encuentra ubicada la empresa.

**EFECTO**

- Deterioro de los recursos tecnológicos de la empresa.
- EL personal que labora en el área informática no realice con eficiencia su trabajo.
- Está expuesto a cualquier evento que cause pérdida para la empresa.

**CONCLUSIÓN**

El departamento de sistemas de la empresa Ircostel Cía. Ltda. no tiene una infraestructura adecuada para salvaguardar los recursos tecnológicos, y la realización de sus actividades.

**RECOMENDACIÓN**

**Directivos**

Realizar la ampliación o renovar el departamento de sistemas con el fin de salvaguardar los recursos que tiene la empresa para desarrollar sus actividades informáticas de manera clara y concisa.

Elaborado por: M.F.M.L	Fecha: 20/04/2016
Aprobado por: O.E.R.C	Fecha: 20/04/2016

## Hoja de Resumen de Hallazgos

Realizada la auditoría informática a la gestión de las TIC del departamento de sistemas de la empresa IRCOSTEL CIA. LTDA., se detectaron los siguientes hallazgos de auditoría.

Tabla N° 5 Resumen de Hallazgos

COMPONENTES	HALLAZGOS
<b>Ambiente de Control</b>	➤ La Empresa no cuenta con un Código de Ética
	➤ Programas de Capacitación y Adiestramiento Informático.
<b>Establecimiento de Objetivos</b>	➤ Indicadores de Gestión Informáticos
<b>Respuesta al Riesgo</b>	➤ Matriz de Riesgos
<b>Actividades de Control</b>	➤ Políticas de Control Preventiva y Correctiva de Mantenimiento
	➤ Manual de Seguridad e Higiene
	➤ Renovación de Claves
	➤ Espacio Físico Inadecuado

**Fuente:** Elaboración propia con información de la Empresa Ircostel Cía. Ltda.

## COMUNICACIÓN DE RESULTADOS

Riobamba, 24 de abril del 2016

Señor Ing.  
Jorge Calle  
Gerente General de Ircostel Cía. Ltda.  
Presente.-

De nuestra consideración:

Reciba un cordial saludo, aprovecho la oportunidad para informarle que una vez realizada la Auditoría Informática con respecto a los recursos tecnológicos de la Empresa Ircostel Cía. Ltda., por el período comprendido entre el e1 de Enero al 31 de Diciembre del 2014, La Auditoría se efectuó de acuerdo a las Normas Generalmente Aceptadas y procedimientos de Auditoría con el fin de evaluar el cumplimiento eficiente de los recursos tecnológicos de información, y para recabar las pruebas pertinentes de acuerdo a la necesidad trabajo.

Los resultados de la Auditoria Informática se presentan en el informe que contiene conclusiones y recomendaciones que permitan tomara las acciones correctivas para el mejoramiento del manejo de los recursos tecnológicos del sistema informático.

Por la atención a la presente, anticipo mis sinceros agradecimientos.

Atentamente,



Milton Morocho

(Auditor Independiente)

Elaborado por: M.F.M.L	Fecha: 24/04/2014
Aprobado por: O.E.R.C	Fecha: 24/04/2014

**ENTIDAD:** Empresa Ircostel Cía. Ltda.  
**NATURALEZA DEL TRABAJO:** Auditoría Informática  
**PERÍODO:** 2014  
**RESPONSABLE:** Milton Morocho

## **INFORME DE AUDITORÍA**

### **Antecedentes**

La Auditoría Informática en la Empresa Ircostel Cía. Ltda., se realizará por primera vez por el equipo de “MOROCHO AUDITORES INDEPENDIENTES” la misma que ayudará a proponer recomendaciones tendientes a mejorar la eficiencia y eficacia de los recursos tecnológicos de información.

La Auditoría Informática fue aplicada en el manejo y demás Normas establecidas por el Control Interno (Coso II), con relación a la tecnología de información, para realizar una evaluación real de la empresa e identificar las deficiencias más significativas de los recursos tecnológicos.

### **Objetivos de la auditoría**

- Elaborar el marco teórico que permita desarrollar la Auditoría de Sistemas Informáticos.
- Evaluar el sistema de control interno a través de la normativa vigente.
- Emitir un informe que contenga conclusiones y recomendaciones para la toma de decisiones oportunas.

### **Alcance**

La Auditoría Informática se realizará a la Empresa Ircostel Cía. Ltda. el período a examinar comprende del 1 de enero al 31 de diciembre del 2014.

### **Introducción**

Con la finalidad de entregar un informe claro se expresa las observaciones y recomendaciones para r medir el grado de seguridad en el manejo de los recursos tecnológicos.

A continuación se presenta los Hallazgos de Auditoría encontrados durante la ejecución del Examen.

### **1.- Inexistencia de un Código de Ética.**

#### **CONCLUSIÓN**

La Empresa no cuenta con un Código de Ética en donde se estipule las normas de comportamiento para todo el personal de la empresa, debido a la falta de compromiso por parte de los directivos de la empresa.

#### **RECOMENDACIÓN**

##### **Directivos**

Es necesaria la implementación de un Código de Ética donde consten todos los principios, normas y valores de comportamiento.

##### **Gerencia**

Sugerir al Departamento de Talento Humano y dar a conocer al personal de la empresa la creación del Código de Ética.

### **2.- Inexistencia de un Programas de Capacitación y Adiestramiento Informático.**

#### **CONCLUSIÓN**

La Empresa no cuenta con un Programas de Capacitación y Adiestramiento en donde se defina detalladamente los manuales de capacitación para todo el personal de la empresa, debido a la falta de compromiso por parte de los directivos de la empresa.

#### **RECOMENDACIÓN**

##### **Gerencia**

Tomar las medidas necesarias para la elaboración de un programa de capacitación y adiestramiento que se ajuste a las necesidades de la empresa, para contar con personal eficiente e idóneo.

### **3.- Implementación de Indicadores de Gestión Informáticos.**

#### **CONCLUSIÓN**

La Empresa no ha diseñado indicadores, para medir objetivamente el grado de eficiencia y eficacia de los recursos tecnológicos de información.

#### **RECOMENDACIÓN**

##### **Gerencia**

Diseñar indicadores de corto plazo, para lograr detectar problemas y así cumplir con las metas establecidas.

### **4.- Matriz de Riesgo**

#### **CONCLUSIÓN**

La Empresa no tiene un matriz de riesgos que permita mitigar y evaluar el impacto que genera y así poder cumplir con sus objetivos planteados.

#### **RECOMENDACIÓN**

##### **Directivos**

Diseñar una matriz de riesgos que permita eliminar los posibles eventos que pongan en peligro a la empresa.

##### **Gerente**

El gerente debe informar a toda la empresa la implementación de la matriz de riesgos.

### **5.- Políticas de Control Preventivo y Correctivo de Mantenimiento.**

## **CONCLUSIÓN**

Por falta de Planificación no se ha diseñado un matriz de prevención y corrección del mantenimiento de los recursos tecnológicos de información.

## **RECOMENDACIÓN**

### **Departamento de Sistemas**

Evaluar y diseñar políticas de prevención y corrección para salvaguardar los recursos tecnológicos de información de la empresa.

## **6.- Manual de Seguridad e Higiene**

## **CONCLUSIÓN**

Ircostel Cía. Ltda. no cuenta con un manual de Seguridad e Higiene debido a la falta de recursos financieros, a la falta de interés de los funcionarios de la empresa.

## **RECOMENDACIÓN**

### **Directivos y Gerencia**

Diseñar el Manual de Seguridad e Higiene que garantice a los empleados condiciones de seguridad, salud y bienestar en un ambiente de trabajo adecuado y propicio

## **7.- Políticas de Renovación de Claves.**

## **CONCLUSIÓN**

Los empleados de la empresa no han realizado cambio de sus claves de acceso durante un tiempo prolongado.

## **RECOMENDACIÓN**

**Departamento de Sistemas**

Crear políticas de renovación de claves de acceso de forma frecuente para aumentar el nivel de seguridad.

**8.- Espacio Físico Inadecuado****CONCLUSIÓN**

El departamento de sistemas de la empresa Ircostel Cía. Ltda no tiene una infraestructura adecuada para salvaguardar los recursos tecnológicos, y la realización de sus actividades.

**RECOMENDACIÓN****Directivos**

Realizar la ampliación o renovar el departamento de sistemas con el fin de salvaguardar los recursos que tiene la empresa para desarrollar sus actividades informáticas de manera clara y concisa.

<b>Elaborado por:</b> M.F.M.L	<b>Fecha:</b> 24/04/2016
<b>Aprobado por:</b> O.E.R.C	<b>Fecha:</b> 24/04/2016

## **CONCLUSIONES**

- IRCOSTEL CÍA. LTDA., desde el inicio de sus actividades se ha manejado con funciones básicas sin implementar Manuales de Ética, Programas de Capacitación, Seguridad e Higiene y políticas de manejo de los recursos, por lo que no se ha podido medir de manera exacta las necesidades y riesgos a los que se puede enfrentar la Empresa.
- IRCOSTEL CÍA. LTDA., no ha realizado una Auditoria Informática lo que ha provocado falencias detectadas en el área evaluada y los riesgos con respecto al manejo de los recursos tecnológicos del sistema informático.
- En el Departamento de Sistemas, no se aplican indicadores de gestión informática que permitan medir la eficiencia en el manejo de los recursos tecnológicos del sistema informático.

## **RECOMENDACIONES**

- Es necesario diseñar Manuales de Ética, Programas de Capacitación, Seguridad e Higiene y políticas de manejo de los recursos tecnológico de la información, adecuados a los requerimientos de la Empresa que brinden seguridad, confianza y un excelente ambiente de trabajo para los directivos y empleados, mediante su implementación depende el funcionamiento correcto de las actividades de la empresa y el cumplimiento de sus objetivos.
- Realizar una Auditoria Informática anualmente con el fin de detectar nuevas falencias y riesgos que están expuestos al manejo de los recursos tecnológicos del sistema informático.

- Es necesario realizar indicadores de gestión informáticos periódicamente, que permitan evaluar el grado de eficiencia y eficacia de los recursos tecnológicos del sistema informático.
  
- Se recomienda a la Empresa IRCOSTEL CÍA. LTDA. tomar en consideración las recomendaciones expuestas en el informe de auditoría, para mejorar el manejo de los recursos tecnológicos del sistema informático y salvaguardarlos

## **BIBLIOGRAFÍA**

Echenique, J. (2001). *Auditoria en Informática*, 2ª ed. México: Mc Graw-Hill Interamericana.

Piattini, M. Peso, E. y Peso, M. (2008). *Auditoria de Tecnologías y sistemas de información*. México: Alfaomega.

Muñoz, C. (2002). *Auditoria en Sistemas Computacionales*. México: Pearson Educación.

Franklin, F. (2013). *Auditoria Administrativa: Gestión estratégica del Cambio*. 3ª ed. México: Pearson Educación.

Rodríguez, J. (2009). *Control Interno*. 2a ed. México: Trillas.

Blanco, Y. (2012). *Auditotía Integral: Normas y Procedimientos*. Bogota: Ecoe Ediciones.

Mantilla, A. (2009). *Auditoría de Control Interno*. 2a ed. Bogotá: Ecoe Ediciones.

Fonseca, L. (2011). *Sistemas de Control Interno para Organizaciones, Guía práctica y orientaciones para evaluar el control interno*. Lima: Publicidad & Matiz.

Maldonado, M. (2011). *Auditoría de Gestión*. 4a ed. Quito: Abya-Yala.

López, R. (2011). *Generalidades en la Auditoría*. México: Eumed.

Aguilera, P. (2010). *Seguridad Informática*. Madrid: Editex.

Cardozo, H. (2006). *Auditoría del Sector Solidario*. Bogotá: Ecoe Ediciones.

Dávalos, N. (1990). *Enciclopedia básica de administración contabilidad y auditoría*. 3a ed. Quito: C.P.E.

Ibanez, P. (2009). *Informática I*. México: Cengage Learning.

Amador, A. (2008). *Auditoría Administrativa Proceso y Aplicación*. México: Mc Graw-Hill Interamericana.

García, A. (2011). *Seguridad Informática*. Madrid: Paraninfo.

De la Peña, G. (2011). *Auditoría Un enfoque práctico*. Madrid: Paraninfo.

Gallo, F. (2010). *Inseguridad Informática*. Madrid: Igor Unnamed.

Global, F. (2007). *El Auditor de Calidad*. Madrid: Fundación Confemetal.

Rodríguez, G. (2009). *Auditoría informática Ylopd desde la experiencia personal y profesional*. Madrid: Santillana.

# ANEXOS

## Anexo 1: Registro de la Superintendencia de Compañías.

SUPERINTENDENCIA DE COMPAÑIAS DEL ECUADOR Página 1 de 1

REPÚBLICA DEL ECUADOR



SUPERINTENDENCIA DE COMPAÑÍAS  
REGISTRO DE SOCIEDADES

CERTIFICADO DE CUMPLIMIENTO DE OBLIGACIONES Y EXISTENCIA  
LEGAL

No. 35417

---

DENOMINACIÓN DE LA COMPAÑÍA:  
**IRCOSTEL CIA. LTDA.**

NUMERO DE EXPEDIENTE: 36700 - 2009      RUC: 0691728579001

DIRECCIÓN: PRIMERA CONSTITUYENTE Y LARREA No.: 23-50    BARRIO:

CIUDAD: RIOBAMBA      TELÉFONO: 032962556

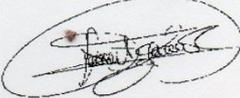
CERTIFICO QUE, SIENDO RESPONSABILIDAD DEL REPRESENTANTE LEGAL, LA VERACIDAD DE LA INFORMACIÓN REMITIDA A ESTA INSTITUCIÓN, LA COMPAÑÍA ARRIBA CITADA HA CUMPLIDO CON LAS DISPOSICIONES CONSTANTES EN LOS ARTÍCULOS 20 Y 449 DE LA LEY DE COMPAÑÍAS

**LA COMPAÑÍA TIENE ACTUAL EXISTENCIA JURÍDICA Y SU PLAZO SOCIAL CONCLUYE EL: 16/11/2039**

CERTIFICACIÓN VALIDA HASTA EL: **31/05/2013**

CAPITAL SOCIAL:    USD \$ 400,0000

POR LA SUPERINTENDENCIA DE COMPAÑÍAS.



Ab. Fausto Robalino Román  
Delegado del Intendente de Compañías de Ambato

FECHA DE EMISIÓN: 29/04/2013 15:46:27

ADVERTENCIA: CUALQUIER ALTERACIÓN AL TEXTO DEL PRESENTE DOCUMENTO, COMO SUPRESIONES, AÑADIDURAS, ABREVIATURAS, BORRONES O TESTADURAS, ETC. LO INVALIDAN.

frobalino 

  
06780029300025411

Anexo 2: Socios o Accionistas de la Compañía

SUPERINTENDENCIA DE COMPAÑÍAS DEL ECUADOR

Página 1 de 1

REPÚBLICA DEL ECUADOR



SUPERINTENDENCIA DE COMPAÑÍAS  
REGISTRO DE SOCIEDADES

SOCIOS O ACCIONISTAS DE LA COMPAÑÍA

Expediente: 36700

Usuario: frobalino

Nombre: IRCOSTEL CIA. LTDA.

DATOS DE LOS SOCIOS / ACCIONISTAS

CAPITAL SUSCRITO DE LA COMPAÑÍA (USD \$):						400,0000
NO.	IDENTIFICACIÓN	NOMBRE	NACIONALIDAD	TIPO INVERSIÓN	CAPITAL	INCAUTADO
1	0602749335	CALLE VIVAR JORGE JAVIER	ESTADOS UNIDOS DE AMERICA	EXT. DIRECTA	200,0000	
2	0602517088	CALLE VIVAR VERONICA ELIZABETH	ECUADOR	NACIONAL	196,0000	
3	0600933758	SJAREZ JULIO CESAR	ECUADOR	NACIONAL	4,0000	
TOTAL (USD \$):						400,0000

CAPITAL ACTUALIZADO A LA FECHA: 29/12/2011 10:51:53

Ab. Fausto Robalino Román  
Delegado del Intendente de Compañías de Ambato

FECHA DE EMISIÓN: 29/04/2013 16:53:50

Se deja constancia que, la presente nómina de socios otorgada por el Registro de Sociedades de la Superintendencia de Compañías, se efectúa teniendo en cuenta lo prescrito en los artículos 18 y 21 de la Ley de Compañías, que no extingue ni genera derechos respecto de la titularidad de las participaciones ya que, en el Art. 113 párrafo segundo, del mismo cuerpo legal, respecto de la cesión de participaciones se dice: "...En el libro respectivo de la compañía se inscribirá la cesión y, practicada esta, se anulará el certificado de aportación correspondiente, extendiéndose uno nuevo a favor del cesionario". Desde luego, el párrafo final del citado artículo determina adicionalmente, que: "De la escritura de cesión se sentará razón al margen de la inscripción referente a la constitución de la sociedad, así como al margen de la matriz de la escritura de constitución en el respectivo protocolo del notario". De lo expresado se infiere que, es de exclusiva responsabilidad de los representantes legales de las compañías de responsabilidad limitada, así como de los Registradores Mercantiles y Notarios con el acto de registro en los libros antedichos y marginaciones respectivas formalizar la cesión de participaciones de las mismas compañías de comercio.

En tal virtud esta Institución de control societario no asume respecto de la veracidad y legalidad de las cesiones de participaciones, responsabilidad alguna y deja a salvo las variaciones que sobre la propiedad de las mismas puedan ocurrir en el futuro, pues acorde con lo prescrito en el Art. 256 de la Ley de Compañías, ordinal 3°, los administradores de las compañías son solidariamente responsables para con la compañía y terceros: "De la existencia y exactitud de los libros de la compañía". Exactitud que pueda ser verificada por la Superintendencia de Compañías, en armonía con lo dispuesto en el Art. 440 de la Ley en materia.

ADVERTENCIA: CUALQUIER ALTERACIÓN AL TEXTO DEL PRESENTE DOCUMENTO COMO SUPRESIONES, AÑADIDURAS, ABREVIATURAS, BORRONES O TESTADURAS, ETC. LO INVALIDAN.

Riobamba, 14 de diciembre del 2011

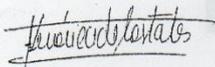
Ingeniero  
Jorge Javier Calle Vivar  
Ciudad

De mi consideración:

Por medio de la presente tengo, el agrado de comunicarle a usted que, en la junta universal de socios, celebrada el catorce de diciembre del 2011, ha sido elegida para que desempeñe el cargo de GERENTE de la compañía **IRCOSTEL CIA. LTDA.** por un período de DOS AÑOS, según consta en el artículo CATORCE del estatuto de la compañía.

La compañía **IRCOSTEL CIA. LTDA.**, se constituyó mediante escritura pública celebrada el día 30 de octubre del 2009, otorgado ante el Notario Cuarto del Cantón Riobamba, Dr. CARLOS MARCELO AULLA ERAZO, aprobada mediante resolución N° SC.DIC. A. 09. 00315 y legalmente inscrita en el Registro Mercantil el 6 de noviembre del 2009 bajo el número 1619.

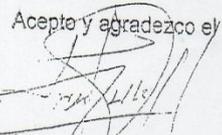
Atentamente,



Ec. Verónica Elizabeth Calle Vivar  
C. I. No. 060251708-8  
Riobamba, 14 de diciembre del 2011.  
Nacionalidad Estadounidense  
Dirección: Rocafuerte No. 21-37 y 10 de Agosto

**ACEPTACION**

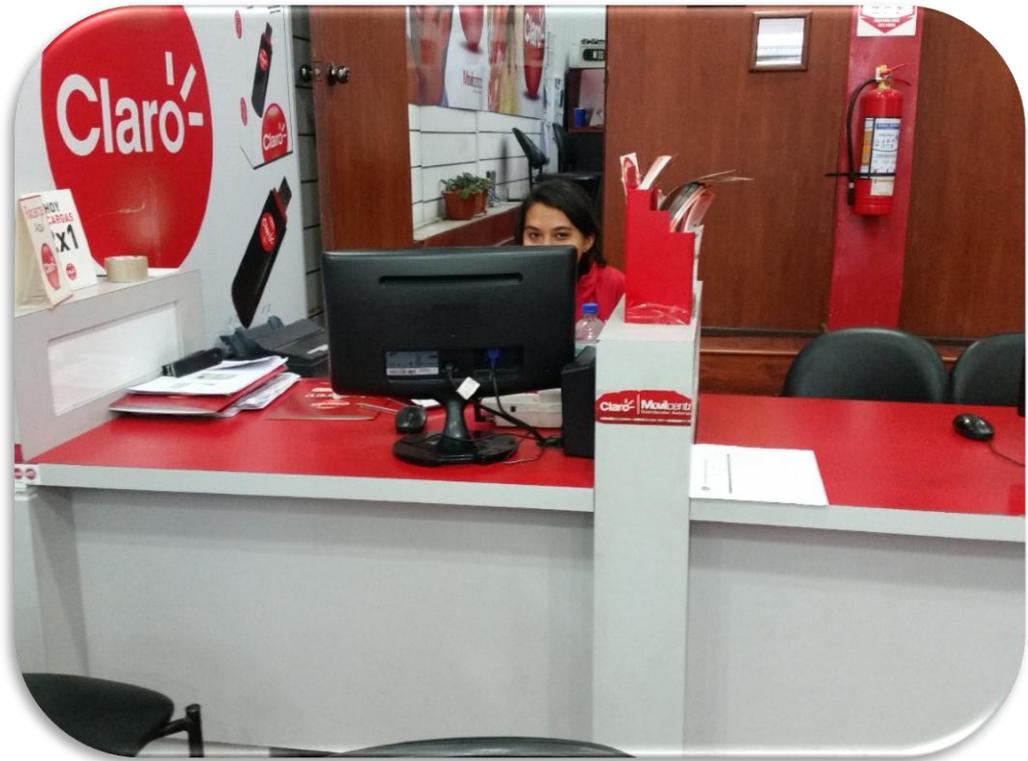
Acepto y agradezco el nombramiento de GERENTE.



Ing. Jorge Javier Calle Vivar  
C.I. 060274933-5  
Riobamba, 14 de diciembre del 2011.  
Nacionalidad Estadounidense  
Dirección: Rocafuerte No. 21-37 10 de Agosto

Anexo 3 : Departamentos de la Empresa Ircostel. Cía. Ltda.





Anexo 4: Departamento de Sistemas de la Empresa Ircostel Cía Ltda.

